The Regulation of Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform

Khaled Ali Aljneibi, LLB, LLM (Dubai)

Thesis submitted to Bangor University
for the degree of Doctor of Philosophy

February 2014

Abstract

Due to the crucial role that electronic evidence is now playing in the digital age, it constitutes a new form of evidence for prosecutors to rely on in criminal cases. However, research into the use of electronic evidence in the United Arab Emirates (UAE) is still in its initial phase. There have been no detailed discussions on the procedural aspects associated with electronic evidence when investigating crimes, or the problems and challenges faced by law enforcers when handling electronic evidence. In addition, there has also been no detailed explanation of the ideal investigation process, such as the processes involved in computer search and seizure, and forensic investigation. As a result, the understanding and awareness of how to regulate and combat criminal cases that rely on electronic evidence is incomplete. In such situations, offenders usually take advantage of this lack of prescription in law. Because the understanding and awareness levels associated with electronic evidence is not perfect in the UAE, the UAE needs to promulgate new rules for handling electronic evidence as its laws are currently focused on traditional eyewitness accounts and the collection of physical evidence. Thus, it is very important that issues related to the existing approaches pertaining to electronic evidence in criminal procedures are identified, and that reform proposals are developed, so that new rules for handling electronic evidence can be adopted to effectively combat crime, by making full use of it.

This thesis examines the problems and challenges currently affecting the regulation electronic evidence in the UAE, and contributes to the body of academic literature in this area. Such a contribution is appropriate in the UAE context, where the law currently lacks sufficient academic input, especially concerning electronic evidence. The thesis makes actual recommendation as to how the substantive law may be reformed in the form of draft articles and includes an analysis as to how the process of prosecution and evidence collection can be facilitated. In particular it suggests that the electronic evidence process should be regulated in order to facilitate effective investigation and make full use of electronic evidence. This will ensure that electronic evidence is used in a transparent manner to preserve the integrity of criminal procedure, thereby safeguarding the accused, whilst at the same time facilitating prosecution and trial proceedings.

I dedicate this thesis to my parents and my wife

Acknowledgements

First and foremost, I wish to express my sincere thanks to the many people who have assisted me during the writing of my thesis. I offer my sincere thanks to my supervisor team, Dr. Yvonne McDermott, for her constructive criticism, valuable suggestions, support and guidance throughout the course of this thesis. I am also grateful to my second supervisor Mr Mark Hyland for his encouragement. I would also like to express my grateful acknowledgement to Professor Dermot Cahill Head of Bangor University Law School for his constant support, guidance, inspiration and encouragement. My work would not have progressed to completion without their, ideas, support, and continual enthusiasm.

Many thanks also go to Mr Stephen Mason who has helped me by reviewing a draft of this thesis. This thesis has greatly benefited from his thoughtful feedback.

I would like express my appreciation to all the participants in the applied study.

Last but not least, I am indebted to my family and my sons (Shouq, Mohammed, Fatima and Omar) who have supported me endlessly. Although my family were physically far away from me the whole time, they were always close to my mind and my heart. Without their support this work would not have been possible.

Declaration and Consent

Details of the Work

I hereby agree to deposit the following item in the digital repository maintained by Bangor University and/or in any other repository authorized for use by Bangor University.

Author Name: Khaled Ali Aljneibi

Title: Mr

Supervisor/Department: Dr. Yvonne McDermott / School of Law

Funding body (if any): Dubai Public Prosecution

Qualification/Degree obtained: PhD

This item is a product of my own research endeavours and is covered by the agreement below in which the item is referred to as "the Work". It is identical in content to that deposited in the Library, subject to point 4 below.

Non-exclusive Rights

Rights granted to the digital repository through this agreement are entirely non-exclusive. I am free to publish the Work in its present version or future versions elsewhere.

I agree that Bangor University may electronically store, copy or translate the Work to any approved medium or format for the purpose of future preservation and accessibility. Bangor University is not under any obligation to reproduce or display the Work in the same formats or resolutions in which it was originally deposited.

Bangor University Digital Repository

I understand that work deposited in the digital repository will be accessible to a wide variety of people and institutions, including automated agents and search engines via the World Wide Web.

I understand that once the Work is deposited, the item and its metadata may be incorporated into public access catalogues or services, national databases of electronic theses and dissertations such as the British Library's EThOS or any service provided by the National Library of Wales.

I understand that the Work may be made available via the National Library of Wales Online Electronic Theses Service under the declared terms and conditions of use (http://www.llgc.org.uk/index.php?id=4676). I agree that as part of this service the National Library of Wales may electronically store, copy or convert the Work to any approved medium or format for the purpose of future preservation and accessibility. The National Library of Wales is not under any obligation to reproduce or display the Work in the same formats or resolutions in which it was originally deposited.

Statement 1:

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree unless as agreed by the University for approved dual awards.

Signed……..(candidate)Date ……

Statement 2:

This thesis is the result of my own investigations, except where otherwise stated. Where correction services have been used, the extent and nature of the correction is clearly marked in a footnote(s).
All other sources are acknowledged by footnotes and/or a bibliography.

Signed……..(candidate)Date……..

Statement 3:

I hereby give consent for my thesis, if accepted, to be available for photocopying, for inter library loan and for electronic repositories, and for the title and summary to be made available to outside organisations.

Signed……..(candidate)Date……..

NB: Candidates on whose behalf a bar on access has been approved by the Academic

Registry should use the following version of Statement 3:

Statement 3 (bar):

I hereby give consent for my thesis, if accepted, to be available for photocopying, for interlibrary loans and for electronic repositories after expiry of a bar on access.

Signed……..(candidate)Date……..

Statement 4:

Choose **one** of the following options

a) I agree to deposit an electronic copy of my thesis (the Work) in the Bangor University (BU) Institutional Digital Repository, the British Library ETHOS system, and/or in any other repository authorized for use by Bangor University and where necessary have gained the required permissions for the use of third party material.	

b)	I agree to deposit an electronic copy of my thesis (the Work) in the Bangor University (BU) Institutional Digital Repository, the British Library ETHOS system, and/or in any other repository authorized for use by Bangor University when the approved **baron access** has been lifted.	
c)	I agree to submit my thesis (the Work) electronically via Bangor University's e-submission system, however **Iopt-out** of the electronic deposit to the Bangor University (BU) Institutional Digital Repository, the British Library ETHOS system, and/or in any other repository authorized for use by Bangor University, due to lack of permissions for use of third party material.	

Options B should only be used if a bar on access has been approved by the University.

In addition to the above I also agree to the following:

1. That I am the author or have the authority of the author(s) to make this agreement and do hereby give Bangor University the right to make available the Work in the way described above.

2. That the electronic copy of the Work deposited in the digital repository and covered by this agreement, is identical in content to the paper copy of the Work deposited in the Bangor University Library, subject to point 4 below.

3. That I have exercised reasonable care to ensure that the Work is original and, to the best of my knowledge, does not breach any laws – including those relating to defamation, libel and copyright.

4. That I have, in instances where the intellectual property of other authors or copyright holders is included in the Work, and where appropriate, gained explicit permission for the inclusion of that material in the Work, and in the electronic form of the Work as accessed through the open access digital repository, or that I have identified and removed that material for which adequate and appropriate permission has not been obtained and which will be inaccessible via the digital repository.

5. That Bangor University does not hold any obligation to take legal action on behalf of the Depositor, or other rights holders, in the event of a breach of intellectual property rights, or any other right, in the material deposited.

6. That I will indemnify and keep indemnified Bangor University and the National Library of Wales from and against any loss, liability, claim or damage, including without limitation any related legal fees and court costs (on a full indemnity bases), related to any breach by myself of any term of this agreement.

Signature: …… Date:…….

Table of contents

List of Abbreviations

ACPO	- Association of Police Chief Officers
CPL	- UAE Criminal Procedure Law
DOJ	- USA Department of Justice
EU	- European Union
ICT	- Information and Communication Technology
IP	- Internet Protocol
IT	- Information Technology
MD5	- Algorithm (Message Digest 5)
MLA	- Mutual Legal Assistance
MLAT	- Mutual Legal Assistance Treaty
MMLA	- Multilateral Mutual Legal Assistance
PACE	- Police and Criminal Evidence Act
PRC	- People's Republic of China
RAM	- Random Access Memory
SHA-1	- Algorithm (Secure Hash)
UAE	- The United Arab Emirates
UK	- The United Kingdom
UN	- United Nations
USA	- The United States of America

Table of Cases

Criminal Case of UAE Federal Supreme Court No. 371/2002, date of decision 14th May 2002, unpublished.

Criminal Case of UAE Federal Supreme Court No. 211/2010, date of decision 25th March 2010, unpublished.

Criminal Case of UAE Federal Supreme Court No. 10/2011, date of decision 6th April 2011, unpublished.

Criminal Case of UAE Federal Supreme Court No. 50/2011, date of decision 19th April 2011, unpublished.

Criminal Case of UAE Federal Supreme Court No. 75/2011, date of decision 31st May 2011, unpublished.

Criminal Case of UAE Federal Supreme Court No. 17/2013, date of decision 2nd July 2013, unpublished.

Criminal Case of Cassation Court Dubai: UAE No. 153/2011, date of decision 2nd May 2011, unpublished.

Criminal Case of Cassation Court Dubai: UAE No. 268/2011, date of decision 22nd August 2011, unpublished.

Criminal Case of Appeal Court Dubai: UAE No. 3422/2010, date of decision 26th August 2010, unpublished.

Criminal Case of Appeal Court Dubai: UAE No. 6962/2010, date of decision 17th March 2011, unpublished.

Criminal Case of Appeal Court Dubai: UAE No. 7003/2011, date of decision 7th June 2011, unpublished.

Criminal Case of Appeal Court Dubai: UAE No. 6732/2012, date of decision 6th January 2012, unpublished.

Criminal Case of First Instance Court Dubai: UAE No. 37784/2009, date of decision 30th May 2011, unpublished.

Criminal Case of First Instance Court Dubai: UAE No. 9913/2010, date of decision 9th May 2010, unpublished.

Criminal Case of First Instance Court Dubai: UAE No. 15432/2010, date of decision 24th November 2010, unpublished.

Criminal Case of First Instance Court Dubai: UAE No. 7690/2012, date of decision 20th September 2012, unpublished.

Australia

R v Hourmouzis (Victorian County Court, decided 30th October 2000, unreported).

The People's Republic of China

Yang Chunning v Han Ying (2005) hai min chuzi No.4670.

The United Kingdom

DPP v Bignell [1998] 1 Cr App R 1.

Kajala v Noble [1982] 75 Cr App R 149.

Masquerade Music v Springsteen [2001] EWCA Civ 563.

R v Governor of Pentonville, ex p Osman [1990] 1 WLR 277DC.

R v Spiby [1990] Crim App R 186.

R v Wood [1982] 76 Cr App R 23.

Sapporo Maru (Owners) v Statue of Liberty (Owners) [1968] 1 WLR 739.

The United States

Columbia Pictures Indus v Bunnell 2007 U.S. Dist. LEXIS 46364 (C.D. Cal. 19th June 2007).

Daubert v Merrell Dow Pharmaceuticals Syllabus (92-102), 509 U.S. 579 (1993).

SEC v Hourmouzis (District Court of Colorado, no 00-N-905 decided 1st May 2000, unreported).

US v Bennett [1966] 4-66-Crim. No. 89 (D. Minn 1966).

Table of Statutes, Regulations and other Official Documents

Constitution 1971 and amended on 1996.

Federal Criminal Procedure Law No. 35-1992 and amended on 2005.

Federal Law No. 8-1974 concerning the Appointment of Experts before the Court.

Federal Law No. 36-2006 concerning International Judicial Cooperation in Criminal Matters.

Federal Law No. 5-2012 concerning the Prevention of Information Technology Crimes.

Federal Penal Law No. 3-1987 and amended on 2005.

Law No. 23-2006 concerning the establishment of the Abu Dhabi Public Prosecution Office.

Law 1968 concerning the establishment of Abu Dhabi Courts and amendment by Law No. 23-2006.

Law 1970 concerning the establishment of the Dubai Courts.

Law 1971 concerning the establishment of the Ras Al Khaimah Courts and amendment by Law No. 3-2011.

Decree No. 11-2006 concerning the establishment of the Ras Al-Khaymah Public Prosecution Office.

Decree No. 8-1992 concerning the establishment of the Dubai Public Prosecution Office.

Australia

Crimes Act 1914.

South Australian Evidence Act (SACEA) 1929.

Canada

Competition Act R.S.C., 1985, c. C-34.

Evidence Act R.S.C., 1985, c. C-5.

France

Code of Civil Procedure Inserted by Law No. 230-2000.

Code of Criminal Procedure Inserted by Law No. 516-2000.

Germany

Code of Criminal Procedure 1987.

Ireland

Criminal Evidence Act 1992.

Italy

Code of Computer Crime 1993.

Code of Criminal Procedure 1988.

Code of Electronic Government 2005.

Portugal

Code of Criminal Procedure amended by Law No. 48-2007.

Singapore

Criminal Procedure Act No. 15-2010.

Evidence (Amendment) Act No. 8-1996.

South Africa

Computer Evidence Act No. 57-1983 (SACEA).

The People's Republic of China

Civil Procedure Law 1991.

Criminal Procedure Law 1979 and amended on 2012.

Electronic Signature Law promulgated by Order No.18 of the President of the People's Republic of China on 2004.

The United Kingdom

Civil Evidence Act 1995.

Computer Misuse Act 1990.

Criminal Justice Act 2003.

Criminal Procedure and Investigations Act 1996.

Police and Criminal Evidence Act 1984.

The United States

Computer Fraud and Abuse Act (CFAA) 1986.

Federal Criminal Procedure Act 1930.

Patriot Act 2001.

Official Documents

Best Practices for Seizing Electronic Evidence submitted by: US Department of Homeland Security.

Code of Practice on Legal Admissibility and Evidential Weight of Information Stored Electronically submitted by: The People's Republic of China.

Good Practice Guide for Commuter-Based Electronic Evidence submitted by: Association of Chief Police Officers' (ACPO) UK.

Guideline for the management of IT evidence submitted by: Australia.

List of Figures

CHAPTER ONE: INTRODUCTION

The use of technology to support and enrich various aspects of life has spread globally. There are many positive aspects to this change; the paperless working environment in the office is increasing communication, accessibility and accuracy. In contrast, the negative aspect of this advancement in technology is that new ways of committing crimes have been introduced. However, numerous measures have been suggested to help overcome this outbreak of cybercrime and the losses resulting from unlawful activities resulting from technology.

Aside from the fact that technology has introduced a novel range of crimes, electronic evidence can also play a significant role in the successful prosecution of crimes.[1] Electronic evidence used in crime detection may lead to more successful prosecutions and more effective capture of criminals involved in any sort of crime. For instance, electronic evidence was instrumental in capturing a serial killer, who had killed ten people.[2] He called himself 'BTK' and was sentenced to ten consecutive life terms in prison for the killings. In his case, deleted data was recovered on a floppy disk held on a church's computer.[3] Moreover, electronic evidence is becoming increasingly prominent when prosecuting diverse criminal cases.

This advancement in technology has also helped criminal entities to grow rapidly and with considerable efficiency, creativity and pace. One example of the use of electronic evidence in a criminal cases in the UAE was a case concerning the issuance of a secret regulation to overthrow the government. In this case the judgment was a conviction, based on electronic evidence, which was obtained from the defendant's computers, discs and audio recordings.[4] There are many other trials and criminal cases that have been, or could be, resolved completely and easily using electronic evidence. This was confirmed by the United States of America's (USA) Department of Justice (DOJ) that reported many cases where electronic media is involved, and electronic evidence is

[1]Linda Volonino and Stephen Robinson, *Principles and Practice of Information Security* (Prentice Hall 2004) 137.
[2]See: Sam Coates, 'Rader Gets 175 Years for BTK Slayings' (The Washington Post 19th August 2005) <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/18/AR2005081800201.html> accessed 24th April 2013.
[3]Ibid.
[4]Criminal Case of UAE Federal Supreme Court No.17/2013 date of decision 2nd July 2013 unpublished.

particularly important in prosecuting criminal cases.[5]

With the passage of time, the structure of computers and the features of internet service are being improved; this has facilitated society's growth and reliance on these media in a number of ways.[6] For example, technology has been instrumental in securing economic, political, social and confidential data. However, as touched on above, this advancement has also enhanced the complexity of the crimes committed. Criminals too, are becoming more and more dependent upon such technologies, and lack of virtual boundaries assists their actions in every possible manner. This feature of electronic technology is making it increasingly complicated for law enforcement bodies to address and regulate such crimes; the advanced technology used is tricky to evaluate for law enforcement agents, forensic experts, judges, attorneys and corporate security experts.[7]

As a consequence criminals are becoming technologically more literate and organised; they can harm people more easily and retain efficient communication channels to help them when planning and committing crimes. Criminal activities are also being increasingly facilitated by the fact that almost every office, hospital and home has electronic devices that are network based, making incursions by cybercriminals easier.

This increased use of technology by criminals when committing crimes has a positive side to it; in particular, the use of computers in the planning stages of crime offers a new body of evidence for law enforcement bodies engaged in the investigation of criminal cases. For example, after the incident at the World Trade Centre in 2001, the criminals' laptops were examined, and electronic evidence assisted authorities in locating plans for the first bombing, and when they were being examined also the second bombing. In that case, about one hundred hard drives were examined.[8] UAE Federal case No.17/2013 involved the use of electronic devices for prosecuting criminals, electronic evidence played an important role in finding the offenders' plans

[5]See: 'Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors' (2007) *US National Institute of Justice* <http://www.law.du.edu/images/uploads/library/evert/DigitalEvidenceinTheCourtroom.pdf > accessed 13th April 2013.

[6]According to Internet World Statistics there were 2,405,518,376 internet users in the world on 30th June 2012 <http://www.internetworldstats.com/stats.htm> accessed 24th October 2013.

[7]Hisham Rustom, *The Procedural Aspects of Cybercrimes* (Modern machinery 1994) 8. (Author's translation from the Arabic).

هشام رستم، الجوانب الاجرائية للجرائم المعلوماتية (مكتبة الالات الحديثة، مصر 1994) ص 8.

[8]Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn, Waltham Mass.: Academic Press/Elsevier 2011) 3.

to overthrow the government.[9]

Location of electronic evidence in murder investigations increases the chances of a verdict of first-degree murder, and in such cases emails and other digital data are the only clues found in an investigation. For instance, in 1996, in a case in Maryland, USA, emails were the only clue found. In this case, a woman named Sharon Lopatka informed her husband that she was visiting friends but the husband found a note, which caused him to contact police about her unusual absence. The investigations into the case found a number of emails exchanged between Lopatka and a man named Robert Glass regarding torture and death fantasies.[10]

In the US, law-enforcement bodies have agreed that the use of advanced technology, which has become common in most criminal cases, is ruining law and order conditions.[11] They have therefore started considering cases in which evidence from advanced technology is put forward.[12] This is also happening in other countries, such as the UK, Australia, Canada, France and Germany, and case law and legislation from these jurisdictions will be referred to throughout this thesis.

However, in the UAE, crimes involving electronic evidence are still treated as simple cases in spite of the huge losses that have been incurred by the entities there. In 2007 about Dh 735 million was lost due to cybercrime.[13] The figure doubled in 2012, when losses amounted to Dh 1.5 billion.[14] Moreover, according to the Kaspersky Company, about 56 per cent of cyber-attacks in the region were from the UAE. Among Europe, Africa and the Middle East, the UAE is ranked 18th for having a high rate of criminal activities.[15] In spite of these losses, law-enforcement bodies are alleged to not be taking cybercrime seriously and are considering only those cases of interest that have some

[9](n 4).
[10] Rachael Bell, 'Internet Assisted Suicide-The Story of Sharon Lopatka' *Crime Library* <http://www.trutv.com/library/crime/notorious_murders/classics/sharon_lopatka/5.html> accessed 16th April 2013.
[11]Linda Volonino and Stephen Robinson (n1)117.
[12]Ibid.
[13]At the time of writing, 1 US$ was 3.67 AED.
[14] Norton Cybercrimes Report (2012) <http://www.norton.com/2012cybercrimereport> accessed 26th April 2013.
[15]Kaspersky LabReport (2012) <http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf> accessed 26th April 2013.

physical manifestation.[16]

Legislators in the UAE have not yet shown that they are prepared to a comprehensively address the regulation of electronic evidence. At present, the most important issues concerning electronic evidence that UAE law enforcement and prosecutors are likely to encounter are the search and seizure, and thereafter, the preservation of evidence extracted from electronic devices. Existing rules of criminal procedure for evidence have been drafted to regulate physical evidence.[17] This thesis aims to show that these rules may not meet the requirements for handling electronic evidence, if it is to be utilised effectively to combat crimes. In 2009, a pertinent criminal case failed in the UAE, after three years under discussion.[18] The facts of the case can be summarised as follows. In 2009, the prosecution complained against the defendant that he had written online statements of complaint to the board of the company: 'The Company was run unprofessionally and immorally, …managers were asking for (sex) in exchange for employment, and if she refuses she then is unsuccessful in interview'. The court of First Instance ruled that the defendant be found not guilty because there was insufficient evidence, and because the forensic report did not refer to the perpetrator of the statements. In addition, the UAE Telecommunications Regulatory Authority failed to find the IP address, and thus identify the person who wrote the online statements. The reason that identification of the person failed was due to the passage of time; over a year had taken place since the incident.[19]

The previous case is just one example of a supporting authority for the argument that electronic evidence in the UAE requires greater regulation. In this case the investigating authorities failed to prove a crime had been committed, largely because the forensic report failed to identify the accused, and the Telecommunications Company failed to find the IP address. In addition, the prosecutors failed to investigate the crime and provide sufficient evidence, and the police officers failed to seize devices containing electronic evidence. In fact, they were unprofessional when dealing with the incident,

[16]Jay Hilotin and Lubna Bagsair, 'Cyber gangs on the prowl in UAE' *Gulf news* (Dubai 3rd February 2011) <http://gulfnews.com/news/gulf/uae/crime/cyber-gangs-on-the-prowl-in-uae-1.756268> accessed 26th April 2013.
[17]See: the UAE Criminal Procedure Law, Chapter Three.
[18]Criminal Case of First Instance Court Dubai: UAE No. 37784/2009 date of decision 30th May 2011 unpublished.
[19]For more information about this case, see: Case Translation: Dubai (2012) 9 *Digital Evidence and Electronic Signature Law Rev*iew 106-107.

and loss of such a simple case raises concerns that more will be lost due to professional issues. Law-enforcement bodies in the UAE need to give as much importance to electronic evidence as they do to physical. This is a reflection of the fact that the use of technology in every aspect of life has increased and the acceptance of such evidence will help the UAE law-enforcement bodies to carry out their investigations more easily when electronic evidence is the only evidence presented to investigate a crime.

1.1 Research questions and objectives

This thesis attempts to investigate whether electronic evidence is sufficiently regulated in the UAE and if not, what reforms can be made to effectively regulate it. The thesis will also aim to highlight the issues posed when introducing electronic evidence in the UAE and what measures can be taken to enhance the utility and effectiveness of electronic evidence. In addition, the thesis seeks to examine the level of knowledge, understanding and awareness of electronic evidence in practical life in the UAE and find the relationship between the lack of rules and the level of understanding and awareness. In addition, the researcher proposes learning lessons from the experiences of other countries and an examination of the way in which the law can be improved.

The research conducted in the field will acquire essential information with reference to the nature of the issue of electronic evidence in the UAE. The collected information will contribute to our academic understanding and make it possible to answer the questions raised in the thesis. The achievement of the objectives of the thesis will lead to the description of the main research question of this thesis.

1.2 Statement of problem

The manner in which rapid advancements in technology are changing the lifestyles of people worldwide demands alterations in the functioning of judicial systems. As more and more criminal cases are reported, the success of lawsuits is affected. In the era of electronic evidence, courts now have to consider the electronic evidence from a variety of crimes, because almost all crimes can at times involve electronic evidence. Based on such circumstances, it is not difficult to predict whether in the near future there will be an introduction of an entirely new era of judicial proof. This is because in cases where crimes are being dealt with, it is becoming essential to provide courts with electronic evidence to prove the wrongdoing of the accused.

Factors like the absence of comprehensive regulation of electronic evidence, and lack of guidelines and instructions pertaining specifically to how to handle electronic evidence, make it more challenging for law-enforcement bodies to tackle the challenges raised by electronic evidence. Undoubtedly, the lack of legal regulation makes judicial activity more complex and can also lead to weaknesses in understanding and level of awareness.

This inattention towards crimes and the features involved in judicial structures results in poor decision-making by judges in cases including electronic evidence.[20] Therefore, it is essential for such judicial structures to integrate knowledge of the electronic evidence involved in crimes to ensure appropriate decisions.[21] This idea was supported by the European Union (EU) when it was presented with the essentials of the project with an elaboration of those positives that would result if there were a European-wide law on electronic evidence for criminal lawsuits.[22]

While dealing with electronic evidence it is necessary for laws and procedures to be instituted to understand the nature of electronic evidence, which differs from other evidence. Therefore, there are many cases failing to reach some beneficial conclusions for the reason that the UAE's Criminal Procedure Law No. 35 of 1992 (CPL) (hereinafter referred to as the UAE's CPL) rules are inadequate to cope with the challenges of electronic evidence. This thesis illustrates that the general rules of UAE's CPL are unsuitable for dealing with electronic evidence, and that there is a need for a structure of laws and procedures to be changed. Moreover, it explains how electronic evidence can facilitate better utilisation of electronic evidence when prosecuting crimes. Furthermore, the study explains how to handle electronic evidence, and how the lack of knowledge of law-enforcement bodies in this area affects the conclusions reached in many of the cases.

1.3 Hypotheses

The thesis will test primary and secondary hypotheses. The primary hypotheses put

[20]Eric Buskirk and Vincent Liu, 'Digital evidence: Challenging the presumption of reliability' (2006) 1, 1 *Journal of Digital Forensic Practice* 19-26. See also: Stephen Mason, gen ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths 2012) chapter 5.
[21]Ibid.
[22] The project was undertaken by Cybex 2005-2007. For further details about this project, see: Fredesvinda Insa and Carmen Lazaro, 'Admissibility of Electronic Evidence in Court: A European Project' in Stephen Mason (eds) *International Electronic Evidence* (British Institute of International and Comparative Law 2008) 1-17.

forward in the work is that the current UAE's CPL rules are insufficient to govern the process of gathering, preservation, presentation and examination of electronic evidence. Moreover, the primary hypotheses investigates the procedures in place to effectively combat crime, particularly cybercrime and to make full and effective use of electronic evidence. The secondary hypotheses examines the grounds for regulating electronic evidence in the UAE, on the presumption that electronic evidence should be regulated because crime grows rapidly and has negative effects on economic efficiency. Furthermore, criminal prosecutions in the UAE are inefficient. In addition, this fact contributes to increased awareness and knowledge.

1.4 Scope of study

Chapter One introduces the significance of the thesis and draws a roadmap for it. The literature review covers the regulation of electronic evidence, and illustrates the mechanisms which help when designing the study. The physical and electronic evidence, and the different kinds of investigations, are then identified in Chapter Two. The aim of this stage of the study is to build a theoretical background with a view of criminal investigation procedures as applied to crimes investigation. The chapter also describes the differences between physical and electronic evidence and the importance of the latter.

The third chapter will take a 'macro-comparison' approach to the regulation of electronic evidence. The discussion in this chapter explores the nature and background to the regulation of electronic evidence in civil and common law systems. The chapter seeks to deduce an organised discussion that addresses how electronic evidence is regulated in common law countries, as represented by the England and Wales and civil law jurisdictions as represented by China. Attention will also be given to issues involved in each system as far as adducing, admissibility, authentication and certification of evidence is concerned in each system. Overall, the aim of the chapter is to examine the background against which regulation of electronic evidence across the two systems functions, and to identify the merits and demerits of each system.

In examining the UAE rules, Chapter Four will address the procedures governing search and seizure, preservation, examination, presentation and authentication of electronic evidence. This chapter will offer a 'micro comparison' approach to criminal

procedure rules and related issues of electronic evidence in the UAE. Chapter Four analyses law-enforcement bodies collection of electronic evidence and related procedures. As the concept of electronic evidence is new and different from typical evidence procedures, law enforcement officers find it somewhat more difficult to deal with than the traditional system. In this procedure of collection of evidence, specifically, the strategies followed are arduous in nature but assist in developing just conclusions about crimes.

In Chapter Five, an applied study will be used to get to the root of the actual problems within the legal system of UAE. In this chapter, a detailed study of UAE legal structures is discussed and evaluated by legal experts and other specialists to ascertain flaws. Subsequently, the findings will be dealt with by the comparison method to understand the state of regulation of electronic evidence in the UAE and how it could be improved.

Chapter six, through reference to other state's laws, provides solutions to the issues raised by the applied study; this methodology is separated into two parts. The first part gives a complete overview of the regulation of electronic evidence, illustrating challenges and problems facing law enforcers with regard to electronic evidence and gaps in the existing criminal procedures of the UAE. The second part describes the manner in which an applicable law may be altered in order to better address the challenges of electronic evidence in the UAE. The scope of the thesis is evident by Chapter Seven, which consists of a conclusion to the research study and findings.

1.5 Significance of study

The thesis puts forth the argument that electronic evidence is one of the most underdeveloped areas in the legal system of the UAE and this is found to be a critical problem. According to Al Mazeina, the UAE faces many difficulties with regard to electronic evidence.[23] To give a practical example, recently a number of money exchange shops in the UAE were subjected to breakout electronic systems, which caused the loss of three million dollar, as a result of fake transfers of balances to persons outside the State. The fact was discovered after Western Union asked for reimbursement. This case was not prosecuted due to the impossibility of acquiring

[23] Khamis Al Mazeina, General Commander of the Dubai Police-UAE, 'New Criminal Phenomena' (conference, Dubai-UAE 22nd February 2012).

electronic evidence from outside the State.[24]

While there is a great deal of attention directed towards improving regulations and laws in different areas with the UAE, it also seems wise to guide the efforts of the academy in the same way. To this end, the thesis will deal with the regulation of electronic evidence in the UAE, problems and challenges resulting therefrom, and how they can be overcome. The literature on the subject and the UAE's legal system's structure will both be evaluated in this project. As the thesis contains original ideas regarding the regulation of electronic evidence, the subject under consideration will attract the attention of many of jurists in other jurisdictions who have suggested many ideas to resolve the issue of regulation of electronic evidence.[25] As far as the researcher is aware, this thesis will present research of this sort for the first time in the UAE, and will propose ideas openly for alterations in legal systems of the UAE. Therefore, it is using a combination of an applied study approach and a doctrinal study to devise ideas that could easily be applied to adjust how electronic evidence is treated within the UAE. The conclusions may serve as the basis for the introduction of such practices in other countries of Middle East as well. Regarding the significance of the study, Dr. Hadef Al Dhahiri, Minister of the UAE Ministry of Justice who was interviewed by the researcher said:

> Academic research in the UAE is currently limited to studying the penal code or crimes, and there is no academic research on procedure law. I think that your research will be of importance for the UAE, especially as there are no academic writings on procedural problems in the UAE. Your research on electronic evidence and result findings will be of interest and will be discussed by the Ministry.[26]

1.6 Methodology

The methodology chosen to realise the objectives of this thesis combined applied social study and a doctrinal study (black letter law), incorporating a quantitative study using comparative elements. The objectives outline the need to acquire an understanding of

---

[24] Amal Al Minshawi, 'Local exchange companies exposed to foreign penetration operations via the "Western Union"' *Emaratalyoum Newspaper* (Dubai 22nd July 2013) <http://www.emaratalyoum.com/business/local/2013-07-22-1.593094> accessed 22nd July 2013. (Author's translation from the Arabic).

[25] Such as: other Arab countries.

[26] See: translated transcript of the interview with the Hadef Al Dhahiri Minister of the UAE Ministry of Justice in Appendix 5.

the shortcomings of the UAE legal system in reference to electronic evidence. In reference to these objectives, the applied study method is well suited because it provides information regarding the practical issues associated with in depth electronic evidence in the UAE from the viewpoints of legal experts and academics. However, in a thesis on the subject of laws, specific criteria should be followed when selecting the research methodology.

The comparative law approach will be one of the research methods used in this thesis. Comparative law is a method of analysing the problems and institutions originating from two or more national laws of legal systems, or of comparing entire legal systems in order to acquire a better understanding thereof, or provide information, and insight into, the operation of the system's institutions or the systems themselves.[27]

The methodological problems associated with undertaking comparative research have been discussed by Zweigert and Kötz, the initial aim of the comparative legal methods was indisputably bold:

> 'Comparative law must resolve the accidental and divisive differences in the laws of peoples at similar stages of cultural and economic development and reduce the number of divergence into the law, attributable not to the political, moral, or social qualities of the different nations but to historical accident or to temporary or contingent circumstances'.[28]

Despite this initial aim of the comparative legal study can now be perceived to be untenable, [29] the comparative legal approach can be use to provide valuable understanding and guidance. That is, not only understanding in the sense of knowledge and comprehension, but also in the sense of appreciating and respecting the operation of the law in other countries. Both drawbacks and pitfalls of the comparative approach need to be addressed and identified.[30] Platsas critically analyses the apple-oranges idiom in relation to comparative legal study:

---

[27] Peter DE Cruz, *Comparative law in a changing world* (3rd edn, Routledge-Cavendish, 2007) 9.
[28] Konrad Zweigert and Hein Kötz, *An Introduction to Comparative Law* (3rd edn, Oxford University Press, 1998) 3.
[29] Ibid.
[30] Mathias Reimann and Reinhard Zimmerman (eds.) *The Oxford Handbook of Comparative Law* (Oxford University Press, 2008) 875.

> An idiom which has captivated the English-speaking world as well as significant parts of the French-speaking is the one which asks people not to compare apples and oranges, they being different in essence…Where does all this leave us in law? In law things are broadly similar…That is not to say that broadly similar artefacts cannot and should not be compared…Theoretically, any law could be compared with any other law, if some common denominator of a valid comparison is found; yet the tendency – it would seem – in the comparative method of law is that we compare 'corresponding' areas of law or what is called 'comparison of equivalents'. [31]

The analysis of comparative approach in this thesis has been included in order to provide examples of reform which can be placed at either end of the electronic evidence regulation. Comparative research has primarily been included when answering the research question, when examining how electronic evidence is regulated in two legal systems, namely the common law and civil law systems. It will examine the general characteristics of the jurisdictions, the main characteristics of the regulatory systems and the characteristics of the rules related to electronic evidence. The 'macro-comparison' draws conclusions from comparing the broader systems of regulation in the two legal systems, it will scrutinise the background of the regulation of electronic evidence in each legal systems, aiming to identify the advantages and disadvantages of each system. [32]

Llewellyn's demonstration of his methodology can be used to identify the purpose of the comparative content of this thesis, 'Any reference to other times and places have a single purpose: to sharpen sight of what is with us here and now, by contrasting it with something different'.[33]

Moreover Gordley argues, 'I do not think the law of a single country can be an independent object of study. To understand law, even as it is within that country, one

[31] Antonios Platsas, 'The Functional and the Dysfunctional in the Comparative Method of Law: Some Critical Remarks' (2008) 12.3 *Electronic Journal of Comparative Law*.
[32] Comparing different system is commonly regarded as a problem, which requires the comparators to understand and describe the common and different features of the particular systems compared. This thesis focuses on comparisons between civil and common systems in relation to a specialized area of law namely the evidential protocols that are applied to the investigation and prosecution of crimes facilitated by the use of modern technology. See: p 33.
[33] Karl Llewellyn, 'Behind the Law of Divorce' 32 Columbia Law Review 1284.

must look beyond its boundaries…' [34]

Von Mahren was put forward the purpose and value of comparative approach, Mahren comments:

> '…This kind of study is useful in that it gives a better understanding of the inherent strengths and weaknesses of given institutional forms. Such understanding has considerable theoretical interest and may also prove of directly practical value by providing perspective and direction for law reform efforts'. [35]

Studying different legal systems requires comparing the ways in which each system provides a solution to the legal problem at hand. The results of this comparison will be used as recommendations for UAE law. An example of how comparative research has been used in this manner in order to assess the regulation of electronic evidence in the UAE and in order to provide proposal to reform. Chapter Three will seeks to explore how electronic evidence is regulated in two legal systems. It is important to acknowledge that while there are some salient features distinguishing the two legal systems, there may not be striking similarities on specific rules on an area of law across jurisdictions belonging to the same legal systems. Due to such irregular variations and for ease in discussions, the researcher prefers to take a case study approach taking one case study country for each jurisdiction to discuss regulation of electronic evidence in common law counties as compared to civil law countries: the England and Wales will represent the common law jurisdictions whereas a case study of People's Republic of China will be undertaken to represent civil law. The choice of each country is premised on the basis that England and Wales and People's Republic of China have salient features of a typical common law and civil law systems respectively. Attention will also be given to issues involved in each system as far as adducing, admissibility, authentication and certification of evidence is concerned in each system. This method allows the discussion of the comparative systems in outline in order to understand holistically the background and the nature of the systems.

---

[34] James Gordley, 'Comparative Legal Research: It's Function in the Development of Harmonized Law' (1995) 43, 4 *The American Journal of Comparative Law* 555.
[35] Arthur Mehren, 'An Academic Tradition for Comparative Law?' (1971) 19 *American Journal of Criminal Law* 624-628.

To manage the legal problems, a distinguished legal methodology was recommended, requiring an analysis of statutes and case law. Although social applied study is now united with legal thought, it remains a difficult task to combine the two different methodologies to achieve a single objective in a single thesis. The differences between an applied study and a doctrinal study include the use of unique research methodology for discussion.[36] In this thesis, the applied study approach is presented in Chapter Five, and the doctrinal elements of the study methodology is discussed in the Chapters Two, Three and Four.

1.7 Literature review

Over recent years, electronic evidence has had a profound effect on both the judicial and the technological worlds. Electronic evidence, with all its challenges and different viewpoints, has become a hotly debated topic among many researchers in different countries worldwide.[37] All these writers have described and shared their thoughts in different books and articles pertaining to the relationship between electronic evidence and a variety of disciplines. Several articles and books focus on electronic evidence and common law [38] and others have focused on electronic evidence in the field of forensics.[39] In 2010, during the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, electronic evidence was one of thirteen topics proposed for further study and research. The following aspects were recommended for study with regard to electronic evidence:

I. Regulation of procedures for the gathering, preservation and analysis of electronic evidence and the admissibility issue.

II. Analysis of different approaches within different legal systems in relation to electronic evidence.

[36]See: section 5.1.
[37]Such as: George Paul, *Foundations of Digital Evidence* (American Bar Association 2008). Michele Lange and Kristin Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know Now* (2nd edn, American Bar Association 2009).
[38]Such as: Stephen Mason (n 20).
[39]Such as: Eoghan Casey (n 8).

III. Regional issues for electronic evidence.[40]

At the European level, electronic evidence has become a topic for many researches. One of the most significant projects, the 'Admissibility of Electronic Evidence in Court: A European Project' (AEEC), dealt with electronic evidence. This project was carried out between 2005 and 2007 in 16 European countries.[41] The main aims of the project were to analyse the regulation of electronic evidence and to identify the legal gaps in the current regulatory situation in European countries in order to improve them. The method used to collect the project data was to pursue a comparative legal study and social science research methodology including both questionnaire and interview. The project revealed a lack of specific regulations pertaining to electronic evidence in European countries.[42] The report concluded with the recommendation that European countries need to prepare specific regulations for handling electronic evidence at both the European and the national levels, as well as to work on developing skills in the field of gathering and storing electronic evidence and improving international cooperation with regard to the electronic evidence.[43]

However, in the UAE, there is no specific written text that highlights the treatment of electronic evidence, whether as a component of the UAE's Procedural Law or in general legislation. Thus, related knowledge reaches the UAE only through the media of seminars and conferences.[44] On the processes of managing electronic evidence, there are no special texts, although the gathering of electronic evidence and other processes associated with this type of evidence plays a vital role in the successful prosecution of criminal cases. Illegally obtained evidence is not only commonly rejected by the court but can also damage the case that is dependent on them, were it to be ultimately declared invalid.

Electronic evidence creates presents an uneasy link between technical and legal developments. However, legal and technical sides often move at separate speeds,

---

[40] See: The United Nations Office on Drugs and Crime (UNODC) <http://www.unodc.org/unodc/en/expert-group-to-conduct-study-cybercrime-jan-2011.html> accessed 25th April 2013.

[41] Austria, Belgium, Denmark, Finland, France, Germany, Greece, Holland, Ireland, Italy, Luxembourg, Portugal, Romania, Spain, Sweden and the United Kingdom.

[42] For further information, see: Fredesvinda Insa (n 22).

[43] Ibid.

[44] Such as: the International Conference on Cyber Crimes.

having their own areas of individuality. A common example from our day to day lives would be to consider two individual bodies moving at different speeds, each having their own momentum, however at the point where they both intersect there is some sort of friction, preventing each reaching its maximum potential. This same relationship arises between technical and legal developments.

At the legal/ technical intersection this means that an individual's personal rights are jeopardised, because criminals are not being convicted or prosecuted for crimes, and exculpatory evidence in electronic form is being overlooked. The reason is that the conviction of a crime is difficult, and in some cases almost impossible, because electronic evidence generates complex issues of handling.[45]

Electronic evidence is not as simple and easy to manage as traditional evidence; in particular, according to Marcella, traditional evidence is typically tangible, with substance, value and form and at times even readily available to touch.[46] For example, evidence such as finger prints, finger nails and hair fibres are visible and even in cases where they are only very slightly visible it is easy to retrieve using certain forensic methods; moreover, if kept in the correct conditions this kind of evidence can survive for years, maybe even decades. This does not apply to electronic evidence, which is held in the form of zeros and numerical data; thus, protecting and preserving it is not an easy job, in some cases encrypted data is only available for a limited amount of time.[47] According to Kerr, electronic evidence can be described as having no physical manifestation.[48] As a result, the rules that apply to other normal physical evidence cannot be made to apply to electronic evidence; a fact that requires judges with a different and broader mind-set.[49] On the other hand, Wilson argues that while the rapid advancement in technology has brought law-enforcement bodies challenges, it has also

[45] David Harvey, *Internet.law.nz: selected issues* (3rd edn, LexisNexis Wellington 2011) 241.
[46] Albert Marcella and Doug Menendez, *Cyber Forensics: a field manual for collecting, examining, and preserving evidence of computer crimes* (2nd edn, Auerbach Publications 2008) 295.
[47] Ibid; this point can be an interesting, and the reader might begin considering the relevant practitioner text written by Stefanie Fischer-Dieskau and Daniel Wilke, 'Electronically signed documents: legal requirements and measures for their long-term conservation' (2006) 3 *Digital Evidence and Electronic Signature Law Review* 40–44.
[48] Orin Kerr, 'Digital evidence and the new criminal procedure' (2005) 105, 1 *Columbia Law Review* 279-318.
[49] Ibid.

brought genuine opportunities.[50] The type and nature of electronic evidence is discussed further in Chapter Two.

The profound differences in physical and electronic evidence also extend to the ways such evidence is gathered. For example, criminal procedural rules of gathering evidence under search warrants state that exact time, location and permission should be acquired before beginning a search, to narrow it down. These requirements are very easily met in the case of physical evidence collection, however in the case of electronic evidence, an entire digital data set must be investigated in specialised labs so that the information or data of importance can then be narrowed down; this takes place after a warrant has been issued.[51] As technology advances it is becoming an extremely tedious and difficult procedure to go over all the information and data on seized drives, because of their increasing memory capacity.[52]

The location of evidence could be another issue associated with handling electronic evidence. In any country where a crime is committed it is tried according to that country's jurisdiction. However in the case of electronic evidence, it is possible that the evidence needs to be collected from another country or is found to be part of a network; consequently issuing search and seizure warrants for electronic evidence is an issue arising from this. Grabosky, Smith, and Dempsey discuss this in their book, identifying the two main challenges facing investigators regarding obtaining evidence from abroad. According to them, collecting evidence by attaining cross-border access is a complicated and bewildering process.[53] The case of two Russians, Vasilii Gorshakov and Aleksei Ivanov, was the first to raise issue of evidence obtained on international hacking. In 2001, the US FBI investigated the Russian suspects' methods of hacking computers, for which they needed to obtain evidence from computer servers in Russia, without agreement or authority from the Russian Federation Government.[54] Various

[50]John Wilson, 'My Space, Your Space, or Our Space? New Frontiers in Electronic Evidence' (2008) 86 *Oregon Law Review*1205.
[51]Ibid.
[52]Erin Kenneally and Christopher Brown, 'Risk sensitive digital evidence collection' (2005) 2, 2 *The International Journal of Digital Forensics and Incident* 101-119.
[53] Peter Grabosky, Russell Smith and Gillian Dempsey, *Electronic theft: unlawful acquisition in cyberspace* (Cambridge University Press 2001) 128.
[54]See: Robert Lemos, 'Russia accuses FBI agent of hacking' *The news web site CNET* (16th August 2002) <http://news.cnet.com/Russia-accuses-FBI-agent-of-hacking/2100-1002_3-950719.html> accessed 24th April 2013.

authors have put great emphasis on this matter, such as Richard Gissel,[55] Jahnke,[56] Brenner and Schwerha.[57] The case showed the difficulty in obtaining evidence from abroad and the importance of international coordination and co-operation. The difficulties arising as a result of search and seizure methods of obtaining electronic evidence in the UAE are discussed further in Chapter Four.

There has been much discussion about whether electronic evidence has the same accuracy and reliability as other evidence; some believe it does, whereas many believe it does not.[58] However, electronic evidence can be reliable, although it is often necessary to take steps to insure the authenticity of complex evidence; as has been demonstrated in test cases.[59] The variance in forensic software and imaging for electronic evidence mean there is a great margin for reduced reliability and accuracy.[60] The authentication of electronic evidence will be further discussed in Chapter Four.

With regard to evidence, theories are accounts or conceptions of what the evidentiary proof process ought to be in terms of its nature and structure.[61] Theoreticians seek to describe, explain, evaluate, regulate or guide the actual parameters that decisions ought to take into account when addressing evidential issues. A number of evidential theories have been proposed. These include: (a) relevance theory; (b) probabilistic theory; (c) foundational theory.[62] This list is not exhaustive, but these are some of the theories that have received considerable scholarly attention. These are discussed briefly below:

A. Relevance Theory

According to this theory, any evidence that has a probative value ought to be admitted,

---

[55]Richard Gissel, *Digital Underworld: Computer Crime and Resulting Issues* (Lulu.Com 2005)128.
[56]Art Jahnke, 'Alexey Ivanov and Vasiliy Gorshkov: Russian Hacker Roulette' (1st January 2005) *CSO Security and Risk* <http://www.csoonline.com/article/219964/alexey-ivanov-and-vasiliy-gorshkov-russian-hacker-roulette?%3E=> accessed 24th April 2013.
[57]Susan Brenner and Joseph Schwerha, 'Cybercrime Havens: Challenges and Solutions' (2007) 17, 2 *The American Bar Association-Business Law Today*.
[58]Eric Buskirk and Vincent Liu (n 20).
[59] For further information about tests for the authentication of electronic evidence see: Stephen Mason (n 20).
[60]See: Fred Cohen, *Digital forensic evidence examination* (4th edn, Fred Cohen and Associates 2012).
[61]Edward Cheng and Albert Yoon, 'Does Frye or Daubert Matter? A Study of Scientific Admissibility Standards' (2005) 91 *Virginia Law Review* 471.
[62] See: Michael Pardo, 'The Field of Evidence and the Field of Knowledge' (2005) 24 *Law and Philosophy* 321-324; Ronald Allen and Michael Pardo, 'The Problematic Value of Mathematical Models of Evidence' (2007) 36 *Journal of Legal Studies*107-109; Michael Pardo and Ronald Allen, 'Juridical Proof and the Best Explanation' (2008) 27 *Law and Philosophy* 223-225.

however slight that probative value may be, unless otherwise specifically excluded by exclusionary rules of evidence.[63] Evidence with probative value in relation to a disputed proposition will be said to be relevant.[64] Thus, relevance is the fundamental foundation of evidence.[65] Any rule that seeks to exclude relevant items of electronic evidence ought to be regarded as a technicality, and an exception to the general rule.[66] Thus, the theory serves a normative role, but fails in its descriptive function of explaining what should be regarded as an item of evidence in the first place. By applying this theory to electronic evidence, relevance theory would hold that relevance is the basis of determining which electronic items of evidence should be proffered. Critics of this theory however, assert that it rests on the presumption that the evidence already exists, and that the only issue is to assess whether or not it has probative weight.[67]

B. Probabilistic Theory

According to this theoretical framework, the basis of admitting evidence lies in its probative value, rather than its relevance.[68] The probative value in this context refers to the strength of such evidence in tendering the proof of relevant facts or factual propositions relative to an issue.[69] In the context of electronic evidence, the admission of that electronic evidence will be determined according to the importance of such evidence in relation to the proof of the disputed proposition. This theory is plausible in the sense that it emphasises the value of evidence in tendering proof; thereby focusing on the role of evidence in the legal process. However, probabilistic theory may be difficult to apply in circumstances where an item of evidence may have limited value when taken in isolation,[70] but when considered together with other items, it generates

[63]Ronald Allen and Richard Kuhns, *Eleanor Swift and Evidence: Text, Cases and Problems* (5th end, Aspen Publishers 2011) 139.
[64]Kenworthey Bilz, 'We Don't Want to Hear It: Psychology, Literature and The Narrative Model of Judging' (2010) *University of Illinois Law Review* 429- 435.
[65]David Schwartz, 'A Foundation Theory of Evidence' (2011) 100 *University of Wisconsin Legal Studies Research Paper* 95.
[66] Michael Risinger, 'Inquiry, Relevance, Rules of Exclusion, and Evidentiary Reform' (2010) 75 *Brooklyn Law Review*1349-1353.
[67]Edward Cheng, 'A Practical Solution to the Reference Class Problem' (2009) 109 *Columbia Law Review* 2081.
[68]Michael Finkelstein and Bruce Levin, 'On the Probative Value of Evidence from a Screening Search' (2003) 43 *Jurimetrics Journal* 265-270.
[69] Davis Deborah and Follette William, 'Rethinking the Probative Value of Evidence: Base Rates, Intuitive Profiling, and the "Postdiction" of Behavior' (2002) 26 *Law and Human Behavior* 133.
[70]Adam Samaha, 'Law's Tiebreakers' (2010) 77 *University of Chicago Law Review*1661-1684.

significant probative weight. Such is the case much circumstantial evidence.[71] Secondly, the theory implies quantification of evidence (so as to determine probative weight).[72] However, this is nearly impossible, as there exist no objective standards for such quantification.[73] Probabilistic theory themselves do not offer such standards.

C. Foundational Theory

This theory was put forward by Professor Schwartz in his seminal article 'A Foundation Theory of Evidence'.[74] Schwartz posits that the foundational basis of evidence is that it has to be probably true, case-specific and assertive.[75] He argues that only items that meet these foundational qualifications can be entered as items of evidence, and that these parameters are a pre-condition to relevance. In the context of electronic evidence, judges need to examine whether or not the electronic item tendered is probably true (i.e. that it really it comes from the source identified), is specific to the case in question, and asserts the position which a party seeks to adduce the evidence for. This theory seems to add only one element that is not emphatically laid out by relevance theory, that is, the need to evaluate the truthful nature of an item of evidence as a pre-condition for assessing its relevance.[76] The other two elements essentially point towards probative value as a basis of evidence, just as suggested by relevance theory. Foundational theory may therefore be regarded as an extension of the relevance theory of evidence.

From the above discussions, evidence theories serves three broad functions: descriptive, explanatory and normative (evaluative and regulative roles). Thus, beyond their theoretical values, which may be regarded as ideals, evidence theories may be of practical value to judges (especially in regard to grey areas or conflicting evidentiary rules that need to be resolved), and to legislators, who may be interested in making regulatory reforms and would wish to be guided by established theoretical frameworks. Foregoing value may be greater in an evolving area such as electronic evidence, which

[71]Susan Haack, 'The Embedded Epistemologist: Dispatches from the Legal Front' (2012) 25, 2 *Ratio Juris* 215-218.
[72]Jonathan Koehler, 'When Do Courts Think Base Rate Statistics Are Relevant?' (2002) 42 *Jurimetrics Journal* 373-375.
[73]Ronald Allen, 'Rationality and the Taming of Complexity' (2011) 62 *Alabama Law Review* 1047-1055.
[74]David Schwartz (n 65).
[75] Ibid.
[76]Ibid.

is not yet as fully established as other traditional forms of evidence. The above discussion has explored three key theories of evidence: relevance theory, probabilistic theory and foundational theory. Attempts have been made to underscore their key propositions, their strengths and weaknesses, and their application in the context of electronic evidence.

With regard to the process for the preservation of electronic evidence, Casey notes that it is a vital step in ensuring authentication.[77] In 2009, The SANS Institute noted in their report that the preservation of electronic evidence has increased in complexity and that additional methodologies need to be adopted to acquire electronic evidence.[78] To regulate all processes associated with the handling of electronic evidence, standards and guidelines have been adopted. There is a set of guidelines that has been published, such as Digital Evidence Standards and Principles,[79] A Guide for First Responders,[80] the Good Practice Guide for Computer Based Evidence[81] and Guidelines for the Management of IT Evidence.[82] In addition, there are a number of international organisations discussed that are competent in researching the issue of electronic evidence, such as the International Standards Organisation,[83] and International Organisation on Computer Evidence.[84]

Many law enforcement agencies have to date already had to resolve issues and complications regarding the management of electronic evidence. Difficulties arise when they have to incorporate different techniques and methods in order to maintain

---

[77] Eoghan Casey (n 8) 12.

[78] See: Paul Henry, 'Best Practices in Digital Evidence Collection' (2009) <http://computer-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/> accessed 20th April 2013.

[79] Digital Evidence Standards and Principles submitted by: Scientific Working Group on Digital Evidence (SWGDE) <https://www.swgde.org/> accessed 4th November 2010.

[80] A Guide for First Responders submitted by: US Department of Justice (USDOJ) <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf> accessed 4th November 2010.

[81] Good Practice Guide for Commuter-Based Electronic Evidence submitted by: Association of Chief Police Officers' (ACPO) UK <http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf> accessed 4th November 2010.

[82] Guideline for the management of IT evidence submitted by: Australia <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016411.pdf> accessed 4th November 2010.

[83] The International Standards Organization (ISO) is most recent development in the Electronic Evidence field. The ISO provides guidance for identification, collection, acquisition, and preservation of digital evidence <http://www.iso27001security.com/html/27037.html> accessed 5th November 2010.

[84] International Organization on Computer Evidence (IOCE) <http://www.ioce.org/core.php?ID=1> accessed 5th November 2010.

electronic evidence as a viable option during the conviction and prosecution of a crime.[85]

The biggest problem faced during electronic evidence collection is that not many trained individuals have the necessary expert skills in operating the software, machines and tools used for electronic data collection, and thus many law enforcers fall behind the criminals in this area.[86] In order to make electronic evidence more viable and easier to use and understand in judicial trials requires considerable expertise, working to make such evidence more standardised and easy to use requires machinery, tools and software that can assist in managing this category of evidence.[87] With regard to computer forensic tools, Casey notes that in order to make the investigator's job easier, more advanced tools[88] must be developed.[89]

The technical and procedural aspects of computer evidence from the investigation perspective have been discussed in detail by Clark and Diliberto.[90] Even inexperienced users of computer equipment can understand their discussions, because explanations of the investigation process and the tools used, along with the methods of search and seizure, are supported by photographs of tools and places where such evidence may be found and evidence analysed. Exploration methods cover the area of methods for examining floppy discs and bulletin boards, the method for breaking and bypassing encryption, court procedures and samples of search warrants.[91]

In many articles and books the main issues and problems discussed in relation to electronic evidence are the technical difficulties faced when using gadgets specifically designed for collecting electronic evidence.[92] In order to collect viable information to handle electronic evidence, the development of both forensic tools and informative devices is necessary.[93] Development and modification in specialised areas of forensics

[85]This is a significant topic, and the reader might begin by considering relevant texts written by writers such as: Christopher Brown, *Computer evidence: collection and preservation* (2nd edn, Rockland MA: Charles River Media 2009).
[86] Anthony Reyes, *Cyber Crime Investigations* (Rockland MA: Syngress Publishing 2007) 191.
[87]Ibid.
[88]Tools such as: Encase and FTK.
[89]Eoghan Casey (n 8) 28.
[90]Franklin Clark and Ken Diliberto, *Investigating Computer Crime* (CRC Press 1996).
[91]For further information about these methods see: Stephen Mason (n 20) 193-195.
[92] Such as: Eoghan Casey (n 8) and Michael Arkfeld, *Arkfeld on Electronic Discovery and Evidence* (3rd edn, Law Partner Publishing 2010).
[93] Anthony Reyes (n 86).

is also a very important feature that needs to be developed. However, through legislation and in response to the needs of law enforcement agencies,[94] advancements have been made in order to convict and prosecute crimes reliant on electronic evidence, such as cybercrime. Policies are now gradually taking shape with the involvement international standards organisations. There is more development and work required to insure appropriate handling of electronic evidence, so that it can be widely used; therefore, the legal establishment and the IT industry must work together to accomplish change. Electronic evidence is still in the early stages of development, it requires time, energy and devotion before it is readily used and accepted in trials in the same way as physical evidence. With the rapid evolution of technology it is important for the law to keep up to date and to work openly with the IT industry in future.

In the UAE, all the above-mentioned challenges involved in handling electronic evidence as confronted by lawyers, judges, prosecutors and police officers are of huge significance.[95] Despite this, in the UAE, there have been no studies about the challenges of using electronic evidence and what procedures can be adopted. Thus, there is a lack in the academic library in this regard, which this thesis aims to fill. At present, in the UAE, newly constructed laws exist relating to the evidence that can be used in criminal enquiries; the intention of these is to eliminate shortfalls and misunderstandings. This is the first research conducted in the UAE regarding the utilisation of electronic evidence to prosecute crimes and the related challenges. Despite the focus on a single country, because this is a global issue, knowledge and understanding of the use of electronic evidence in the UAE has implications for the rest of world, especially other countries in the Middle East. Public consciousness may enforce improvements in electronic evidence. It will also ensure that electronic evidence is used in a very clear and translucent way.

In brief, the purpose of this study is to identify the issues and problems that arise in prosecution when evidence is solely electronic. As a result, this work studies the amalgamation of IT and law, to transform and bring to life a totally new era of law and prosecution.

[94] Such as: The People's Republic of China. For further information, see: section 3.4.2.
[95] See: section 5.3.

1.8 Terminology

Generally speaking, the term 'evidence' refers to anything that is acceptable as such to a court of law; it should help the judge to evaluate the scenario in a just manner. Thus, it comprises all the information and material submitted to a court by the parties concerned with facilitating the court to settle their dispute.

Evidence has two main types, the first is physical evidence and follows the fashion of starting with an oath, testimony of witnesses, fingerprints, etc., whereas the other sort is non-traditional, referred to as electronic evidence. Each of these kinds of evidence varies in its admissibility and integrity.[96] While the traditional form of evidence has long been understood, electronic evidence could not be understood clearly, because it is new and has less literature to support its existence, specifically in the UAE.

Electronic evidence is available in digital or binary form, consisting of the numbers 0 (pulse absent) and 1 (pulse present).[97] It originates from a multitude of sources including seized PC hard drives and ISP records, real-time email messages, backup media, chat-room logs, web pages and digital network traffic. It also includes local and presumptive databases, electronic directories, memory cards, wireless devices and digital cameras.[98] Evidence generated by digital systems is broader in scope than the electronic evidence produced by an analogue system. Therefore, the term 'digital evidence' is confined to evidence produced using digital technology, although its application is wider than that of electronic evidence since it extends to cell phones and digital audio and video devices, which are the prevailing technologies at present. This section of the thesis contains legal and technical terms and other terms that require understanding.

1.8.1 Definition of the term 'electronic evidence'

In the last few years, the term 'electronic evidence' has taken on several different definitions.

A set of accepted terms have been provided by leading organisations and academics in

[96]See: Fred Cohen (n 60).
[97]Chet Hosmer, 'Proving the integrity of digital evidence with time' Spring (2002) 1, 1 *International Journal of Digital Evidence*
<http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf> accessed 29th November 2010.
[98]Ibid.

the field to delineate the area. Some of these definitions are presented below:

Electronic evidence refers to the kind of 'information which either has been stored or been transferred through a computer and either supports or disproves the scenario presented regarding an offense'.[99] The definition of this phenomenon, as suggested by the Standard Working Group on Digital Evidence (SWGDE) is that it refers to 'piece of information that has been either stored or transferred in digital form'. [100] The International Organization of Computer Evidence (IOCE) defined it as the 'information stored or transmitted in binary [101] form that is dependable in court'.[102] Association of Chief Police Officers (ACPO) defined it as 'a piece of information stored or transferred by computer'.[103] Lastly, there is also the definition offered by Schafer and Mason, 'electronic evidence: data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence'.[104]

Based on these definitions we can explain the phenomenon as the generation of evidence by the entry of some sort of information by a user on a computer. However, a computer generates information when given a request to do so by an operator and when it processes the information. Thus, the list of electronic evidence includes databases, application programs, operating systems, electronic and voice mail messages and records, computer-generated models, and other instructions stored in a computer's memory.

Generally, countries legislative structures offer no specific definitions for electronic

[99]Eoghan Casey (n 8) 7.
[100]See: Standard Working Group on Digital Evidence (SWGDE) <https://www.swgde.org/> accessed 4th November 2010.
[101]The word 'binary' was later changed to 'digital'. See: Carrie Whitcomb, 'An Historical Perspective of Digital Evidence' Spring (2002) 1, 1 *International Journal of Digital Evidence* <http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf> accessed 5th November 2010.
[102]See: International Organization of Computer Evidence (IOCE), 'G8 Proposed principles for the procedures relating digital evidence' (2000) <http://www.ioce.org/fileadmin/user_upload/2002/G8%20Proposed%20principles%20for%20forensic%20evidence.pdf> accessed 15th November 2010.
[103]See: Association of Chief Police Officers, 'ACPO Good Practice Guide for Digital Evidence' (March 2012) <http://library.npia.police.uk/docs/acpo/digital-evidence-2012.pdf> accessed 15th November 2010.
[104]See: Stephen Mason (20) 27.

evidence. However, many countries include a definition of the phenomenon of legislative structure through references. For example section 2 (1) of the Irish Criminal Evidence Act 1992 provides:

> "document" includes—
> (i) a map, plan, graph, drawing or photograph, or
> (ii) a reproduction in permanent legible form, by a computer or other means (including enlarging), of information in non-legible form'.[105]

In the case of documentary evidence, the French Civil Code defines it as proof in written form, with some conceptual terminologies, characters, figures or any other signs or symbols involved, no matter what is their medium or manner of transmission.[106] This article includes some references to electronic evidence.

A more direct reference can be found in the UK and Canada. The Police and Evidence Act 1984 in the UK put forth a definition of this phenomenon as 'information stored in any electronic form'.[107] However, the definition used in Canada was altered along with the structure of its legislation in 1997, when the Uniform Law Conference of Canada suggested alterations to the structure of the definition so that it could conform to a state applicable to features like hearsay rule, best evidence rules and authentication. These different suggestions of definitions of the phenomenon created more issues and therefore the idea of creating a Uniform Act was suggested to promote a logical legal structure in this regard.[108] This suggestion resulted in the definition of the Canada Evidence Act in 1998, which defined it as the computer system, electronic documents, data, and the electronic document system. The nature of electronic evidence as a definition is quite broad, as it includes both soft and hard copies of data stored in a computer.[109]

In the UAE, there is no direct definition of the term 'electronic evidence' or 'digital evidence' in any extant statutes, with the exception of Article 1 of Federal Law No. 5 from 2012 concerning the Prevention of Information Technology Crimes. In this Act, the terms 'electronic information' and 'electronic document' are defined as follows:

---

[105] See also: Electronic Government Code of the Republic of Italy 2005, Article 1.
[106] Civil Procedure Code of the French Republic Inserted by Law No. 230-2000, Article 1316.
[107] The Police and Criminal Evidence Act of 1984, s 20 (1).
[108] Canada Uniform Law Conference, available at: <http://www.ulcc.ca/en>.
[109] Canada Evidence Act R.S.C., 1985, c. C-5, s 31.8.

Electronic Information: 'Any piece of information that is saved, processed, produced and transmitted with the use of information technology, specifically in the form of texts, voice, pictures, numbers, letters, codes, signs, etc.'[110]

Electronic Document: 'A document that is saved, extracted, copied, exhibited, or transferred by electronic means on some electronic or some tangible medium and is accessible in a feasible manner'.[111]

In short, the term 'electronic evidence' is used widely, but is commonly used to denote digital evidence only, which creates confusion. It is suggested that the term 'electronic evidence' is generative, rather than specific, in that it encompasses all forms of data, whether produced by an analogue device or in digital form.[112] Evidence generated in digital form is typically on a larger scale than electronic evidence produced by analogue device. Accordingly, the term 'digital evidence' is restricted to evidence produced by digital technology, but, as previously stated, its application is wider than electronic evidence since it extends to cell phones and digital audio and video. These two forms of evidence should not be confused because different evidential and procedural requirements apply to each, in that they must meet their respective technical, scientific and legal standards or requirements to be admissible as evidence at trial. In the UAE, the meaning of electronic evidence has not yet been discussed. Case law merely emphasises the admissibility of email evidence, but does not explain what is meant by the term 'electronic evidence'.[113] This absence of any specific provision explaining this term may leave judges in the UAE with scant opportunity to make meaningful decisions about what electronic evidence is.

It is noted that, in the UAE courts there is a preference for terms such as 'computer-produced evidence' or 'computer printout'. However, it is not clear whether these terms are intended to extend to electronic evidence. It is consequently appropriate to look at the definition of the term 'computer' under UAE law.

---

[110] The UAE Federal Law No.5 of 2012 on the Prevention of Information Technology Crimes, Article 1.
[111] Ibid.
[112] There are many people who make the mistake of classifying analogue evidence as electronic evidence, which it is not, Schafer and Mason made it clear that there is a clear difference between analogue evidence and electronic or digital evidence. For further information, see: Stephen Mason (n 20).
[113] Such as: Criminal Case of UAE Federal Supreme Court No. 50/2011 date of decision 19th April 2011 unpublished.

1.8.2 Interpretation of the term 'Computer'

The word 'computer' is defined as 'a system or a device that is capable of carrying out a progression of operations in an explicitly and distinctly defined method'.[114] It is also described as a machine that can accept data in prescribed form, process it, and provide the consequence of processing it using a machine or process.[115] As a result, the word 'computer' has been defined as a generic term to include almost any kind of processing unit. Nevertheless, not all machines can be defined as computers.[116]

In the Oxford English Dictionary, the term computer is described as: 'An electronic automatic device that performs mathematical or conceptual operations freq. with definition of word prefix as some, analogue, digital, electronic computer'.[117]

In the UAE, the word 'computer' is not defined in Federal legislation or by any evidential statutes. However, the national legislation of other states (such as the US,[118] Singapore,[119] Australia[120] and South Africa[121]) has provided such a definition. In the UK the term computer is defined by the Civil Evidence Act 1968,[122] as 'a machine for storing and processing information'.[123] This definition extends the scope of the computer by looking at the capacity of a device. Any device can be regarded as a computer if it is capable of recording, storing, processing, retrieving or producing information. However, in later Acts[124] the UK decided to make no attempt to define what a computer is. This is because the word 'computer' is now in common usage in the English language and judges are capable of construing its meaning.

Since there is no statutory definition of the word 'computer' in the UAE, it is submitted that different interpretations may be given to the meaning of the word, creating opportunities for lawyers and prosecutors to argue over its applicability in computer-

[114]Christopher Millard, *Legal protection of computer programs and data* (Sweet and Maxwell 1985)1-15.
[115]Ibid.
[116]Stephen Mason (n 20)1.
[117]Oxford English Dictionary (electronic edition) (3rd edn, 1997 and Additions).
[118]In the US the word 'computer' is defined by the Federal legislation on Computer Fraud and Abuse Act of 1986 (CFAA) 18 U.S.C, s1030.
[119] The Singapore Evidence (Amendment) Act No.8 of 1996, s 3(1)
[120]South Australia Evidence Act (SAEA) of 1929, s 59A.
[121]South Africa Computer Evidence Act (SACEA) No.57 of 1983, s 1.
[122] The UK Evidence Act 1995 replaces the UK Civil Evidence Act 1968.
[123] The UK Civil Evidence Act1968, s 5 (2) and the relevant reference is now the meaning of a 'document', which is provided for in Section 13 of the Civil Evidence Act 1995.
[124] For examples, the UK Computer Misuse Act of 1990, the Police and Criminal Evidence Act of 1984 and the Copyright, Designs and Patents Act of 1988.

related cases. Consequently, they must be capable of explaining and defining the technical aspects or the working processes of the computer itself; otherwise, they may have to hire a computer expert to explain technical details. In practice, the meaning of 'computer' in the UAE will be construed by the judge, and so will be interpreted based on the facts of the particular case.

Nonetheless, lawyers, prosecutors and judges must be prepared for possible objections that may arise around the technical and general definition of 'computer'. Accordingly, a clear definition must be established, because different interpretations will result in diverse outcomes when determining the relevance, reliability and acceptance of electronic evidence.

1.9 Conclusion

With the rapid advancement in the features of crimes, the crime rate could lead to the birth of a new branch of legal studies and a new set of evidence when conducting investigations. This increased rate of crime has greatly increased the importance of electronic evidence. Investigating cases of crimes containing electronic evidence is a somewhat more difficult task than the traditional investigation strategy. As electronic media has its own features, and needs to be dealt with accordingly, it requires a unique treatment in the legislative system. This requirement of electronic evidence requires alterations to the structure of the legal systems of those countries that are too traditional in nature and capable of dealing only with physical evidence. Changes in the system will help the electronic evidence to work effectively. Electronic evidence serves the same purpose as investigation procedures, as do the other sorts of evidence, because it is also a piece of information that serves to present the facts of a case. However, electronic evidence is sensitive in nature and relevant experience and training is required for its handling.

Aside from this discussion, the fundamental question to ask is, whether and to what extent, criminal procedure law is sufficient to govern the process of the gathering and the preservation of electronic evidence. The Council of Europe's Recommendation No R (95) was the first to attract attention to electronic evidence by connecting criminal

procedural law with information technology.[125] As the process of collecting electronic evidence becomes more technical, legislation becomes more challenging when mens rea must be proved beyond reasonable doubt. In future it will be further complicated, since everything will be stored in digital format or in similar intangible forms. Investigating crimes and prosecuting criminals may also be difficult and challenging, and any negligence in the process of gathering and preservation of electronic evidence will result in failure in prosecuting cases. Therefore, UAE lawmakers must strive to improve and update the rules covering the processes of handling electronic evidence. This chapter has discussed the significance of the thesis and shown why academic research is important in field of electronic evidence. Setting the objective of the thesis as to examine the problems and challenges of electronic evidence in the UAE, the thesis aims to contribute to the body of academic thought in the area. Such a contribution seems appropriate for the UAE, where the law lacks sufficient academic input, especially in the area of electronic evidence.

Thus, the method of applied study is appropriate for collecting more information concerning the UAE law to sustain the arguments of this study. It is felt that the combination of two methods is the best way of achieving the objectives of this thesis. It should be made clear that in the discipline of law there is a distinct concept of research methodology. There is a distinct legal methodology for solving legal problems. A mere legal discussion of a problem involves, for instance, interpretation, case law and comparison. The difficult task here lies in attempting to combine social science research methodology with legal methodology to construct a comprehensive thesis. It is true that socio-legal thought has developed considerably in recent years, but legal thought still relies on a unique research methodology in argumentation. The researcher in this thesis will attempt to combine legal methodology with applied social science methodology.

Chapter One also reviewed some literature to deliver an overview of key challenges facing the treatment of electronic evidence. The chapter concluded by clarifying some useful terminology.

In brief, this chapter has provided a background to the thesis in order to open up the discussion points covered by the research questions in the coming chapters. In order to

[125] See: 'Explanatory Report to the Convention on Cybercrime' (ETS 185) (2001) <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm> accessed 15th April 2013.

understand physical and electronic evidence, and the different kinds of investigations, the next chapter will look at the distinction between two types of evidence, and introduce the UAE's legal system.

CHAPTER TWO: THE JUDICIAL SYSTEM IN THE UAE AND THE NATURE OF ELECTRONIC EVIDENCE

Following on from the road map for this thesis in Chapter One, this chapter aims to provide a general review of the legal system in the UAE. In addition, it aims to provide a fundamental overview of the nature of electronic evidence. The law defines the principles and rules governing relations between nations and within nations; the legal system is the form taken by a state or party when establishing the principles and rules of law to be used for protecting people, the maintenance of their honour and security of their money. In general, the legal system is based on one of three basic systems: common law, civil law and religious law or combinations of these.

The UAE is a civil law country that has been influenced by the legal systems of civil law countries including Egypt and France. In the first part of Chapter Two, the researcher aims to introduce the judicial system and explore evidentiary rules. The researcher also aims to track the development of the UAE's CPL since its foundation in 1992, until its most recent amendment in 2005. Understanding of basic information associated with the legal and judicial system is essential as background providing an explanation and understanding of the legal system, and how the law handles electronic evidence.

This chapter also aims to describe the distinction between cybercrimes and physical crimes; and offers a brief analysis of cybercrime, explaining the legal response to such crimes. Currently, cybercrimes is taking on many shapes and forms. ICT has revolutionised communication, commerce and entertainment; it has given rise to cyber or modern crime, also called 'computer-related crime' and 'high-tech crime', i.e. the use of electronic communication networks for criminal purposes or for the purpose of destroying information or systems.

Traditional crime and cybercrime are similar in nature, as they both result in violations of the rules and laws of a state; however, the background to cybercrime differs from conventional crime, as modern technology and computers are key requisites. As a result, law enforcement agencies in the UAE are facing complex challenges; particularly as cyber criminals are often educated, organised and well-equipped, making

it difficult to combat their activities, gather evidence, locate criminals and prosecute offenders. Difficult questions are also arising in relation to the development of suitable criminal procedural laws, which is necessary to ensure that electronic evidence is adequately dealt with.

In order to demonstrate the characteristics of electronic evidence, the remainder of this chapter will address the manner in which electronic evidence differs from other forms of evidence, by examining the types and the nature of electronic evidence. Pursuant to the above, it is appropriate to include the following:

I. A brief overview of the judicial system and evidentiary rules;

II. Review the UAE legal system and the development of the UAE's criminal procedure law;

III. Define physical crime and cybercrime parameters;

IV. Discuss the types and the nature of electronic evidence; and

V. Detail the processes for criminal investigation of cybercrime and physical crime.

2.1 The judicial systems and evidentiary rules

The legal system is based on one of a combination of three basic systems: common law, civil law and religious law.[1] In most countries, the system of criminal justice is in a constant state of transformation. This is mainly due to the introduction of political, social and economic reforms intended to improve the effectiveness and efficiency of judicial proceedings'.[2] For instance, the legal systems of some countries, such as Italy, have transformed to become combative and adversarial systems, diminishing investigatory and inquiring components.[3] Investigative and adversarial systems are diverse, and united under specific conditions.[4] Prior studies show that the inquisitorial

[1]There are many views regarding to legal systems, some scholars say there are two legal systems, others say three and some say five. See further: Peter Cruz, *Comparative law in a changing world* (3rd edn, NY: Routledge-Cavendish c 2007).
[2]See: Arie Freiberg, 'Non-Adversarial Approaches to Criminal Justice' (2007) 16, 4 *Journal of Judicial Administration* 205.
[3]Ibid.
[4]Kristi Kernutt, 'Civil Law V Common Law Systems: Are They So Different?' (1999) *Oregon Review of International Law* 31.

system originated from a foundation of laws, codes and statutes, [5] whereas judicial decisions rely on case precedents and legislation. Hence, judges in such systems have more concrete decision-making powers than civil judges do. In fact, they tend to take on judicial autonomy.[6] Inquisitorial judges only implement legislative laws in specific cases; whereas adversarial judges take into account a combination of diverse aspects. They tend to consider factual evidence, analyse statues, and exercise great discretion over their vast decision-making powers. Thus, they can exploit authority to reach a conclusive decision.[7]

However, judicial precedents tend to restrict the decision-making power of judges in adversarial systems, while an inquisitorial judge is free of such restrictions. Hence, inquisitorial judges are able to independently concede to or repudiate the views of their seniors. However, in reality, they are under pressure to support the judicial precedents set in higher courts because otherwise their decisions are subject to challenge therein.[8]

2.1.1 Evidentiary rules of civil law versus common law systems: regimes and implication

The description of legal systems as either common law or civil law [9] is commonly recognised, although there is no agreement as to the exact categorisation of global systems. Nearly every jurisdiction inclines towards one or other of these groups in some way. It is essential in this section to understand the differences between the two legal systems, before studying the dissimilarities as they apply to particular rulings on electronic evidence.[10] Before any discussion of the traditional dissimilarities between the two systems, it is imperative to mention that both systems share many elements. Indeed, distinctions that were previously very noticeable are rapidly diminishing. Primarily, the main differences between civil law and common law legal systems result from their routine methods and principles; especially in terms of: (a) overall rules that adjust the admission of evidence; (b) use of judicial precedent; (c) the activity and role

[5] Peter Cruz (n 1) 46.
[6] Ibid.
[7] Kristi Kernutt (n 4).
[8] Ibid.
[9] This could be an interesting topic, and the reader might begin by considering the relevance of practitioner texts, such as: Mirjan Damaska, *The faces of justice and state authority: a comparative approach to the legal process* (New Haven; London: Yale University Pressc1986).
[10] Chapter Three will seek to address how electronic evidence is regulated in common law countries, as represented by the England and Wales, and civil law jurisdictions as represented by China.

of counsel in court proceedings; (d) activity of parties and their control of court proceedings; and (e) the relationship between the legislature (as characterised by legislative provisions) and the courts (as exemplified in court explanations).[11] Since these differences underpin the judicial system, they form a vital context within which evidentiary regulation regimes are anchored. Thus, it is beneficial to examine the differences between civil and common legal systems on an evidence basis generally, before examining variations in specific regulations on electronic evidence.

2.1.1.1 Rules on the admissibility of evidence

The common law system works by first establishing complex rules of evidence, which are considered general rules.[12] However, there are some exceptions and restrictions, which commonly effect regulations pertaining to the administration of hearsay evidence.[13] Case law, which is now commonly coded, was the reason for the development of complex exclusionary rules of evidence. This is now an important element of the whole system. As different cases were heard, different rulings in court led to alterations in the rules of evidence.[14] New rulings changed subsequent rules, leading to a clear distinction between former rules and new rules, with the latter taking precedent over the former. This is the reason for the complexity that is found in common law.[15]

The civil law system works so that assessment of evidence is established on a 'free evaluation principle'.[16] This relies on the presiding judicial officer making a judgment or ruling according to the case at hand, rather than being restricted to strict rules and those formed according to the relevant codes. This system shares some similarities with the essential exclusionary regulations formed in relevant codes.

The 'free evaluation principle' permits a broader scope for the admission of evidence

[11]See: Charles Koch, 'Envisioning A Global Legal Culture' (2003) *Social Science Research Network*.
[12]Matthew King, 'Security, Scale, Form, and Function: The Search for Truth and the Exclusion of Evidence in Adversarial and Inquisitorial Justice Systems' (2001) 12 *International Legal Perspectives* 186.
[13]Colin Tapper and Rupert Cross, *Cross and Tapper on Evidence* (12th edn, Oxford University Press 2010) 66.
[14]Kevin Clermont, 'Standards of Proof in Japan and the United States' (2004) 37*Cornell International Law Journal* 273.
[15]See: Mirjan Damaška, *Evidence law adrift* (New Haven; London: Yale University Press 1997).
[16]For a discussion on the free evaluation of evidence in civil law jurisdiction courts, see: Mark Klamberg, *Evidence in International Criminal Trials: Confronting Legal Gaps and the Reconstruction of Disputed Events* (Martinus Nijhoff Publishers 2013) 117.

than that under exclusionary rules, which is limited. This aspect differs from common law's systematic and complex exclusionary rules. The civil law system does not usually require juries. Thus, the judge is the sole fact finder and applier of the law. Given their professional competency they are believed to be better equipped to rule on what evidence is to be admitted or otherwise. This explains why there is less motivation in civil law to form complex exclusionary rules.[17] It has been debated that the reason for many of the exclusionary rules in the common law system is due to the dependency on jurors to pass verdicts. Without knowledge of the rules, there is more scope for them to make errors when measuring the evidence, failing to assess accurately what should or should not be admitted. The trial process by jury as it is intended to stimulate a just, impartial and lawful fact finding procedure is consequently controlled by a complex set of court rules.[18]

2.1.1.2 Court proceedings and parties activity

Court procedures in common law systems are mostly confrontational, whereas civil law jurisdictions are typically interrogational. In confrontational systems, the parties, through their attorneys play a leading role in identifying issues, carrying out examinations, presenting evidence and involving experts to resolve evidential concerns and even for discovery. In an interrogational approach to court proceedings judges are generally likely to play a leading role. This is specifically in relation to the desire to frame concerns for determination, the involvement of experts and the investigation of witnesses.[19]

2.1.1.3 The judicial function

Common law is defined by judicially active explanations, according to which, the courts are involved in forming interpretations, not only to implement statutory provisions, but also to resolve issues associated with unfinished, confusing or contradictory statutory provisions.[20] Thus, common law jurisdictions include numerous cases of laws formulated by judges in the form of judicial practices. This occurs to such

[17]William Pizzi and Luca Marafioti, 'The New Italian Code of Criminal Procedure: The Difficulties of Building An Adversarial Trial System on A Civil Law Foundation' (1992) 17, 1 *The Yale Journal of International Law (YJIL)*.
[18]See: David Johnson, 'Crime and Punishment in Contemporary Japan' (2007) 36, 371 *LexisNexis* 385.
[19]See: Valerie Hans, 'Introduction: Citizens as Legal Decision Makers: An International Perspective' (2007) 40 *Cornell International Law Journal* 303-304.
[20]Paul Finn, *The common law in the world: the Australian experience* (Centro di studi e ricerche di dirittocomparato e straniero 2001) 1-3.

an extent that common law courts have traditionally played a substantial law-making role by means of active judicial interpretations. In contrast, the courts in civil law systems are not usually as involved in the law making process. They implement the pre-existing law, rather than forming judicially active explanations. This is based on the assumption that the making of judicially active judgments would involve a separate law making process, which would be political based, and so should be reserved for the legislature. The making of any changes or resolutions by the court would reduce the importance of parliamentary supremacy over legislative issues.[21] Therefore, in a civil law system any injustice or confusion in the law should be referred back to the legislature.

2.1.1.4 The judicial precedent

The idea and role of judicial precedent is an important aspect of the judicial and legislative relationship and has a differing role in the two jurisdictions. The decisions of the courts have less precedential value under civil law jurisdictions.[22] The supposition is that it is the responsibility of the legislature to devise adjustable laws that can be applied to multiple cases, on a case by case basis by the court, after formation. Any unfinished, confusing or contradictory issues would then be handled by a code promulgating body or the legislature, and not the court. Thus, even when higher courts form a ruling on an issue, that court or a lower court will not be under any obligation to follow this. This means that civil law systems are of the opinion that judges should not be the sources of laws and that their adjudications are simply the application of existing codes and should not bind decision-makers in later cases. In recent years, civil law courts have followed the precedents set by the higher courts, even though such decisions are guides rather than obligatory.[23]

Conversely, judicial precedents are a prominent characteristic of common law systems. Decisions made by the higher courts are obligatory for lower courts to follow when ruling on similar matters. Practically, judicial precedent is used because it is unlikely that the legislature, in the development of law making, would have predicted all

[21] Ibid.
[22] Oscar Chase and Helen Hershkoff, *Civil Litigation in Comparative Context* (Thomson West 2007) 260-262.
[23] Linda Greenhouse, 'The Nation: Judicial Intent; The Competing Visions of the Role of the Court' (New York Times 7th July 2002) <http://www.nytimes.com/2002/07/07/weekinreview/the-nation-judicial-intent-the-competing-visions-of-the-role-of-the-court.html> accessed 10th January 2013.

possible situations that could arise. Higher courts cannot pass laws, to cover all possible situations. [24] Theoretically, the reason for judicial precedent in common law jurisdictions is that applying the same law to a similar set of facts should result in a similar result and lead to equality and consistency. This is why courts carry out active judicial interpretation when seeking to resolve unfinished cases or those with questionable features.[25]

2.1.2 UAE's legal system [26]

The UAE is a federation comprising seven Emirates,[27] and its jurisdiction is based on civil law. Egyptian, French and Islamic law heavily influences the legal system. There are three main sources of law in the UAE: legislation, Islamic Sharia and custom. The judiciary does not engage in law making; however, reference is sometimes made to the decisions of higher courts; such as legal principles issued by the Cassation Court or the UAE Federal Supreme Court. The judiciary is divided into the local and federal judiciary by virtue of Article 104 of the Constitution, which provides that "the local judicial authorities in each Emirate shall have jurisdiction in all judicial matters not assigned to the Union judicature in accordance this Constitution". Consequently, each Emirate deals with legal affairs locally. Article 105 of the Constitution allows that parts of, or an Emirate's entire jurisdiction can be transferred to the federal courts upon the request of the Emirate. Abu Dhabi,[28] Ras Al Khaimah [29] and Dubai [30] established and maintained their own judicial systems, which are therefore not dealt with federally. Regional or Federal UAE courts are similar to most other courts and as such are divided into criminal and civil courts. The Sharia court is a separate third division, which was initially created in order to adjudicate personal disputes. Both criminal and civil courts have a Court of First Instance, Court of Appeal, and Court of Cassation, the latter

[24]Christopher Mueller and Laird Kirkpatrick, *Evidence* (4th edn, Wolters Kluwer Law and Business 2009) 34.
[25] See: Anne Kuhn, 'Societe Nationale Industrielle Aerospatiale: The Supreme Court's Misguided Approach to The Hague Evidence Convention' (1989) 69 *Boston University Law Review LexisNexis*1011-1014.
[26]This section based on the content of article has been published as: Khaled Aljneibi, 'Search and seizure for electronic evidence: procedural aspects of UAE's legal system' (2013) 10 *Digital Evidence and Electronic Signature Law Review*.
[27]The United Arab Emirates (UAE) is a federal country that comprises seven Emirates, namely: Abu Dhabi, Dubai, Sharjah, Ajman, Umm Al-Qaywayn, Ras Al-Khaymah and Al-Fujayrah.
[28]Law of 1968 concerning the establishment of Abu Dhabi Courts and amendment Law No. 23 of 2006.
[29]Law of 1971 concerning the establishment of the Ras Al Khaimah Courts and amendment Law No. 3 of 2011.
[30]Law of 1970 concerning the establishment of the Dubai Courts.

having the same status as the Federal Supreme Court of the UAE.[31] Federal laws are applied in the courts of the UAE, and local courts apply federal laws first, that is a Civil Code or Criminal Laws. In areas where there are no federal laws, the emirates of Abu Dhabi, Ras Al Khaimah and Dubai pass laws and issue decrees.

Each of the three courts, the Court of First Instance, the Court of Appeal and the Court of Cassation, requires a different number of judges to hear each case. The Court of First Instance is presided over by one judge; the Court of Appeal is presided over by three judges; and, the Court of Cassation is presided over by five judges. The highest court in the UAE is the Federal Supreme Court, which is presided over by five judges.[32] There are only Courts of Cassation in three of the emirates: Abu Dhabi, Dubai and Ras Al Khaimah; elsewhere cases are heard by the Federal Supreme Court, the latter only addresses issues of law.[33] The lower court has to adhere to the legal principles and decisions developed by the Federal Supreme Court and the Court of Cassation.

The prosecutorial service in the UAE is a part of the judicial system,[34] and is divided into a local and federal prosecution. Ras Al Khaimah,[35] Dubai [36] and Abu Dhabi [37] have formed an independent public prosecution office, so are not overseen by the Federal Public Prosecution Authority. A federal and local public prosecution are responsible for interrogation,[38] and accusation,[39] and are also responsible for referring the indicted to the court if found guilty.[40] Another obligation is the overseeing of detention facilities and penitentiaries.[41]

Generally, in the UAE,[42] when a criminal offence has occurred, the act will be prosecuted and reported within the state where the act took place.[43] Upon report of the crime at the local police station the investigator will take statements and gather

[31]The UAE Constitution of 1971, Article 95.
[32]Ibid, Article 96.
[33]Ibid, Article 99.
[34]The UAE Criminal Procedure Law, Article 5.
[35]Decree No. (11) of 2006 concerning the establishment of the Ras Al-Khaymah Public Prosecution Office.
[36] Decree No. (8) of 1992 concerning the establishment of the Dubai Public Prosecution Office.
[37] Law No. (23) of 2006 concerning the establishment of the Abu Dhabi Public Prosecution Office.
[38]The UAE Criminal Procedure Law, Article 65.
[39] Ibid.
[40]Ibid, Articles 120 and 121.
[41]Ibid, Article 6.
[42]UAE state security cases will be prosecuted in the Abu Dhabi, the capital of UAE.
[43]The UAE Criminal Procedure Law, Article 142.

information from relevant persons.[44] After preliminary investigation of the case is complete, the local police will send details to the public prosecutor within 48 hours of the defendant's arrest.[45] Thereafter, the public prosecution office will investigate the case, listen to witnesses, and take statements in order to decide either to drop the matter, or to refer it to the court within 21 days of receiving the case from police.[46] If the matter has not been completed and the prosecutor requires further time, they may apply for extension from the court.[47]

The UAE's legal system is similar to the legal system of common law countries, including the UK. The same standard of proof applies to criminal cases, and in both countries, the prosecution has the burden of proof. Similarly, the police have to gather evidence for the prosecution to establish the case. There is no jury and also no Magistrates Court in the UAE and different evidentiary rules exist; although in both countries evidence can be declared inadmissible and unreliable in certain circumstances.

2.1.3 Developing UAE's criminal procedure law

The UAE's CPL normally contains all applicable procedures for criminal cases and thus determines the legal norms and standards, which have to be followed when gathering evidence. The agency administering the UAE's CPL also helps parties with trial preparation, thereby ensuring that an impartial verdict can be reached.

The UAE's CPL divides the investigation into three core stages. In the first stage, evidence is gathered. In the second stage, a preliminary investigation is undertaken and in the third stage a trial takes place. The main objective of the UAE's CPL is to ensure that the relevant authorities follow all the appropriate procedures, thereby safeguarding the rights of the suspect. The UAE's CPL is different from the Penal Code, which details different criminal offences and sentences. The UAE's CPL developed in stages and is heavily influenced by Egyptian and French law, whilst the law of evidence is

[44]Ibid, Article 30.
[45]Ibid, Article 47.
[46]Article 110 of the UAE Criminal Procedure Law provides that the detention period is 7 days, renewable up to 14 days by the prosecutor.
[47] Article 110 of the UAE Criminal Procedure Law provides that judges may extend the detention period for another period not exceeding 30 days renewable at the request of the public prosecutor after hearing the accused's statements.

based on custom and Islamic laws.[48] When initial procedural laws came into existence, no records were kept and each case was decided on a case by case basis with no system of precedent.

On the 15th June 1992, the UAE's CPL, which established modern procedures for the investigation of criminal cases,[49] rendered it mandatory to record decisions and established rules for cross-examinations, as well as appeals.[50] Various articles[51] of the UAE's CPL were changed on the 14th March 2005, but these changes did not affect the rules governing evidence, or pertain to the gathering of evidence stored on computers.[52] However, sophisticated technology has made it more difficult to gather information; and it is important that capabilities are enhanced.

2.1.4 UAE legal system and evidentiary rules

The three crucial concepts of evidence law are: burden of proof, relevance and admission. The first concept refers to the obligation to prove or disprove certain facts; i.e. those that arise as a result of a dispute between two parties in a case. However, the second refers to the ability to recognise the existence of facts in the form of evidence.[53] This helps in making decisions that would not otherwise be applicable in the absence of evidence. The third element is admissibility of evidence, which is a question of law and is determined by the court.[54]

Prosecutors apply two concepts to physical and electronic symptoms simultaneously. Formerly, it was the obligation of prosecutors to provide necessary the facts when bringing cases. This role remains the same, even in the case of the diversity of evidence, such as physical or electronic evidence. Similarly, it is the duty of the judge to assess the relevance of evidence, irrespective of its nature. Besides, admissibility of evidence is a process based upon two steps, namely the legislative and the judicial. The former

---

[48] Jodat Jihad, *Brief explaining of the UAE Criminal Procedure Code* (2nd edn, Dubai Police Academy Publications 2008)18. (Author's translation from the Arabic).
جوده حسين جهاد،الوجيزفي شرح قانون الاجراءات الجزائية لدولة الامارات (أكاديمية شرطة دبي،2008) ص18.

[49] The UAE Criminal Procedure Law, Chapter Two.

[50] Ibid, Chapter Three.

[51] Articles 3, 16, 17, 20-24, 28, 33, 36, 44, 75, 85, 87, 92, 107, 111, 115, 119-120, 126, 128, 134-135, 137, 156, 158, 160, 165-166, 168, 172, 179-181, 184, 187-188, 194, 229, 234, 236, 240-241, 244, 249, 286, 306, 315-316.

[52] For example, the Singapore Criminal Procedure Code ss 39 and 40 allows the police to access computers and encrypted information.

[53] See: Peter Murphy and Richard Glover, *Murphy on evidence* (12th edn, Oxford University Press 2011).

[54] Ibid.

refers to the admissibility of law and the latter to the admitting of reliable decisions by judges. Legal provisions initiate and form an evidential basis, whether this is acceptable or not. Secondly, the judge will scrutinise the accepted evidence and decide upon its probative value. There is a diversity of physical evidence: for instance blood, fingerprints and weapons, which judges scrutinise to assure admissibility. However, in the case of electronic evidence, neither the legislation nor the judiciary can address or evaluate it. Therefore, it is appropriate to consider the role of the judge in admitting this form of evidence in the UAE.

2.1.4.1 Determining the judges' role in admitting evidence under the legal system of the UAE [55]

In the UAE, any method can be followed to prove a crime under the UAE criminal system. This evidential freedom enables judges to decide what is the most authentic material by which to reveal the truth.

The expectation is that judges must not determine a case based on personal belief, opinion or emotions. The rules of law has to be followed by judges when reaching decisions; and decisions must be based on logical justification. The way in which decisions are decided by judges may not be challenged by the Court of Cassation or Supreme Court, as it is not in their capacity to review any decision. Nevertheless, the court will consider whether the judge has followed the precedents and made a logical judgment. Although a judge is not required to provide justification for their understanding, they are responsible for supporting their decisions with inferences. A judge is required to provide information about the previous decisions that they have used as a precedent when reaching their judgment. There is no need for a judge to provide details of why they have used particular evidence. To reach a decision, a judge is not bound to establish facts, but must take responsibility to provide evidence to support their own conclusions. At all grades, the criminal judiciary is bound to the doctrine of freedom of proof and judicial understanding to reach decisions.

Article 209 of the CPL provides the judge with the power to identify what evidence is to be considered material to the case. Article 209 was applied by the Emirates Federal Supreme Court when it held 'In criminal proof, the judge has the ultimate power to take

[55](n 26).

any evidence from any source to reach the truth …'.[56] Accordingly, in the UAE Federal justice system, evidence must be appraised by the judge, and, furthermore, the judge must evaluate whether any contravention of the law has taken place such as to render the evidence inadmissible.

The principles on which judges' conclusions are based are also used in trials and by other judges. This helps judges to assess, through using their own knowledge when presiding over legal proceedings, whether the evidence is obtained from reliable sources. The decision noted down by the judges in the court is to be based on truth and fairness. Judges are required to review evidence, providing affirmation about the appropriateness of the evidence for the prosecution. Article 179 of the CPL provides that: 'the court may of its own accord, during the examination of the case, order the producing of any evidence deemed necessary to reveal the truth'. It is the duty of a judge, before convicting an alleged perpetrator, to scrutinise the evidence and check that it is sufficient to find a person guilty of the crime.[57] During the prosecution stage, all doubt relating to the evidence necessary to find the perpetrator guilty would be interpreted.[58] For evidence to be acceptable in any case, it must, in essence, be legitimate and judicially acceptable. The principle of legitimate and judicially acceptable evidence adduced in criminal proceedings means that not only must criminal procedure respect the rules of law, but also the suspect's rights. Article 26 of the UAE Constitution provides that:

> 'Personal liberty is guaranteed to all citizens. A person may not be arrested, searched, detained or imprisoned except in accordance with the provisions of the law.
> A person may not be subjected to torture or to degrading treatment'.[59]

To build a case on the evidence, it is important to present that evidence in the court during proceedings. According to the provisions of Article 209 of the CPL, the case document must include evidence that is presented before the judges during the course of

[56] Criminal Case of UAE Federal Supreme Court No.50/2011date of decision 19th April 2011 unpublished.
[57] Criminal Case of UAE Federal Supreme Court No.10/2011 date of decision 6th April 2011 unpublished.
[58] Criminal Case of UAE Federal Supreme Court No.211/2010 date of decision 25th March 2010 unpublished.
[59] The UAE Constitution, Article 26.

the trial.[60] The evidence is collected during interrogation, trial, and investigation phases respectively. Having such security measures in place confirms that judges have made decisions in the light of professional learning, not on the basis of personal knowledge. With this principle in place, the importance of oral pleading is enhanced, as judges will arrive at their decisions and obtain understanding from the evidence unveiled before the court. Oral pleading is conducted before the parties to a case.[61] Therefore, judges need to be given training on how to appraise new types of evidence, for example electronic evidence.

The UAE's legal position is somewhat similar to that in civil law jurisdictions. For example, in some jurisdictions, judges are permitted to use all types of proof,[62] as demonstrated in the following examples:

In France, Article 427of the Code of Criminal Procedure provides:

> 'Except where the law provides otherwise, violations may be established by any mode of proof and the judge decides by his personal conviction.
> The court may not base its decision on evidence that it made during the discussions and contradictory submissions discussed before him'.[63]

In Italy, Article 192(1) and (2) of the Code of Criminal Procedure provides:

'Evaluation of the test;

I. The judge evaluates the evidence giving an account in the reasoning of the decision and the criteria used.
II. The existence of a fact cannot be inferred from evidence unless it is serious, precise and consistent'.[64]

In Germany, Section 261 of the Code of Criminal Procedure provides:

> 'Free Evaluation of Evidence;

[60]The Court of First Instance is presided over by one judge; the Court of Appeal is presided over by three judges and the Court of Cassation and the Federal Supreme Court is presided over by five judges.
[61]The UAE Criminal Procedural Law, Articles 165 to 170.
[62]See: the relevant jurisdictional chapters for more detail in Stephen Mason, gen ed, *International Electronic Evidence* (British Institute of International and Comparative Law 2008).
[63]Criminal Procedure Code of the French Republic Inserted by Law No. 516-2000, Article 427.
[64]Criminal Procedure Code of the Republic of Italy 1988, Article 192(1) and (2).

> The court shall decide on the result of the evidence taken according to its free conviction gained from the hearing as a whole'.[65]

It is for the judge to measure the extent to which an item of proof can be relied upon. The selection of the type of evidence by the parties is therefore unfettered, regardless of whether that evidence is in physical or electronic form. In contrast, in common law jurisdictions, complex rules exist to govern evidence, based on both statute and case law.[66]

To summarise, when deciding to accept evidence in a case, a judge's professional knowledge and understanding plays a vital role. The only disadvantage in this field is that electronic evidence requires expertise at times, and not all legal professionals in a case will have such skills. The courts in the UAE do not have equipment to evaluate electronic evidence. There are no standards provided by legislation or the judiciary against which evidence obtained can be compared. The UAE court also lacks relevant rules, making the regulation of electronic evidence challenging.

Certainly, a better understanding of electronic evidence is pivotal for law enforcement, and this requires systematic and modern methods to identify criminal behaviour and to gather evidence, so that perpetrators can be brought to justice. In this context, it is particularly important to confirm that electronic evidence has been gathered in a correct way, when brought forward for the purpose of criminal proceedings. As the gathering of electronic evidence relies on very different procedures to the traditional seizure of physical goods by the police, and requires relevant technical expertise, it is important that only skilled electronic evidence specialists are involved, and that standard procedures are followed in order to ensure that electronic evidence is less subject to challenge and being declared inadmissible.[67]

International co-operation is also pertinent, as very often websites, which may be used to commit crimes, are located outside the UAE. Thus, it is desirable to adopt global

[65]Criminal Procedure Code of the Federal Republic of Germany 1987, s 261.
[66]For which see: Stephen Mason, gen ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths 2012) for the following jurisdictions: Australia, Canada, England and Wales, European Union, Hong Kong, India, Ireland, New Zealand, Scotland, Singapore, South Africa and the United States of America.
[67]See generally: Arthur Cockfield, 'Towards a Law and Technology Theory' (2004) 30, 1 *Manitoba Law Journal* 383-399.

procedures, similar to regional measures such as the European Council Directive on Cybercrime,[68] because this will enhance the prosecutor's ability to secure, collect and exchange electronic evidence. This will enable pursuance of a globally harmonised approach, as all countries are affected in similar ways by cybercrime.[69]

It would be beneficial to have clearly defined rules on the subject of electronic evidence, to specifically deal with its collection, presentation, preservation and how to assess its weight. It would also be helpful to have agreed standards for the electronic equipment that is used to copy electronic evidence. Introduction of these elements would strengthen the integrity of the criminal justice system.[70] Thereby allowing for the adoption of a particular legal framework for crimes, as well as best practice guidance for the investigation and prosecution and up-to-date handling of maintenance and archival procedures,[71] as well as procedures for how to present evidence in court; all of which are significant elements when dealing with criminal acts.

2.1.4.2 Determining the role of the parties in providing evidence under the legal system of the UAE [72]

Under the Federal laws of the UAE, all facts must be proven by evidence. In criminal proceedings, the prosecutor must prove their case beyond any reasonable doubt.[73] They must also establish that the accused intended to commit the crime. Article 5 of CPL provides that: 'The public prosecution is part of the judiciary; it investigates crimes and directs indictments in accordance with the provisions of this Law'. Article 7 also provides that the public prosecutor is responsible for initiating and proceeding with the lodging of the criminal action. In fact, the burden of proof in criminal proceedings alternates between the parties, much as it does in other jurisdictions, since Article 179 of the CPL provides that: 'The court may of its own accord, during the examination of

[68]Convention on Cybercrime (Budapest 23.XI.2001).
[69]P. I. Yong, 'New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime' (December 2011) *Wuhan University China* 5 <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/Cyber_cp_china_Pi_Yong_Dec11.pdf> accessed 10th April 2013.
[70]Ibid, 4.
[71]Stuart Cameron, Digital Evidence (FBI Law Enforcement Bulletin, August 2011) – note his references <https://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/august-2011/digital-evidence> accessed 4th October 2013; see also Stephen Mason, (n 66) chapter 3 for further discussions and additional references.
[72](n 26).
[73] Reasonable doubt is doubt, which makes one hesitate as to the correctness of the conclusion.

the case, order the production of any evidence deemed necessary to reveal the truth'. This article was applied by the Emirates Federal Supreme Court when it held: '… The judge has the power to search for evidence to prove the fact'.[74] In criminal cases, the defendant is not asked to present evidence to prove his innocence: the prosecution must establish evidence against the defendant. In contrast, the defendant has the right to challenge the evidence and present his own evidence to refute claims that he committed the alleged acts.[75]

For the purposes of investigation, an alleged perpetrator is required to provide the pass codes for any lockers and his computer system to the authority. There are different approaches involved here. The first is when the person who is charged is not liable to provide security codes, to provide facsimiles of the documents stored in his computer, or to insert a command to outstrip viruses. The second approach is when the accused is required to give security information to access their safe, which only applies if legitimate orders have been issued from the court. The second approach is of great importance as it helps to obtain passwords, which can then be used to obtain additional information during the investigation. This rule is applied where information is kept safely in the safe, but is not password protected information held in electronic format. [76]

In the UAE, only the first approach is applied when the accused is not required to present evidence in order to prove their innocence. On the contrary, it is up to the prosecution to prove that the accused is guilty.

Basic information about the legal and judicial system is essential in providing background to explain and further understanding of the legal system, and how crimes and electronic evidence are handled in the UAE.

2.2 Physical crime and cybercrime

Computers and networking technologies are used for routine work in developed countries and this same trend can be observed in developing countries. A dramatic information revolution has taken place over the course of the second half of the

[74]Criminal Case of UAE Federal Supreme Court No.75/2011 date of decision 31st May 2011 unpublished.
[75]The UAE Criminal Procedure Law, Article 2.
[76]Abdel Fattah Hijazi, *principles of the criminal proceedings in the computer and Internet crimes* (Dar Al Fikr Al jami Egypt 2006)198. (Author's translation from the Arabic).
عبدالفتاح حجازي، مبادي الاجراءات الجنائية في جرائم الكمبيوتر والانترنت (دار الفكر الجامعي مصر 2006) ص 198.

twentieth century, which continues, and is intrinsic to nearly every field: education, finance, telecommunications, health care, businesses and government.[77]

ICT (Information and Communication Technology) has had an immense impact, and the whole world has become a global village due to the internet, as the Internet connects all countries.[78] ICT does not only refer to collecting, transmitting and storing electronic data and information, but also enables communication, broadcasting and computing.[79]

ICT is used to describe a combination of hardware and software; hardware is the devices or machines, such as televisions, routers, phones, fax, switches and computers, etc. and infrastructure such as fibre optic and landline cables, transmitters for radio activity, systems with microwave technology and ground satellite stations. Software covers applications and operating systems, as well as additional ICT features, which exchange, store and process information and data. Expert human input is required for the installation, operation, management and maintenance of software and hardware, which in turn requires information, planning and designing.[80]

Therefore, electronic evidence has become extremely important for cybercrime investigations. Nowadays, most documents are stored digitally, as the storage capacity of hard drives has continuously increased and is also inexpensive.[81] Hence, large quantities of information are stored electronically.[82] Any electronic documents, including text, digital videos and pictures,[83] can assist investigators in solving crimes and therefore constitute important evidence at trial.[84] There are multiple types of crimes, and this thesis recognises that electronic evidence can be implicated in both cybercrimes and physical crimes. However, this thesis will focusing predominantly on

---

[77]United Nations, 'International review of criminal policy – United Nations manual on the prevention and control of computer-related crime' (1999) Global Centre for Information and Communication Technologies in Parliament <http://www.ictparliament.org/node/2128> accessed 10th October 2012.
[78]Ibid.
[79]Jabiri Bakri, 'A Holistic Approach for Managing ICT Security in non-Commercial Organization' (DPhil thesis, Stockholm University Sweden 2007) 3.
[80]Ibid.
[81]Scott Giordano, 'Electronic Evidence and the Law' (2006) 6, 2 *Information Systems Frontiers* 161.
[82]Chet Homer, 'Proving the Integrity of Digital Evidence with Time' (2002) 1, 1 *International Journal of Digital Evidence* <www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf> accessed 4th October 2012.
[83]Jill Kwiatkowski, 'Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images' (2002) 10 *Journal of Law and Policy* 267.
[84]Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn, Waltham Mass.: Academic Press/Elsevier 2011) 14.

electronic evidence in relation to cybercrime, rather than physical crimes; this does not preclude the fact that electronic evidence pertains to cybercrime and physical crime.

It is furthermore important to distinguish cybercrime from computer crime. When a computer is used to commit an offence, a cybercrime has been committed, whereas a computer crime takes place when a computer, data, program or similar object is targeted.[85] Accordingly, it is necessary to explain some of the similarities and distinctions between physical and cybercrimes.

2.2.1 Physical crime and cybercrime: similarities and distinctions

Cybercrime and physical crime are similar, since unlawful activities are undertaken in both cases and certain basic elements can be established.[86] In relation to both kinds of crime, one can identify three elements: a causal relationship, a result and conduct;[87] however, when a cybercrime is committed, the computer is used as the means to commit the crime and the crime may also have global consequences. It is unnecessary for the criminal to be close to the victims during an attack. Instead, the perpetrator may be located in a different country. Another distinction is that cybercrime can take place automatically and rapidly, affecting many victims simultaneously; it can also be carried out anonymously.[88] Thus, when a person breaks into a home to steal something, a physical crime takes place, whilst hacking into a computer or a network in order to gain illegal access to files constitutes a cybercrime.

Fraud can be either a physical crime, or a cybercrime. When a person tries to profit through dishonest or unfair means, or by breaching customer confidence or trickery, a physical crime takes place, although when this takes place over the internet, this fraudulent conduct constitutes a cybercrime. Another example is child exploitation. When someone victimises minors for indecent reasons (i.e. abuse or pornography), a physical crime is committed, whilst a cybercrime takes place if the criminal uses

---

[85] Marc Goodman and Susan Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 3 *Journal of Law and Technology* <http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php> accessed 6th October 2012.

[86] Susan Brenner, 'Is There Such a Thing as "Virtual Crime"?' (2001) 4, 1*California Criminal Law Review* 1.

[87] Ibid.

[88] Report to Congressional Requesters, Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats US Government Accountability Office (2007) <http://www.gao.gov/assets/270/262608.pdf> accessed 7th October 2012.

networks and computers to illegally victimise/abuse the minor(s).

Having differentiated between cybercrime and physical crime in general, it is now apposite to look at the classifications of cybercrimes in the UAE.

2.2.2 UAE law and cybercrimes

It is important to assess whether the UAE law distinguishes between physical crime and cybercrime. Cybercrimes are regulated by Federal Law No.2 of 2006 of the Prevention of Information Technology Crimes (this law repealed and replaced by Federal Law No.5 of 2012 on the Prevention of Information Technology Crimes), which outlaws the following kinds of crime:

Threatening or blackmailing people to perform or not perform any act over the internet.[89] Intercepting, receiving or unlawfully eavesdropping on any communication sent over the internet or any other technological device.[90] Committing forgery of any documentation that belongs to a corporation, local or federal public entity or the local or federal government.[91] Gaining unauthorised access to any network or computer system.[92] Usually, all major cybercrime activity involves gaining access to a computer or system without obtaining the consent of the person who either owns or is in charge of the computer, system or network. Typically, a hacker gains access to the system or network by copying and/or reading information, modifying data or information stored and/or downloading data.[93] Sexual exploitation takes place when men or women commit online acts of fornication or prostitution.[94] Concealing profit and money laundering can also take place online.[95]

In cyberspace, one of the most profitable areas for criminals is computer fraud and unfortunately, this takes many different forms. The most typical computer fraud involves contractual crimes, credit card scams, offering fake jobs, etc. Computer fraud is the act of stealing property, money, cheques, credit or services with the help of a

[89]The UAE Federal Law No.5 of 2012 on the Prevention of Information Technology Crimes, Article 9.
[90]Ibid, Article 8.
[91]Ibid, Article 4 (1).
[92]Ibid, Articles 2 (1), 5, 6, and 7.
[93]David Bainbridge, *Introduction to Computer Law* (6th edn, Ashford Colour Press Ltd. 2008) 291.
[94]The UAE Federal Law No.5 of 2012 on the Prevention of Information Technology Crimes, Article 13.
[95]Ibid, Article 19.

computer.[96] There are two types of computer fraud:

- Data fraud is committed when an information technology machine, or the internet, is used to obtain details and numbers associated with a credit card or a similar card illegally.[97]

- Money fraud is committed when the internet is used to steal money from others.[98]

There are many ways to manipulate electronic devices illegally. The aforementioned are the most prevalent, however, there are a range of other crimes that can be committed using the internet or on any other technological device. For example, public morals are prejudiced when the internet is used to arrange, produce, distribute or sell products, which are contrary to public morals.[99] A person's or a family's privacy can be abused through the distribution of online news, and pictures, etc.[100] Religious abuse can also take place online.[101] Online access can be gained to websites and contents can be modified or destroyed.[102] Not only this, but online access can also be gained to confidential data or government held information.[103] The sale of narcotics can take place online, or can be facilitated.[104] Public order and morals can be disturbed online through the promotion of ideas, which disrupt the peace.[105] Terrorist organisations can be assisted through websites or the sharing of information.[106] Websites can be established for the purpose of human trafficking or to facilitate human trafficking.[107]

All of these matters are addressed by the law, thereby ensuring that many aspects of cybercrime can be prosecuted. The issue is that most cybercrime is an expansion of a conventional crime, it is only the medium that has changed. Therefore, it can be argued that existing laws, which deal with traditional crime, are not inadequate and

[96]Ibid.
[97]Ibid, Article 11.
[98]Ibid, Article 10.
[99]Ibid, Article 12.
[100]Ibid, Article 16.
[101]Ibid, Article 15.
[102]Ibid, Article 14.
[103]Ibid, Article 22.
[104]Ibid, Article 18.
[105]Ibid, Article 20.
[106]Ibid, Article 21.
[107]Ibid, Article 17.

inappropriate, but just that combating cybercrime raises additional problems. The most efficient way to combat cybercrime and all crime linked to computers involves focusing on developing methods to collect electronic evidence.

2.3 The types and the nature of electronic evidence

Developments in cybercrime have added a new electronic and digital dimension, that is making it difficult to apply traditional legal concepts. Millions of computer users worldwide can easily utilise advanced technology for unlawful practices and it is therefore important to explore in what ways electronic evidence differs from traditional evidence. It is also important to distinguish evidence that displays class characteristics and evidence that has individual characteristics, as it is only the latter that can be used to link a criminal to the crime.[108] This distinction is particularly important in relation to cyberspace as users are often anonymous and trade is conducted without a unique identification number. Whilst class characteristics can prove helpful in relation to identifying whether electronic evidence has been deleted or encrypted, individual characteristics can identify particular evidence, for example the unique number that a printer assigns when a page is printed.[109] Hence, "the value of class physical evidence lies in its ability to provide corroboration of events with data that are, as nearly as possible, free of human error and bias. It is the thread that binds together other investigative findings that are more dependent on human judgments and, therefore, more prone to human failings".[110] By classifying electronic evidence into categories, it is easier to establish a case, since class evidence suggests that it was likely that a person was involved, whereas individual characteristics establish a strong link between the person, their electronic trail and the crime.

2.3.1 Types of electronic evidence

As per the manual issued by the USA Department of Justice (DOJ), log files, cookies, metadata, and IP addresses are among the forms of electronic evidence generated by a computer.[111] This evidence is found on different programs, in various data and formats.

---

[108] Eoghan Casey (n 84) 17.
[109] Ibid, 18.
[110] Richard Saferstein, *Criminalistics: An introduction to forensic science* (10th edn, Prentice Hall 2010)18-19.
[111] See: USA Department of Justice<http://www.justice.gov/> accessed 7th October 2012.

It can be obtained from e-mail, social interaction sites, and from different websites.[112]

Certain multimedia gadgets like audio-video devices, digital photos and words must be presented before the court. These forms of evidence can be either printed as a hard copy or displayed via a projector screen. Some scholars divide electronic evidence into three categories, namely: computer storage, hybrid, and computer generated evidence.[113] All three evidence-recording methods are explained from a diverse perspective. Kerr explains that computer-stored evidence is based upon individual interference in computer programmes. This programmer-based interference, such as word-processing files, forms one type of electronic evidence. However, computer-generated evidence has led to a generation of evidence not involving humans. This type of evidence includes programs such as cookies and metadata, etc.[114] However, the third type of evidence refers to a combination of both types above mentioned. The measures of difference between various forms of electronic evidence are their integrity and volatility.[115]

There are three different forms of cyber trails, each having specific characteristics. These forms serve as a foundation stone for differentiating between two types of electronic evidence, namely computer-generated and human-generated electronic evidence. The first is explicit, though not printable: for instance metadata, net browsing history or log files. The fragility of the evidence requires a special forensic tool specified for proper treatment: such tools are needed for collecting, examining and presenting in court. Admittedly, this helps when attaining accurate information because it lacks human involvement. Careful scrutiny must be undertaken to ensure the absence of interference during the process of collecting and examining evidence.[116]

The second form is referred to as explicit and printing-specific: for instance, power-point slides, digital pictures, Word, and Excel spread-sheets, etc. These types of evidence are printable in their existing forms and have two advantages over computer-generated evidence. Firstly, they provide the law with the ability to address current electronic evidence. Secondly, they make comprehending, addressing and

[112]Ibid.
[113]Orin Kerr, 'Digital Evidence and the New Criminal Procedure' (2005) 105 *Columbia Law Review* 279.
[114]Ibid.
[115]Ibid.
[116]Ibid.

differentiating between evidence relatively easy for the legislature.[117]

UAE legislation, for example, neither classifies electronic evidence nor addresses evidence forms. It is useful to consider the kinds of evidence admissible in court. These can generally be divided into three main categories. The first category is 'documentary evidence', which originates from documents. The second category of evidence is 'physical evidence', which is derived from diverse sources, such as fingerprints, photographs, handwriting and electronic machines. The final category is 'expert evidence', i.e. evidence prepared by experts in the field, who provide their opinions at trial. Thus, a question arises, regarding into which category the electronic evidence falls, although answering this question is far from easy.

A. Electronic evidence as documentary evidence

The term 'documentary evidence' refers to evidence that is taken from a document, which has been prepared during the investigation and may include direct or hearsay evidence. A document may also be produced as real evidence. The normal understanding of the word 'document' appears to require writing or some other mode of inscription through which information is communicated. Some researcher[118] consider electronic evidence to be documentary evidence since 'documentary evidence' denotes evidence in the form of text, symbols, drawings, etc. and its essential characteristics are also no different to documentary evidence; as both help in establishing the case.

In the UAE, the words 'document' and 'computer output' are not defined by statute, although the term 'electronic document' is defined in Article 1 of Federal Law No. 5 of 2012 concerning the Prevention of Information Technology Crime.[119] In the UK,[120] Section 13 of the Civil Evidence Act 1995 defines a 'document' as: 'Anything in which information of any description is recorded'. Hence, a broad definition has been adopted, which also covers computer output.[121]

---

[117] Ibid.
[118] Such as: Peter Stephenson and Keith Gilbert, *Investigating Computer-Related Crime* (2nd edn, CRC Press 2013).
[119] See: section 1.8.1.
[120] See also: the Singapore Computer Misuse Act of 1993, s 2 (1).
[121] UK Law Commission Report, the Hearsay Rule in Civil Proceedings (Law Com No 216, 1993). The Law Commission proposed a broad definition for the term "document", so that any format is covered, including computer-generated information.

However, electronic evidence is different from documentary evidence. Electronic evidence is often in paper form as a medium, but expressed in writing in the form of electronic evidence in text, graphics, and other electronic equipment electronic information transformation processes. However, with documentary evidence, the symbols are essentially different. Writing is not equivalent to documentary evidence; expert conclusions, inquests and records, e.g. witness testimony can be expressed in writing but it is not documentary evidence. In addition to writing, electronic evidence, in the form of information held by the network server, smart card, IP Address, phone SMS or camera pictures, can be used to help prove a case.[122]

B. Electronic evidence as physical evidence

'Real evidence' refers to evidence, which exists in a physical form and which can be inspected and produced in court. Real evidence is found on a wide variety of physical objects including fingerprints and handwriting, etc. each of which are obtained using similar investigative processes.[123] Some consider[124] that electronic evidence constitutes physical evidence, particularly if physical evidence is broadly construed. However, this may not be persuasive for three reasons. Firstly, the term 'physical evidence' would become too broad and would include types of evidence with different characteristics to those in the physical evidence group. Secondly, electronic evidence is different from physical evidence since it maintains its properties and is thus authentic. In contrast, the physical evidence does not always retain its properties and authenticity. Thirdly, electronic evidence is based on information, that is stored on computers and other equipment and so the data has no physical form, whereas real evidence by definition has a physical form. Thus, it is difficult to say whether electronic evidence is physical or 'real' evidence.

C. Electronic evidence as expert evidence

Some researchers[125] believe that electronic evidence constitutes expert evidence since it

[122] See: section 2.3.2.
[123] Hjn Rooyen, *The A-Z of investigation: A practical guide for private and corporate investigators* (Crime Solve 2004) 8.
[124] Such as: Eoghan Casey (n 84), and Debra Shinder and Michael Cross, *Scene of the cybercrime* (2nd edn, Arlington: Syngress Publishing Inc. 2008).
[125] Such as: Larry Daniel and Lars Daniel, *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom* (Syngress 2011).

represents the conclusions of experts, particularly because electronic evidence is scientific. However, others argue that expert reports only confirm the authenticity and integrity of the electronic evidence and do not constitute reports on content.[126]

In conclusion, since electronic evidence is available in digital or binary form the characteristics of this evidence make it extremely difficult to classify. It could be said that electronic evidence is a mixture of several categories.

In the UAE, the choice of evidence is ordinarily unfettered and, in principle, any means are permissible. However, the weight of evidence depends on the form of the evidence. There are two forms of relevant evidence: direct such as the confession of the accused and witness testimony and indirect, such as the fact that the accused was arrested whilst carrying objects related to the crime. Direct evidence bears greater weight than indirect evidence. With regard to electronic evidence or computer-generated evidence, the question is generally one of evidentiary value: What value or weight should be attached to the evidence? In the UAE, statute law does not provide any guidance on this issue; but instead the court has to consider in each case how much weight it should attach to a particular form of electronic evidence. Thus, electronic evidence is independent evidence, that differs from other types of evidence and requires special attention. Therefore, it is important to consider the particular characteristics of electronic evidence.

2.3.2 The nature of electronic evidence

It is vital for the court to identify the particular characteristics of electronic evidence. Undoubtedly, the characteristics of evidence, electronic or physical, cannot be compared as like for like, since each form has a different criteria.[127] Evidence in electronic format has a number of features, which create challenges that are not found in relation to physical evidence. The essential point about electronic evidence, which is not readily understood by many judges, prosecutors and lawyers, goes to the complexity of the topic and the nature of the characteristics of electronic evidence.[128] By failing to have a fundamental knowledge of the field, prosecutors and the electronic evidence specialists responsible for investigating a case are in danger of committing serious

[126] The examination and the expert report will further discussed in Chapter Four.
[127] See: Stephen Mason, *Electronic Evidence* (n 66) chapters 1 and 2.
[128] See: the result of the applied study on section 5.3.

errors. It is for this reason that judges, prosecutors, lawyers and electronic evidence specialists should consider it vital that they begin to gather electronic evidence. Consequently, it is essential to clarify some of the characteristics of electronic evidence, as outlined below.

A. Electronic evidence is scientific evidence

Electronic evidence consists of data or information in an intangible electronic format, which cannot be understood by applying natural human senses, but which requires hardware and software to enable the data and information to be rendered readable. As a result, a user cannot falsify or create data or information in electronic format without proper hardware devices.[129] A special characteristic of electronic evidence requires a specific skill in the electronic evidence field. The expert should have expertise or skills such as knowledge of hardware devices and software. Their expertise is extremely crucial when establishing whether there is a loss of any electronic evidence due to using any programs or tools or being destroyed. Thus, specialised training is of the greatest value for forensic experts as a means of keeping up to date.[130]

B. Electronic evidence is variable evidence

Technological changes are taking place rapidly and electronic evidence is vulnerable, as the IT environment can be variable, a fact that can affect discovery and disclosure. Whilst eyewitnesses, fingerprinting and other evidence has been used in trials for hundreds of years, the way in which such evidence is gathered and interpreted in legal proceedings has hardly changed. This is in marked contrast with electronic evidence that requires judges, prosecutors and lawyers to remain abreast of changes.[131] It could be argued that this characteristic of electronic evidence, and the rapid changes in technology, make it extremely difficult to adopt specific procedural or evidentiary rules for managing electronic evidence as new rules will swiftly become outdated. Following this line of reasoning, it can be said that the absence of these rules could do more harm than good.[132] Within the last decade, conducting criminal activities and gathering

[129] Stephen Mason, *Electronic Evidence* (n 66) 28.
[130] There are more than 69 worldwide universities and colleges lists by the Electronic Evidence Information Centre offering tertiary qualifications in digital forensics.
[131] Stephen Mason, *Electronic Evidence* (n 66) 29-30.
[132] See: section 5.3.

criminal prosecution evidence is considered to be a constituent of both computers and communication technology. No doubt, judges, lawyers, investigators and prosecutors face criminal issues pertaining to electronic evidence. Admittedly, certain new features of electronic evidence are making old laws obsolete and impracticable. Although judges can conduct an evaluation and acceptance of electronic evidence, they will be unable to judge electronic evidence confidently, due to short provisions and guidance. Consequently, appropriate legislation must be presented for tackling electronic evidence. Technology is growing rapidly and as it does, the rules are also evolving.

C. Electronic evidence can be transmitted and replicated

Electronic evidence can be transmitted and replicated, in contrast to physical evidence. For example, documentary based evidence exists in the physical world and is sent by one party to another, by courier or postal service, it is also uncopied.[133] In contrast, electronic evidence in the digital world can be sent to an unlimited number of individuals via telecommunications and computer networks. This phenomenon is described as networked communication. In essence, electronic evidence is a duplicate and can be copied.[134] The volume of information or data, which has to be inspected for the prosecution to establish a case, can often be enormous.[135] The ability to copy and transfer electronic evidence does not only cause jurisdictional issues, but also introduces problems in relation to its gathering and preservation. In this regard, Rashid Lootah Head of the Electronic Evidence Unit at the Criminal Evidence and Criminology Department- Dubai Police said:

> There is no doubt that electronic evidence has a different nature from other evidence. As an example, fingerprints indicate the offender's presence in a place and do not need an explanation or analysis. However, it is not easy to determine electronic evidence locations. It needs more searches and analysis.[136]

[133] Ross Anderson, *Security Engineering* (2nd edn, Wiley Publishing Inc. 2008) 78.
[134] George Paul and Jason Baron, 'Information inflation: Can the legal system adapt?'(2007) 13, 3 *Richmond Journal of Law and Technology* 1-41.
[135] For an estimate of the volume of data, see: 'How much information?' (2000) University of California at Berkeley <http://www2.sims.berkeley.edu/research/projects/how-much-info/> accessed 27th January 2012.
[136] See: translated transcript of the interview with Major Lootah in Appendix 5.

D. Electronic evidence is challenging

Investigators encounter several challenges when they deal with electronic evidence, as most information is usually found on a system comprising many layers; and only a small amount of the data held will be important for the purpose of the investigation.[137] In addition, electronic evidence does not represent original evidence, but is only an abstract version of the evidence and the entirety of which may be irretrievable.[138] Moreover, where evidence has been changed or deleted, the level of abstraction is further increased and the added abstraction can result in mistakes.[139] Electronic evidence is usually circumstantial evidence, as for example another individual may have used the computer.[140] Another challenge for investigators to overcome, occurs where there is an element of evidence dynamics that impacts on electronic evidence. For example, data can be overwritten or the time on all files can be falsified, so that reconstruction and documentation of evidence becomes more difficult.[141] Additional problems encountered by investigators include the fact that electronic evidence is often stored in different locations, for example on cloud computing systems located in different countries, or on other computers; and that the amount of data stored may be substantial.[142] More fundamentally, cybercrime is executed by powerful computers and is extremely difficult for investigators to identify offenders, which in turn renders it much more difficult to trace and evaluate electronic evidence.

E. Electronic evidence contains embedded information

Unlike physical evidence, electronic evidence can provide information about the time and date that changes were made, when a copy was printed and can also help in tracing the person who created the record; whereas a paper record does not generally provide information as to its history.[143] As a result, electronic evidence is inherently richer in information than physical evidence,[144] providing metadata.[145] Metadata also provides

[137] Eoghan Casey (n 84) 25.
[138] Ibid, 25.
[139] Brian Carrier, 'Defining digital forensic examination and analysis tool using abstraction layers' (2003) 1, 4 *International Journal of Digital Evidence* 3-5.
[140] Eoghan Casey (n 84) 26.
[141] Ibid, 27.
[142] Ibid, 32.
[143] Amanda Ngomane, 'The Use of Electronic Evidence in Forensic Investigation' (DPhil Thesis, University of South Africa 2010) 34.
[144] Ibid, 35.

information about events; regarding the time when documents came into existence.[146] This additional metadata may also be employed to assess whether certain theories, proposed by either the defence or prosecution, are true.[147] Undoubtedly, there are many other differences between physical and electronic evidence, which impact on the applicable procedures governing gathering and investigation. Thus, it is necessary to understand the methods that can be employed in order to investigate cases involving electronic evidence.

2.4 The criminal investigation of cybercrime and physical crime: procedural aspects of UAE's legal system

Criminal investigations are a prerequisite for criminal proceedings, in that the purpose of an investigation is to instigate the legal process.[148] Therefore, a criminal investigation is an organised, systematic way of investigating the truth,[149] which commences upon the commission of a crime and continues until the beginning of legal proceedings.[150] Thus, investigation leads to prosecution.[151]

In any crime, misconduct can be detected through a detailed investigation by management, an internal auditor reviews, internal controls and notifications from employees and customers. Conversely, investigation and detection involves the process of identifying and tracking electronic evidence in a digital world. Evidence can take many forms, for example charts, graphics, diagrams, tunes, images and sounds. This is also referred to as an electronic trail, and can be important evidence due to its probative value.[152]

Whilst the detection of cybercrime can be fraught with difficulties, it is possible to establish a link between individuals and online activities and to perceive the internet as

---

[145]Mark Krotoski, 'Effectively Using Electronic Evidence Before and at Trial' (2011) 59, 6 *United States Attorneys' Bulletin* <http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf> accessed 13th October 2012.
[146] Ibid.
[147]Ibid, 54.
[148]Ross Gardner, *Practical crime scene processing and investigation* (2nd edn, Taylor and Francis 2011)1.
[149]Hjn Rooyen (n 123) 25.
[150]C. Joubert, ed, *Applied law for police officials* (3rd edn, Juta Legal and Academic Publishers 2009) 223.
[151]Hjn Rooyen (n 123) 25.
[152] Fred Galves and Christine Galves, 'Ensuring the Admissibility of electronic evidence forensic evidence and enhancing its probative value at trial' (2004) 1, 19 *Criminal Justice Magazine* <http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html> accessed 17th February 2012.

an extended crime scene.[153]

In the UAE, the investigation of physical crime or cybercrime is governed by Federal Law No.35 of 1992 concerning the Criminal Procedure Law. The UAE's CPL outlines several provisions, which authorise the police to report criminal cases, gather information, take statements, carry out searches of premises and equipment, seize evidence, execute summons and warrants and conduct prosecutions. Part III of Chapter II of the UAE's CPL gives the prosecution the power to investigate criminal cases, including the right to attend court. The investigative process is always the same, irrespective of whether cybercrimes or conventional crimes are being investigated. However, the issue raised is whether it is sufficient to rely on the prosecution to investigate the case, especially since the UAE's CPL is more suitable for non-cybercrime offences. Therefore, we should ask: to what extent does the UAE's CPL cover cybercrime cases?

Regarding the first point, cybercrime investigators maintain that the UAE's CPL is comprehensive and sufficient for the purpose of cybercrime investigations. For instance, the requirement to record how evidence has been gathered, as well as the investigation process itself is a requirement under Chapter II of the UAE's CPL,[154] which has to be strictly adhered to; relevant procedures must be followed using the prescribed forms. However, there are no UAE laws requiring that the recovery process for electronic evidence be only undertaken by authorised persons such that there, is no interference with the electronic evidence.

Whilst electronic evidence is recognised by common rules, no distinction is made between evidence produced by a computer and original statement documents. Therefore, the UAE's CPL should be followed when a crime is being investigated and electronic evidence collected. As crime investigations can be complex, it is also important to develop specific procedures for investigating electronic evidence. For example, the investigation phase could be divided into the following five phases: (1) using early triage steps to focus on key events and transactions, (2) identifying leads from both the forensic examiner and the agent, (3) addressing user attribution issues, (4)

[153]Eoghan Casey (n 84) 29.
[154] The UAE Criminal Procedure Law, Articles 30-138.

filling gaps in the evidence, and (5) proving events abroad.[155] The first phase ensures that voluminous data is rendered more manageable. Through discussions between the parties, during the second phase, evidence is exchanged. The third phase focuses on who the owner of the computer is and who the author was, and the fourth phase assess evidentiary gaps. Meanwhile, the last phase is useful when there is an international element to the crime, and also to establish a timeline.[156]

However, as the UAE's CPL does not currently detail any particular procedures for the search and seizure of electronic evidence, the police can choose what action they take. Normally, the police visit the physical location where an incident took place in order to collect information and to document the crime. The complainant's statement, witness statements and possibly statements of any suspects are recorded as required under Part III of the UAE's CPL. Relevant devices and equipment are then transferred to the Forensic Laboratory for further examination and to extract evidence. This process is set out in the UAE's CPL and applies to all crimes and all evidence. It is therefore important to supplement the CPL by detailing procedures for gathering and seizing electronic evidence. Judge Al Kaabi said regarding this:

> In reality, we used the general rules; in some cases it is difficult to apply these rules for electronic evidence. Electronic evidence is different from other evidence, so we face some challenges when used these rules.[157]

Unlike the UAE, in the UK, the Association of Chief Police Officers (ACPO) has developed a Good Practice Guide for Digital Evidence, which details procedures for evidence recovery, search and seizure processes, disclosure and the preservation of evidence.[158] Similarly, in 2003, Australian authorities adopted 'Guidelines for the Management of IT Evidence' for computer-based crime and which address important topics, such as rights, custody, investigation, management and evidence.[159]

Whilst cybercrime has persistently increased, law enforcement agencies, as well as the judiciary have struggled to cope with the peculiarities arising from electronic evidence,

[155]Mark Krotoski (n 145) 55.
[156]Ibid, 55-58.
[157]See: translated transcript of the interview with Judge Mohamed Al kaabi in Appendix 5.
[158]Association of Police Chief Officers (ACPO) '*Good Practice Guide for Digital Evidence*' (March 2012).
[159]Standards Australia Handbook: HB- 171: Guidelines for the Management of IT Evidence.

and the problem is likely to be compounded if legislation does not close existing regulatory gaps.

Thus, it is particularly important to assess how far existing common rules and principles can be applied to cybercrime cases, which rely on electronic evidence. The gathering, conservation, communication and presentation of electronic evidence has to comply with the rules and principles governing evidence and electronic evidence. Electronic evidence, that contravenes these rules and principles, since it has been obtained through unlawful means, has to be declared inadmissible in order to preserve the integrity of the UAE's criminal justice system. For example, it is important that it clarifies whether the particular searches, which are undertaken, have to be clearly stated in any search warrant and to confirm which search protocols have been followed; whether any search can be conducted; or whether a particular team has to be set up to provide certain information, i.e. to filter the data and furnish only what is permitted by the warrant.[160] Similarly, the weight of electronic evidence is negated or decreased if the integrity of security has been breached, the electronic evidence has been changed or the evidence has been contaminated.[161]

2.5 Conclusion

Technological advances have given rise to crimes in a great variety of forms. This chapter has provided a brief overview of the legal system in the UAE, discussed the development of the UAE's Criminal Procedure Law, including Federal Act No. 35 of 1992 concerning criminal procedure and its amendment, as well as Federal Act No. 5 of 2012 on the Prevention of Information Technology Crimes, and has concluded that rules and procedures must be developed for handling electronic evidence as it is becoming more common. Public companies should also be subjected to standard regulatory checks, for example, by regularly gathering electronic evidence, thereby subjecting industry sectors to more vigorous scrutiny. This could increase corporate

[160]Howard Cox, 'Recent Developments and Trends in Searching and Seizing Electronic Evidence' (2011) 59, 6 *United States Attorneys' Bulletin* 72-73
<http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf> accessed 13th October 2012.
[161]Richard Boddington, Valerie Hobbs and Graham Mann, 'Validating digital evidence for legal argument' (2008) *Edith Cowan University Australia* 3
<http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1041&context=adf > accessed 23th October 2012.

accountability and safeguard against corporate fraud.[162]

It is also important that underreporting of crime is addressed, particularly since companies often fear that reporting crime will be detrimental to a company's reputation and financial standing, as it diminishes investor/shareholder trust. However, if crime is not reported and investigated, criminal behaviour continues. Despite this, many companies often prefer to pursue civil proceedings, as only the civil burden of proof has to be supported, although electronic evidence still plays an important role and the same holds true in relation to audits.

The remainder of the chapter reviewed the types and characteristics of electronic evidence and found that electronic evidence takes on different characteristics from physical evidence. Finally, the chapter examined crime investigation, as well as the procedural aspects that currently govern crime investigations in the UAE, and concluded that it is important that rules and procedures be specifically developed for electronic evidence, particularly for gathering evidence, as electronic evidence gives rise to new facts, which in turn require new regulations.[163] For example, traditional search and seizure rules are conceptualised on the premise that a property is searched and items retrieved; however, in relation to computer searches, the police has to first seize the device/computer and subsequently carry out a search of that device/computer, meaning there are two stages.[164] It is also important that any new criminal procedural rules are also in line with existing investigative procedures.[165] In this context, it is also important to take inspiration from other countries, which face the same difficulties, in order to promulgate the most suitable criminal procedure rules for handling electronic evidence.[166]

[162]Linda Volonino, 'Electronic Evidence and Computer Forensics' (2003) 12, 27 *Communications of the Association for Information Systems* 2
<http://faculty.usfsp.edu/gkearns/Articles_Fraud/Fraud_Deterrence.pdf> accessed 23th October 2012.
[163]Orin Kerr 'Digital Evidence and the New Criminal Procedure' (n 113) 62.
[164]Orin Kerr, 'Search Warrants in an Era of Digital Evidence' (2005) 75 *Mississippi Law Journal* 85.
[165]Brian Carrier and Eugene Spafford, Getting Physical with the Digital Investigation Process (2003) 2, 2 *International Journal of Digital Evidence*.
[166]Orin Kerr, 'Digital Evidence and the New Criminal Procedure' (n 113) 62.

CHAPTER THREE: REGULATION OF ELECTRONIC EVIDENCE IN CIVIL LAW AND COMMON LAW SYSTEMS: A CASE STUDY OF CHINA AND ENGLAND AND WALES [1]

Recent dynamic changes in technology have significantly affected the characteristics of transactions, and the storage and exchange of information and intelligence, with almost all information now being saved or exchanged in electronic form. [2] Important information can now be saved electronically using electronic tools, which can be a good source of evidence. In particular, taking the relevance of data into consideration this would lead to the finalisation of relevant facts and solve pertinent issues. Moreover, numerous crimes can now be committed by employing electronic means using the internet, as highlighted in the previous chapter.

The significant increase in electronic documents, dealings, crime and fraud is affecting many different sectors. [3] Different jurisdictions are experiencing difficulty with the management of electronic evidence. There are some specialised rules in place, but many states still utilise traditional rules of evidence, particularly in relation to documents, and then implement corresponding analyses. Even those countries with specialised rules are still facing a number of obstacles. It is important to work on certain omissions that would not have been thought of previously, because technology tends to keep evolving and such changes cannot be forecast in legislation.

The consequence of the dearth of specialised or comprehensive rules suggests that the nature of the legal system, and the jurisprudence of any state will have a substantial impact on the rules for administering electronic evidence.[4] This chapter investigates how electronic evidence is regulated by the two legal systems; the common law and the civil law systems. It is important to recognise that while there are some prominent features distinguishing the two legal systems, there may not be noticeable similarities in particular rules in areas where laws extend across territories that belong to the same legal system. For example, Brazil, Germany and France are traditionally civil law

[1] Scotland and Northern Ireland have different legal systems and are not the same as England and Wales.
[2] Jill Anderson, Neil Williams and Louise Clegg, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2nd edn, Sydney: LexisNexis 2009) 105.
[3] Ibid.
[4] Ibid.

jurisdictions. However, these countries do not have identical rules of evidence as each country frames its own rules to suit its legislative intent and judicial values.[5] In the same way, the UK, the US, Canada and Australia are all characteristically classified as common law jurisdictions, although the rules of evidence are exclusive to each country and depend on statutory provisions and standards set out by each countries' courts.[6] For ease of discussion, and because of imbalance, the researcher has decided to contrast the regulations pertaining to electronic evidence in common law countries with that in civil law countries. To achieve this a case study will be discussed for each jurisdiction. England and Wales will represent common law jurisdictions, while China will represent civil law jurisdictions. Both countries were selected on the basis that each has prominent characteristics associated with common law and civil law systems respectively.

The object of this chapter is to produce an organised study that addresses the regulation of electronic evidence across the two systems. Some may argue that China and England and Wales might not be examples of best practice for each jurisdiction; notwithstanding they are valuable examples, as there are many significant lessons to be learned from both.[7] The problems in each system concerning the presentation, acceptability, verification and authentication of evidence are also investigated. The study will also ascertain the advantages and disadvantages of each system, offering information regarding how each model deals with the process of gathering, analysing and presenting electronic evidence.

3.1 Common law jurisdiction: England and Wales

England and Wales follow the common law system. This fact has played an important role in spreading this jurisdiction internationally, as the system was disseminated to other countries during the era of colonisation. Court proceedings in England and Wales are mostly adversarial, particularly at the discovery stage and when the prosecutor is formulating the trial issues.[8] The main feature of English law is the obligation of the

[5] Matthew King, 'Security, Scale, Form and Function: The Search for Truth and the Exclusion of Evidence in Adversarial and Inquisitorial Justice Systems' (2001) 12 *International Legal Perspectives* 185-192.
[6] Ibid.
[7] See: section 3.7.
[8] See: Gary Slapper and David Kelly, *The English Legal System* (9th edn, London: Routledge-Cavendish 2009) Chapter 1.

lower courts to follow the decisions of the higher courts, under the principle of *stare decisis*.[9] In this case, the doctrine of judicial precedent is followed, which recognises the need to follow the previous ruling from a higher court whenever similar matters arise. Judges in England and Wales are active in finding solutions that support legal lacunae. The principle of stare decisis and judicial activism make it compulsory to scrutinise any statutory provision closely, with relevant judicial precedents, to find out the actual legal position on any issue. Many laws controls on admissibility of evidence have been formed through judicial precedent and laws made by judges. All the courts are supposed to follow the decisions of the Court of Appeal and Supreme Court, because of the quality of the principle of the judicial precedent from these sources.[10]

3.2 Civil law jurisdiction: China

There is no agreement as to whether China is a civil law jurisdiction; however, it there is agreement that it is definitely not a common law jurisdiction.[11] For this reason, before categorising and sampling the People's Republic of China (PRC) as a civil law jurisdiction some explanation must be given. Classification of the PRC as a civil law jurisdiction did not agree by some scholars. From the top-down view of law, Jane Fu argues that the PRC is a common law legal system. One expressive source that China has to access to a common law jurisdiction is Hong Kong legal system which is jurisdiction based on common law and has continued to enjoy rule of common law after returning to China.[12] He believed that since the reform and opening up policy which was applied since the 1980s, China started to look into the common law jurisdictions especially in the areas which are related to the business and economy issues.[13]

According to Peerenboom the Chinese legal system could be characterized as common law with respect to political law issues, family law and professional law with respect to commercial cases.[14]

---

[9]John Langbein, 'Historical foundations of the Law of evidence: A view from the Ryder sources' (1996) 96, 5 *Columbia Law Review* 1168-1194.
[10]Charles Arnold-Baker, *The Companion to British History* (3rd edn, Loncross Denholm Press 2008) 484.
[11]John Quigley, 'Socialist Law and the Civil Law Tradition' (1989) 37 *American Journal of Comparative Law* 781-792.
[12] Jane Fu, *Corporate Disclosure and Corporate Governance in China* (Kluwer Law International 2010) 12.
[13] Ibid.
[14] Randall Peerenboom, 'The X-Files: Past and Present Portrayals of China's Alien Legal System' (2003) *Global Studies Law Review* 47.

However, studying the rulings of the court in comparison to the literature confirms the view that the PRC is a civil law jurisdiction. When a law or rule is decreed by the legislative arm (National People's Congress, NPC) or the NPCs Standing Committee, then the Court's explanation of rules and laws is restricted. Courts cannot rule on the legitimacy, validity or constitutionality of a rule or law.[15] This is in accordance with civil law traditions. The court's role over the application of laws is restricted, rather than delivering active interpretation, as it ad confines the court's law making powers.[16] In accordance with the Resolution on Strengthening the Legal Interpretation of Laws, and also of the PRC's Constitution it is only the authority of the Standing Committee for the National People's Congress that is a legislative division.

The PRC's Constitution makes the court accountable to the NPC. It is not possible for Chinese courts to practice active judicial interpretation due to the lack of a separation of powers.[17]

Chinese court practices are typically interrogational, with judges playing a leading role during court case and trial, including the taking of evidence. For example, in Chinese civil procedures, judges make a substantial proportion of decisions. The parties and the court are not restricted to what the parties have pleaded, while in common law jurisdictions parties are restricted by the proceedings in the content of their pleadings.[18] When it comes to the presentation and admission of evidence, judges in Chinese courts reserve the choice to inspect evidence at any phase of the proceedings, without having to wait for a single evidence-taking phase, as is usually the routine with common law. It is a prominent feature of a typically civil regime to lay more stress on substantive justice than on procedural technicality. This is in contrast with the common law regime. As Zhong and Yu stated:

> 'It is the aim of the Chinese civil court to find out the "objective truth" completely. This would mean that the truth found out by the court and the facts given must be compatible with each other. The court is supposed to look into, investigate and find evidence to prove a certain fact when a party

[15] Peter Corne, 'Creation and Application of Law in the PRC' (2002) 50 *American Journal of Comparative Law* 369-396.
[16] Ibid.
[17] Jianhua Zhong and Guanghua Yu, *Establishing the Truth on Facts: Has the Chinese Civil Process Achieved This Goal?* (Florida State University College of Law 2004) 413-416.
[18] Margaret Woo, 'Law and Discretion in the Contemporary Chinese Courts' (1999) 8, 3 *Pacific Rim Law and Policy Journal* 588-589.

> is not able to do so. Thus, the court has to check all the appropriate facts even if they haven't been claimed or are undisputed'.[19]

Therefore, throughout the court case and trial phase, judges are involved participants and are able to undertake a detailed questioning of the parties or witnesses, so as to collect evidence. The main feature of the civil law system is active participation, as was mentioned above. Legally qualified professional judicial officers oversee all of the issues dealt with in Chinese courts, because Chinese courts have no jury or assessor system and have restricted exclusionary rules of evidence.[20] This is typical of a routine civil law jurisdiction, and signifies the commitment of the Chinese court to the 'free evaluation principle', which is fundamental to the civil law system.

The lack of stare decisis is another characteristic of China's legal principles that places it within the civil law system is that stare decisis is not a principle of China's jurisprudence.[21] But like many other contemporary civil law countries, the Chinese courts have developed a form of practical stare decisis. The Supreme People's Court, the country's highest court, provides descriptions to the lower courts on how law should be interpreted and applied.[22] There are two major reasons for this. First, while the Supreme People's Court has the power to interpret the law, it shares this power with both the legislative body and the executive branch; this shared responsibility has led to inconsistent interpretations. Second, the Chinese courts are more concerned with substantive justice than with consistent results, so even given the Supreme People's Court's suggested interpretations, precedent is not a concept the Chinese view as dominant.[23]

3.3 Electronic evidence regulation in civil law and common law systems

The positions of the PRC and England and Wales as typical civil law and common law jurisdictions respectively, have been recognised. This section will now study the rulings

[19] Jianhua Zhong and Guanghua Yu (n17) 437- 438.
[20] Mo Zhang, 'International Civil Litigation in China: A Practical Analysis of the Chinese Judicial System' (2002) 25, 59 *Boston College International and Comparative Law* 93.
[21] June Dreyer, *China's Political System: Modernization and Tradition* (8th edn, Pearson 2011) 173.
[22] Jianhua Zhang and Guanghua Yu (17) 437.
[23] Ibid, 437–438.

on electronic evidence in the two countries. This section begins with an overview of electronic evidence rulings in both countries. Then the legal status in close reference to comparable concepts of evidence is compared and contrasted in both systems.

3.3.1 An overview of electronic evidence regulations in England and Wales

The most significant legislative provisions to this research are found in the UK's Civil Evidence Act 1995. The law in the England and Wales identifies and indirectly provides for electronic evidence; however, there is no specific law for electronic evidence and no express or direct reference to electronic evidence in England and Wales statutes per se. Discussion regarding the position of England and Wales's on electronic evidence rulings must be based on the general rules of evidence. An example of this is Section 20 (1) of the Police and Criminal Evidence Act of 1984 which states that evidence includes 'any information stored in any electronic form contained in a computer'. This certainly means electronic information, which brings electronic evidence into the jurisdiction of general rules of evidence.

3.3.2 An overview of electronic evidence regulation in China

The courts of the People's Republic of China usually follow the basic laws and principles of Chinese evidence law to decide upon the implementation, admissibility and management of electronic evidence. This is because the PRC has no focused or comprehensive regulatory system for handling electronic evidence. For this reason, to understand the regulations on electronic evidence in the PRC, as a civil law jurisdiction, there are key procedural laws to understand court proceedings, including presentation and admission of evidence. The two key procedural laws are: (a) Civil Procedure Law of the People's Republic of China[24] and (b) Criminal Procedure Law of the People's Republic of China, which regulates criminal procedure.[25]

There are also some regulations that are not thorough, but are important in the assessment, admissibility and probative value of electronic evidence. This is because

[24]Civil Procedure Law of the People's Republic of China [China]. Adopted at the Fourth Session of the Seventh National People's Congress on 9th April 1991 and promulgated by Order No. 44 of the President of the People's Republic of China on 9th April 1991 <http://www.china.org.cn/english/government/207343.htm> accessed 23th January 2013.

[25]Criminal Procedure Law of the People's Republic of China [China]. Adopted by the Second Session of the Fifth National People's Congress on 1st July 1979, and amended pursuant to the Decision on Amending the Criminal Procedure Law of the People's Republic of China adopted by the Fourth Session of the Eighth National People's Congress on 17th March 1996 <http://www.unhcr.org/refworld/docid/3ddbcd4e7.html > accessed 23rd January 2013.

they are relevant to several elements of electronic evidence. These comprise the Certification Authority Regulations and the Electronic Signature Law of the People's Republic of China (referred to as the Electronic Signature Law). The Certification Authority Regulations have provisions associated with verification and certification. These are the main matters affecting the admission of documentary evidence, including those in electronic form. The Electronic Signature Law allows for the admissibility of electronic evidence and thus has an effect on authentication as a concept of evidence. Certain provisions of these laws and the exact way in which they control electronic evidence are observed below comparative to the England and Wales electronic evidence regulation.

Besides the current enacted laws, decisions made in the China Supreme People's Court would be considered as playing a crucial role in understanding and explaining the legality and admissibility of electronic evidence. This is because it has been observed that while China as a civil law jurisdiction does not maintain the concept of judicial precedent and state decisis, the judicial interpretations that have been given by the China Supreme People's Court on the rules of electronic evidence remain powerful and persuasive legally. The procedural laws have clear specifications related to conditions for admissibility. This is why the court interpretation is of greater value for assessing the probative force of the electronic evidence presented. The law tends to give judges a wider option from which to discover information based on all evidence presented.

3.4 A comparison of electronic evidence regulation: selected aspects

The following comparison and contrast between the two judicial systems discusses only those few cases of evidence that are comparable between the systems. This is for two reasons. Firstly, the scope of the law of evidence is so extensive that in this limited study it is not possible to discuss all elements of the law in relation to electronic evidence regulation in both systems. Secondly, it is a challenge to compare or contrast two systems, as each system does not have exactly equal or contrasting regulatory provisions. Civil law systems, as represented by the PRC and common law systems, as represented by England and Wales, have different, but also some similar requirements which electronic evidence must meet in order to be admitted in court. Provided below are the requirements mentioned in the procedural laws of the two countries.

3.4.1 Scope and admissibility of electronic evidence: England and Wales

There is a basic rule in relation to documentary evidence that only original documents can be presented, except when it can be proven that it is appropriate to the situation of the case to allow an exception. It is also stated that electronic documentary evidence consisting of computerised communications, including e-mails, are subject to the documentary rules of evidence.[26]

In 1993, the Law Commission recommended eight points for consideration by the Government relating to hearsay evidence. The recommendations were fully accepted and adopted within the Civil Evidence Act, issued in November 1995.

Section 1 of the Civil Evidence Act 1995 provides that:

> 1. 'In civil proceedings evidence shall not be excluded on the ground that it is hearsay.
> 2. In this Act:
> a) 'Hearsay' means a statement made otherwise than by a person while giving oral evidence in the proceedings which is tendered as evidence of the matters stated; and
> b) References to hearsay include hearsay of whatever degree.
> 3. Nothing in this Act affects the admissibility of evidence admissible apart from this section'. [27]

Sections 2 to 6 of the Civil Evidence Act 1995 imposed a number of safeguards and supplementary provisions with regard to the admissibility of hearsay evidence. However, no statutory regulation regarding the probative value of hearsay evidence has been provided.[28] Thus, electronic evidence falls under the hearsay rule but computer-produced evidence may be regarded as either real or hearsay, depending on the facts of the case.[29] For example, a computer printout was regarded as real evidence in the

[26]See: Peter Murphy and Richard Glover, *Murphy on evidence* (12th edn, Oxford University Press 2011). 235.
[27]Civil Evidence Act 1995, s 1.
[28]Steven Teppler, 'Digital data as hearsay' (2009) 6 *Digital Evidence and Electronic Signature Law Review* 9-24.
[29]The computer evidence does not fall comfortably within the traditional classifications of evidence. Nevertheless, a confession made online is admissible under s.76 of the Police and Criminal Evidence Act 1984. Furthermore, a confession will be excluded if the prosecution does not disprove beyond reasonable doubt any claim that the confession was either obtained by oppression of the person who made it, or "in consequence of anything said or done which was likely, in the circumstances existing at the time, to render unreliable any confession which might be made by [the defendant] in consequence thereof". See: Colin Tapper, *Computer Law* (4th edn, Longman 1989) 375.

Sapporo Maru (Owners) v Statue of Liberty (Owners) [30] and *R v Wood*,[31] while in the *DPP v Bignall* [32] the printout was regarded as hearsay.

The court in England and Wales has been given broader options to decide the degree to which documentary evidence can be presented. This was undertaken through the Civil Evidence Act 1995, which included a legislative amendment to the documentary rules of evidence. This led to a change of focus, from stressing the original as a standard for acceptability as evidential value.[33] The acceptability of evidence is linked to the weight of the electronic evidence and its actual evidential value according to the Civil Evidence Act 1995. This is mentioned in Sections 8 and 9 of the Civil Evidence Act, which provides a basic guideline for the admission of any document for the purposes of presenting evidence in the court. Section 8 of the Act provides as follows:

> '(1) Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved-
> (a) By the production of that document, or
> (b) Whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such manner as the court may approve.
> (2) It is immaterial for this purpose how many removes there are between a copy and the original'.[34]

As long as the document is authenticated, this provision allows the use of any document with evidential value to prove pertinent facts in civil court proceedings. In civil

[30][1968] 1 WLR 739. In this case, the record of radar readings showing the location of two ships involved in a collision is real evidence. The readings were automatically recorded by mechanical devices without human intervention. 'Mechanical' means 'automatic' and includes electrical, electronic and chemical methods of recording as opposed to just mechanisms made up of machines.

[31][1982] 76 Cr App R23. In this case, the computer printout of a calculation was put forward by a chemist who had performed an analysis on a metal stolen by the accused, which was admissible as real evidence because the computer was used as a calculator. While in *R v Spiby* [1990] Crim App R 186, the telephone printouts from the hotel's computer, which had automatically logged the lifting of the phone receiver and the making of the call, were admissible as real evidence.

[32][1998] 1 Cr App R 1. In this case, the respondents (two police officers) were charged with hacking under s.1 of the UK Computer Misuse Act 1990 and were convicted by the Magistrate's court. On appeal to the Crown Court, the officers contended that their use of a computer even for private purposes was not an unauthorised access offence under s.17 (5) of the UK Computer Misuse Act 1990. The court allowed their appeal. The prosecutors then appealed to the Queen's Bench. This appeal was dismissed. The Queen's Bench held that no offence committed under s.1 of the Computer Misuse Act 1990. The respondents had the authority to access this under s.17 (2) (s) and (d) of the Computer Misuse Act 1990. Therefore, they did not fall within s.17 (5) and thus, they had not committed an offence.

[33]See: Hodge Malek, Jonathan Auburn and Roderick Bagshaw, *Phipson on Evidence* (17th edn, Sweet and Maxwell 2010).

[34]Civil Evidence Act 1995, s 8.

proceedings, the parties do not have to authenticate any form of evidence unless the opposing party requires them. This means that at the disclosure stage, providing both parties do not challenge the authenticity of the evidence, the evidence is admitted and the judge accepts the evidence as being reliable.[35]

Obiter dicta of English judges appears to prove that the best evidence rule is no longer of any value in civil cases. For example, Parker LJ in *Masquerade Music v Springsteen*[36] stated as follows: '(i) in my judgment, the time has come when it can be said with confidence that the Best Evidence Rule, long since on its deathbed, finally expired'.[37] Although this view was held, it may not be regarded as a final judicial interpretation, but points rather towards the court's willingness to raise reliable and legitimate secondary evidence to equal primary evidence. Through Section 8 (2) of the Civil Evidence Act 1995, moves between an original and a copy will affect acceptability as long as the copy is legitimate.

There are some additional guiding principles related to electronic evidence in Section 9 of the Civil Evidence Act 1995. These relate specifically to cases where original or physical evidence has been modified into electronic form. The section provides as follows:

> '(1) A document, which is shown to form part of the records of a business or public authority, may be received in evidence in civil proceedings without further proof.
> (2) A document shall be taken to form part of the records of a business or public authority if there is produced to the court a certificate to that effect signed by an officer of the business or authority to which the records belong'.[38]

Acceptance of records, without any constraint of form, allows electronic data to be part of the records and therefore brings electronic evidence within the capacity of Section 9's regulation of evidence. To prevent any type of uncertainty, Section 9 (4) explains the meaning of records as 'records in whatever form'.[39] Extensive judicial discretion in relation to Section 9's provision are to be found in Subsection 9 (5), which permits the

[35]Stephen Mason, *Electronic Evidence* (3rd edn, LexisNexis Butterworths 2012) 317.
[36][2001] EWCA Civ 563.
[37]Ibid.
[38]Civil Evidence Act 1995, s 9.
[39]Ibid, s 9(4).

court to order that some provisions of the section will not be implemented. Consequently, the subsection states: 'the court may, have regard to the circumstances of the case; direct that all or any of the above provisions of this section do not apply in relation to a particular document or record, or description of documents or records'.[40]

The English (Divisional) High Court noted that the rule only applied to written documents, not to tapes or films, by taking the stance that, whenever an original document does not exist then it should be not accepted (*Kajala v Noble*).[41] The ruling was linked to acceptability of a videotaped copy of original news footage by the BBC, and this is what Ackner LJ said:

> 'The best evidence rule had been completely ruled out by the board now, whereby only the best evidence had to be presented in court. What remains of the rule is that original documents are required when they are available. In such a case, secondary or copy of the document would not be enough. Therefore, at present, the rule of the board is not limited to the best evidence. In fact, all appropriate evidences can be submitted… In our judgment, the old rule did not encompass videos or tapes and was limited to written records, while in the new rule videos and tapes are included and the positivity or negativity of evidences affects weight and not present ability'.[42]

Later in *R v Governor of Pentonville, ex p Osman*, Lloyd LJ stated that the best evidence rule had become a rule of practice or procedure.[43]

The Criminal Justice Act 2003 also brought about a change in relation to criminal trials, whereby it simply removed the best evidence rule in criminal processes. Section 133 [44] of the Act provides:

> 'Where a statement in a document is admissible as evidence in criminal proceedings, the statement may be proved by producing either -
> (a) the document, or
> (b) (whether or not the document exists) a copy of the document or of the material part of it, authenticated in whatever way the court may approve'.[45]

---

[40]Ibid, s 9(5).
[41][1982] 75 Cr App R 149.
[42] Ibid.
[43][1990] 1 WLR 277, DC.
[44]Section 27 of the Criminal Justice Act 1988 has similar provisions.
[45]Criminal Justice Act 2003, s133.

However, observers have remarked that the English and Welsh courts currently place less emphasis on the original than ever, and even electronic evidence is being admitted into criminal courts without proper authentication.[46]

Originality of documents is a key issue when presenting documentary evidence when working with the best evidence rules in England and Wales. Section 9 of the Civil Evidence Act 1995 imposes that documents tendered are correct for records of public authority or a business. It also calls for the production of a certificate of authenticity signed by the corporations and businesses to which the records belong. Section 9 provides:

> '(2) A document shall be taken to form part of the records of a business or public authority if there is produced to the court a certificate to that effect signed by an officer of the business or authority to which the records belong'.[47]

Normally, the Civil Evidence Act 1995 presents no thorough guidelines regarding how validation of a document should be done. This makes it a judicial option to decide the approach and standards through which the legitimacy of documents in doubt should be decided.

3.4.2 Scope and admissibility of electronic evidence: China

The wide range of records that can be presented as evidence in Chinese courts is apparent in their definition of evidence and also in the statutory specification of what can be categorised as evidence for use in civil and criminal trials. It is stated in Article 42 of the Chinese Criminal Procedure Law that: 'All facts that prove the true circumstances of a case shall be evidence'.[48] This shows that the criterion for the admittance of evidence in China is easier than that for England and Wales, which are comparatively more constrained. Whether electronic material would be sufficient evidence is not stated in Criminal Procedural Law. However, this can be understood by the general definition, which accepts any fact proving the true conditions of a case as suitable evidence. In *Yang Chunning v Han Ying* the Beijing Hai Dian District People's

[46]For which see: the IALS Think Tank proposal to the Law Commission <http://ials.sas.ac.uk/news/IALS_Think_Tank.htm> accessed 30th October 2013.
[47]Civil Procedure Act 1995, s 9 (2-3).
[48] The Chinese Criminal Procedure Law, Article 42.

Court accepted evidence of text messages to prove a contract for a loan and noted that the name in the text message was an electronic signature.[49]

It was further accepted in Article 42 that 'video and audio materials' which are basically electronic materials are good evidence.[50] Civil Procedure Law is also more thorough in its listing and acceptance of a broad range of types of evidence. Three classifications that seem to match electronic evidence under Chinese Civil Procedure Law comprise: 'material evidence, audio-visual reference material and documentary evidence'.[51] Verification appears to be the main measure for admissibility. In criminal cases there is a provision that verification is required for any evidence to be used before being admitted as proof of any fact. In addition, in civil cases admission of audio visual evidence has more judicial discretion, as is shown in Article 69 of the Civil Procedure Law which states that: 'The people's court shall verify audio-visual materials and determine after examination whether these can be taken as a basis for ascertaining the facts'.[52]

In many situations, electronic evidence, instead of being primary or original evidence, has taken the form of secondary evidence. This is because of the common nature of electronic evidence as reproducible, and the ease of converting physical evidence into electronic form (for example by way of scanning). However, this leads to doubt as to the extent to which Chinese laws would accept electronically reproduced evidence. Article 69 of Chinese Civil Procedure Law relates to this issue; it states:

> 'Any document submitted as evidence shall be the original one. Material evidence shall also be original. If it is truly difficult to present the original document or material, then reproductions, photographs, duplicates or extracts of the original may be submitted'.[53]

Article 69 of the Chinese Civil Procedure Law is comparable to the Common Law Best Practice principle of presenting evidence. This is an essential characteristic of common law rules of evidence, as mentioned in the Code of Practice on Legal Admissibility and

[49] *Yang Chunning v Han Ying* (2005) hai min chuzi NO.4670, Beijing Hai Dian District People's Court. For more information about this case, see: Case Translation: (2008) 5 *Digital Evidence and Electronic Signature Law Review* 103–105.
[50] Ibid, Article 42 (7).
[51] The Chinese Civil Procedure Law, Article 63(1-3).
[52] Ibid, Article 69.
[53] Ibid, Article 68.

Evidential Weight of Information Stored Electronically (referred to as the BSI Code of Practice) and Sections 8 and 9 of the UK's Civil Evidence Act 1995.[54] As per the BSI Code of Practice the following standards must be achieved to enable electronic evidence to be used: 'the authenticity, integrity and availability of electronically stored information, to the demonstrable levels of certainty required by an organisation'.[55]

In England and Wales the judge has the discretion to decide how and by whom the authentication is handled. In contrast, China has strict regulations concerning the authentication and verification of documents. Authentication has only to be undertaken by a Certification Authority, which is a government agency, or by Certification Service Providers, which are organisations assigned and authorised by the government to conduct third party certification and the verification of authenticity. It could be said that this is beneficial because the authentication and verification processes are given to experts found in the certification agencies. For example, only organisations properly licensed by the National Government's nominated regulatory agency, Ministry of Information Industry (MII), can conduct authenticity verification, as stated under the Electronic Signature Law.[56] This is in contrast to the position in England and Wales, where judges with a lack of extensive knowledge of electronics retain the right of discretion to evaluate and conclude whether and how authentication should be performed. It is stated in Section 9(2) of UK's Civil Evidence Act 1995:

> '(2) For the purposes of paragraph (2)-[57]
> (a) A document purporting to be a certificate signed by an officer of a business or public authority shall be deemed to have been duly given by such an officer and signed by him; and
> (b) A certificate shall be treated as signed by a person if it purports to bear a facsimile of his signature'.[58]

[54] Standards Institution (BSI) BIP0008, the 'Code of Practice for Legal Admissibility and Evidential Weight for Information Stored Electronically' (BIP0008).
[55] Ibid.
[56] Law of the People's Republic of China on Electronic Signature ("Electronic Signature Law" or "ESL") Order No. 18 of the President of the People's Republic of China. For more information about the Electronic Signatures Law of China see: Minyan Wang and Minju Wang, Electronic Signatures Law of China, translation and introduction (2005) 2 *Digital Evidence and Electronic Signature Law Review* 79 – 85.
[57] In reference to (2), which mandates these bodies or officers to authenticate their documents.
[58] Civil Evidence Act 1995, s 9 (2).

In brief, China allows public authorities and officers of businesses to participate in the authentication and verification of documents initiating from them. Conversely, in England and Wales, the rule is that there is a presumption that documents from a public authority are presumed to be correct, but it does not prevent another party calling into question whether the document is actually correct.

3.5 The process of gathering, analysing, preserving and presenting electronic evidence in the England and Wales compared to China

Before distinguishing between the advantages and disadvantages of each system it is necessary to illustrate the roles that an investigator may have with respect to the gathering, analysing and presentation of electronic evidence in criminal proceedings in China's and England and Wales's legal systems.[59]

The common rules for evidence in China guide the process of gathering, analysing and presenting electronic evidence. In contrast, in England and Wales the handling of this evidence is guided by the Police and Criminal Evidence Act 1984 (PACE). Reference is also made to the Association of Chief Police Officers (ACPO) guidelines, which are recommended steps for the procedure of gathering, analysing and presenting electronic evidence in order to ensure it is acceptable in a legal case. The guidelines require that parties collecting any evidence should not tamper with the evidence stored on an electronic device. Original data can be accessed by a third party as long as they are experts and can explain their actions. Finally, any process performed on the electronic evidence should be preserved for verification by a third party.

Although the regulation of electronic evidence in China and England and Wales is not at the same level, the process of gathering, analysing and presentation is almost identical. For the evidence to be acceptable in a legal case the process should be carefully undertaken in order to avoid tampering with the original information. In China the evidence rules advocate that evidence presented should be in its original state.[60]Aside from issues over the admissibility of electronic evidence, the weight of original evidence in a legal case is crucial. In England and Wales a judge might determine whether an item of evidence is authentic first, and then remove it from the case if they determine that it is not authentic. Once evidence is admitted, it is the

[59]The scope of this thesis is limited to electronic evidence in the criminal proceedings.
[60]The Chinese Civil Procedure Law, Article 69.

members of the jury who decide whether the accused is guilty of the allegations or not. The members of the jury do not determine the authenticity of the evidence. In addition, Section 78 of the Police and Criminal Evidence Act 1984 (PACE) is an exclusionary rule exercised by the judge.[61]

3.5.1 Search and seizure process for electronic evidence

Nelson noted that evidence gathering is a complex and expensive process that depends upon the type of evidence to be gathered.[62] There are two main methods used in the process of gathering electronic evidence. One is the use of searches, raids or inspections, which are performed by those agencies undertaking the process of gathering. Some agencies confiscate digital information, while others make a copy or take images of the digital information.[63] In England and Wales searches, raids or inspections are permitted by search warrants; and this system also operates in China.[64] Rules governing these searches are stated under PACE 1984 part II. Different chapters of PACE 1984 part II explain what an officer can do under different circumstances.

In China, the Criminal Procedure Law governs the gathering process. Under Chinese criminal procedure law judges, prosecutors and investigators have the authority to gather evidence.[65] Recently according to the amendments in criminal procedure law, the authorities responsible for gathering evidence can obtain help from a technical expert or institution if necessary.[66] Confiscation is a widely used method in China because it retains the originality of the evidence.[67]

With regard to copying and detaining data, the Chinese use rules prescribed for video and voice data. However, in 2010 a new judicial explanation detailed special stipulations in respect of copying, collecting and preserving electronic data.[68] With

---

[61]See: Rupert Cross and Colin Tapper, *Cross and Tapper on Evidence* (12th edn, Oxford 2012).
[62]See: Sharon Nelson, Bruce Olson and John Simek, *The Electronic Evidence and Discovery Handbook: Forms, Checklists And Guidelines* (New York: American Bar Association 2006) 1-2.
[63]Ibid.
[64]See: the Chinese Criminal Procedure Law, Articles 109 -113.
[65]Ibid, Article 43.
[66]Ibid, Article 10.
[67]Adam Cohen and David Lender, *Electronic Discovery: Law and Practice* (2nd edn, London: Aspen Publishers 2011) 101.
[68]PI Yong, 'New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime' (2011) <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/Cyber_cp_china_Pi_Yong_Dec11.pdf> accessed 10th January 2013.

regard to the seizure of electronic evidence, the Chinese have special rules dealing with mail and telegrams.[69] In England and Wales, seizure is permitted by Section 19 of PACE, 1984. Section 20 of PACE extends the authority of seizure to computerised data or information. It also depends on the level of authority the gathering agency has, as there are some agencies that do not have the authority to confiscate. Finally, the consent of the party being investigated can be given consideration in some cases.

The other method used in the gathering process is compelled discovery. This occurs where the party being investigated is asked to produce the required information. This is in contrast to search, raid and inspections in which investigators search for the evidence. The Criminal Procedure and Investigations Act 1996 (CPIA) covers the disclosure method in England and Wales. Later, in 2007 the Investigation of Protected Electronic Information: Code of Practice was published to deal with encrypted materials. The Code provides guidance that can be followed when requiring the disclosure of protected electronic data.[70] In this case, the company or individual being investigated is supposed to produce the evidence in a format, which is acceptable in court. This method is commonly applied in cases where additional information is required after a search, inspection or raid is performed.[71]

Using the above methods there are steps that must be followed in order to ensure that the evidence collected is valid for use in a legal case, and to prevent any alterations. Firstly, one must try to stop any attempt at evidence destruction by the party being investigated. For example, in a case where emails are to be used as evidence the automatic delete feature can be disabled. If investigators suspect that there are some deleted files then hard drives can be confiscated. This right exists under PACE, 1984 Section 19. This applies mostly when using the raid, inspection and search method.

The second important step in this process is the identification of data relevant to the legal case. In a case where the search or raid method is used, after ensuring that all data destruction possibilities are eliminated then the evidence gathering team has to determine where the evidence may be located.

---

[69] See: the Chinese Criminal Procedure Law, Article 116.
[70] See: Investigation of Protected Electronic Information: Code of Practice, Paragraph 3.12.
[71] Ronald Rivest, *The MD5 Message Digest Algorithm* (MIT Laboratory for Computer Science 1992) 21.

Once the requisite data has been gathered the professionals collecting it are supposed to examine the process followed and determine if it was forensically correct. If so, then the last step before starting to analyse the data is to make a copy of the evidence collected for security purposes. This ensures that during the analysis process any procedure performed on the evidence does not cause alterations to the original data, and if it does, that the original can be used as proof. Finally, the custodian of the evidence should be known from the analysis stage until presentation. In China, the gathering process has been a disadvantage in many legal cases, because alteration mostly occurs at this stage and then leads to nullification of the evidence.

3.5.2 Preservation process for electronic evidence

The People's Republic of China has no specialised and comprehensive regulatory regime for preservation electronic evidence. In dealing with electronic evidence pre-existing Chinese evidence rules are applied.[72]

In the case of England and Wales, The Good Practice Guide for Computer Based Evidence, which was initially published by the Association of Chief Police Officers in England and Wales in 2009, provides more precise guidelines. This later became known as the ACPO Guide and is of great help to investigators dealing with various kinds of electronic evidence, covering some areas such as internet, video and CCTV evidence as well. Guidance for the forensic examination of computers is also contained in this document, along with the methods for copying a disk, giving the investigators detailed insights into the gathering of electronic evidence and concerning how to deal with it. Audit trails, biometric data, application logs, application metadata, badge reader logs, intrusion detection system reports, internet service provider logs, network traffic, firewall logs, transaction records and database contents are among the kinds of electronic evidence that an investigator must learn about.

It is also noted in this document that mobile devices, mini computers and portable media players and gaming consoles can contain evidence. This can be an issue for the forensic expert, as knowledge that is more technical is required to deal with such evidence, though the guidelines for dealing with this type of evidence are established. Investigators may also have to deal with cases that involve substantial servers, storage

[72]The Chinese Civil Procedure Law, Article 74.

devices, and evidence on different networks; this requires technical skill and expertise.

This is a challenge that many investigators have to face, even though the process of handling this evidence is not clearly spelled out by current best practice guidance. This makes it particularly crucial to have better and more detailed insights into forensic science and how to use it properly, which makes it difficult for investigators to possess the necessary skills and knowledge necessary for all the techniques and scenarios. However, it is true that one person cannot know everything, and therefore knowing when to ask for help is essential. Because of this, the ACPO Guide contains an entire section discussing when the investigators must seek help. A document cannot possibly include all possible scenarios, as various cases may need different approaches that have not been incorporated in the document. There is no separate section pertaining to investigations on the internet, but it is recommended in the document that the investigator should have knowledge of this area.

It is extremely beneficial for evidence to be forensically sound. That is, the accuracy and validity of the original data must not be lost when handling the electronic evidence. The following are the four principles suggested by the ACPO Guidelines on how electronic crime scenes should be dealt with:

Principle No 1: The data that has been acquired and is in the computer or on any storage device should not be edited by any action that the agencies of law enforcement or its agents make, as the court relies upon it.

Principle No 2: If any person accesses the original data from the computer or the storage device that has been seized as evidence, then they must give a valid explanation for doing so.

Principle No 3: It is necessary to save the audit trail and other means that are used to obtain the electronic evidence, in order for the third party to have a detailed insight about the process used.

Principle No 4: The officer in charge of the case must make sure that all the laws and principles are abided by.

Although it may not be possible for the investigators to apply all these principles in all

cases, it is still necessary for them to know them. In contradiction of Principle No. 1, in practice it is not possible to use an original system without causing any changes to it if one wishes to collect electronic evidence. However, the originality of the evidence is not questioned if Principles No.2 and No.3 are abided by. If any piece of information is changed due to the investigator accessing it, this must be documented and proper skills and expertise are required to do so.[73]

3.5.3 Analysis process for electronic evidence

Analysis refers to the process of interpreting the gathered evidence and putting it into a coherent and meaningful format. The process determines the importance of the evidence in a legal issue. Depending on the type of case, electronic evidence has to be analysed by a forensic expert before it is presented in a court of law. Analysis of electronic evidence should not be done on the original evidence in order to avoid any alterations. There are different types of analyses that are undertaken on gathered evidence before it is presented in a court.

The first type of analysis is the determination of the time when the events in the gathered evidence occurred; this is referred to as timeframe analysis. This is important in a case where there is the need to associate the use of the electronic device to an individual at a particular time. Another type of analysis is undertaken to discover and recover hidden data; this is referred to as data hiding analysis. All information related to the issue is gathered during the evidence gathering process. In the analysis stage the applicability of the information is determined in a process called application analysis; this also determines the relationships between files.[74]

Finally, in some case, an analysis is undertaken in order to determine the individuals who may have used an electronic device at a particular time. In this case the responsible parties can be identified even if they are unknown. The steps above should lead to a conclusion about the gathered evidence in relation to the legal case in question. After drawing a conclusion based on the analysis process the expert involved is required to document their findings for presentation in a court of law. In China the use of

[73]Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn, Waltham Mass.: Academic Press/Elsevier 2011) 232.
[74]See: Joan Feldman, *Essentials of Electronic Discovery: Finding and Using Cyber Evidence* (New York: Glasser Legal works 2003).

professional agencies like KPMG are used for analysis electronic evidence.[75] In England and Wales, ACPO has set out guidelines on examination and analytical procedures for electronic evidence.

3.5.4 Presentation process for electronic evidence

The presentation process involves explaining the analysed evidence in a simple manner so that all interested parties can understand. The law of evidence in China requires a forensic expert.[76]

In England and Wales PACE, 1984 Section 81, provides for advanced notification of an expert to be present to a court of law. All the steps followed in the analysis should be written down in a comprehensive format for presentation. Presentation is made to the jurisdiction and also to any interested audiences. The forensic expert should present detailed findings, supporting documents and a glossary. If, during the gathering and analysis process there was a process that altered the original data this should be explained during the presentation stage.[77] It should also be proven that precautions were taken to prevent any additional materials affecting the original data.

When presenting electronic evidence to the court it is very important to be able to account for what has happened from the time the evidence was gathered to the time a forensic expert examined it. This is why possession of the evidence should be known at all times. Failure to account for the whereabouts of the evidence at any one time may mean there have been alterations and thus invalidation.

During presentation of electronic evidence the analysis steps and results should be presented together with the evidence analysed. The documents help the court determine the validity of the evidence. Under PACE, 1984 Section 78(1) the evidence can also be termed invalid. Both the prosecution and defence counsel use documents to find points to prove legally. In England and Wales, this is referred to as points to prove. As the documents are presented to an interested audience, it is crucial to make the evidence understandable in order for it to be effective. This is done by communicating the

[75]For further information about KPMG's work in this regard, see: <www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/digital-evidence-recovery-0906.pdf> accessed 16th April 2013.
[76]The Chinese Civil Procedure Law, Article 61.
[77]See: Rupert Cross and Colin Tapper (n 61) 541-542.

meaning of the evidence in laymen's language.

3.6 Evaluation of each model with regard to electronic evidence regulations

A number of advantages and disadvantages affecting each system, particularly in relation to the regulation of electronic evidence have been presented above. The advantage of the England and Wales common law active judicial interpretation is its flexibility and ability to adapt in a way that leads to impartial and just results. However, this active judicial interpretation can also be a reason to revert to doctrines that cause a hindrance when obtaining justice. As depicted in the *Kajala v Noble* case, discussed above, the English court generally considers the best evidence rule to be no longer applicable, thus it has now been removed.[78] However, shortly after this case an exception to the rule was brought in stating that when the original document exists then it should be presented in the court instead of the secondary one. Such exceptions to the general rule cause uncertainty to litigants, since a litigant would not be able to forecast the outcome. Such exceptions are quite typical of common law systems.

This differs from civil law where the court will usually apply the law as it stands to the particulars of the case. The limited systematic exceptions to general rules help achieve a better understanding of the law for those litigants who might want to use electronic evidence in their cases. Moreover, with the civil law position, the result would be comparatively easier to forecast because there is barely any judicial activism and the courts usually implement the law as it is, following a plain and ordinary application of meaning.

Both systems of jurisdiction have benefits and drawbacks in terms of their requirements for the authentication and verification of electronic documentary evidence. As demonstrated by England and Wales's position, the Common law allows for a presumption of regularity that can be challenged. The discretion of the judge in authentication and verification allows them to control the proceedings to a broader extent. The judge can also alternate with easier means of authentication, whenever the suggested method becomes challenging or excessively unsatisfactory to litigants. This leads to minimal bureaucracy and backlog of documents to be verified.[79] Conversely, in

[78]See: section 3.4.1.

[79]By way of example, see the article by Stephen Mason, 'Electronic evidence: A proposal to reform the presumption of reliability and hearsay' (2014) 30 *Computer Law and Security Review* 80-84.

the civil law system, as demonstrated by the Chinese position, where expert and particular authentication agencies carry out verification and authentication neither litigants nor courts have substantial control.

The executive agencies or certification organisations are given a significant role in judicial processes by the civil law position. When these agencies are slow to carry out their roles, either due to bureaucracy or work backlog, then the same delay will also occur affecting the proceedings of the court. However, an advantage of the civil law position is that reliability of authenticity is guaranteed. This is through the participation of expert agencies that use experts with capable skills to verify the authenticity of electronic documents. Electronic evidence is a product of complicated technology. Giving powers to a judge, who might not have the necessary knowledge of how that technology works, could lead to unreliability.

From the discussion it is clear that electronic evidence has a wide range of definitions in various regions. There are no specific rules governing the process of gathering, analysing and presenting electronic evidence as these vary from one region to another. This is an advantage in England and Wales and China, and the world at large. Improving technology has helped a great deal when solving criminal cases. Whilst the process may be a solution to many issues in legal cases, one of the major disadvantages is that it is a very expensive process.

Gathering evidence is the most crucial stage. If care is not taken at this stage, the evidence can be termed as invalid due to simple mistakes. Due to this, different regions have guidelines for the performance of this process. For instance, we have the ACPO guidelines in England and Wales and KPMG forensic technology services to ensure a successful process of gathering, analysing and presenting electronic evidence. The analysis is crucial. If an expert is not able to relate evidence to the legal issue in question then it is useless. Finally, if the presentation is not effectively made then the other two stages are pointless because the jurisdiction has to be convinced by the presentation. All three stages must be undertaken effectively if electronic evidence is to be termed valid for resolving a legal issue.

3.7 UAE lessons from comparative approach

Some may argue that England and Wales and China may not be the best international

models with regard to the regulation of electronic evidence. However, there are many lessons to be learned from each country. The regulation of electronic evidence is not confined to one legal system or a specific geographic area, but it is a worldwide issue. The previous discussion of the regulation of electronic evidence in different legal systems seeks to establish that each system faces the same issues and each are seeking a solution. The overwhelming presence of electronic evidence in England and Wales and China encourages each seek to implement solutions to those problems which have emerged. The 'macro-comparison' approach used in this chapter aims to offer many lessons for the UAE to learn from the experiences of England and Wales and China in this field. The first lesson can be learnt from England and Wales in relation to the gathering, preservation, analysis and presentation of electronic evidence. As exemplified by the specialised and specific methods set as reference when dealing with electronic evidence within legal rules in the English and Welsh model.[80]

In general, crime may be explained by the concurrence of three factors: motivation, opportunity and the absence of regulation. Presently, in the electronic era, crimes have shifted from their traditional conception, with the rapid proliferation and astuteness of digital technology. In the absence of guidelines in the UAE, there should be procedures in place to help lawyers, prosecutors, judges, investigators to deal with electronic evidence, once it is agreed that obtaining and seizure of such evidence is necessary.

There are a set of published guidelines, which spell out the basis of how to handle electronic evidence properly. This could prove to be a huge support for investigators seeking to fulfil their requirements regarding the collection of evidence. Further to the ACPO guide there are many others such as; the Electronic Crime Scene Investigation: A Guide for First Responders which is a set of guidelines published by the U.S Department of Justice (USDOJ) in 2001.[81]

Many sources of electronic evidence are referred to in this guide, in particular how certain evidence should be dealt with. Best Practices for Seizing Electronic Evidence: A Pocket Guide for First Responders is was published by the US Secret Service in 2006.[82]

[80]The situation in the UAE will be further discussion in Chapter Four.
[81]See: Forensic Examination of Digital Evidence: A Guide for Law Enforcement <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf> accessed 11th January 2013.
[82]See: Best Practices for Seizing Electronic Evidence v.3A Pocket Guide for First Responders <http://info.publicintelligence.net/usssbestpractices.pdf> accessed 11th January 2013.

This guide details electronic crimes in which computers have been used and could serve as a foundation on which to create a standardised operating procedure. This is also of immense help for obtaining a better perception of how to detect electronic evidence exhaustively, ensuring that a convenient method is adopted which makes the investigation error free.

Due to the various challenging situations that may arise with regard to electronic evidence, it is necessary for the investigator to use forensic science principles in accordance with various situations. The guidelines for guaranteeing that electronic evidence is gathered, stored and investigated properly are presented. However, eliminating and reducing the risk of error is mandatory when selecting a proper method to handle electronic evidence in court. Lessons can also be learned from the requirements for authentication and verification of electronic documentary evidence in each system and their advantages and disadvantages.

3.8 Conclusion

This chapter discussed the rules concerning electronic evidence in civil law systems and common law systems through means of a case study of the People's Republic of China and England and Wales as respective representatives of each system. Recently the use of electronic evidence has increased tremendously leading to alterations in different jurisdictions and legal systems concerning the rules of evidence to enable utilisation of electronic evidence. Most of the major and similar points in relation to the acceptability of electronic evidence in both systems have been noted. Some dissimilarities were also illustrated, due to the general interpretative traditions of the two systems.

As per the above study, the English and Welsh and Chinese laws relating to the acceptability of electronic evidence, principally where there are (electronic) copies of the original would be acceptable in both jurisdictions, assuming their reliability can be recognised. The Civil Evidence Act 1995 and the BSI Code of Practice stress the reliability of documents. This is similar to Chinese procedural laws, which stress the requirement for authentication and verification of documents. Both regimes have regulatory systems, especially civil procedural laws, that have changed the debate on electronic evidence from one of acceptability to probative or evidential value. This is a similarity of both systems. The most significant matter relating to electronic documents

is their authentication and verification, because evidential weight will be highest where the requisite document can be validated. In a civil law system (China's position) the authentication and verification processes are well defined by law and in the domain of authentication agencies that falls under the executive label. This differentiates them from the common law system, where the judge exercises more discretion regarding the integrity of electronic evidence. The next chapter discusses the regulation of electronic evidence in the UAE, also presenting a case study.

CHAPTER FOUR: IT ENVIRONMENT AND UAE's CRIMINAL PROCEDURE LAW: PROCEDURES GOVERNING SEARCH AND SEIZURE, PRESERVATION, EXAMINATION, PRESENTATION, AND AUTHENTICATION OF ELECTRONIC EVIDENCE

A successful criminal investigation depends on the analysis and gathering of evidence. The use of electronic evidence has increased in the past few decades as courts have permitted into evidence e-mails, digital photographs, word processing documents, and files saved from accounting programs, internet browser histories, the contents of computer memory, computer backups, digital logs, computer printouts and digital video or audio files. However, in the age of the computer and networked devices, the remit regarding investigation and disclosure of electronic evidence is extremely wide, ranging from files on a digital camera to the complex operation of algorithmic codes used. As reliance on ICT increases, so does vulnerability; increasingly, the availability of connectivity and communication through the Internet exposes people to the activities of e-criminals.

Technology has facilitated the commission of many forms of cybercrimes and powerful computers are used for the execution of such crimes. The Internet allows fraudsters instantaneous direct access to millions of potential victims around the world at minimal cost.

The ability of a computer to send, save, and delete information and rendering data intangible poses a challenge to the normal process of collecting evidence in a criminal investigation. Naturally, this influences the theory and process of evidence collection by permitting electronic evidence restoration and data recovery. In a normal system, evidence is palpable and gathered via the direct handling of materials. In contrast, evidence gathered in the electronic environment needs to be handled by applying a different methodology. This method is often guided by programs that go into the core of the computer system in order to restore data that has been 'deleted'. It may also provide links to connections made over the network system, including to whom, when, where, what and how a message has been transmitted. This, however, requires the employment of an electronic evidence specialists.

The methods of electronic evidence recovery are increasingly relevant, in view of the rapid advances in ICT. Often the criminal leads the way in creating opportunities to commit hi-tech crimes by utilising various technologies. It is recognised by both law enforcement and technology analysts that the use of advanced technology to support or perpetrate crime will increase as the ability of offenders rises in conjunction with the rapid advancement of electronic communication and technology devices.[1] As a result, judges, prosecutors, lawyers and computer experts need to be more technologically perceptive. Not only this, they need to be more knowledgeable and skilled than the offenders they pursue,[2] especially when investigating and detecting cybercrime cases.

High-tech facilitated cybercrimes present a considerable challenge to UAE law enforcement and criminal procedural law, and so this chapter aims to examine whether the UAE Criminal Procedure Law is sufficient to govern the process of gathering, preservation, examination and presentation of electronic evidence. It will ask: Can existing regulations stand alone or is supplementary legislation needed? It is therefore appropriate to examine the following:

I. The collection of electronic evidence;

II. The UAE's search and seizure procedures for electronic evidence;

III. The preservation of electronic evidence in the UAE;

IV. The examination of electronic evidence in the UAE;

V. The presentation of electronic evidence in the UAE and the importance of expert reporting; and

VI. The authentication of electronic evidence in the UAE.

4.1 Collection of electronic evidence

The primary responsibility of law enforcement agents has been the investigation and

[1]Fred Galves and Christine Galves, 'Ensuring the Admissibility of electronic evidence forensic evidence and enhancing its probative value at trial' Spring (2004) 19, 1 *Criminal Justice Magazine* <http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html> accessed 17th February 2012.

[2]Michael Coren, 'Digital evidence: Today's fingerprint, Electronic world increasingly being used to solve crimes' (Cable News Network CCN 31st January 2005) <http://edition.cnn.com/2005/LAW/01/28/digital.evidence/> accessed 30th January 2012.

gathering of evidence.[3] The purpose of obtaining such evidence is to find a connection between the suspect and the crime, which has occurred.[4]

According to successive investigations, according to Bryant, the electronic evidence gathered is implemented in a supportive enquiry.[5] Stephenson noted that, in order for it to be admitted by the court, evidence should be legally and adequately collected.[6] Therefore, according to Bryant, the investigator should be an expert with experience utilising the methods necessary to gather evidence of this kind.[7]

First, an investigator must have a clear idea of how supporting evidence, as related to a crime is likely to be composed.[8] This means that the investigator must have adequate direction with regard to the search for electronic evidence, and recognise such evidence when it is found.[9] According to Gahtan, the investigator must have relevant information about how to select what software applications and computer systems should be searched to obtain evidence.[10] Lange and Nimsger, indicate that the process of finding electronic evidence is a complex one, as it is difficult to locate the evidence held in a computer storage system.[11]

This is mainly due to the intangible and often transient nature of the information and data, especially in a networked environment. Technology makes it possible to record information and data, but also renders the process of investigation for evidence vulnerable to defence claims of technical errors, detrimental interference, malfunction or fabrication. Such claims can lead to an admissibility of evidence ruling from the court.[12]

Hence, it is pivotal that the methods used to preserve such evidence are forensically sound and remains unaltered wherever possible. However, the acquisition of data,

---

[3]Debra Shinder and Michael Cross, *Scene of the cybercrime* (2nd edn, Arlington: Syngress Publishing Inc. 2008) 30.
[4]Anthony Reyes and Jack Wiles, *The Best Damn Cybercrime and Digital Forensics Book Period* (Syngress 2007) 12.
[5]Robin Bryant, *Investigating digital crime* (John Wiley and Sons Ltd. 2008) 50.
[6]Peter Stephenson, *Investigating computer-related crime* (CRC Press LLC. 2000) 88.
[7]Robin Bryant (n 5) 77.
[8]John Lentini, *Scientific protocols for fire investigation* (Taylor and Francis Group LLC. 2006) 115.
[9]Gregory Kipper, *Wireless crime and forensic investigation* (Taylor and Francis Group LLC. 2007) 58.
[10]Alan Gahtan, *Electronic evidence* (Carswell Thomson Publishing 1999) 31.
[11]Michele Lange and Kristin Nimsger, *Electronic evidence and discovery: What every lawyer should know* (2nd edn Chicago: ABA Publishing 2009) 23.
[12]Ian Walden, *Computer Crimes and Digital Investigation* (Oxford University Press 2007) 205.

which is stored on a hard drive, causes changes to the original hard drive, as is the case with most other computer systems and mobile phones.[13] As a result, it has become important to retain data on live systems; for example, in *Columbia Pictures Indus v Bunnell*,[14] the Court pointed out that discoverable information also extended to data held on Random Access Memory (RAM) on a Web server. However, this does not mean that investigators should be legally required to preserve all evidence, or that they should not be permitted to change anything; instead, investigators and forensics should be required to properly document the way they handle electronic evidence, so that the risk of that evidence being invalidated is at least minimised.[15]

Hence, the handling of the evidence and the documentation of the handling is key to establishing forensic soundness, although care should be taken to ensure that minimal changes are made to the electronic evidence, so that it remains accurate and authentic.[16] Furthermore, investigators, who deal with volatile electronic evidence, ought to additionally note down the date, the time and the tools, which they employed, as well as the MD5 hash value of the outputs.[17]

Another important concept when investigating cyber-crimes through electronic evidence trails is evidence integrity. Integrity is important for assuring the validity of the evidence and is normally established by comparing digital fingerprints taken when the evidence was collected with digital fingerprints taken at a later stage. This requires knowledge of cryptographic hash values and message digests, the latter consisting of an algorithm, which generates a particular number in relation to particular input. A different input generates a different number and this makes it possible to compare digital fingerprints, since a different number will be created for the same output if the digital fingerprint is changed.[18] MD5 and SHA-1 are frequently used algorithms that use a particular input and create a particular output, known as a message digest or fingerprint. For example, the MD5 algorithm employs the data to calculate a 32 letter and number combination code rendering duplication nearly impossible. The MD5 or

[13]Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn, Academic Press 2011) 19.
[14]*Columbia Pictures Indus v Bunnell* 2007 U.S. Dist. LEXIS 46364 (C.D. Cal. 19th June 2007).
[15]Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (n13) 20.
[16]Ibid.
[17]Ibid.
[18]Ibid, 22.

other algorithms prove to be useful tools for establishing evidence integrity and should be employed when carrying out a digital investigation; thus, investigators should document the MD5 value at the collection stage and subsequently, so that it can be established that the electronic evidence acquisition process has not altered the electronic evidence.[19]

However, MD5 and SHA-1 cannot establish whether the evidence has been altered by the person, who collected the evidence prior to generating the MD5 or SHA-1 value; that suggests that much depends on the integrity of the person, collecting the electronic evidence. MD5 and SHA-1 can also serve as class evidence or individual characteristics, since for example the value is placed in a class of similar parts. A unique MD5 value can serve as an individual characteristic, and is superior to a file name or size, as, instead of carrying out a keyword search, a hash value search can be conducted since an identical hash value can be used to identify files, even when the names do not match.

Another key aspect of any investigation is that it has to be objective and free of bias; this requires the evidence to be conclusive; Casey suggests that 'a peer review process' is undertaken, which scrutinises whether there is any prejudice or flaw.[20] Investigators should ensure that their findings can be repeated, so that they can be verified by independent experts. Therefore, it may therefore be useful to adopt a procedure that ensures an independent forensic expert can repeat the tests. This also requires that methods be documented, as this makes it possible for verification to take place.[21]

4.2 Search and seizure for electronic evidence

The objective of any investigation is to find the truth and prove the facts. All persons involved in gathering evidence must have these objectives in mind when searching for and seizing evidence. Regarding this, a question arises as to what the possible sources of electronic evidence are.

Undoubtedly, the identifying and probable confiscation of evidence is the first step in the gathering of electronic evidence.

[19]Ibid, 23.
[20]Ibid, 24.
[21]Ibid, 25.

Electronic evidence can be found in the following places:-

- Gateway log files and servers;
- Recycle bin folders or temporary folders;
- Instant messages or electronic mail;
- Records of times of user creation, access or deletion and;
- Internet/intranet folders.

However, in general, most data and information is stored on personal computers and company servers.[22]

After detection of adequate evidence, that evidence must be retrieved from the location.[23] An understanding of the vital foundations related to electronic proof is mandatory for helping the investigator to secure vital evidence.[24]

The ways in which the evidence detected is captured must be legal, otherwise the evidence loses its integrity and value, and the court may not accept it.[25] Moreover, Kanellis says that the general rule with a forensic procedure is to gather evidence securely and with extra care. This rule should never be neglected.[26] During the investigation, it is almost impossible for investigators to maintain the safety and security of electronic evidence.[27] Therefore, when collecting evidence investigators should keep in mind its importance in the criminal proceedings.[28] In legal proceedings, evidence that has been improperly handled is inadmissible.[29]

---

[22]Olen Hrycko, *Electronic discovery in Canada: Best practices and guidelines* (2nd edn, CCH Canadian Limited 2007) 143.
[23]Steve Anson and Steve Bunting, *Mastering windows network forensics and investigation* (Indianapolis: Wiley Publishing Inc. 2007) 11.
[24]Michele Lange and Kristin Nimsger (n11) 89.
[25]Christopher Brown, *Computer evidence: Collection and preservation* (2nd edn, Rockland MA: Charles River Media 2009) 47.
[26]Panagiotis Kanellis, *Digital crime and forensic science in cyberspace* (Idea Group Publishing 2006) 58.
[27]Ibid, 273.
[28]Debra Shinder and Michael Cross (n 3) 211.
[29]Steve Anson and Steve Bunting (n 23) 11.

4.2.1 Search and seizure for electronic evidence: procedural aspects of the UAE's legal system [30]

In the UAE, procedures with regard to the investigation and gathering of evidence are given in Part III of the UAE's CPL. Chapter 1 clarifies the process of investigation; Article 30 explains the gathering of general information about crimes and evidence by the police; Article 35 explains the reporting of crimes, and Article 36 details the documentation procedures. Chapter IV outlines several provisions that give powers to the police to search and seize evidence under the supervision of the prosecutor. Articles 51, 52, 53, 54, 55, 56, 57, 58, and 59 explain the search for evidence; Articles 60 and 61 cover the seizure of evidence. All these procedures comprise the general rules for all crimes and offer no guidelines as to best practise. In other words, they cover traditional crimes such as theft, rape and murder as well as crimes involving the use of information technology. An interviewee who practices as a forensic expert at the Telecommunication Regulatory Authority of the UAE supported this finding. When asked, in what manner it can be said that the UAE's CPL is appropriate to cover electronic evidence, he stated:

> I believe electronic evidence needs special care, because electronic evidence has a different nature and criteria. For example, if we need to seize a computer, which is a tool of crime, we can use general rules of search and seizure. However, if the evidence cannot be found on that computer it could be in another place, so we need take other procedures. As a result, I think it becomes extremely difficult to seize electronic evidence by general rules of the UAE's CPL.[31]

The problem of a lack of guiding principles for the search and seizure of electronic evidence proceeds from the ease with which electronic evidence can be altered, lost or destroyed. For example, the RAM in a computer will contain a great deal of information relating to the state of the computer, such as the processes that are running, whether it is connected to the Internet, and what file systems are being used. Immediately that a computer is switched off, a large part of this volatile data is lost. In an interview

[30]This section is based on the content of an article has been published as: Khaled Aljneibi, 'Search and seizure for electronic evidence: procedural aspects of UAE's legal system' (2013) 10 *Digital Evidence and Electronic Signature Law Review*.

[31]Ahmed Al Ketbi, forensic investigator at Telecommunications Regulatory Authority of the UAE, Interview conducted (January 2013Dubai-UAE). See: transcript of the translated interview with Al Ketbi in Appendix 5.

conducted in the UAE, one of the interviewees interviewed by the researcher stated:

> We use traditional methods when dealing with technology; we use no update rules when evidence is seized, we do not use databases to ensure preservation of evidence etc. All of this could lead to lots of opportunity to prove and discover crimes. For example, switching off the electricity when seizing a computer can lead to the loss of evidence. [32]

4.2.2 Search and seizure for electronic evidence: with a warrant [33]

If a person is accused or suspected of a crime, it is important for the investigator to present suitable evidence against that person. His home or office can be searched to establish where there is any incriminating against him. In the case of the presence of considerable evidence of proof of the crime, the evidence of that crime must be confiscated.[34]After seizing the evidence, investigators must put all the relevant devices in a bag and seal it to be sent to the laboratory.

When defining search-warrants, one needs to elucidate the sphere of influence of the investigatory methods. Legal judges and scholars have a broader scope at their disposal to explain search warrants. This can be defined as a private area, used to discover obsolete and hidden material that is necessary for conducting an investigation.[35]

Arcaro regards it as a written document that provides judges with the authority and enables officers to enter and search a specific place for a specific item.[36] Moreover, it gives them the authority to confiscate offensive items of evidence. Thirdly, search warrants are also defined as documents intended for searching for evidence in a private place.[37]

Evidence is initially collected by the investigators and police, typically, after the crime has taken place. In the course of collecting evidence, investigators not only interrogate but also search items, confiscate evidence, enter private property and detain and arrest suspects. Search warrants must be obtained from the authority that has the appropriate

---

[32]See: translated transcript of the interview with Professor Elbushra in Appendix 5.
[33](n 30).
[34]The UAE Criminal Procedure Law, Article 75.
[35]Amal Osman, *Criminal Evidence and Scientific means of Investigation* (Dar Nahda Al Arabiah, 1975) 4. (Author's translation from the Arabic).
أمال عثمان، الاثبات الجنائي ووسائل التحقيق العلمية (دار النهضة العربية مصر1975) ص 4.
[36]Gino Arcaro, *Basic Police Powers: Arrest and Search Procedures* (4th edn, Emond Montgomery Publications 2009) 222.
[37] Ibid.

power to issue notices. Police must acquire a permission letter before commencing the search. [38]

The search warrant must be obtained to gather sufficient information for obtaining sufficient and appropriate evidence. This evidence helps to confirm that the accused person is responsible for the crime. The evidence collected during the course of an investigation is crucial. The law extends privacy in the public interest and that of the parties, as is their legal right, by keeping evidence confidential. [39]

In line with the CPL, after receiving a report from the complainant, the police investigator will search and seize the suspect's computer for data recovery purposes. Article 30 of the CPL provides that: '… the judicial police shall inquire about crimes, search for their perpetrators and collect the necessary information and evidence for investigation and indictment'. Police search and seizure must be carried out properly, because it determines the admissibility of any evidence presented in court.[40] Thus, before any search or seizure of evidence can be carried out, a police investigator must take into consideration that she or he needs to obtain a search warrant, as set out in CPL Article 53:

> 'The judicial police officer may not inspect the dwelling of the accused without a written authorization from the public prosecution unless the crime is in the process of being of committed and there are strong indications that the accused is hiding in his house, objects or papers which may lead to the truth ...'.[41]

This Article provides that any search for evidence requires a search warrant that has been issued by a public prosecutor.

The CPL outlines several requirements for obtaining a search warrant. Committing a

---

[38] Jodat Jihad, *Brief explaining of the UAE Criminal Procedure Code* (2nd edn, Dubai Police Academy Publications 2008)18. (Author's translation from the Arabic).
جوده حسين جهاد،الوجيز في شرح قانون الاجراءات الجزائية لدولة الامارات (مطبوعات أكاديمية شرطة دبي،الطبعة الثانية 2008) ص 18.

[39]Mahmoud Mustafa, *Explain Criminal Procedure Law* (Dar Nahda Al Arabiah1998) 240. (Author's translation from the Arabic).
محمود مصطفى، شرح قانون الاجراءات الجنائية (دار النهضه العربية، مصر1998) ص 240.

[40]In any event, for the evidence to be admissible, it must be judicial and legitimate. See: section 2.2.4.1.

[41]The UAE Criminal Procedure Law, Article 53.

crime is the first of these.[42] The commission of a crime gives the prosecution the assurance that a crime has occurred and needs to be investigated. Moreover, it must be demonstrated that the crime committed is of a grave nature and punishable. A search warrant cannot be obtained if no crime has been committed. There is also no need to obtain a warrant merely to assuage doubt.

Hence, to issue a search warrant, the crime must be categorised as a felony or misdemeanour, that if proven would incur a prison sentence. The criminal law of the UAE classifies punishments into three categories:

1. Felonies, punishable by three years or more of imprisonment, or by death.[43]

2. Misdemeanors, punishable by a minimum of one week to three years in prison, or by a fine not exceeding 1000 Dh.[44]

3. Petty misdemeanors, punishable by a minimum of 24 hours to 10 days in prison or by a fine.[45]

It is important to draft and execute the search warrant in the light of the requirements for electronic evidence collection. Hence, the officer involved in the search process must take great care when applying for a search warrant.

4.2.2.1 The subject of search warrants [46]

Normally, search warrants are intended for the search and seizure of physical items. The search warrant is meant to facilitate the acquisition of the fruit of the crime, related objects and instrument, for instance cash, drugs and stolen property. The investigator searches all areas covered by the warrant and confiscates any objects obviously or likely to be related to the crime.

Regarding the seizure of evidence, the CPL does not mention the requirement to list the things that have to be seized. This is possibly due to the nature and scope of the CPL, in that it covers crimes in a general sense. Article 61 of the CPL provides that:

---

[42]Ibid, Article 72.
[43]The UAE Federal Penal Code, Article 28.
[44]Ibid, Article 29.
[45]Ibid, Article 30.
[46](n 30).

> '… The judicial police officers have to sequestrate the objects which may have been used in the perpetration of the crime, resulted therefrom or if the crime has been committed thereon; in addition to whatever may lead to the truth in the matter'. [47]

Taking into account the broad scope of Article 61 of the CPL, it can be said that an electronic device may be seized pursuant to a search warrant.

As a result, the seizure of materials outside of the search warrant will not entirely negate that seizure. However, it is suggested that because electronic evidence can be found on physical items such as CDs, diskettes and computer hard drives this justifies the seizure of these physical items for further investigation to follow the electronic trail associated with the gathering of additional evidence. As a head of the Electronic Evidence Unit at the Criminal Evidence and Criminology Department- Dubai Police, noted:

> There is no doubt that electronic evidence has a different nature from other evidence. As an example, fingerprints indicate the offender's presence in a place and do not need an explanation or analysis. However, it is not easy to determine electronic evidence locations.[48]

The other issue of concern relates to what to seize, and can be compounded when an entire computer system or a computer linked to a network and sources of electronic evidence exist in a number of different geographical locations. For instance, it is usually necessary to establish the number of computers on a network, and the different types of network connections, such as the internet, e-mail, cellular data networks and wireless connections. In addition, it may also be necessary to establish whether or not there are any third party services on the internet that can be used to store data remotely. Data can be deleted on the remote server before being captured.

4.2.2.2 Scope of the search warrant [49]

The sphere and influence of items to be searched and that are liable to be seized are defined by the search warrant. [50]

---

[47]The UAE Criminal Procedure Law, Article 61.
[48]See: translated transcript of the interview with Lootah in Appendix 5.
[49](n 30).
[50]Mahmoud Mustafa (n 39). (Author's translation from the Arabic).
محمود مصطفى، مرجع سابق .

Law enforcement officers should describe the evidence and materials that are the subject of the search warrant, as officers can only confiscate objects covered by the search warrant.[51] The search warrant can be regarded as a map or guide to use to perform a short and immediate investigation.

Different search warrants are issued to secure two different classes of evidence, hardware and software. A computer is made up of two critical components. One is the hardware and the other is the digital component. Computer monitors, storage devices, and motherboards are examples of hardware. Programs and other data in soft form are examples of software. Each component is interdependent and cannot be used in isolation. Procedures used to use investigate these two vital components of computers are distinct. Highly sophisticated forms of data are stored in digital form, in programs, and the hardware component is the container-storage device. Data can include information that should not be dispersed, instruments of crime and evidence, etc. Consequently, in the case of hacking a computer system, the hardware cannot be regarded as criminally illegal, or as having evidential use or being instrumental in the criminal act. The hardware is merely the location of the crime. In such circumstances, investigators should obtain search warrants to form mirror copies of hardware, rather than confiscating it.[52]

The obtaining of evidence is difficult when the evidence searched for is part of a complicated network, as in the case of a local area network. Although it is not a difficult task for an investigating officer to seize the entire suspect infrastructure, network, peripherals and PC-workstations, this is not necessarily practical, as it will affect the business or the offices of the organisation, to such an extent that business might cease.[53]

It is complicated and problematic to locate electronic evidence. It is particularly important to carefully search for influential data. Mostly, investigating officers face a

[51] Jodat Jihad (n 38) 359. (Author's translation from the Arabic).
جوده حسين جهاد، مرجع سابق، ص 359.

[52] US Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2009) 43.

[53] This is a significant topic, and the reader might begin by considering the following US technical texts, as well as the relevant practitioner texts written by lawyers: Eoghan Casey (n 13); Carl Franklin, *The Investigator's Guide to Computer Crime* (Charles C Thomas Publisher 2006); Ralph Clifford, *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime* (3rd end, Carolina Academic Press 2011).

large amount of tangled data and are in only limited contact with the real investigation. Much of this data is irrelevant to the subject of the investigation, or to those who are not accused as culprits or the crime act evidence.[54] Moreover, searches may cover legal data or privileged files. These incidences unavoidably expand the sphere of the influence of the search beyond the boundaries of the search warrants. This only occurs when the search subject's documents are not fully incorporated in the warrant.[55]

Specifically this may be when the investigating officer is oblivious to the scope of the search documents, or it may be due to the practical difference between diverse documents and the criminal data.[56] Conducting a complete examination of the crime site and a forensic investigation can be assisted by making a mirror copy of a hard drive. However, with information present that is not relevant to the investigation, the difficulty is separating important data from surplus.[57] Consequently, nowadays scholars and the courts minutely examine the scope of searches. There is dual point of view here, which focuses on the language and nature of the warrant. In some cases, warrants may be concealed when searching for something specific.[58]

The next approach to the subject is the anti-particularity approach and is supported by many scholars. Franklin says that in cases where individuals have a lot of time and uncertainty at their disposal one may adhere to an extensive and understandable search warrant. This can assist in sorting the evidence. Moreover, he says that if it is going to be possible to locate the desirable evidence it is important to limit the search warrant.[59] Clifford states that the computer related data might be added to the search warrant.[60]

Computers can help when searching different forms of data hidden on another computer. This can limit extra time needed and financial costs incurred when executing searches. The skill of the cybercriminal means that they are able to conceal evidence that incriminates them more effectively than traditional criminals, thus technology

---

[54]Ibid.
[55]See: Susan Brenner and Barbara Frederiksen, 'Computer Searches and Seizures: Some Unresolved Issues' (2001/2002) 28 *Michigan Telecommunication and Technology Law Review*.
[56]Ibid.
[57]Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (n13) 110.
[58]Jonathan Jacobson, *Antitrust Law Developments* (6th edn, American Bar Association 2007) 740.
[59]Carl Franklin (n 53) 162.
[60]See: Ralph Clifford (n 53) 134.

based searchers are essential.[61] Furthermore, such searcher can help officers to recover files deleted by the criminals. The mirror copy approach is quite helpful here also.

With regard to where the authorities might conduct the search and seizure process, Article 51 of the CPL states: '... Inspection means the search of the body, clothes or luggage for any trace or things related to the crime or required for the investigation'. Thus, the police investigator is only allowed to search a suspect's body, clothes, luggage or things. The word 'things' in Article 51 of the CPL is defined widely enough to cover searching a computer to find electronic evidence because a computer falls within the scope of the word 'things'.

The main question arising here is whether computer software is also subject to inspection on this basis. Although the wide scope of the word 'things' in Article 51 of the CPL, would allow computer software to be inspected, between 1992 (the date of issue of the CPL) and 2013, this provision was not tested. There remains a need to test that the word 'things' covers electronic evidence.

Conversely, the national legislation of countries such as France, the US, Canada and the UK, incorporates rules governing the search for evidence from computers. In France, Article 57(1) of the France Criminal Procedure Code inserted by Law No.239-2003 allows judicial police officers, or judicial police agents under judicial police supervision, to access computer systems and search for any data stored on a suspect's computer or other computer systems, provided the data is accessible from the initial system or is available to the initial system. In the US, the Federal Criminal Procedure Act 1930, after amendment, extended the scope of inspection to include computers, phones and other electronic devices. In Canada, section 16 of the Competition Act allows a person who has been authorised, to search any data contained in or available to, a computer system. In the UK, section 1 of the Computer Misuse Act 1990 allows authorities to search computer software.

To draw the preliminary limitations of a search is a difficult task. It is important that it is structured to help get evidence outside of the knowledge of the officer. It may assist in concealing, disguising and encrypting the evidence. Thus, limitations to the

[61]John McLean, 'Homicide and Child Pornography' in Eoghan Casey (ed), *Handbook of Computer Crime Investigation* (Academic Press 2010) 361-373.

investigation resulting from the search may create hurdles in the process of searching and confiscating electronic evidences. Moreover, it can bring an untimely end to police collection of evidence.

Consequently, law-enforcement officers frequently employ the mirror-copy approach when conducting forensic investigations. In the UAE, officers can create a mirror copy and perform limitless searches under the extensive language of the UAE's CPL. However; this can only be done in cases of non-availability of provisions to perform the work. Admittedly, police officers are offered a broader horizon to perform the task. These are not limited by specific rules affecting their actions when seizing and searching items. These officers are empowered to confiscate anything that they suspect to be relevant to the investigation, aside from items directly related to the evidence. This grants flexibility to investigators when performing research, something that is vital when managing the novel characteristics of electronic evidence.

4.2.2.3 Execution of the search warrants [62]

The act of executing a conventional search warrant precedes the searching of in some cases, where a warrant is necessary to grant entrance to and search of a site.[63] Traditionally, executing a search warrant occurs in three stages. First, to knock and notify, second, to observe the place of the search to insure a search pattern that is applicable to the crime scene.[64] For instance, searching small places such as bedrooms is regarded as a zone search, while a search of a larger or outdoor space, for example a backyard, may be require a grid search.[65]Conducting a search occurs in the second stage: for instance, searching and dragging items in order to open and empty containers.[66]

Entering the property defined on the warrant without permission is the final stage, when evidence is collected and confiscated.[67] Searches for the evidence are made thoroughly. The search operation is carried out as per the techniques established in the previous stages.

---

[62](n 30).
[63]Gino Arcaro (n 36) 232.
[64]Ibid.
[65]Ross Gardner, *Practical Crime Scene Processing and Investigation* (2nd edn, CRC Press 2012) 125.
[66]Ibid.
[67]Ibid.

In contrast, the execution of an electronic evidence search warrant relates to the execution of the procedure of forensic data analysis. This search is categorised as either a pre-digital or a digital search. The former refers to site-based searches and is regarded as an initial stage when compared with a traditional search. It is sub-categorised into two stages: first, as the means to notify and observe the search location's tangibility, and second to nominate the mechanism for an accurate search. In the final stage, it will identify the specific digital devices covered by the search warrant and media, such as documents, audio recordings and video events. [68]

These processes are essential to show that initial responders do not corrupt the crime scene. They also provide evidence in real form. Moreover, they track the evidential collection process from the real data to that to be shown in the courtroom.[69] The next sub-stage includes a specific process related to the computer hardware. For instance, labelling computer wires, connections and power endings. This is something frequently suggested by most forensic investigating officers.[70] To save and close certain programs like RAM running programs is necessary to implement these procedures. [71] RAM preserves the temporary data and helps it to travel between the internet and hard disk. Admittedly, if the power is switched off any temporary data not properly saved in the RAM will be lost.[72]

It is necessary to give due importance to operating systems such as Linux, UNIX, Macintosh and Windows XP, 7 and 8. Every system employs a different mechanism to store and run the files previously preserved in the RAM.[73] For instance, in a Windows Operating System, if the computer is shut down the RAM data will be immediately removed.[74] It is important to label all the cables attached to the computer. This is to

---

[68]Hilali Abdullah, *Inspect Computer Systems* (Dar Nahda Al Arabiah 1997)125. (Author's translation from the Arabic).

هلالي عبدالله، تفتيش نظم الحاسب الآلي (دار النهضة العربية مصر 1997) ص 125.

[69]Jay Siegel, *Forensic Science: The Basics* (Taylor and Francis Group 2007) 43.

[70] Anthony Reyes, Kevin O'Shea, Richard Brittson, and James Steele, *Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors* (Syngress 2007) 147-149.

[71]Ibid.

[72]Scott Mueller, *Upgrading and Repairing PC* (20th edn, Que Publishing 2011) 417.

[73]Ibid.

[74]Allen Kent, James Williams and Albert Holzman, *Encyclopedia of Computer Science and Technology* (Marcel Dekker Incorporated 1987) 161.

facilitate reassembly of the computer system.[75]

The next cyber search stage is digital searching. This does not rely on tangible movements when executing a search. This is because it works with the help of the data. Moreover, it employs certain novel off-site processes that can be adopted by the investigating forensic officer.[76] No doubt, different people at different times employ diverse methods to achieve and explore evidence. This can be done by exploiting the hardware devices confiscated in the initial stages. It is important for investigating officers to keep themselves abreast of computing developments. This can help them to differentiate between database programmes, electronic mail files, telephone lists, as it stores visual and audio data from one to the other. The evidence gathered at this stage is necessary to insure positive outcomes from the crime or the crime scene object. The historical data provided on the defendant's computer can show the demographics of the data accessed by the hackers. The second type refers to child pornography, spoof website-making tools, etc. Both of these searching stages are distinct but related. The pre-digital processes are likely to have an implicitly negative impact upon the digital searching procedure. It is important to apply the notifying processes in a narrow manner, since it is responsible for informing residents when executing search warrants. Concealing the scope of the warrant will prevent the suspect from destroying, contaminating or hiding criminal evidence.[77] Consequently, it is important for the initial responder to secure the site of the crime and the digital and tangible searching sites in case of the application of procedures of announcement.

Physically it is crucial to prevent the suspect from reaching the crime scene and search sites. Moreover, people must be prevented from reaching and accessing cyber data by the various means afforded by wireless connections and networks.[78] Certain techniques can be adopted to protect the seized data, such as disconnecting phone lines, inspecting booby-traps placed on the computer and terminating the network connections between

[75] Robert Moore, *Search and Seizure of Digital Evidence: An Examination of Constitutional and Procedural Issues* (University of Southern Mississippi 2003) 86.
[76] Orin Kerr, 'Search Warrants in an Era of Digital Evidence' (2005) 75 *Mississippi Law Journal* 85-91.
[77] Ralph Clifford (n 53) 135.
[78] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (n13) 627.

crime scene computers.[79]

O'Shea described at least one area of danger. He stated that it is crucial to bridge the gap between prosecutors, law enforcement and security professions.[80] He believes that some clues are more helpful that others for identifying digital media's tangibility, because it allows the processing of important opportunities to acquire evidence in the form of data. This data may be included in search warrants.[81] For instance, in a case where there are two computers involved in a hacking investigation, for instance if the suspected family has two computers one in the lounge and one in the bedroom, the investigating officer may first confiscate the computer placed in the bedroom.[82]

Moreover, it is usually difficult to predict the location of electronic evidence due to computer networking. He underscores the fact that criminals and subjects being investigated must show an accurate digital container to the investigating officer.[83] For instance, when investigating a case of child pornography, officers should aim to collect evidence from a large container, such as a removable disk or hard drive.[84]

It is important for investigating officers to examine digital media thoroughly instead of relying upon clues. Officers may choose to access electronic crime scene evidence using wireless techniques, even at the time of a crime site inspection.[85] The greatest problem when using a designed network connections is that any outsider can destroy or control the crime scene evidence, even remotely. They can do so by erasing data and implanting false evidence. For instance, a new cybercrime called piggybacking can use wireless network connections to attain a wire free connection.[86] Certain processes are considered as tampering with evidence of contamination and involve wire-free methods, such as applying certain methods to preserve the crime site and the search subject.[87]

---

[79]Anthony Reyes, Kevin O'Shea, Richard Brittson and James Steele (n 70) 142.
[80]Ibid.
[81]Ibid.
[82]Ibid.
[83]Ibid.
[84]Ibid, 145.
[85]See: Gregory Kipper (n 9) 58.
[86]Ibid, 17-21.
[87]James Byrne and Donald Rebovic, *The New Technology of Crime, Law and Social Control* (Criminal Justice Press 2007) 29.

In the UAE, search warrants can only be incorporated and implemented by the prosecuting officer. It is the public prosecutor's role to execute the search warrant personally, or to give it to the investigation officer and the police officers enlisted in Article 33 of the CPL. Where the public prosecutor hands the execution of the warrant over to police officers, it is obligatory for these officers to follow the warrant and execute the procedural instructions of the public prosecutor. Moreover, they must execute the warrant under the rule of law and within the scope timeframe specified. Under UAE statutory law, there are no time limits for search warrants; the public prosecutor when issuing the search authorisation will define the search time.

The CPL authorises police officers to search and seize evidence because they represent the competent authority. However, searching and seizing electronic evidence requires not only an authorised person be present but also an appropriately qualified person.

The CPL outlines several provisions, which authorise the police to report on criminal cases, enabling them to gather information, take statements, carry out searches of premises and equipment, seize evidence, execute summons and warrants and conduct prosecutions. There are no rules in the UAE regarding the necessity for qualified digital evidence specialists to accompany the police officer searching for electronic evidence. Thus, the possibility of loss of electronic evidence may be high due to lack of experience or skill.

In addition, observance of legal requirements, such as the need for a search warrant and police officers to engage in search and seize activities in the hunt for evidence is particularly beneficial, because any contravention of the law or a court order will result in irregularity that may effect the evidence derived from the seized computer. Moreover, if the knocking and notifying technique is applied to a site search it will place the integrity of the undiscovered evidence in jeopardy. This is because the suspect can easily destroy the electronic evidence utilising simple techniques like Hotkey (a technique that uses a combination of different computer keys, like Shift-Ctrl-A, to permit the user to implement keyboard specific applications). A search process can be easily executed by conducting surprise visits and adopting snooping techniques. These will help assist the police in avoiding the concealing and destruction of evidence. Consequently, it seems that a sneak and peek search warrant may be preferred over the

classical knock and notify warrant when there is a need to perform a more thorough search.

With the advancements that have occurred in information technology, a change in the pattern of criminal offences has been seen. This means that current laws are not as effective as they were previously. The American Patriot Act [88] and the Australian Crimes Act of 1914 contain a series of exclusions and corrections made in response to recent crimes, such as rules associated with sneak and peek search warrants. Significant legal orders have been established to keep pace with the changes to the pattern of search warrants.

According to the Australian Crimes Act of 1914, the system of search warrants has been altered and the officer carrying out a search is required to provide notification in advance when carrying out a search.[89] It is also mentioned in section 3H of the Australian Crimes Act of 1914 that an officer carrying out a search must reveal his identity and produce a search warrant. The search warrant should contain all relevant data related to the search, including the title of the officer, and the date and / or place of the warrant's issuance. It is also decreed that the officer should show himself to the suspect when the search is carried out.[90] There are cases, however, when officers have been allowed to go inside a residence without prior notice or declaration.[91] According to the new legal order presented to the Federal Parliament, officers will also have the authority to enter premises and carry out a search without an announcement.[92] The Crimes Act claims that officers have the right to keep all necessary instruments ready when carrying out a search. These instruments are to be used to inspect and evaluate information, in order to decide whether or not it should be confiscated.[93]

The conventional process of informing the suspect of a search operation increases the risk of losing potential evidence, as the suspect is likely to delete it. Deleting electronic evidence is extremely easy; it takes just a single click. Section 213 of the Patriot Act in the USA makes it legal for officers to run a search without making an announcement.

[88] The US Patriot Act, 18 USC 201-16 (2001).
[89]The Australian Crimes Act 1914, s 5 S 3ZS (1) (A).
[90]Ibid, s P 1AA Div 2 S 3H (4).
[91]Ibid, s Div 5 S 3ZS (2).
[92]Tom Allard, 'New Secret Search Powers' (the Sydney Morning Herald (Sydney) 1st August 2007) <http://www.smh.com.au/articles/2007/07/31/1185647903263.html> accessed 20th September 2013.
[93]The Australian Crimes Act 1914, s 3k (1).

The officer can look into, save and transfer data (which might be potential evidence) without informing the owner of the premises, or any other person present at the time of search. It must, however, be confirmed that there is a chance that were the search announced the suspect would delete all potential evidence before this type of search being carried out. While it is more efficient to search without prior notice so that the suspect is taken by surprise and cannot delete any evidence, searching without warning should be restricted to protect people's privacy.

4.2.2.4 Search location [94]

Today computers have emerged as an important constituent of a person's life. Everyone ranging from individuals and organisations to the public and private sector are dependent upon computer systems to perform their day-to-day activities. For instance, certain activities like financial transactions, communications, and internet-based social events, banking, shopping, social networks; entertainment and education are performed via computers. Police officers often remove hardware devices such as CDs and floppy disks, to perform off-site examinations of a crime scene.

Consequently, most searching and confiscating processes have both a specific and a general effect on the person or organisation that is the subject of a search. This is because digital techniques nowadays serve as crucial to conducting a business. In the case of the interruption or deprivation of these, businesses can suffer harmful effects. Concisely, one can say that a majority of people, organisations and businesses are now engaged in computer-based or computer-reliant ventures. In such circumstances, it is difficult for the police officer to conduct on-site and off-site searches for an extended period time. Indeed, most businesses are against the removal of computers off-site. This stance is the result of fear of losing their position in the market due to loss of technology and information upon which their work activity depends. Consequently, the site of a search tends to result in practical difficulties when performing a search and confiscating both crime scene and external evidence. The execution officer's analysis of a crime scene is necessary to conduct an onsite electronic evidential search. This can help them with gathering information available relating to the search warrant.[95]

---

[94](n 30).

[95]Some of the problems are illustrated (amongst other authors) by Anthony Reyes, Richard Brittson, Kevin O'Shea and Jim Steel, *Cyber Crime Investigations Bridging the Gaps Between Security*

Moreover, it is probable that investigators will conduct an on-site search by accessing different files and folders and examining hard-copy documents and the properties of the files.[96] For instance, when conducting cyber-stalking offences, a person may employ e-mail and chat rooms to perform victim harassment.

Information is usually saved in the RAM of a computer, so in the case of issuance of a search warrant against the computer of an offender, the investigating officer may conduct a wholly on-site search.[97] It is important to do this because RAM is a volatile and non-permanent storage device. If the power supply to the computer is cut off, the entire RAM data is deleted.[98]

An off-site search may be defined as a laboratory search. This takes place when the investigating officer shifts an entire set of computer-based data such as documents, files, and programs to a laboratory setting to conduct a thorough search, in order to obtain evidence and exclude unnecessary data.[99] There has been much debate over on-site and off-site search performance among investigators, forensic officers and scholars. It is argued that officers may face certain technical and logistic restrictions when conducting search operations. This may arise due to processes such as electronic evidence recovery and analysis procedures, which generate a potential for research.[100] Therefore, off-site search is recommended by US DOJ guidelines in general and by most forensic officers in particular.[101]

It is mostly argued that certain extraneous variables are controlled in a better way in laboratory settings, rather than at search locations. For instance, such circumstances as time, expert and technical assistance, temperature, and resolving password protection problems are easier in a laboratory setting.[102] However, Bernner believes that it is not important to perform off-site cyber searches.[103] She argues that adaptation of automated search techniques, for instance key-word searches, is more time effective than the hard

---

Professionals, Law Enforcement, and Prosecutors (Elsevier/Syngress 2011); Susan Brenner and Barbara Frederiksen, 'Computer Searches and Seizures: Some Unresolved Issues' (2002) 8, 39 *Michigan Telecommunication and Technology Law Review*.

[96]Ibid.

[97]Anthony Reyes, Kevin O'Shea, Richard Brittson and James Steele (n 70) 169.

[98]Allen Kent, James Williamsand Albert Holzman (n 74) 161.

[99]Susan Brenner and Barbara Frederiksen (n 55).

[100]Ibid.

[101]Peter Toren, *Intellectual Property and Computer Crimes* (Law Journal Press 2003) 8-27.

[102]Anthony Reyes, Kevin O'Shea, Richard Brittson and James Steele (n 70) 169.

[103]Susan Brenner and Barbara Frederiksen (n 55).

drive searching approach.[104]

The UAE public prosecution has greater authority to execute search warrants. They are authorised to decide the place of a search and whether it should be conducted on-site or off-site.[105] In practice, the effect of searching and seizing electronic evidence on businesses and third parties is ignored under the searching procedures prevalent in the UAE. This is due to the lack of limitations upon the authority of the investigating officer. The execution officer is regarded as the leader and expert when assessing relevant methods to employ to execute the search warrant under the CPL.

Consequently, it is important to give the issue due importance rather than not. No doubt, UAE-based investigating officers may continue to enjoy the authority to create a mirror copy and other crime scene evidence for a detailed search. However, this authority should be situation specific. It should not be applied in impractical situations under which it is impossible to perform a site-based digital search. It is important for law enforcement officers to demand off-site search permissions in their search warrants. Justifiably, a search may be done on the grounds that the crime scene search is usually less achievable and because of the absence of other relevant method. The concisely-designed criminal procedural laws serve as a basis for a more effective and efficient crime investigation. The reason behind this is that it underscores the new quality of evidential searches. In the case of obtaining electronic evidence, many of the searching and confiscating rules have become inappropriate and inapplicable. The best may be taken from a range of other jurisdictions and may serve as a role model for UAE electronic searching techniques, thus they may gain assistance from them for the effective search and confiscation of evidence.

4.2.3 Search and seizure for electronic evidence: without a warrant [106]

Laws and judicial regulations should be followed to collect electronic evidence. These regulations are the same as those followed when collecting physical evidence. The reasons for developing and following these standards are not only that personal privacy is maintained but also that appropriate and reliable evidence is collected. Hence, laws have been developed that permit investigators to enter a person's private property using

[104]Ibid.
[105]The UAE Criminal Procedure Law, Article 53.
[106](n 30).

search warrants and to call for the accused after issuing subpoenas to obtain sufficient and appropriate evidence. There are also exemptions available to the law. These exemptions are constructive from the perspective of the accused, as they have prevented investigators from entering their private property to collect evidence, on several occasions. Warrants for searches are very important in those situations where obtaining evidence is very critical for case proceedings. However, search warrants on the other hand play a crucial role in preventing human rights violations. Admittedly, if the law is not embedded with such exceptions then it is not easy to apply provisions to provide timely justice based in truth.

In conclusion, statute law not only ensures the privacy of accused persons but also bestows officers, who assure laws are in place, with unprecedented powers. [107]

These exceptional powers do not require official search warrants for confiscation and search, and some exemptions become impractical when warrants are obtained. This may make it apparent that a crime has occurred. Hence, with the help of judicial precedents and statutes, an investigator can enter private premises without any authorisation or official search warrants.

In line with the CPL, the police are allowed to enter a suspect's premises and search for relevant materials without the provision of a search warrant. These circumstances are provided for in Article 53 of the CPL: '... The crime is in the process of being committed and there are strong indications that the accused is hiding in his house objects or papers which may lead to the truth'.[108] In this situation, the police need not obtain a search warrant. The second exception provided for in Article 54 of the CPL covers the situation in which:

> '… The judicial police officer, even in cases other than a crime that is in the process of being committed, may inspect dwellings of persons put under surveillance, either according to a provision of law or a decision by a judge, should there be strong indications that they may be suspected of perpetrating a felony or a misdemeanour'.[109]

---

[107]Mohammed Abdull Mohsen, *Protection of the Private Life and individuals Rights facing computer crimes* (Al salasel for printing and publishing 1992)11. (Author's translation from the Arabic).
محمد عبدالمحسن، حماية الحياة الخاصة للافراد في مواجهة الحاسب الالي (ذات السلاسل للطباعة والنشر 1992) ص11.
[108]The UAE Criminal Procedure Law, Article 53.
[109]Ibid, Article 54.

Searches conducted without a warrant, and confiscation of electronic evidence is not entertained in the CPL. For historical objects, law enforcement officers and public prosecutors are bound to follow the law in warrantless searches. For example, as occurs when the wrong key is put into a lock, and the key fails to open the lock. However, there are no circumstances, for instance, in which there is authority issued to seize data where that data may become lost. There are no options available to avoid the destruction of software and hardware components. Digital material is more vulnerable to searches through digital media.

4.3 Impact of other laws in relation to electronic evidence: regional issues

Due to the unseen and temporary nature of electronic evidence, the collection of such evidence to investigate crimes, and in order to the prosecute criminals involved in such crimes can be challenging. This is especially the case in a networked environment, which is based in different localities. This is due to the globalisation of the cyber-crimes. Therefore, the collection of electronic evidence has become a challenge for regulators due to the 'location problem'. Major jurisdictional issues can arise due to the temporary nature of crimes, and the fact that people and evidence in different countries can be involved. Relevant evidence may be available on a server, which is in another location, while the person who carried out the crime and the person accused of it are in the same jurisdiction. The case of *the Queen v. Steven Hourmouzis* supports this argument.[110] In Australia, in 1999, Hourmouzis sent between six and seven million emails dispersing misleading financial information, causing the price of the Rentech company shares on the US NASDAQ to double. Steven then sold his own shares in the company and made a profit of $17,000 before the information was repudiated and the price of the shares fell. However, because the case was subject to a criminal prosecution requiring a high standard of proof, the prosecution was compelled to prove the time of the incident, its location, determine the jurisdiction, identify the method, and find and gather evidence. The case showed the ease of access to millions of online victims at no financial cost to the criminal. It also demonstrated the problems involved in gathering evidence to prove a case and in determining judicial authority and competence.

Practical examples of this issue in the UAE arose when the Dubai police received a

[110] *R v Hourmouzis* (unreported Victorian County Court, decided 30th October 2000) 85. See also: *SEC v Hourmouzis* (unreported, District Court of Colorado, no 00-N-905 decided 1st May 2000) 85.

report that there was hacking on a company's exchange, the system had been breached and funds transferred out of the state.[111] In another example, a European hacked a company in the UAE and addressed its customers through email, asking them to change their bank account numbers, and sending them his account number. The accused managed to grab three million dollars. The company discovered the penetration when they received emails from customers asking for goods that had not arrived. These issues are still being prosecuted, due to the difficulty obtaining evidence from abroad.[112]

The location of the crime is the first problem faced. As per the common international law principle, a trial must take place in the same state territory that the crime was committed. However, the law of criminal territory does not synchronise with the sovereignty of the territory. According to the law in the UAE regarding the determination of jurisdiction, when any person commits a crime in any jurisdiction of the state which can include any part of the land, water or even air space under the country's sovereignty, this law is applicable to them. If the crime or any part or activity related to that crime is committed, or if the result has been, or is intended to be, realised therein, than the same law is applicable.[113] This concerns the site where the crime occurred, but to add crimes that are carried another country has implications for jurisdiction.

To prosecute international cyber-criminals, there have been changes in criminal law and territorial reach has been extended. Hence, the conflict of jurisdiction has been acknowledged mainly in the environs of cyberspace. The UAE government is also planning to implement an extra territorial principle in order to address activities associated with cybercrime. This is because there has been an increase in cybercrime that has adversely affected society. This involved implementing the national law to crimes committed and terminated outside the jurisdiction and the principle of the territory as the norm of jurisdiction for criminal law. The nature of these crimes makes it impossible to extend jurisdiction when it comes to dealing with cybercrimes. The jurisdiction question is commonly seen as a problem for criminal law, and it has a crucial impact on the investigation of these crimes and proceedings within the domain

[111]Khamis Al Mazeina, General Commander of the Dubai Police-UAE, 'New criminal phenomena in the UAE' (conference, Dubai 22nd February 2012).
[112]Ibid.
[113]The UAE Federal Penal Law No. 3 of 1987, s 16.

of criminal prosecution.

Another issue that is reported in other countries is the presence of electronic evidence as part of a network, or where there is a connection to the Internet or another computer. Issuing search and seizure warrants for electronic evidence is an issue that arises from this. The general principle regarding the search and seizure of evidence according to the law in the UAE states that only the computer system that is found in the suspect's house can be seized or searched and no other computer can be, whether it is on the premises or not. According to Article 53 of UAE's CPL, the suspect's entire house can be searched for papers and objects.[114] However, if there is another computer in a remote jurisdiction this may raise an issue in relation to sovereignty and territory. If there was greater understanding between national law enforcement agencies, these issues could be handled. A mutual understanding would include assisting one another in gathering information and sharing it in the form of intelligence or evidence. Therefore, pursuant to this matter, it is appropriate to illustrate some of the legal procedures in place to obtain evidence from abroad.

4.4 Legal procedures to obtain evidence from outside country

It is essential for law enforcement agencies and investigating officers to gain sufficient understanding of the methods used when obtaining evidence from other nations. If no procedures are developed to help in the searching and seizure of electronic evidence then conventional approaches must be followed to obtain sufficient appropriate audited evidence.

4.4.1 Mutual Legal Assistance (MLA)

MLA instruments are used to transfer evidence from one jurisdiction to another. These instruments help where cases are being committed in different jurisdictions.[115] In other words, MLA can also be defined as the method under which one state requests assistance from another state.[116] The reason is to commence or continue a trial for a criminal offence. The definitions of MLA focus on two completely different aspects but

[114]Article 103 of the German Criminal Procedural Act extends the search warrant to other places and persons for the purpose of apprehending the accused, or to follow up traces of a criminal offence or to seize certain objects.

[115]See: Jody Westby, *International Guide to Combating Cybercrime* (American Bar Association 2003) 44.

[116] William Gilmore, *Mutual Assistance in Criminal and Business Regulatory Matters* (Cambridge University Press 1995) xii.

are of equal importance. The techniques established in MLA are easily executed and not readily overwhelmed by political factors. The reason for this is that the courts and lawyers demand them. As per the second definition of MLA, the mechanism can be performed after acceptance of an accord from both states.

4.4.1.1 Bilateral Mutual Legal Assistance Treaty (MLAT)

This technique binds countries to assist each other when obtaining evidence for a public trial. Applying this mechanism, evidence is collected for the petitioning country by the other country.[117] It is an important tool for collecting information from other countries. In it, details are provided to address difficulties that have arisen when interacting with law enforcement. Details are also provided to redress dual criminality and changing cooperation requirements.[118]

Agreements between countries under MLAT are limited to a set number of offences and methods.[119] This is the reason that a bilateral MLAT does not exist that can contribute to resolving issues to obtain evidence electronically. Even today, the conventional style of legal assistance is made available for the searching and collection of electronic evidence from different countries. During investigations, bilateral MLAT agreements also assist when the conviction policies in countries are unequal and all the information required is received and sent from the person with authority. [120] Electronic evidence is easily altered and can be lost with a single click. This is the reason why traditional styles of mutual assistance are deemed to be inappropriate for the collection of evidence using an electronic source. [121] The MLAT is also incompatible when it comes to collecting electronic evidence, because strict and decisive actions need to be taken.

4.4.1.2 Multilateral Mutual Legal Assistance (MMLA)

Efforts are now being exerted to bring about improvements in performance and co-operation. This is done by adopting various measures, such as sending the accused or the person guilty of a crime to the country in which he committed the crime, giving

---

[117] Jamel Al Saqer, *The Procedural Aspects of Internet crimes* (Dar Nahda Al Arabiah 1998) 82. (Author's translation from the Arabic).
جميل الصغير، الجوانب الاجرائية للجرائم المتعلقة بالانترنت (دار النهضة العربية مصر 1998) ص82.

[118] Ibid.

[119] Ibid.

[120] Hisham Rustom, *The Procedural Aspects of Cybercrimes* (Modern machinery 1994) 100. (Author's translation from the Arabic).
هشام رستم، الجوانب الاجرائية للجرائم المعلوماتية (مكتبة الالات الحديثة مصر 1994) ص100.

[121] Ibid.

legal assistance in additional circumstances, and also supporting co-operation by arranging combined training programs. The best examples of this are the Council of Europe, Asian-Pacific Economic Co-operation, G8,[122] and the UN. All the countries within each group have an agreement to assist and respond to each other to minimise the suppression of criminal prosecution.

4.4.2 Rogatory Letters

These are letters of request issued from the judiciary of one country to another.[123] These are usually only relevant if the required help falls outside the MILAT's sphere of influence. That is to say, in a case when the requesting country does not hold any kind of multilateral or bilateral MILAT along with the requested country. [124] Therefore, these may be regarded as a default mechanism for following international courtesy rules. Moreover, these prevent law enforcement officers from issuing rogatory letters to attain evidence.[125] On the other hand, scholars have suggested that modern methods like e-mails should be adapted for the purpose of processing rogatory letters.[126] Adopting emails as the basic letter-transmitting medium will give rise to transformations that will profit cross–border searches in the pursuit of criminals. It will also assist in accelerating rogatory letter processing.

Although there is a Federal law in the UAE regulating matters of international cooperation, to date, the participation of the UAE in efforts of international co-operation has been insufficient. The UAE Federal law No.36 of 2006 concerns International Judicial Cooperation in Criminal Matters covering the procedure of the extradition[127] and retrieval[128] of persons, and the procedure of the mutual judicial assistance in criminal matters.[129] However, there are no rules covering procedures for obtaining evidence from abroad. The established rules and regulations in the UAE are not effective or sufficient to control the retrieval of electronic evidence. Regarding this

---

[122] The G8 is group of eight countries; France, Canada, Germany, Japan, Italy, the UK, the Russian Federation, and the US.
[123] Ilias Bantekas and Susan Nash, *International Criminal Law* (2nd edn, Cavendish Publishing 2003) 143.
[124] Hisham Rustom (n120) 102.
هشام رستم، مرجع سابق، ص 102.
[125] Ibid.
[126] Ibid.
[127] The UAE Federal law No.36 of 2006 concerning International Judicial Cooperation in Criminal Matters, Articles 6-32.
[128] Ibid, Articles 33-37.
[129] Ibid, Articles 43-63.

matter, Judge Al kaabi said:

> In terms of crimes committed outside the country, there are rules governing this issue. But, in terms of evidence I think there is a gap in the laws in this field, there is no rule regulating this issue.[130]

These provisions are also not adequate to underwrite events that entail cross-border searches. There are no covenants available to drive Internet Service Providers' (ISP) to withhold information or help in investigations. Today, using letters to perform the search and property confiscation is a challenge in the UAE. These letters define precise actions and are intertwined with procedures central to bureaucracy and diplomacy. Consequently, MLA is the most commonly recommended method for the cross-border transfer of electronic evidence. Attaining cross border evidence is a difficult procedure in the UAE, and there are no rules covering this. When the researcher queried the President of the UAE's Federal Supreme Court, Judge Abdul Wahab Abdul, on this, he said:

> …The UAE laws did not deal with this issue [obtaining electronic evidence from abroad], so we are facing a gap. I think this issue must deal with the new law of electronic evidence.[131]

They may adopt the rogatory letters method but it is an impractical method for performing the necessary tasks. This is because it can impeded the essential timely nature of a response, depending upon the demographics and properties of the electronic evidence. Lieutenant-Colonel Al Hajiri, Director of the Criminal Investigation Department's-Electronic Crime Section- Dubai Police supported this view:

> We are facing difficulties in gathering evidence from abroad. There are no conventions and effective international cooperation in this field. As an example, our department has been applying for evidence from abroad since 2010 and even now we have not had it. It can take more than 3 years to get evidence.[132]

4.5 The preservation of electronic evidence in the UAE

The location of the crime is the starting point for criminal investigators to detect crime.

[130]See: translated transcript of the interview with Judge Mohamed Al kaabi in Appendix 5.
[131]See: translated transcript of the interview with Judge Abdul Wahab Abdul in Appendix 5.
[132]See: translated transcript of the interview with Al Hajiri in Appendix 5.

Thus, success or failure with regard to procedures for detecting crime is dependent on the preservation of evidence. Undoubtedly, the key element of any criminal investigation is the preservation of evidence, because any error maintaining evidence cannot be corrected. A practical example of this was given by forensic experts from the UAE when he stated: 'there are many cases where we lost the evidence due to bad handling…one of the cases is when the analyst deletes evidence when handling the case and we cannot get it back again'.[133] In this regard, Article 35 of the UAE's CPL states: '… They have to take all precautionary measures necessary for the preservation of the crime's evidences'. Therefore, when seizing evidence, a police investigator must ensure that evidence is marked, identified and preserved to maintain its integrity. Thus, when dealing with electronic evidence, the police investigator should be aware of the nature of the information system because he or she may have overlooked or ignored evidence, thinking that it is not of importance, and may have destroyed or changed it inadvertently.

The preservation of electronic evidence demands clear procedures, requiring precision, resulting in trust with regard to the electronic evidence. Judge Abdul Wahab Abdul, the President of the UAE Federal Supreme Court, supports this argument, when calling for reform to the UAE laws with regard to gathering evidence and the creation of special rules for handling electronic evidence.[134] Police investigators need to prove that no information has been added or changed, and that all media has been secured during the seizure of the evidence.[135] This view was also supported by Major Lootah, head of the Electronic Evidence Unit at the Criminal Evidence and Criminology Department-Dubai Police. When asked about whether the UAE needed to regulate electronic evidence by law, he said:

> Yes, to ensure that all procedures were followed properly and all evidence had not been tampered with. The existence of rules will help us to ensure that all forensic experts or police members follow all the correct procedures and can also be checked by a third party.[136]

[133]See: translated transcript of the interview with Al Ketbi in Appendix 5.
[134]The 4th International Conference on Cyber Crimes (UAE 14th December 2011).
[135]See: Johan Vacca, *Computer Forensic: Computer Crime Scene Investigation* (2nd edn, Charles River Media Inc. 2005) 154-155.
[136]See: translated transcript of the interview with Lootah in Appendix 5.

In criminal law, there is no rule in the UAE concerning the preservation of electronic evidence. However, the process of preserving electronic evidence begins prior to its seizure. In practical terms, the process starts when an individual takes a photograph of the computer system once the relevant computer has been located. The wires connecting it to the system must be marked for future identification or reconnection; the computer must also be marked as evidence and must eventually be transported to a safe place. Finally, the seized computer must be stored properly and preserved in a suitable environment, because high temperatures can destroy the data on a hard drive. Thus, the storage conditions should be stable, safe and moderate.[137]

All preventive measures need to be taken to guarantee that there is no tampering with the evidence gathered, especially when there is variable data in the memory of a computer that is still running. Under such conditions, a computer specialist should make a copy of the hard disk to preserve the data before shutting down the computer. In contrast, some believe that the investigator should conduct a full backup of all computer data before it is processed or reviewed, because if data is not backed up then evidence can become vulnerable to modification or damage by the investigator.[138] In an interview conducted in the UAE, a forensic expert interviewed by the researcher said:

> When we reach the search and seizure place, we must take an overview of the location and imagery. We then look at the device and determine its condition, is it in running or not. Are there any other devices connected to it or not. Is there a Wireless Access Point or not. All these things and more are important because it affects the search and seizure of the evidence and any oversight could lead to the loss of evidence.[139]

In this process, data can be analysed in detail, and the investigator should navigate through all computer files, without touching the original hard drive. Once an investigator detects evidence, then they are under an obligation to preserve it.[140] However, when insuring the security of the evidence, care should be taken to guarantee that it does not lose its originality. For the surety of the evidence we must attain a

[137] The temperatures in the UAE during the summer months can reach to 50°C.
[138] In Australia, Standards Australia 2003 has established a set of generic standards for managing electronic evidence.
[139] See: translated transcript of the interview with Al Ketbi in Appendix 5.
[140] Brian Paperback, *Hacking exposed Linux* (3rd edn, McGraw-Hill Osborne Media 2008) 567.

holistic understanding of how to preserve evidence. These should adopt a cautious manner, such as that suggested in the United States Secret Services' Pocket Guide for First Responders, which suggests the following guidelines:

1. Do not try to use an 'off' computer in search of proof;
2. All the devices associated with the computer must be photographed from all sides, including cords and other attachments;
3. Do not start up an "off" computer;
4. In the event that the computer is already "on", take photographs of the screen;
5. If the computer is "on" and in a sleep state, press the space bar or move the mouse in order to display the current image. Take a photograph of the active image;
6. Unplug the power cord from the computer;
7. For subsequent recognition of connected devices, label or draw and illustration of the cords;
8. Remove or disconnect all devices and cords from the computer;
9. Store elements such as fragile cargo/packages and parts that have been used for transportation;
10. Other additional storage media must be seized;
11. Other hazardous material such as magnets, radio transmitters etc., must be kept separate;
12. Along with the computer and its accessories, the instruction manual, documents and notes must be gathered;
13. Make a sequential written statement about the process of confiscating the computer and its components;
14. In the event that the computer is attached to a network server, expert help must be sought; and

15. Make sure that no one interferes with the crime scene with the exception of accredited staff.[141]

Evidence that has been corrupted, damaged or not handled with care is inadmissible in a court of law. Therefore, securing the evidence gathered in proximity to its natural condition is mandatory, and accordingly, the above guidelines must be followed.[142]

In brief, electronic evidence needs to be validated if it is to have any evidentiary value. It is essential to put into place a legal strategy for electronic evidence, to prove that the method used for its preservation is appropriate and that the evidence has not been altered since it was seized. Undoubtedly, existing rules and regulations will help to avoid any accusations of tampering with evidence. A lawyer interviewed by the researcher said:

> We now apply the general rules of evidence, which I think we can use as a framework. However, the nature of electronic evidence requires us to look beyond these rules. Undoubtedly, electronic evidence needs more attention concerning search, seizure or examination. The general rules cannot cover this process.[143]

4.6 Examination of electronic evidence

Examination of electronic evidence, describes the study of the legal aspects of the techniques and computer investigation methods used for examination, identification, preservation, and presentation of possible electronic evidence, so that it will be acceptable at trial. The aim of the forensic process is to comprehend fully the extent of the suspect's crime related computer activities. The forensic examination of electronic devices involves analysis of the electronic device that has been collected as evidence through the use of a variety of techniques and tools.[144]

To conduct a forensic investigation, examination skills and knowledge of electronic devices and systems is particularly essential. This is especially the case when forensic analysis is conducted parallel to the investigative process, and both the prosecutors and

[141] For more information see: the US Secret Services' Pocket Guide for First Responders <http://info.publicintelligence.net/usssbestpractices.pdf> accessed 22nd October 2012.
[142] Johan Vacca (n135) 224.
[143] See: translated transcript of the interview with the anonymous Lawyer in Appendix 5.
[144] See: Computer Crime: The UN Manual adapted by Editor Michael O'Brien <http://www.unlimitedinvestigations.com/computer_crime.htm> accessed 22nd October 2012.

investigators clearly understand the process, particularly so as to ensure the reliability of evidence.

Forensic analysis is becoming more prominent worldwide, particularly as it offers security to e-commerce. Consequently, this method has been adopted in many countries, such as the US and the UK, in the search to solve criminal cases, intellectual property disputes and cyber-crimes.[145]

Therefore, forensic investigators typically act to identify, retrieve and recover evidence from any technology device with the aim of combating crime. Forensic investigators must have fundamental up to date knowledge and skills.[146] For instance, a forensic investigator should acquire expertise or skills such as identification of cyberspace issues, knowledge of investigative crime, and knowledge of types of evidence, and of the presentation of findings. In this respect, it is appropriate to look at the background and definition to electronic device forensics, the procedures associated with electronic evidence examinations and techniques and tools of electronic evidence examination.

4.6.1 Electronic device forensics: background and definition

The law of evidence is founded on a paper-based system, in which evidence is physical in nature. Nevertheless, with the advance of information, communication and computer technology the nature of evidence is becoming more elusive.

In accordance with the Cambridge International Dictionary of English, the meaning of the word 'forensic' comes from the Latin word referring to the study of data or information relating to a crime. It has also been described as the process of exploration of details about a crime, by scientifically examining the substances or objects involved in the crime.[147]

Since at least 1966, courts of law have been faced with challenges relating to the admission of computer-related evidence.[148] In such instances, most litigation has

[145] See: Peter Sommer, 'Computer Forensic: An introduction' *vial virtual city* <http://www.virtualcity.co.uk/vcaforens.htm> accessed 22nd October 2012.
[146] See: Jack Bologan, *Fraud auditing and Forensic Accounting: New tools and techniques* (John Wiley and Sons 1987) 86-88 and 92.
[147] See: Cambridge International Dictionary of English, Economy edition (Cambridge University Press 1995).
[148] *US v Bennett*, [1966] 4-66-Crim. No. 89 (D. Minn, 1966). This case is the first success fully prosecuted case (in a federal US jurisdiction) and involved the criminal case of a computer programme who worked

followed existing rules of evidence for guidance as to whether to admit evidence into proceedings. Consequently, there have been many notable evolutions towards standardisation in electronic evidence forensics; however, the field remains in transition. Its origins are in practical acquisition and there are a series of evidence issues related to inspections that have now been overcome, predominantly by law enforcement personnel using training in technology. The field has progressed to a point where, at the national level, best practice standards and certification are being considered. However, internationally, there is no single intervention or standard practice to apply, nor is there a generally-accepted governing body for the field.[149]

The transitional nature of the field impacts upon attempts to characterise or analyse it. The following sections examine the essential properties of electronic evidence forensics by reflecting upon milestones in practice, definitions and perspectives achieved by those actors who have shaped the field's history.

The 1980s saw a burgeoning need to manage computer-based evidence, mainly involving mini-systems or mainframe computers. Use of the PC platform proliferated during the 1980s and early 1990s, resulting in widespread recognition that new techniques were required for the preservation of electronic evidence.[150] In 1984, New Scotland Yard in the UK formed a Computer Crime Unit. In the UAE, the Dubai police established the Department of Criminal Laboratory in 1981, which was then transformed into a general department in 2000 with the creation of a special unit for managing electronic evidence. The first specific forensic imaging tool, IMDUMP, emerged in the USA, and was superseded in 1991 by a tool called Safe Back.[151] In the UK during the same year, another disk-imaging application, entitled Data Image Back-

---

on a reporting system for overdrawn checking accounts for the National City Bank of Minneapolis. The defendant, whose personal checking account was with the same bank, and subject to the same processing system, accessed the program to hide a growing personal debt. The situation was discovered when a computer failure caused processing to revert back to manual methods. See: Donn Parker, 'Rules of ethics in information processing' (March 1968) 11, 3 *Communication of the ACM* 198-201; and Kevin Quinn, 'Computer Crime: A Growing Corporate Dilemma' (1978-79) 8, 1 *Maryland Law Forum* 48-62.

[149]Alan Brill, Mark Pollitt and Carrie Whitcomb, 'The Evolution of Computer Forensic Best Practices: An update on Programs and Publications' (2006) 1, 1 *Journal of Digital Forensic Practice* 2-11.

[150]George Mohay, Alison Anderson, Byron Collie, Olivier De Vel and Rodney Mckmish, *Computer and Intrusion Forensics* (Artech House Inc. 2003) 7.

[151]Ibid, 113.

up System (DIBS), was produced.[152]

Computer forensics practitioners begin to organise and evaluate their techniques and practices. In 1993, the FBI led and hosted the first global Law Enforcement Congress on computer evidence. Subsequent conferences let to the 1995 formation of the International Organisation on Computer Evidence (IOCE), and the 1997 meeting resolved to develop best practice standards.[153] Around this time, audio and video technologies were moving from analogue to digital, leading practitioners to consider whether the same principles of computer forensics could be applied to all types of electronic evidence.[154]

Efforts to define the principles of computer forensics resulted in 1999 in the adoption by the IOCE of proposals authored by member organisations, namely the Scientific Working Group on Digital Evidence (SWGDE),[155] from the USA, and the Association of Chief Police Officers (ACPO) from the UK. In 2001, the first Digital Forensics Research workshop was held, bringing together experts from the private sector, military and academic circles to examine cardinal problems and research requirements in the field.[156]

Currently, much attention has been focused on the improvement of policies intended to address the challenges associated with handling electronic evidence.[157] There are two key reasons for this close attention: first, electronic evidence has necessitated a number of strategies and requirements to ensure that the evidence gathered is admissible.[158] In the electronic evidence gathering process, inspections must meet certain conditions and fulfil set out procedures, such as the careful handling required to ensure that evidence is

[152]Austen, J., 'Some stepping stones in computer forensics' (2003) 8, 2 *Information Security Technical Report* 37-41.
[153]Alan Brill, Mark Pollitt and Carrie Whitcomb (n149).
[154]Carrie Whitcomb, 'An historical perspective of digital evidence: A forensic scientist's view' (2002) 1, 1 *International Journal of Digital Evidence* 2.
[155]In the US, a Scientific Working Group (SWG) has been formed by the US Federal Bureau of Investigation (FBI) Laboratory to work on computer evidence. The works include improving discipline practices and building consensus with the federal, state and local forensic community partners. The Scientific Working Group Image Technology (SWGIT) is closely associated with the Scientific Working Group Digital Evidence (SWGDE).
[156]The Digital Forensic Research workshop also gives new life to an idea recommend several years earlier - reviewed journals, leading to the institution of the International Journal of Electronic Evidence.
[157]Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (n 13) 9.
[158] Ibid.

preserved. Law enforcement authorities require definitive procedures in order to conduct effective inspections: the ability to identify and prosecute a criminal effectively is based on a legitimate gathering of electronic evidence.[159] For this purpose, many countries have endeavoured to establish guidelines and develop electronic investigation systems.

Secondly, the way in which judges, prosecutors and other law enforcement authorities deal with evidence in court may also be affected by the use of electronic evidence.[160] Evidence is usually presented in court; however, electronic evidence, such as computer output evidence, may not be suitable for representation as conventional forms of evidence.[161]

4.6.2 The procedures law on electronic evidence examination

In the UAE, forensic examination of electronic devices is extremely new, and at present, there is no specific statute to explain the details of forensic examination of electronic devices. Conversely, many countries have guidelines about how to examine electronic evidence. For example, in the UK,[162] experts must follow an established Code of Practice and General Professional Principles, as is the case in the USA,[163] Australia[164] and Singapore.[165]

In line with normal practice in the UAE, experts begin by first conducting a physical check of seized electronic device; this is then photographed and registered as an item for forensic examination (The process will be further elaborated on when discussing the techniques and tools used for forensic examination of electronic evidence).

---

[159]For further details in a formalisation of computer forensics see: Axel Krings, 'A Formalisation of Digital Forensics' (2004) 3, 2 *International Journal of Digital Evidence*.

[160]For observations on the challenges of dealing with electronic evidence on the basis of traditional procedures and doctrines see: Robert Moore, 'To View or not to View: Examining the Plain View Doctrine and Digital Evidence' (2004) 29, 1 *American Journal of Criminal Justice* 57.

[161]For further argumentation about the use of computer printouts in the court see: John Robinson, 'The Admissibility of Computer Printouts under the Business Records Exception in Texas' (1970) 12 *South Texas Law Journal* 291. Also see: John Vacca, *Computer Forensics: Computer Crime Scene Investigation* (2nd edn, Cengage Learning 2005) 3.

[162] See: the UK Code of Practice, via Academy of Experts <http://www.academyofexperts.org/> accessed 22nd October 2012.

[163]See: Handbook of Forensic Services, revised 2007 US Department of Justice, FIB Laboratory Division <http://www.fbi.gov/about-us/lab/handbook-of-forensic-services-pdf>.

[164] See: Australia High Tech Crime Centre (AHTCC) via Australia Federal Police (AFP) <http://www.afp.gov.au/> accessed 22nd October 2012.

[165] See: Singapore Techno Forensic Branch, Technology Crime Division, Criminal Investigation Department (CID) via SPF <http://www.spf.gov.sg/abtspf/cid.htm> accessed 22nd October 2012.

Certainly, establishing procedures and rules for the examination process is particularly beneficial in order to offer a framework for handling electronic evidence that ensures the quality of any examination. When an expert is called to testify, the details of the procedures and techniques used will be revealed as the focus is on the duty of the expert to establish that the evidence is original, has not been altered during the investigation, and that the result of the forensic examination is genuine and reliable. Subsequently, the UAE will need to remain cognisant of this issue in the future, and also work on upgrading laboratories with the latest devices and equipment to guarantee both accuracy and reliability.[166] Thus, it is necessary to understand what tools have been used by forensic investigators to conduct forensic examinations.

4.6.3 Techniques and tools of electronic evidence examination

In an interview conducted in the UAE, forensic experts interviewed by researcher explained the techniques and tools utilised in electronic evidence examination in the UAE. One participant said:

> Electronic evidence can be examined and analysed using several techniques. These can be divided into two main types of tools; tools for copying and tools for analysis. All these tools must be accredited by organizations and bodies. If not, we must test the tool internally.[167]

He also added: 'where the original evidence is retained and analysed we use the copy only. But there are cases where you cannot take a backup of the evidence then we examine the original evidence'.[168]

When conducting an investigation, it is essential for the forensic investigator to consider the appropriate tools and techniques for the investigation and analysis of electronic evidence in relation to the three main stages "[a]cquisition, [a]nalysis [and] [presentation]".[169] 'An essential toolkit should consist of various software such as

[166]For instance, in the US, there is a project known as the NIST CFTT (the National Institute of Standards and Technology Computer Forensic Tool Testing), which is supported by the US Department of Justice's National Institute of Justice (NJI) Federal, state, local enforcement agencies and the NIST itself to promote efficient and effective use of computer technology in the investigation of crimes involving computers; available at <http://www.cftt.nist.gov/> accessed 22nd October 2012.
[167]See: translated transcript of the interview with AL Ketbi in Appendix 5.
[168]Ibid.
[169] Brain Carrier, 'Open Source Digital Forensics Tools' (September 2003) <http://www.digital-evidence.org/papers/opensrc_legal.pdf> accessed 26th March 2012.

backup, authentication, decryption, disk editing, log file auditing, IP tracking, data recovery, and file examination', though recovering data also requires a "hardware imaging tool", so that ambient data can also be recovered.[170] During the first stage, the digital system is saved; this step is comparable to taking pictures or fingerprints, and since it is not known at that point what may be considered important evidence all electronic evidence must be saved. Frequently, this involves taking copies of hard disk, also known as images. It is crucial that the tools that are chosen minimise any scope for alteration to the electronic evidence.[171] During the second stage the saved data is examined and identified and grouped into the following three categories of evidence:

- 'Inculpatory evidence: That which supports a given theory;
- Exculpatory Evidence: That which contradicts a given theory; and
- Evidence of tampering: That which cannot be related to any theory, but shows that the system was tampered with to avoid identification'.[172]

Hence, it is important that at this stage, files and directory contents are examined and also that deleted data is recovered and the scientific method employed in order to arrive at conclusions on the basis of the evidence obtained.[173] The scientific method consists of observation, formulating a hypothesis, based on the observations, and then making predictions, which can be tested before a conclusion is drawn.[174] Tools are employed so that, for example, deleted file names or other contents can be listed; it is also important that a copy be used that matches the original so that a MD5 check can also be performed.[175]

Techniques vary and depend on the type of operating system the criminals use, for example Unix, Windows and Macintosh. Moreover, forensic analysis requires investigators to be aware of the different versions of these operating systems that exist,

---

[170]Brett Pladna, 'Computer Forensics Procedures, Tools, and Digital Evidence Bags: What They Are and Who Should Use Them' <http://www.infosecwriters.com/text_resources/pdf/BPladna_Computer_Forensic_Procedures.pdf> accessed 20th April 2012.
[171] Ibid.
[172]Ibid.
[173]Ibid.
[174]Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (n13) 204.
[175]Brain Carrier (n169).

for example: "Windows XP, Windows Vista, Windows Server 2003 or 2008....Windows CE" [176] or Linux, BSDs. Solaris, AIX, HP-UX, IRX to name a few.[177] Hence, a Windows forensic analysis differs from a Macintosh forensic analysis. Investigators therefore have to consider whether they are investigating a handheld device, a network, embedded systems or wireless networks, since for each the method of investigation differs and requires specific expert knowledge.[178] Furthermore, as technologies grow rapidly, electronic evidence experts must constantly update their knowledge to adopt a positive attitude when conducting quality based investigations to reduce crime.

In the marketplace, there are a variety of forensic tools available to assist in the recovery of electronic evidence; such as Get Slack, NTI-DOC, GetTime, Net Threat Analyser, Get Free, and so on. The forensic expert must ascertain which are the most suitable techniques and tools for each investigation.[179] They must, therefore, be familiar with a variety of practices and tools with which to search the relevant software.

Whilst the first two stages of an investigation can be rather technical and thus similar from country to country, the final presentation stage differs depending on the particular rules pertaining to evidence in the jurisdiction where the case is being prosecuted.[180] Hence, electronic evidence gathers also must have clear guidance in legal matters as well as understanding the tools necessary to perform the task.[181] This is particularly important since the tools and techniques used by forensic experts, could be subject to cross-examination and the underlying scientific structure and methodology of such techniques and tools may be questioned.[182]

The forensic expert also has to be able to explain the process of gathering and

---

[176] Eoghan Casey, *Handbook of Digital Forensics and Investigation* (n 61) 210.
[177] Ibid, 302-303.
[178] Wayne Jansen and Rick Ayers, 'An overview and analysis of PDA forensic tools' (2005) 2.2 *Digital Investigation* 120-132.
[179] See: Albert Marcella and Robert Greenfield, *Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer crimes* (Auerbach Publications 2002) 380-387; Current Computer Forensic Tools (Module 6) The Computer Hacking Forensic Investigator (CHFI) via *Tiburon Technical* <http://tiburontechnical.com/computer_hacking_forensic_investigator.htm> accessed 6th February 2012.
[180] Brain Carrier (n169).
[181] Irons A., Stephens P. and Ferguson R., 'Digital Investigation as a distinct discipline: A pedagogic perspective' (2009) 6.1and 6.2 *Digital Investigation* 82-90.
[182] Lei Pan and Lynn Batten, 'Robust performance testing for digital forensic tools' (2009) 6.1and 6.2 *Digital Investigation* 71-81.

recovering electronic evidence to the judge. Hence, "a tool must be reliable and relevant" in the UAE.[183] However, in the UAE there is no specific guideline dealing with this issue, unlike in the USA; where the Daubert[184] guidelines have been developed in order to scrutinise reliability of evidence.[185] In the USA, a pre-hearing takes place during which it is determined whether the evidence is reliable and relevant; this requires the judge to assess the techniques and methodology employed.[186] The following questions may be asked by the judge in order to reach a decision:

- 'Testing: Can and has the procedure been tested?
- Error Rate: Is there a known error rate for the procedure?
- Publication: Has the procedure been published and subject to peer review?
- Acceptance: Is the procedure generally accepted in the relevant scientific community?'[187]

The first guideline, requiring testing, aims to establish accuracy and two kinds of tests are employed. The false negative test establishes that the tool lists all data from the input, whilst the false positive test establishes that no new data is added to the output; the National Institute for Standards Technology's Computer Forensic Tool Testing group has promulgated methodologies for testing tools.[188]

Error rates refers to whether the digital forensic tools deliver either of one of two types of error: 'Tool Implementation Error or Abstraction Error'. The former can result due to incorrect details or bugs contained in the code, and the latter arises when decisions made are not 100% certain because the data has been processed differently or due to 'data reduction techniques'.[189] The third requirement is that the method has been published and reviewed, whilst the last guideline requires that the procedures have been carefully evaluated.[190] Thus, it would be advisable to have similar rules of guidance in the UAE.

---

[183] See: translated transcript of the interview with AL Ketbi in Appendix 5.
[184] *Daubert v. Merrell Dow Pharmaceuticals Syllabus* (92-102) 509 U.S. 579 (1993).
[185] Brain Carrier (n169).
[186] Ibid, 3.
[187] Ibid.
[188] Ibid, 4.
[189] Ibid, 5.
[190] Ibid, 6-7.

The techniques and tools employed to examine electronic evidence, therefore have to be carefully selected, as otherwise, a case may be lost, since evidence, which has been obtained during a search and seized, is considered unreliable. Therefore, it has to be assessed whether the UAE's current procedures for managing electronic evidence are sufficient to deal with crimes. This means it is important to discuss expert opinions and rules.

4.6.4 The forensic expert opinion rule in the UAE

The aim of using an expert is to provide the court with information that would otherwise be unavailable. This means that expert evidence will only be admitted if the court is not in a position to make a decision regarding a fact by itself.

In the UAE, the use of expert evidence in court is regulated by the Federal Law No 8 of 1974. The expert is regarded in the same manner as any other witness, with the judge retaining the power to determine whether his or her evidence is admissible. Article 26 (1) of the Federal Law No 8 of 1974 provides that: 'The advice given by the expert shall not constrain the work of the court'. Forensic expert evidence is admissible as the medium for demonstrating the reality in matters of concern; as explained by the Emirates Federal Supreme Court: 'The judge has a power to accept or reject the forensic expert report'.[191]

The above must be understood by the forensics expert, because the general rules of expert evidence include the field of technology. The range of technological evidence is vast and continually expanding. An obvious point to consider here, is the extent to which 'experts' must have qualifications and/or experience and whether lack of the same influences the weight of his or her evidence and its admissibility. It is submitted that the answer to this depends on the circumstances of each case. If, for example, the case requires exceptional skill and knowledge on technical aspects, its lack would obviously affect both the weight and the admissibility of electronic evidence presented by the forensics expert. Thus, it is essential for the forensic expert to possess ICT qualification or have experience handling electronic evidence. The significance of this contention is supported by one forensic expert who commented:

[191] Criminal Case of UAE Federal Supreme Court No. 371/2002 date of decision 14th May 2002 unpublished.

> Merely turning on a subject's computer without following forensic procedures may alter critical data stamps and erase data contained in temporary files. An experienced computer forensic technician can quickly identify potential evidence.[192]

Nevertheless, according to Allinson, the perception that any person working within the IT field is an expert and, therefore, could serve as an expert witness is untrue, because not all will meet the definition of a 'responsible person' having fulfilled the required level of responsibility, knowledge, skill, experience or training. These requirements are extremely influential in establishing the reliability of a computer audit trail within an organisation.[193]

Furthermore, forensic expert testimony can be questioned when the evidence produced is open to interpretation because a complex computer system may have unanticipated operating errors that can result in catastrophic crashes and data corruption. Therefore, the forensic expert must be able to explain in detail how the analysis has been conducted and also learn how to quantify and account for resulting uncertainties, including those affecting the system clock on the computer that represents the time, date and sequence of events. Determining whether the system clock is accurate can be a challenging task in a networked environment.[194]

According to Palmer, the techniques and conclusions reached by forensics experts are acceptable in today's courts, because they have been used previously in court or other similar settings as persuasive evidence for authorities. In fact, forensic analysis is yet to be tested to any great extent by lawyers in judicial proceedings or analysts 'in investigations of computer misuse'.[195] In the UAE, no challenge has yet been posed by a lawyer to expert evidence produced by a forensics expert. This situation indicates either that expert testimony is reliable or that lawyers do not yet understand how best to challenge it. In this regard, a forensic expert, when asked if there have been any objections or questioned conclusions when presenting expert reports at court, he said:

---

[192]Grant Bayley, 'Cyber sleuths on e-crime trail' (22nd May 2001) *Australian IT* <http://archive.2600.org.au/archives/2600-list/msg10716.html> accessed 11th January 2011.
[193]Caroline Allinson, 'Audit Trails in evidence: Analysis of Queensland case study' (2003) 2 *The Journal of Information, Law and Technology*.
[194]Eoghan Casey, 'Error, Uncertainty and Loss in Digital Evidence' (2002) 1, 2 *International Journal of Digital Evidence*.
[195]Gary Palmer, 'Forensic Analysis in the Digital World' (2002) 1, 1 *International Journal of Digital Evidence*.

> In fact, no, the judge is only looking for the conclusion not for the procedures. In contrast, the level of lawyers' knowledge about electronic evidence or expert report is very low. Therefore, she or he cannot discuss the reports.[196]

In addition, expert prosecution witnesses must be prepared to undergo cross-examination conducted by lawyer capable of testing the accuracy of the scientific evidence presented. In this regard, it must be stated that the method used to cross-examine in an adversarial system may be not appropriate when testing scientific evidence. Erroneous inferences may be drawn from the results presented or from leading questions, and, with the growth of this type of evidence, it is anticipated that 'challenges' to expert scientific evidence will increase.

Therefore, it is proposed that judges, prosecutors, lawyers and other court officers have much to learn about electronic devices systems and that this should be urgently addressed. They require additional knowledge to enable them to understand the opinions of, and technological terms used by, forensic experts when describing how electronic devices and systems work, and the methods of retrieving and preserving data. For the purpose of effectively using electronic evidence, a forensic expert must establish the reliability of the computer software used in any part of the analysis and also note that there has been no mishandling of the evidence presented. In other words, a forensic expert must be prepared to explain the integrity of his or her methods because a single small error may adversely affect the perceived quality of any evidence. In addition, the laboratory itself must have standard operating procedures. The forensic expert must comply with Standard Operating Procedures (SOP) and its protocols, which will protect the evidence from challenges relating to reliability made by lawyers.[197] As a result, the issue of authenticating will arise; this is discussed below.

4.7 Authentication of electronic evidence

Authentication is an essential principle applied in digital forensics; it has been described as a process designed to ensure that the evidence acquired is the same as the original; however, this is technically inaccurate, since an active computer changes all the time

[196] See: translated transcript of the interview with Lootah in Appendix 5.

[197] See further: Shayne Sherman, 'A digital forensic practitioner's guide to giving evidence in a court of law' (conference, Australia 2006) <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1032&context=adf> accessed 26th January 2011.

and any evidence acquired is only representative of a particular moment in time. This is also true for computers that are networked, so that in these instances, it is necessary to acquire evidence in transit.[198] Reed explicates:

> 'Authentication means satisfying the court that (a) the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate. As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available or via technological features in the system or the record'.[199]

Authentication can be divided into two distinct processes; firstly, the investigator who obtains the evidence, must confirm that the evidence, which has been acquired, is the same as the evidence that is shown to the court, and secondly, it has to be confirmed that the files, which are shown in court, have originated from the defendant's system.[200] Another issue related to authentication is that the chain of custody of electronic evidence has to be maintained; this enables each person to give evidence in court and confirm that the electronic evidence shown corresponds with what was found at the investigation stage. Casey proposes that a chain of custody form is employed, so that electronic evidence chain is properly recorded, so that when it has been transferred, the name of the person to whom it has been transferred and the reasons for the transfer are known.[201]

During the interview process, the researcher found that in the UAE, there is an internal procedure used to ensure the authentication processes. For example, the Telecommunications Regulatory Authority in the UAE have internal procedures accredited by the US ASCLD/LAB (ISO 27001: 2005). On the other hand, the Electronic Evidence Unit at the Criminal Evidence and Criminology Department of the Dubai Police use internal procedures. Almost all of the interviewees agreed that these procedures are not enough to ensure that all are followed properly, and the UAE needs to identify existing legal rules to ensure that all forensic experts or other legal members

[198] Eoghan Casey (n13) 21.
[199] Reed, C., 2 CLSR (1990-1991) 13-16, cited from Peter Sommer, 'Downloads, logs and captures: Evidence from Cyberspace' (1997) 5, 2 *Journal of Financial Crime* 14.
[200] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (n13) 21.
[201] Ibid.

follow the correct procedures.[202]

In terms of truthfulness, another issue is legitimacy. Notwithstanding, it can be perceived as problematic whether or not data has been tampered with or distorted; after origination from a particular source, electronic evidence can be altered or reformulated. For example, a video or audio tape can be tampered with or edited by removing parts, or by the laying on of one image over another, etc. The original or first form is dissimilar, basically, to the latter in terms of the content which is due to later alteration.[203]

One can bypass a password, or manipulate data in various ways and save information on a computer's hard disk or as emails. Text messages can also be captured, read, and even changed by a corrupt operator working for the GSM network on which the conversation or message was sent. Likewise, telefaxes may be captured and changed at will. This is in contrast to a letter or parcel, which is sent by a courier or the Post Office. These are rarely affected in this way, and so it is not normally practicable to alter a letter. Therefore, it is clear that an electronic copy can be easily altered as compared to a hard copy of a document.[204]

Confidentiality is another issue of authenticity. To store sensitive information in a safe place and to restrict access to authentic users is dependent on a network's or a system's capabilities. By using secrecy measures, one can ensure that only designated parties can access the specified information available on computers. The word 'access' now has a diversified meaning, such as reading as well as viewing, printing, or acquiring the knowledge that a specific asset exists. Therefore, only those with admission rights will enjoy access.[205]

Easy access on the part of third parties or unwanted readers of electronically generated information can subject such information to forgery, imitation, alteration, and change.

---

[202]See: transcript translated of the Interviews in Appendix 5.
[203]Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (n13) 234.
[204] Ibid.
[205]Charles Pfleeger and Shari Pfleeger, *Security in Computing* (4rd edn, Pearson Education Inc. 2006) 10.

Consequently, confidentiality is in question.[206]

The integration of evidence is of significant importance. A guiding rule must be followed in any investigation.[207] Regarding the evidence in court, the leading party ought to offer details of time, location and date of gathering, and should also indicate if the evidence has not been manipulated since its collection.[208]

In terms of the exhibition of electronic evidence, certain standards must be adhered to.[209] According to Schetina, Green and Carlson, the dependency of electronic evidence at trial relies on that evidence having not been tampered with.[210]

The defence usually relies on challenging the truthfulness of evidence in court.[211] Many authors claim that it is the chief aim of the defence to cast doubt on, and highlight the ambiguity of the prosecution's evidence when it is presented to the court. This point is also long-established by Casey, who emphasises that cross examination is when attorneys seek to disclose hidden facts and flaws in the evidence that may be due to the investigation process.[212]

It has been demonstrated above that the court must have adequate confidence that the evidence has not been altered. Thus, the investigator must be able to exhibit the truthfulness of that evidence in court. Similarly, the prosecution should be capable of showing that any evidence has not been altered between the time it was gathered and the time it was presented in court. Thus, the prosecutor attains an edge by proving at trial that the evidence has been retained secure from any change or alteration.[213]

Furthermore, the investigator should always engage in the best practices of law enforcement, for instance by working through standards for the confiscation of

---

[206] Andrew Chukwuemerie, 'Affidavit Evidence and Electronically Generated Materials in Nigerian Courts' (2006) 3, 3 *Social Science Research Network* 185.
[207] Albert Marcella and Doug Menendez, *Cyber forensics: A field manual for collecting, examining, and preserving evidence of computer crimes* (2nd edn, CRC Press LLC. 2007) 12.
[208] Thomas Duerr, Nicholas Beser and Gregory Staisiunas, 'Information Assurance Applied to authentication of Digital Evidence' (2004) 6, 4 *Forensic Science Communications* 1.
[209] Paul Bergman and Sara Berman, *The criminal law handbook: Know your rights, survive the system* (12th edn, Nolo 2011) 400.
[210] Erik Scheting, Ken Green and Jacob Carlson, *Internet site security (*Addison-Wesley 2002) 351.
[211] Russell Smith, Peter Grabosky and Gregor Urbas, *Cyber criminals on trial* (Cambridge University Press 2004) 81.
[212] Eoghan Casey (n13) 75.
[213] Peter Stephenson and Keith Gilbert, *Investigating computer-related crime* (CRC Press LLC. 2010) 133.

computers and for obtaining electronic evidence. In short, ascertaining the real status of the evidence or documents is called authentication. Challenges with regard to genuineness, veracity and discretion of the pieces of evidence gathered are difficult to handle because of their implications regarding broadcasting, usage and storage. These are the main challenges associated with using electronically generated evidence.

The extraction of evidence from a computer system to make certain that it is as original as the legitimate initial computer record, requires validation through authentication. For example, there may be some doubt that evidence was altered before it was gathered; such doubts can have a negative impact on the evidence. There are many examples where lawyers have criticised the authenticity of electronic evidence. They claim that theoretically there is a possibility of fabrication that arises with such evidence. On the other hand, were judges more familiar with electronic evidence, they might require additional proof to determine the truthfulness behind the doubts of the attorney. As a result, requisite standards for electronic evidence are becoming increasingly prominent with advancements in ICT.

4.8 The presentation of electronic evidence in the UAE

After the investigation has been carried out, and once what appears to be sufficient evidence has been obtained, the final stage in the criminal justice system is the prosecution of the case. The prosecutor will exhibit evidence with the purpose of presenting it in accordance with criminal standards; that is noting that the accused is guilty of committing some, or all, of the crimes with which he has been charged. In contrast, the lawyer will be concerned about tendering evidence that either contradicts or challenges the story of those events indicated by the prosecution, or alternatively offer a different story, with the purpose of raising doubt in the mind of the judge to assure acquittal of the accused. The essence of any event is to provide information to uncover the truth, whether in the form of argument or evidence in an opening statement, or in a closing or evidential argument. As a result, a clear presentation of evidence in court by the forensic expert or the prosecutor is necessitated, as summed up by Burns, who states:

> 'The presentation typically takes the form of a report, and the scientist must be prepared to explain this report in such a way that a typically science-phobic judge is able to comprehend it. Presentation is everything'.[214]

The process of the disclosure of evidence is governed by rules and procedures designed principally to protect the rights of the accused. Under UAE laws, the process of disclosure of evidence and presentation in court is governed primarily by the UAE's CPL.[215] The UAE's CPL details the nature of the duty placed upon the investigator and the prosecution to disclose the evidence obtained. As regards electronic evidence, whether obtained from the accused, the victim, third parties or generated by the investigators themselves, it may reveal a range of issues that need to be addressed, whether by a lawyer, the prosecution, or by the judge.

A first issue the problem associated with electronic evidence arises from the failure by the prosecutor to disclose in court the process involved in the collection of electronic evidence. This failure may result in evidence being inadmissible. The reason for this may be due to the absence of rules and regulations governing processes for collecting electronic evidence. In a criminal case in the UAE, a functionary of a company was accused of promulgating inside information about commercial projects by sending emails to the firms competitors. The Judgment stated in the First Instance Court [216] found the defendant innocent of any charges. The court did not find the evidence convincing, and ruled that there was no accuracy in the process of search and seizure. Moreover, more than one employee used the computer. The Appeal Court [217] upheld the First Instance ruling, noting that the prosecutors' presentation did not explain how the electronic evidence had been obtained, thus the court was not convinced, and threw out the conviction.

In another criminal case in the UAE, defendants gained unauthorised access to a banks

[214]Burns, D C, 'When used in the criminal legal process forensic science shows a bias in favour of the prosecution' (2001) 41.4 *Science and Justice* 271.
[215] See: section 2.1.4.1.
[216]Criminal Case of First Instance Court Dubai: UAE No.7690/2012 date of decision 20th September 2012 unpublished.
[217] Criminal Case of Appeal Court Dubai: UAE No.6732/2012 date of decision 6th January 2012 unpublished.

computer system (HSBC Bank) and stole (45000Dh). The First Instance Court [218] ruled that after careful perusal of all evidence, the evidence was insufficient for a conviction. The Appeal Court [219] supported this judgment, ruling that it is not enough for a conviction that there is evidence, but that it should be shown clearly how this evidence was gained, and the evidence must be linked to the accused, something not confirmed by the forensic report.

The second aspect to consider is when a crime occurs abroad and, therefore, foreign-sourced evidence may comprise a key element of the prosecution's case and will be subject to the disclosure obligations of the court. This situation may present particular problems, arising from the traditions in the different foreign jurisdiction when disclosing evidence, and a lack of standardised rules in the area of the presentation of electronic evidence.

Briefly, the presentation of evidence during the judicial trial process is critical to a case. However, in order for electronic evidence to be effective, the evidence must not only tell the story, but must also be easily understood. The judiciary has little information about the process undertaken during the evidence collection. It may not be fully aware of the process, and its scientific and technological understanding may be insufficient with regard to securing and examining electronic evidence. Therefore, forensic experts have an upper hand when presenting electronic evidence. [220] To this end, the presentation of electronic evidence in court should involve an incessant search for new and innovative ways to present electronic evidence.

4.9 The case of the UAE's Ministry of Education as an example of electronic evidence practices in the UAE

4.9.1 The facts of a case

On 5th April 2010, the Public Prosecution referred the respondent to the Al Qusais police station for the following:

First: Gaining unauthorised access to a computer system (the computer server at the

[218] Criminal Case of First Instance Court Dubai: UAE No.9913/2010 date of decision 9th May 2010 unpublished.
[219] Criminal Case of Appeal Court Dubai: UAE No.3422/2010 date of decision 26th August 2010 unpublished.
[220] See: section 5.3.

UAE Ministry of Education) without obtaining the consent of the person who owns or is in charge of the computer, with the result of deleting stored data and personal information.

Second: Malfunction of access to the UAE Ministry of Education service and data sources through an information technology device.

The Prosecutor called for punishment under Articles 1, 2, 3, and 5 of the Federal Law No. 2 of 2006 on the Prevention of Information Technology Crimes (before modifying and replaced by Federal Law No. 5 of 2012). The accused denied the accusations.

In accordance with the above-mentioned facts, the respondent committed two cybercrimes. The first was unauthorised access, and deleting data from the computer server of the UAE Ministry of Education. The second type was malfunction, i.e. preventing people from using the e-service.

The defendant had worked with the UAE Ministry of Education for eight years as an administrator of its networks, and by virtue of this work experience he knew the password on the computer server and how it worked. The defendant had been transferred to work in Abu Dhabi. At 8:09 a.m. on 5 April 2010, the defendant used the Director-General's computer in Abu Dhabi to penetrate the computer server at the UAE Ministry of Education located in Dubai.

As stated in the forensic report the respondent had:

I. Deleted files running the email system resulting in the stoppage of internal e-mail systems in the Ministry.

II. Deleted storage files for photocopiers.

III. Deleted database files for the Web portal at the Ministry, which led to a stop in all e-services.

IV. Deleted all backup files.

Witness (A) testified that the defendant knew the password for the computer service and also how it worked. He also added that the password for the computer service had not been changed since the defendant's transfer to work in Abu Dhabi.

Witness (B) testified that he saw the defendant enter the Director-General's office at about 7:30 a.m.

A forensic expert testified that he had checked all devices and found the penetration took place via the Director General's computer using a password (Administrator), which gave access to the administrator's network. He added that the hack was successful on the first attempt, demonstrating the hacker's full knowledge of the device's password and system.

The defendant's solicitor argued that the accusation was fabricated, and the Director-General stated, in a newspaper a week after the incident, that there had been no breakthrough in the case. The defendant argues that the technical failure had been due to the use of a CD-ROM containing a virus. He added that the forensic report had not proven who the hacker was, and could not confirm that the device in the Director General's office was used for the hack. They argued that another device may have afforded access and that the accused was not the only one who knew the password.

The Dubai Court of First Instance [221] considered the case and concluded that there was not enough evidence to find the defendant guilty. The court's decision depended upon the forensic report used to prove the truth of the case. The court acknowledged that the forensic report did not prove the defendant had been responsible for the action. Moreover, as there were no clear procedures to show how the evidence to identify the accused was obtained, the charge was based on conjecture. The recommendation, was therefore, acquittal. The case then became the subject of an appeal by the Public Prosecution.

The Appeal Court [222] accepted both the appeal and the subject.[223] The court of appeal ruled that the first court had the authority to decide upon the weight that should be attached to given evidence that may repudiate or prove a crime. Decisions by courts are not supervised, as long as they lead logically to a ruling. Based on this reasoning the court ruled to deny the appeal and endorsed acquittal of the defendant.

---

[221] Criminal Case of First Instance Court Dubai: UAE No.15432/2010 date of decision 24th November 2010 unpublished.

[222] Court of appeal in the UAE it can hear and or make a decision in both fact and point of law, while court of cassation deals with legality issue which may be raised.

[223] Criminal Case of Appeal Court Dubai: UAE No.6962/2010 date of decision 17th March 2011unpublished.

The Public Prosecution contested this ruling, claiming that it was based solely on insufficient evidence and there was evidence not presented to the court, in the form of the defendant's confession when asked in a pre-trial detention session. The Court of Cassation [224] held that the court has the power to take or reject evidence as long as it leads logically to a court ruling.[225] However, it stated that judgment must mention all facts and evidence included in the case, and since the court did not mention the confession of the defendant in the pre-trial detention session, the case must be returned to the appeal court to rule again.

On 7th June 2011, the Court of Appeal [226] ruled that the accused was guilty of the charge, based on the defendant's knowledge of the password for the computer service and knowledge of how it worked, and the accused's expertise. The defendant contested this ruling.

The Court of Cassation [227] dismissed the appeal and upheld the conviction. The court was satisfied with the overall conclusions of the appeal court and held that the appeal court had full freedom to make such decisions.

4.9.2 Observations of the case

The case of the UAE Ministry of Education raised several significant issues about the legal system relative to electronic evidence.

First, the case raised the issue that cybercrime and electronic evidence requires a high standard for burden of proof; therefore, if the respondent is to be convicted, the judge must be satisfied beyond doubt that the respondent is in fact guilty. The decision of the first instance court was legally acceptable and initially upheld by the Appeal Court, despite the fact that it was later rescinded.

Second, in this case the procedures for gathering electronic evidence were challenged by the prosecutor and the forensics expert on the grounds that the plaintiff had failed to clarify how the evidence was gained; thus, the judges were unable to understand how

[224] Criminal Case of Cassation Court Dubai: UAE No.153/2011 date of decision 2nd May 2011 unpublished.
[225] The Court of Cassation is considered the last resort in the UAE. The UAE court legal system is alike to its French counterpart, while different to the UK.
[226] Criminal Case of Appeal Court Dubai: UAE No.7003/2011 date of decision 7th June 2011 unpublished.
[227] Criminal Case of Cassation Court Dubai: UAE No.268/2011 date of decision 22nd August 2011 unpublished.

the evidence had been obtained. In addition, the forensic expert's report proved only the damage and not the perpetrator.

Third, in the present case there were several additional points to be taken into consideration for the future. For example:

I. Failure to regulate electronic evidence may lead to different judgments; the Judge did not convict because there were unclear procedures. Therefore, clear procedures must be set out for gathering electronic evidence.

II. There is no trustworthiness directed toward the forensic report; therefore, the report can easily be challenged. Since the forensic report was unable to prove the perpetrator, it is recommended that criminal procedures should provide specific provisions on the above matter.

III. The prosecutor and forensic expert were unable to explain the extremely complex IT methodologies and concepts to the court. This reveals a need to prepare and develop the capabilities of the legal specialists to establish the veracity of such evidence.

IV. Absence of protection programs and precautionary measures. The password on computer had not been changed since the transfer or termination of the employee, and so stricter interior precautionary measures must be regulated for.

This case clearly demonstrates the importance of establishing regulations on electronic evidence. The rules used for electronic evidence may not always cover cybercriminals practices or fill in the gaps left by Criminal Procedure Law.

4.10 Conclusion

As technology rapidly grows, the process of collecting electronic evidence becomes increasingly technical. The detection and investigation of crimes is becoming more challenging, as accusations must be proven beyond a reasonable doubt. In the future, this task will become more difficult, since all data will be stored in electronic format or in other invisible forms. This situation with regard to the detection of electronic evidence can lead to unsuccessful prosecutions. Prosecuting criminals becomes more complex when the prosecutor is indecisive about whether to charge an individual under

UAE Federal Law No.5 of 2012 for Information Technology related crime, or under the UAE's CPL, because the description of the charge will be found in UAE Federal Law No.5 of 2012 and the process of collecting evidence and burden of proof will be found in the UAE's CPL.

However, the fight against the crime will be rendered more effective if laws and procedures that are more effective are introduced to govern the process of detection and investigation. It is therefore of the utmost necessity to update laws. The (TWGECSI) Technical Working Group for Electronic Crime Scene Investigation presented their opinion in this regard, stating: 'In order to win the case; the investigators must follow proper procedures required in collect electronic evidence'.[228]

Criminal offenders such as fraudsters are constantly progressing in their mastery of the skills needed to perpetrate fraudulent activities using ICT. In order to succeed in the prosecution of crimes, the law must be effective at curbing unlawful activities.

This chapter has provided details about the rules and methods for gathering electronic evidence under the UAE's Criminal Procedure Law, in order to answer the question of whether the UAE Criminal Procedure Law is sufficient to govern the process of gathering and preserving electronic evidence in cases of crime. Can it stand alone or does it need supplementary legislation? However, this chapter also aimed to present some of the challenges facing the prosecution of crimes in relation to electronic evidence. Indeed, electronic evidence has different characteristics creating several challenges for judges, prosecutors, lawyers, forensics experts and investigators when collecting, preserving and presenting it.

The following points highlight the current inadequacies in the system, and propose recommendations for the improvement of rules regarding electronic evidence:

1. Due to lack of a specific provision in the UAE on the manner of gathering electronic evidence in voluminous form or in a complex situation, detailed provisions on how to handle complex evidence, such as electronic evidence, must be set out. The procedures for gathering electronic evidence under the UAE's CPL must be complemented and

[228] See: TWGECSI, 'Electronic Crime scene investigation: A guide for first responders' (2001) <https://www.ncjrs.gov/pdffiles1/nij/187736.pdf> accessed 28th October 2012.

supplemented by additional rules, in order to provide an efficient working procedure with regard to crime detection and investigation. The UAE's CPL cannot stand alone or remain static and needs to be reviewed, particularly in the area of the right of search and seizure of electronic evidence. This is because any shortcomings in the process of investigation result in failure to prosecute a case successfully.

Therefore, specific rules for the search and seizure of electronic evidence are necessary. The importance of this is further underscored because the rules contained in the UAE's CPL are insufficient to address the various investigation techniques required for electronic evidence. These rules also effect the administration of the criminal justice system in the UAE. Furthermore, the UAE Government must play a pivotal role, by providing more skilled computer forensics experts and enforcement officers.

2. Due to the lack of a specific provision in the UAE, or guidelines relating to forensics expert reports regarding electronic evidence presentation to the court, it is recommended that the Criminal Proceeding Law or the UAE Federal Law No 8 of 1974 should provide specific provisions on the above matter. Insufficient understanding on the part of forensics experts, who are untrained in the legal requirements for tackling electronic evidence, mean that their efforts cannot be presented in court. Furthermore, the status of cybercrime is not well defined.

3. There is no specific provision about who has the authority to access computer data or appropriate methods of dealing with encrypted evidence. There is a need to find reference or rules to manage electronic evidence.[229]

The above recommendations are made in order to provide ideas to legislators when reviewing existing provisions, and further, to help them prepare better to cope with the challenges raised by the development of ICT.

In summary, in order to effectively combat criminal crime cases and make full use of electronic evidence, the evidence collected must not only be relevant, reliable and authentic but should also be communicated and presented effectively to the judge. The judge, on the other hand, must apply IT concepts to cybercrime cases and provide effective grounds for judgment when either rejecting or admitting electronic evidence.

[229]Such as: France, the US, Canada and the UK. See: section 4.2.2.2.

According to Cross, poor understanding of technology on the part of 'makers of the law' is the reason for this failure.[230] Moreover, the prosecutor must be smart enough in assembling and presenting electronic evidence at trial such that its credibility and lucidity cannot be challenged. Clearly, the electronic evidence may be as substantial in quantity as possible.

In this age of technology, the improvement of the UAE's legal rules relating to electronic evidence can only properly take place by considering international cooperation. This is one area of the law of evidence in which it becomes feasible for the developed UAE to acquiesce to a set of uniform rules of evidence in order to regulate its use in cybercrime cases. Therefore, the above challenges, problems and recommendations must be taken into account by legislators to guarantee that UAE judges will be able to deal with the issues associated with electronic evidence and cyber-crimes more effectively.

[230]Debra Shinder and Michael Cross (n 3) 655.

CHAPTER FIVE: APPLIED STUDY: CURRENT ISSUES IN RELATION TO ELECTRONIC EVIDENCE FROM THE PERSPECTIVE OF LEGAL EXPERTS AND OTHER SPECIALISTS, TOWARDS THE REGULATION OF ELECTRONIC EVIDENCE IN THE UAE

A number of aspects relating to electronic evidence regulation are discussed in the preceding chapters on the basis of the descriptive legal study. Nevertheless, the dimensions of practical experiences were left ambiguous and so require more investigation and study. For this purpose, research tools relating to social science research will be employed in the remainder of the thesis. Quantitative and qualitative methods will be used. The goals set out by the researcher will be accomplished and a new understanding of relevant problems will be provided by presenting the perspectives of various legal experts and practitioners.

The main objective of this chapter is to delineate the practical issues effecting electronic evidence in criminal practice in the UAE. This will make a valuable addition to literature on the regulation of electronic evidence in the UAE, and will be done by filling the existing lacuna that prevails due to the dearth of academic resources. This applied study will comprise questionnaires and interviews. Hence, it will offer a basis for testing the hypotheses and provide evidence to support those arguments put forward in the previous chapters.

The author's primary hypothesis is that the legal regime and Criminal Procedure Law in the UAE is insufficient to govern the process of gathering, preservation, presentation and examination of electronic evidence. The researcher focuses on supporting this hypothesis with both empirical data and legal investigation. Additions must be in compliance with the UAE laws, and fill areas that are currently lacking in adequate scholastic contribution.

The viewpoints and stances of the legal experts, forensic expert, and academics will provide valuable supporting evidence, by offering an insight into current thinking on the regulation of electronic evidence in the UAE. Applied methodology offers a practical approach to indicate the problems associated with electronic evidence in the UAE. It must reflect information based on the theoretical background discussed in the

earlier chapters and reveal existing practical issues regarding electronic evidence in the UAE.

The chapter is divided into two main sections. The initial part provides a discussion of the research methodology used for this applied study. In this section, the plan of the study, including the formation of research questions, hypotheses and research methods is discussed in detail. The second section deals with the outcomes and gives an evaluation of the applied study. It provides both a description and a concise discussion of the outcomes from both the questionnaire and the interviews. At the close of the chapter, a summary of the results derived from the study is provided.

5.1 The research methodology

The most basic definition of the term "methodology" is that it is a plan of action, the process or design on the basis of which particular methods are chosen and used. It offers a connection between the research questions and the methods used to achieve the intended results.[1] Therefore, it can be said that methodology influences the choice of methods, techniques and procedures employed to collect data related to a research question or hypothesis.[2]

There exists a distinct understanding of what comprises research methodology in law. Legal problems can be solved using a discrete legal methodology. Intricate understanding is required to merge social science research methodology with legal methodology in order to compose a thorough thesis. During recent years, the socio-legal idea of research has progressed substantially, however legal thought still continues to apply a distinctive research methodology when delivering arguments.[3] The vital issue here is: what is its relationship to this study?

The answer is, that in this study, the author is attempting to merge legal methodology with social science methodology. The research methodology comprises of two main approaches, i.e. qualitative and quantitative.[4] The first is suitable for the researcher to

---

[1]Michael Crotty, *The foundations of social research: meaning and perspective in the research process* (Thousand Oaks, Calif.; London: SAGE 1998) 3.
[2] Ibid.
[3]Lee Epstein and Gary King, 'Rules of Inference, the Exchange Empirical Research and the Goals of Legal Scholarship' (2002) 69, 1 *The University of Chicago Law Review* 122.
[4]Ian Dobinson and Francis Johans, *'Qualitative Legal Research' Research Methods for Law* by Mike McConville and Wing Hong Chui (eds) (Edinburgh University Press Ltd 2007) 18-19.

conduct a thorough study of the research phenomena. A qualitative approach raises questions such as 'why' and 'how' when investigating research phenomena. On the other hand, a quantitative approach includes answers to questions like 'what', 'where', and 'when'. The first approach is appropriate when focused samples are used instead of large samples. The second approach is employed for studying research phenomena when mathematical data is required. It usually involves gathering data from a large sample, using survey techniques and statistical models to investigate research hypotheses.[5]

Methodology can also be defined as the rationale behind the research, as methods are created for use in reference to the methodology. The interview is a popular method that is widely used in practice, to support researchers pursuing a qualitative methodology. In the case of quantitative research, the method commonly applied is the questionnaire. It is increasingly the case that researchers are employing a combination of qualitative and quantitative methods. In such studies, the results derived using quantitative methods are then explained in depth with the assistance of the findings from qualitative methods.[6]

The significance and role of planning a research methodology and methods connects to the logical foundation for the study. In this regard, the researcher attempts to provide logical reasons for why one method is used for collection instead of another.

It is extremely important for the researcher to choose a suitable research methodology, as the appropriate strategy is determined by the application of vital factors: the type of data gathered, and where and when to gather it. The research methodology must be chosen when considering the nature of the research issue at hand and the information required to resolve the issue. In other words, the researcher needs to decide on an approach, which he wishes to follow when carrying out the study, yet the selected approach must also be appropriate to the issue being researched.[7]

The primary intention here, considering lack of resources, is to gather more data to answer the questions raised by the thesis. For this purpose, the author will combine questionnaire and interview methods as the tools for gathering and evaluating

[5]Nigel Gilbert, *Research Social Life* (2nd edn, Sage Publication 2001) 32-34.
[6]Ibid.
[7]Ian Dobinson and Francis Johans (n 4).

information that is essential for answering the research questions. The interviews and questionnaires used will be designed so that are suitable for collecting information regarding the lack of electronic evidence regulations under UAE's Federal Law No. 35 of 1992 in Criminal Procedure Law. The interviewer will facilitate discussion regarding the laws in place for dealing with electronic evidence, and the level of awareness and understanding of electronic evidence in the UAE.

5.2 Research methods

The given chapter uses a variety of approach methods for the purpose of gathering and analysing data. The process of combining mixed methods for research has now become an articulated and renowned method, as the third major research approach or research paradigm, when combined with qualitative research and quantitative research.[8] This method is called data triangulation and applies widely in the field of social sciences. The mixing methods, for example employing survey data and interviews, can be considered as more in depth forms of triangulation.[9]

The thesis is based on the assumption that combining questionnaires and interviews to gather data will help the researcher understand more complicated problems regarding the matter under study, thereby producing an image of electronic evidence. The items asked were tailored according to the pilot study. Three questionnaire items were eliminated following the pilot, and one open-ended question inserted to allow more opportunity for the participants to convey their viewpoints.

The participants answering the questionnaire were chosen on a random basis from Federal and local courts, Federal and local police departments, and Federal and local prosecution services across seven Emirates. However, the selection of the interviewees was done according to a purposive sampling technique. These processes will be discussed in more detail later.

5.2.1 Questionnaire

The questionnaire is one of the most commonly employed and effective tools employed for data collection. Its main advantages are that it is not only easy to develop but is also

[8]Burke Johnson, 'Toward a definition of Mixed Methods Research' (2007) *Journal of Mixed Methods Research* 112.
[9] See: Abbas Tashakkori and Charles Teddlie, *SAGE Handbook of Mixed Methods in Social and Behavioral Research* (2nd edn, Thousand Oaks, Calif.; London: SAGE 2010).

flexible and appropriate for the swift collection of large amounts of information in a form that can be easily processed.[10]

The questionnaire issued was designed in such a way that the anonymity of the respondents would be guaranteed. Moreover, the questionnaire did not request any personal information. It is hoped that this will have encouraged the participants to express their opinions freely when answering. Interviewer bias is not a concern as it is completely excluded when using this type of questionnaire.

Using a questionnaire is a valid, consistent and appropriate technique for data acquisition and well-suited to the objectives of the study. Brace is of the view that the function of the questionnaire is to draw out the necessary data in order to help the researcher answer the aims of the study.[11] Many questionnaires are formed with the objective of assessing an individual's behaviour towards a specific matter of concern, which is referred to as a state of promptness, a propensity to respond to or act in a particular way when certain stimuli are encountered.[12]

To obtain qualitative data, open-ended questions are used to which the respondents then give written responses, which can be used as illustrative quotations, or to identify new avenues and issues for exploration. In an open-ended question, there are no response options available to the respondents. Instead, there is a blank space, which they are required to complete. An example of an open-ended question would be: Do you have Comments? If yes, write them below.

The researcher attached an 'Abstract of Study', a 'Letter of Consent', and a 'Letter from the research Supervisor' with the questionnaire to explain the reason for gathering the data. The rights of the respondents and important details about the research are also highlighted on the questionnaire cover page. These were important steps to insure that the response rate would be high and that the responses given would have reliability and

[10] Ibid.
[11] Ian Brace, *Questionnaire Design: How to Plan, Structure and Write Survey Material for Effective Market* (2nd edn, London; Philadelphia: Kogan Page 2008) 6.
[12] Abraham Oppenheim, *Questionnaire Design and Attitude Measurement* (London: Continuum 2001) 24-25.

credibility. [13]

The questionnaire was peripherally developed around the broad aims of the thesis. The research questions formed the primary basis for developing the questionnaire and it was carried after the second year of study. This enabled the researcher to be clear on the general ideas that required testing. The first step was to brainstorm, after which the research questions were written down and were further narrowed down to determine those that would be included in the questionnaire. The basis of the questionnaire was logical and practical because an important concern for the researcher was the need to save time. A few comments from academics were also put forward by the researcher.[14] After this, the questionnaire was checked by academics and legal consultants to verify the content of the questionnaire items.[15] The Arabic version of the questionnaire was modified so that it could be easily understood by the respondents. After this, the researcher asked four apposite legal experts (judge, lawyer, prosecutor and police officer) to examine the questionnaire. This step was significant since it delivered valuable observations with regard to the design of the questionnaire, its transparency, and the way in which the respondents interpreted the questions. When the final version of the questionnaire was prepared, all these observations were taken into consideration.

Two requirements were taken into account when developing the questionnaire. The first one was to keep the questionnaire short, because the respondents may not have sufficient time to complete a lengthy questionnaire. The second was that only a few personal questions be asked in the questionnaire. These related to position and experience and did not cover broader demographic data such as income, family members and education. All the closed questions were designed to be 'opinion questions', which required the respondent to give a response on a scale or using a ranking system.[16]

The questionnaire, in its final form, was comprised of four sections. In the first, the respondents were required to choose profession-type and average practical experience.

[13]Details of adopted ethical research principles were explained to the participants through letters and on the cover page of the questionnaire. See Appendix 3: translation of the questionnaire (English); and Appendix 1: translation of letter of consent (English).
[14]The comments were provided by the supervisor Dr. Yvonne McDermott and the College's Ethics Committee.
[15]The checks were performed by two academics from UAE University.
[16]Bill Gillham, *Developing a Questionnaire* (London: Continuum 2000) 34.

The second section consisted of eight statements with which to explore the level of knowledge and understanding of electronic evidence. In this section, the respondents were asked to choose one of the multiple options available (I know/I don't know). Then, in the third part, the respondents were asked to select one of the given (Yes/No) choices in relation to twelve statements. This part of the questionnaire was comprised of questions intended to discover what aspects affect the regulation of electronic evidence in the UAE.

The next set of questions were based on a Likert scale design. This was a simple three-degree scale, with the options agree, unsure or disagree. The respondents were also asked to give their comments, recommendations, and opinions regarding the supporting arguments, if any, at the end of the statements. The main focus of this section was on measuring how far the respondents agreed or disagreed on the regulation of electronic evidence in the UAE. The intention behind asking for comments was to understand the reasons underlying their attitudes. The order of the questions was from general to particular. Various questions belonging to different categories were directed towards assessing the legal expert's attitudes towards electronic evidence regulation in the UAE.

There are a set of rules on the basis of which a sample is chosen. One of the essential steps in any research study is "Sampling". Hence, it was extremely important for the researcher to choose a suitable sampling strategy. In this case, the researcher chose a 'simple random sample'. There were two factors that determined the size of the sample. Standard errors can be reduced significantly if a larger sample is used. Meanwhile, cost and time also have to be considered. Therefore, the size of the sample should be chosen taking into consideration these two factors.[17]

Four groups were formed to administer the sample: prosecutors, lawyers, police officers, and judges. These participants were randomly selected from: Federal and local courts, Federal and local prosecution, and Federal and local police departments, across seven Emirates. There is no credible total figure for the number police officers, lawyers, prosecutors, and judges in the UAE. For this reason, a sample of 200 appears to be suitable for this research. With regard to reliability, the researcher decided to use

[17]Arlene Fink, *How to Sample in Surveys* (2nd edn, Thousand Oaks [Calif]; London: SAGE 2002) 43-49.

Cronbach Alpha's reliability scale in SPSS to measure the questionnaire's reliability.[18]

After deciding on the aspects relating to the size and method of sampling, the researcher embarked on the fieldwork. The completion rate after the primary responses was 63%; the researcher decided to do improve in this by asking respondents to answer face-to-face. This action increased the response rate to 94.2%, a rate, which is high enough for the study purposes. After checking the questionnaires, only the completed questionnaires, with no skipped questions, were adopted for analysis.

5.2.2 Interview considerations

Interviews were used as a second method in this research. Any conversation that follows a structure and has an objective is called an interview. The interview is something more than the impulsive exchange of opinions in daily conversations, and includes a vigilant questioning strategy and methodology with the aim of acquiring knowledge that can be systematically tested.[19]

Interviewing is suitable when the objective of a research study is to research an organisation, a company, a process or a policy.[20] In the case of interviews, researchers have the opportunity to gather information from a number of stances relating to a specific matter. It is a suitable method for illuminating the complexities of the problem and allows the researcher to explore unofficial truths regarding a process or organisation.[21]

The main issue of concern in this study relates to electronic evidence as gathered by specialised persons in the field. "How" and "Why" questions assist with the collection of such information in an effective manner. The results from the questions will be confirmed by carrying out a comparison with academic writing that is available in the field of electronic evidence, and the experience of other jurisdictions in its regulation.[22] Despite the fact that interviews are both -money and time- consuming, the study is

[18]The researcher would like to thank Dr. Jani Kassab Statistics Supervisor at Bangor University for re-checking the results of the questionnaire.

[19] Steinar Kvale and Svend Brinkmann, *Interviews: Learning the craft of Qualitative Research Interviewing* (2nd edn, Los Angeles; London: SAGE 2009) 3.

[20]Keith Punch, *Introduction to Social Research: Quantitative and Qualitative Approaches* (London: Sage Publication 2004) 144.

[21] Christine Daymon and Immy Holloway, *Qualitative Research Methods in Public Relations and Marketing Communications* (London: Routledge 2002) 105-106.

[22]For a discussion; see Robert Yin, *Case Study Research: Design and Methods: Third publication: Applied Social Research Methods Series* (4th edn, SAGE Publications 2008).

small-scale and conducted in an easily accessible geographical area: the UAE, the researcher's home country. Thus, costs were kept to a minimum.

While questionnaires are appropriate in cases where a large sampling is required, interviews are also ideal for groups of smaller numbers. The selection of interviewees has to be vindicated. In view of this, it was ensured that the selection of interviewees was based on logical reasons. Although there was some choice when it came to interviewing officials, there were a very small number of experts available to be interviewed. There were a limited number of interviews conducted, and most were undertaken with members of the official authorities who were considered 'key', thus, the selection process was "purposive".[23]

The researcher had to select interviewees with a particular objective in mind, since their opinions would be vital to the investigation. The act of choosing the interviewees in a deliberate manner was completely justified. The researcher purposively selected twelve participants for interview (two each from the categories judges, academics, police officers and forensic investigators, and one each from the categories lawyers, and prosecutors, and the Minister of the UAE Justice and the General Director of the Institute of Training and Judicial Studies).

It is often considered that in face-to-face interviews respondents are likely to disclose more information when they consider the researcher to be a trustworthy and a reliable person.[24] Consequently, the researcher anticipated that the interviewees might ask him to prove his credibility. The first step taken by the researcher was to contact the interviewees. Following this step, the researcher delivered a 'Letter of Consent', a 'Letter from the research Supervisor' and an 'Abstract of Study', to each informant via e-mail or fax. The third step was to contact the interviewees and communicate the time and place arranged to conduct the interviews. The time allocated for each interview was between 30 and 45 minutes. Following return of the consent forms the interviewer obtained spoken permission from the interviewees to record their interviews. A digital voice recorder was used to record the interviews. This device was such that the recorded files could be transferred to the computer. In total, nine interviews were required but three interviews could not be recorded since those interviewees did not

[23]Martyn Denscombe, *The Good Research Guide* (Buckingham: Open University Press 1998) 15.
[24]Ibid, 110-111.

agree to the recording. The interviews were conducted in Arabic so that the interviewees did not face any difficulty in communicating their message clearly and confidently. All the interview questions and responses were translated into English. Two translation specialists reviewed the translations so that credibility could be confirmed.[25]

There are three major classifications for interviews, these are: structured, semi-structured and unstructured.[26] In this study, the most suitable method for gathering information from the selected participants was deemed to be to conduct a semi-structured interview. The interviews conducted can best be described as 'elite' interviews. The definition of the term 'elite interview' is:

> 'When an interview is carried out with a person who holds a position of authority, or particularly expert or authoritative, individuals who have the ability to give responses with deep understanding and an ample knowledge of the topic being studied by the researcher'.[27]

The type of interview was semi-structured. This required that the researcher would only ask questions of an open-ended nature. The underlying assumption here was that the interviewees were experts who could introduce new avenues of exploration.[28] For the purposes of the study, the researcher arranged interviews with people who hold authority and occupy top positions; for example the Minister of UAE Justice, the President of the UAE Federal Supreme Court, the Head of the Fujairah Federal Court of the First Instance, the Legal Advisor to the UAE Ministry of Interior, the chief prosecutor and lawyer and other officials.

The questionnaire findings assisted the researcher to design interview questionnaire taking into account themes resulting from the initial surveys. The interview questions were devised to elicit extra information and insight into the topic under study.[29] Taking into consideration the fact that these were elite interviews, the researchers asked for comments on topics instead of asking direct questions. Adequate time was given to the

[25] Abdullatif Peran (PhD in Translation) and Ashraf Mahmud, certified legal translators at the UAE Ministry of Justice.
[26] Colin Robson, *Real World Research: A Resource for Social Scientists and Practitioner Research* (3rd edn, Chichester: Wiley 2011) 270.
[27] Bill Gillham, *The Research Interview* (London: Continuum Press 2000) 81.
[28] Bill Gillham, *Case Study Research Methods* (London: Continuum 2000) 64.
[29] All transcripts are included in Appendix 5.

interviewees to express their knowledge and understanding and explain their interpretations of the problem.[30]

The first interviewee was Ahmed Al Ketbi, forensic investigator for the Telecommunications Regulatory Authority of the UAE. The questions asked when interviewing him related to technical procedures, practical problems, and recommendations for reform.

The second interview was with Judge Dr. Mohammed AL kaabi, President of the UAE Federal First Instance Court-Fujairah. The questions in this interview related to practical problems faced by judges with regard to electronic evidence in the UAE, and his opinion regarding the rules covering electronic evidence. The interview was not recorded since Judge Mohammed did not agree to this.

The third interviewee was with Professor. Mohamed Elamin Elbushra, Managing Director of the African Centre for Criminal Justice Researches and Studies, Legal Advisor at UAE Ministry of Interior, and Dean of the Studies and Research Centre at the Arab League – Naïf Arab University. The questions in this interview related to the rules covering regulation of electronic evidence. The interview concentrated on how far the UAE's Criminal Procedure Law rules could be interpreted and applied to electronic evidence, shortcomings, recommendations, and proposals for reform.

The fourth interview was with Major Rashid Lootah, head of the Electronic Evidence Unit at the Criminal Evidence and Criminology Department of the Dubai Police. The questions in this interview focused on all examination procedures and analysis of electronic evidence, highlighting the difficulties and challenges requiring further regulation.

The fifth interview was with Lieutenant-Colonel Saeed Al Hajiri, Director of the Criminal Investigation Department's electronic crime section of the Dubai Police. The main aim of this interview was to attain verification of the practical difficulties and challenges faced by police officers when gathering and sizing electronic evidence.

The sixth interview was with Judge Dr. Abdul Wahab Abdul, President of the UAE Federal Supreme Court. Judge Dr. Abdul Wahab provided an important outline of

[30]Ibid.

opinions regarding the shortcomings in electronic evidence regulation and the necessity for a special procedural law to regulate all processes associated with handling electronic evidence.

The seventh interviewee was Younis Al belooshi, Chief Prosecutor, Dubai Public Prosecution. The questions in this interview focused on the challenges faced by prosecutors with regard to electronic evidence and on providing solutions and recommendations.

The eighth interviewee was a lawyer, and since he asked for anonymity this is preserved. He has over 15 years of experience and the interview was not recorded. The objective of this interview was to cover the problems faced by lawyers with regard to electronic evidence.

The ninth interviewee was Dr. Mohammed Al Kamali, General Director of the Institute of Training and Judicial Studies in UAE. The questions in this interview focused on the problem of the authenticity of electronic evidence in the UAE and the importance of training and development in this area.

The tenth and eleventh interviews were with Dr. Ali Hamouda, Head of the Dubai Police Academy and a police officer, who asked for anonymity and that the interview be unrecorded. The aim of these interviews was to clarification their opinions towards regulation of electronic evidence in the UAE. These interviews were an important which represented a dissenting opinion to regulate electronic evidence in the UAE.

The twelfth interviewee was the Minister of the UAE Justice, Dr. Hadef Al Dhahiri. The purpose of this interview was to discuss the opinions introduced in the previous interviews and to discover the UAE's views on the regulation of electronic evidence.

The interviews demonstrated widespread agreement about the weaknesses associated with electronic evidence regulation in the UAE. Almost all the participants [31] agreed that the UAE's Criminal Procedures Law is not adequate to cover electronic evidence processes and that we must propose a Federal law and adopt relevant guidelines in order to regulate electronic evidence.

[31] Three out of twelve of the interviewees' believe that the UAE does not need to regulate electronic evidence by imposing special rules.

5.3 Analysis and results of the applied study

The questionnaire for this study was a mixed-survey instrument including open and close-ended questions. The open-ended items provided space for the respondents to answer with their own subjective comments. The open-ended questions were included in section four of the questionnaire. The questionnaire was written in Arabic for the Arabic speaking participants, but it has been translated into English as accurately as possible, although there may be some linguistic variances.

Although this was a social science interview, it was relatively easy to evaluate the questionnaire. Multiple variables demanding thorough analysis using correlation packages were absent in this study. Hence, "Microsoft Excel" was sufficient to handle the data. The data was fed into the software so that it could be processed in a form that would be helpful to fulfil the study objectives.

With reference to demographic information and questions about average amount of practical experience, the figure (1) shows that approximately 33% of respondents have 7 to 10 years practical experience. In addition, around 28% of participants have 11 to 15 years practical experience. Thus, the majority of the respondents 61% can be considered to have sufficient practical experience to give valuable responses. Figure (1) shows the results of the analysis.

Figure 1: Average practical experience.

Average practical experience.

	What is your profession type					
Answer Options	**Judge**	**Prosecutor**	**Lawyer**	**Police officer**	**Response Percent**	**Response Count**
3-6 Years	10	25	14	4	26.5%	53
7-10 Years	12	14	22	17	32.5%	65
11-15 Years	13	10	11	21	27.5%	55
16 Years and over	15	1	3	8	13.5%	27
					answered question	200
					skipped question	0

1- Awareness and understanding level of the electronic evidence in the UAE

The respondents were asked to choose one of two options available (I know/I don't know) to rate their own familiarity with eight statements to explore the depth of their knowledge and understanding of electronic evidence in general.

A. The difference between electronic evidence and other kinds of evidence

The familiarity of the participants with: "The difference between electronic evidence and other kinds of evidence", is show in figure (2). The majority of the participants, 68%, were able to differentiate between electronic evidence and other kinds of evidence. The highest success rate can be found amongst judges (78%), with 54% for lawyers. This means that almost half of lawyers could not differentiate between electronic evidence and other kinds of evidence. This is supported by the one lawyer who was interviewed; he said: 'The main challenge is the understanding of the electronic evidence. I think the level of understanding concerning electronic evidence and how it is collected and analysed is low'.[32] Figure (2) shows the results of the analysis.

Figure 2: The difference between electronic evidence and other kinds of evidence.

The difference between electronic evidence and other kinds of evidence.						
	What is your profession type					
Answer Options	Judge	Prosecutor	Lawyer	Police officer	Response Percent	Response Count
I Know	78%	68%	54%	72%	68.0%	
	39	34	27	36		136
I don't know	22%	32%	46%	28%	32.0%	
	11	16	23	14		64
					answered question	200
					skipped question	0

B. Methods of gathering electronic evidence

To investigate whether police officers, lawyers, prosecutors, and judges were familiar with methods for gathering electronic evidence or not, the participants were asked a question on this. The total number of sample claimed not to have any knowledge was 79%, while the highest percentage (26%) of police officers replied that they applied these procedures. Figure (3) shows the results of this analysis.

[32] Anonymous lawyer Interview conducted (February 2013 Sharjah-UAE). See: transcript translated of the interviews in Appendix 5

Figure 3: Methods of gathering electronic evidence.

Methods of gathering electronic evidence.						
	What is your profession type					
Answer Options	Judge	Prosecutor	Lawyer	Police officer	Response Percent	Response Count
I Know	18%	24%	16%	26%	21.0%	
	9	12	8	13		42
I don't know	82%	76%	84%	74%	79.0%	
	41	38	42	37		158
					answered question	200
					skipped question	0

The most serious problem that faces those gathering electronic evidence is lack of knowledge; this can lead to lost or inadmissible evidence. In support of this view, forensic investigator said:

> There are many cases where we lose evidence…The problem is the nature of electronic evidence. Electronic evidence is intangible evidence it's not like other evidence. The difficulty lies in how to find the evidence and get it. The investigator's experience plays an important role in finding evidence and the recovery. If the investigator doesn't have enough experience we will not be able to find the evidence. The error here was not a procedural or criminal intelligence problem, but the investigator's experience.[33]

An investigation should be carried out to determine the admissibility of any evidence adduced in court. A police officer must ensure that all relevant procedures have been strictly followed. Thus, before any action leading to the search and seizure of electronic evidence is carried out, the investigator must take into consideration that he/she needs a search warrant first, and must follow all the rules written in the warrant. Searching without a warrant is not allowed in the UAE legal system, except under circumstances, as stated in Chapter Four.[34]

However, some cases need urgent action, especially those where electronic evidence is key. Time getting a search warrant can lead to loss of evidence. To probe this issue, the researcher asked Lieutenant-Colonel Saeed Al Hajiri about it, he said:

[33] Ahmed Al Ketbi, forensic investigator at Telecommunications Regulatory Authority of the UAE, Interview conducted (January 2013 Dubai-UAE). See: transcript translated of the interviews in Appendix 5.
[34] See: section 4.2.2.3 and section 4.2.3.

> Our department received a report that there is hacking on the government website, after proving this status and during our taking of action, the suspects were deleting the evidence and we cannot prove the crime.[35]

It is therefore appropriate to look at this issue when regulating electronic evidence. Furthermore, knowledge of the methods for gathering electronic evidence is extremely important because lack of knowledge can result in inefficiency that will affect the collection of electronic evidence.

C. Placement of electronic evidence in the cybercrime scene

The statement, 'placement of electronic evidence in cybercrime scene', was put to the participants. The aim of the above statement was to investigate whether or not the respondents know that electronic evidence can be found in different places, also that it can be found in the UAE or abroad. The analysis revealed that 83% of the participants claimed not to have any knowledge where to look for electronic evidence, or where it could found. This is shown in figure (4).

Figure 4: Placement of electronic evidence in the cybercrime scene.

Placement of electronic evidence in the cybercrime scene.						
	What is your profession type					
Answer Options	Judge	Prosecutor	Lawyer	Police officer	Response Percent	Response Count
I Know	16%	26%	4%	22%	17.0%	
	8	13	2	11		34
I don't know	84%	74%	96%	78%	83.0%	
	42	37	48	39		166
					answered question	200
					skipped question	0

It is important that investigators be aware of the potential locations where electronic evidence may be found. Without this knowledge, some evidence may not be seized. Lack of expertise or skill of the investigator is among the factors leading to loss of evidence and inefficient combating of criminals. As a result, qualified people must collect electronic evidence to avoid loss of evidence. Chief Prosecutor Younis Al belooshi supported this view:

[35] Lieutenant-Colonel Saeed Al Hajiri, Director of the Criminal Investigation Department's-Electronic Crime Section- Dubai Police, Interview conducted (January 2013Dubai-UAE). See: transcript translated of the interviews in Appendix 5.

> There are a number of issues and challenges are faced with regard to electronic evidence in the UAE. There are issues relating to how to get the evidence, challenging on the search, seizure, and preservation processes. Most of these procedures are understood by police officers, lawyers, prosecutors, and judges. There is no technician present during a seizure of electronic evidence.[36]

Professor, Elbushra [37] argued that we should rely on qualified people when handling electronic evidence; he added: 'The person must have qualifications and must pass a number of courses'.[38]

With regard to evidence located abroad, UAE law enforcers face challenges such as time to obtain evidence and lack of international cooperation. Lieutenant-Colonel, Al Hajiri gave a practical example of this issue, stating that the Criminal Investigation Department's Electronic Crime Section of the Dubai Police had applying for evidence from abroad since 2010, and even then did not have it.[39] When asked about the regional issue of electronic evidence and whether UAE laws can deal with this issue, Judge Al Kaabi said (and almost all of the interviewees also supported this view)[40]:

> …I think there is a gap in the laws in this field, there is no rule regulating this issue [obtaining evidence abroad]. I guess this can be dealt with by standard international criminal procedures.[41]

D. Methods of preservation of electronic evidence

As shown in earlier chapters, electronic evidence can be altered, lost or destroyed and there is possibility that it may not be possible to retrieve all evidence or data, as a consequence of poor handling when collecting electronic evidence. This is one of the main reasons for lost evidence. Therefore, in order to investigate this issue, the participants were asked if they were familiar with what preservation methods should be

[36] Younis Al belooshi, Chief Prosecutor–Dubai Public Prosecution, Interview conducted (February 2013Dubai-UAE). See: transcript translated of the interviews in Appendix 5.
[37] Professor Mohamed Elamin Elbushra, Managing Director at African Centre for Criminal Justice Researches and Studies, Legal Advisor at UAE Ministry of Interior, Dean of the Studies and Research Center at Arab League – Naïf Arab University, Interview conducted (January 2013Abu Dhabi -UAE). See: transcript translated of the interviews in Appendix 5.
[38] Ibid.
[39] See: translated transcript of the interview with Al Hajiri in Appendix 5.
[40] See: transcript translated of the interviews in Appendix 5.
[41] See: translated transcript of the interview with Judge Al kaabi in Appendix 5.

used when gathering electronic evidence. The analysis of the participants' answers revealed that the majority (80%) of police officers were claimed unfamiliar with the procedures to be followed to guarantee the preservation of electronic evidence. As a result, the percentage of possibility to lose electronic evidence is extremely high. In fact, this was one of the main reasons for suggesting a pertinent need to regulate electronic evidence. Figure (5) demonstrates the result of the analysis. Interviews supported this view, Forensic investigator Al ketbi said: '…There are many cases where we have lost the evidence due to bad handling...'. He also gave an example of bad handling:

> Without naming names, one of the authorities in the UAE told us that one of its staff disseminated and misused a body of information. After investigation we found that the authority had formatted the computer. As a result, we were unable to get the evidence. It was due to bad handling from the authority.[42]

Figure 5: Methods of preservation of electronic evidence.

Methods of preservation of electronic evidence.						
	What is your profession type					
Answer Options	Judge	Prosecutor	Lawyer	Police officer	Response Percent	Response Count
I Know	2%	18%	4%	20%	11.0%	
	1	9	2	10		22
I don't know	98%	82%	96%	80%	89.0%	
	49	41	48	40		178
					answered question	200
					skipped question	0

E. Procedures for electronic evidence examination

As discussed earlier, the procedures for examining electronic evidence should be clear to any party, and must be documented. Accordingly, participants were asked to rate their familiarity with the "procedures for electronic evidence examination". 89% of all respondents claimed not to have any knowledge regarding the procedures of electronic evidence examination. Figure (6) shows the result of the analysis.

[42] See: translated transcript of the interview with Al ketbi in Appendix 5.

Figure 6: Procedures for electronic evidence examination.

Procedures for electronic evidence examination.						
	What is your profession type					
Answer Options	Judge	Prosecutor	Lawyer	Police officer	Response Percent	Response Count
I Know	8%	18%	2%	16%	11.0%	
	4	9	1	8		22
I don't know	92%	82%	98%	84%	89.0%	
	46	41	49	42		178
					answered question	200
					skipped question	0

Therefore, the statement raised the issue of a guarantee when examining procedures and reaching valid conclusions. As one of the interviewee said:

> I think that we need own procedures dealing with all processes starting with seizure, preservation and examination of electronic evidence. When it has; nobody can argue and also it will be assurance that all procedures have been followed by the investigator.[43]

Regarding reaching valid conclusions, the head of the Electronic Evidence Unit at the Criminal Evidence and Criminology Department- Dubai Police said:

> The results from the forensic expert's report are only a personal view of the expert. We can ensure by internal audit that all procedures were followed are correct, but we cannot ensure the conclusion.[44]

Forensic examination is very new in the UAE and at present there are no specific rules to explain the detailed aspects of a forensic examination. As a result, one of the benefits of finding rules covering the examination procedures is convincing the judge. Through the existence of rules we can ensure that all forensic experts or members of the police follow the correct procedures.

F. Techniques and tools for electronic evidence examination

The participants were presented with the following statement to discover their familiarity with 'Techniques and tools for electronic evidence examination'. The analysis showed that almost all the respondents (94.5%) claimed not to have any

[43] See: translated transcript of the interview with Al ketbi in Appendix 5.
[44] See: translated transcript of the interview with Lootah in Appendix 5.

knowledge about the techniques and tools used for examining electronic evidence. Despite the fact that this is a technical matter, police officers, lawyers, prosecutors, and judges should have basic knowledge about the tools and techniques used for restoring and analysing electronic evidence. Such understanding is extremely important for discussing forensic reports, as is essential to know that evidence deleted from a device can be backed up or recovered using certain tools and techniques. Not only that but it is also important to ensure that the tools used are upgraded to guarantee an appropriate level of reliability and accuracy. Figure (7) shows the result of the analysis.

Figure 7: Techniques and tools for electronic evidence examination.

Techniques and tools for electronic evidence examination.						
	What is your profession type					
Answer Options	Judge	Prosecutor	Lawyer	Police officer	Response Percent	Response Count
I Know	4%	12%	2%	4%	5.5%	
	2	6	1	2		11
I don't know	96%	88%	98%	96%	94.5%	
	48	44	49	48		189
					answered question	200
					skipped question	0

G. Forensic expert's reports of electronic evidence

The next statement focused on the forensic experts' reports. The participants were asked to respond to the statement: 'Forensic expert's reports of electronic evidence; how to get the results, presented and discussed'. The analysis of the participants' knowledge revealed that many of the respondents (87%) claimed not to have any knowledge on how to attain forensic reports results or how to present and discuss these reports. Only a small percentage (26%) of the prosecutors had this knowledge. However, only 4% of the police officer and lawyers respondents reported that they had this knowledge. Judge Al kabi said: '…It is hard for judges to understand the technical terminology'.[45] One forensic investigator said: 'In fact, the judge is only looking for the conclusion not for the procedures. In contrast, the level of lawyers' knowledge about electronic evidence or what should be in an expert's reports is very low. Therefore, he/she cannot discuss the reports'.[46] Figure (8) demonstrates the result of the analysis.

[45] See: translated transcript of the interview with Al kabi in Appendix 5.
[46] See: translated transcript of the interview with Lootah in Appendix 5.

Figure 8: Forensic expert's reports of electronic evidence.

Forensic expert's reports of electronic evidence (how to get the results, presented and discussed).						
	What is your profession type					
Answer Options	Judge	Prosecutor	Lawyer	Police officer	Response Percent	Response Count
I Know	18%	26%	4%	4%	13.0%	
	9	13	2	2		26
I don't know	82%	74%	96%	96%	87.0%	
	41	37	48	48		174
					answered question	200
					skipped question	0

H. Challenges and problems of cybercrimes in relation to electronic evidence

Section two of the questionnaire concluded with the following statement: 'challenges and problems of the cyber-crimes in relation to electronic evidence'. The aim of this statement was to probe into police officers', lawyers', prosecutors' and judges' knowledge about the challenges and problems resulting from the need to collect electronic evidence. The results demonstrated that a significant percentage of the participants (74.5%) claimed not to have any knowledge regarding the difficulties that can arise as a consequence of utilising electronic evidence. Figure (9) illustrates the result of this analysis.

Figure 9: Challenges and problems of cybercrimes in relation to electronic evidence.

Challenges and problems of cybercrimes in relation to electronic evidence.						
	What is your profession type					
Answer Options	Judge	Prosecutor	Lawyer	Police officer	Response Percent	Response Count
I Know	28%	30%	26%	18%	25.5%	
	14	15	13	9		51
I don't know	72%	70%	74%	82%	74.5%	
	36	35	37	41		149
					answered question	200
					skipped question	0

Judge Al kabi said:

> We face many challenges, the main challenge I think is a lack of experienced judges, and a low level of understanding and awareness. The reason for this could be the limited number of cases that contain electronic

> evidence and the age of the judges, as well as, the lack of training and specialised workshops.[47]

This idea was supported by another interviewee, a legal advisor at UAE Ministry of Interior. Elbushra affirmed that cybercrime and electronic evidence is a new topic with global implications, and that in the UAE handling of this issue is in the early stages. At present, the level of understanding and awareness is very low. In the UAE, there are no academic courses, training courses or workshops in the field of electronic evidence or cybercrime. Cybercrime is a high tech crime, which requires a high level of knowledge. Many members of society are victims of cybercrime; they do not know how to handle this type of crime or even maintain the evidence. Many people lose accounts, and their crimes are discovered only accidentally. Thus, we need more focus on such topics, as they will help us to increase our level of knowledge and find ways to fill the gaps in the law.[48] According to David Wall, one of the main problems when studying crimes is the lack of statistical evidence because many offences are not reported.[49]

A practical example, between 2010 and 2013 was that many people in e-government services in the UAE had their accounts hacked and experienced fraudulent use of their credit cards; 16 million UAE Dh was stolen, but the crime was only discovered accidentally.[50]

Raising knowledge and awareness of this issue is extremely important since at present defendants are more knowledgeable than the judges, prosecutors and investigators. In order to raise the level of knowledge of judges, prosecutors and lawyers, the United Nations Interregional Crime and Justice Research Institute (UNICRI) conducted a two-phase program called "Cybex" over a period of three years (2008-2010), across 21 European and 3 South American countries, with the result that they improved judges', prosecutors', and lawyers' knowledge of electronic evidence.[51] A similar project would

---

[47] See: translated transcript of the interview with Al kabi in Appendix 5.
[48] See: translated transcript of the interview with Professor Elbushra in Appendix 5.
[49] See: David Wall, *Crime and the Internet* (Taylor and Francis Group 2001).
[50] Mohammed Fodah, 'Gang stolen credit card data of banks customers' *Emaratalyoum Newspaper* (Dubai, 19th September 2013) <http://www.emaratalyoum.com/local-section/accidents/2013-09-19-1.607865> accessed 19th September 2013.
[51] For further information see:
<http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079if09pres_cybexrev.pdf>.

be of great benefit to the UAE. As one of the interviewees commented: 'I think we need to focus more on training, we need qualification courses'.[52]

The core aim of the above statements was to investigate whether levels of awareness and knowledge about electronic evidence in the UAE are sufficient to effectively support the full use of that electronic evidence, and to explain whether all of forensic experts and legal specialists can overcome the difficulties and problems that may occur when using electronic evidence. The analysis illustrates that on average almost 80 percent of respondents,[53] did not have sufficient knowledge of the processes used to obtain electronic evidence. As a result, from the evidence in section two of the questionnaire we can say that in general the participants did not have adequate knowledge about electronic evidence gathering or preservation processes, nor did they understand the relevant procedures for examination of this kind of evidence.

2- Practical issues of electronic evidence in the UAE

In section three of the questionnaire the participants were asked to select one of options given; they were to answer either yes to affirm applicability and no to affirm lack of applicability and presented with twelve statements. The main aim of this section was to measure attitudes of the police officers, lawyers, prosecutors, and judges towards aspects of the electronic evidence field, which they found applicable to the UAE, in order to demonstrate the most significant issues associated with electronic evidence regulation in the UAE. The analysis of results of this section of the questionnaire are represented in Figure (10).

[52]See: translated transcript of the interview with Al Hajiri in Appendix 5.
[53]The percentage who said I don't know: 32+79+83+89+89+94.5+87+74.5×100 ÷8= 78.5%

Figure 10: Ranking of twelve principle issues of electronic evidence in the UAE.

The respondent is asked to select from twelve negative aspects of electronic evidence field which they thought were applicable in the UAE (You can select an unspecified number).					
	What is your profession type				
Answer Options	**Judge**	**Prosecutor**	**Lawyer**	**Police officer**	**Response Percent**
There are no specific rules' governing search and seizure of electronic evidence.					
Yes	46	44	35	35	80%
No	4	6	15	15	20%
Response Count	50	50	50	50	
There is no procedures guide for electronic evidence preservation.					
Yes	46	36	43	40	82%
No	4	14	7	10	18%
Response Count	50	50	50	50	
Procedures for examining electronic evidence are not documented.					
Yes	7	21	16	7	25.50%
No	43	29	34	43	74.50%
Response Count	50	50	50	50	
Unqualified people collect electronic evidence.					
Yes	1	25	5	19	25%
No	49	25	45	31	75%
Response Count	50	50	50	50	
There is no technician present during a seizure of electronic evidence.					
Yes	13	34	22	24	46.50%
No	37	16	28	26	53.50%
Response Count	50	50	50	50	
Limited specialists of electronic evidence.					
Yes	33	32	20	35	60%
No	17	18	30	15	40%
Response Count	50	50	50	50	
Do not update laboratories of electronic evidence.					
Yes	1	14	5	14	17%
No	49	36	45	36	83%
Response Count	50	50	50	50	
Absence of international cooperation.					
Yes	31	31	24	26	56%
No	19	19	26	24	44%
Response Count	50	50	50	50	
Non-reporting of cyber-crimes.					
Yes	7	18	5	21	25.50%
No	43	32	45	29	74.50%
Response Count	50	50	50	50	
Absence of protection programs.					
Yes	10	14	10	14	24%
No	40	36	40	36	76%
Response Count	50	50	50	50	
Lack of coordination between departments and the regulatory bodies.					
Yes	7	21	6	10	22%
No	43	29	44	40	78%
Response Count	50	50	50	50	
Absence of awareness and indicative programs.					
Yes	44	37	31	39	77.50%
No	6	13	19	11	24.50%
Response Count	50	50	50	50	
				answered question	**200**
				skipped question	**0**

This table reveals that respondents found the top five most significant issues regarding electronic evidence regulations, as applicable in the UAE, were as follows:

I. There are no procedures or guidance for electronic evidence preservation. 82%

of the respondents believed that in the UAE there are no guidelines or principles to follow when gathering electronic evidence and that this is the most prominent issue.

II. There are no specific rules' governing search and seizure of electronic evidence. This problem ranks second, with 80% of the respondents suggesting action is needed.

III. Absence of awareness and indicative programs was the third issue, with 77.5% of respondents confirming that there is lack of awareness or sensitising programs.

IV. The idea that there are: 'limited specialists in the field of electronic evidence', took fourth place at 60% of total responses.

V. The fifth most significant issue was the lack of international cooperation or agreements; 56% of the participants stated that there is no agreement between the UAE and other countries for handling electronic evidence.

This means that regulation of electronic evidence was thought to be a significant problem by police officers, lawyers, prosecutors, and judges. In fact, these five principles are the foundation of this thesis; in particular, that electronic evidence must be regulated in the UAE. The results of section three returned the same results as found in section two, where the regulation of electronic evidence was reported as important. It is the researcher's opinion that electronic evidence falls under the umbrella of the UAE's Criminal Procedure Law. All such procedures for handling electronic evidence require tougher regulation.

This view is also supported by the findings of the interviews; the President of the UAE's Federal Supreme Court said:

> I agree with you that we face many challenges and difficulties with regard to electronic evidence, the Emirates is an advanced technology State and must have legislation, laws, and judges adapted to this development. I believe that we face procedural problems related to electronic evidence. There are no rules covering search and seizure processes, we don't know how to preserve electronic evidence or how to examine it. The judges now apply general rules of evidence which I think is not commensurate with the nature of electronic evidence and Criminal Justice. I have a viewpoint in

> this respect; the UAE must have procedural law, which regulates electronic evidence. We have a penal law on cybercrimes but we don't have procedural law. The judge faces many challenges when handling electronic evidence, it is very difficult to understand procedures or how to deal with this kind of evidence, a judge is trying to apply general rules, but I think they do not apply. On the other hand, the cognitive level of judges concerning electronic evidence is low because lack of courses and lack of law regulates this field. Finally, I must restate my opinion that we need the creation of a new law dealing with electronic evidence.[54]

He also added when asked, **'**How can the Emirates judges be sure of the reliability and authenticity of the electronic evidence?':

> Clearly, because there is a shortage of laws we depend on the forensic report and for me this represents a weakness in judgment. When a judge rules, based on the opinion of another person not his mind, this can lead to the prejudicing of justice. However, if we have clear rules the judge will be able to make a decision.[55]

Another perspective in this argument is given by Judge Al kaabi, who points out that a lack of regulatory procedures represents a real challenge in the UAE. He adds that in reality, the UAE's judges apply general rules; thus, in some cases it is difficult to apply these rules for electronic evidence. Electronic evidence differs from other evidence, so the UAE's judges face challenges when applying general rules.[56] Similarly, a Chief Prosecutor [57] and Lawyer [58] interviewed by the researcher in an interview conducted in the UAE stressed that there is a gap in the UAE law. The UAE's Criminal Procedures Law cannot cover electronic evidence processes. In the UAE the judge now applies the general rules of evidence, which are useful as a framework only. However, the nature of electronic evidence requires that we look beyond these rules. Undoubtedly, in the areas of search, seizure and examination, regulations that are more specific are necessary to handle electronic evidence. General rules cannot cover this process, so it is essential to introduce procedural law designed for electronic evidence. In contrast, three of the interviewees believe that the UAE's CPL rules are appropriate to cover electronic

[54] See: translated transcript of the interview with Judge Abdul Wahab in Appendix 5.
[55] Ibid.
[56] See: translated transcript of the interview with Judge Al kaabi in Appendix 5.
[57] See: translated transcript of the interview with Younis Al belooshi in Appendix 5.
[58] See: translated transcript of the interview in Appendix 5.

evidence.[59] Ali Hamouda, Head of the Dubai Police Academy, believes that finding a procedural law for electronic evidence will restrict the authority of the judge. Judges in the UAE legal system have freedom when sentencing. A new law will prevent judges from needing to rely on this, because there will be legal rules to apply when deciding to admit or reject evidence.[60]

He added, when asked, that some people believe that the CPL suffers from procedural problems, especially when dealing with electronic evidence, such as the use of search warrants, and that new rules are needed:

> The UAE has modern laws, and the CPL is also a modern law and is always being reviewed. In 2005, the CPL was reviewed and many rules were changed, but there was no change in evidence rules, so this rule is adequate and there is no need for change. Finding special rules requires special people to apply them, which is currently not available in UAE.[61]

A police officer interviewed by the researcher mentioned some practical problems associated with applying special rules of electronic evidence. He said:

> In practice, the application of specific rules is trickier than the application of general rules. If we have specific rules for electronic evidence, that means we must follow up all these rules and this is very difficult. The police officer must follow all the rules, and if he violates this order, the evidence will not have any value. The police officer must take action fast in order to seize evidence, and fast action may lead to not following some rules, and therefore may make the proceedings null and void. General rules give police more freedom over search and seizure.[62]

3- Measuring attitudes of the police officers, lawyers, prosecutors, and judges towards the regulation of electronic evidence in the UAE

Section four of the study was designed to elicit a 'scale response'; the questions related to the key task on the questionnaire, which was to measure the attitudes and opinions of the respondents relative to possible solutions, in order to regulate electronic evidence in the UAE. A 3-point Likert scale was used rather than a 5-point scale, as the researcher

[59] Ibid.
[60] See: translated transcript of the interview with Ali Hamouda in Appendix 5.
[61] Ibid.
[62] See: translated transcript of the interview with anonymity police officer in Appendix 5.

wanted to find agreement or disagreement, the strength of the agreement or disagreement was not relevant. After each statement the participant was asked to provide recommendations and comments, if any, to support their choice. The core objective for asking for recommendations or comments was to discover why the participants held their opinions; there were a number of useful comments, to offer clarifications for the numerical quantitative results.

The figures below have been designed to illustrate the percentages of the participants' responses, beginning with the respondents' opinions regarding possible solutions that can be offered to regulate electronic evidence.

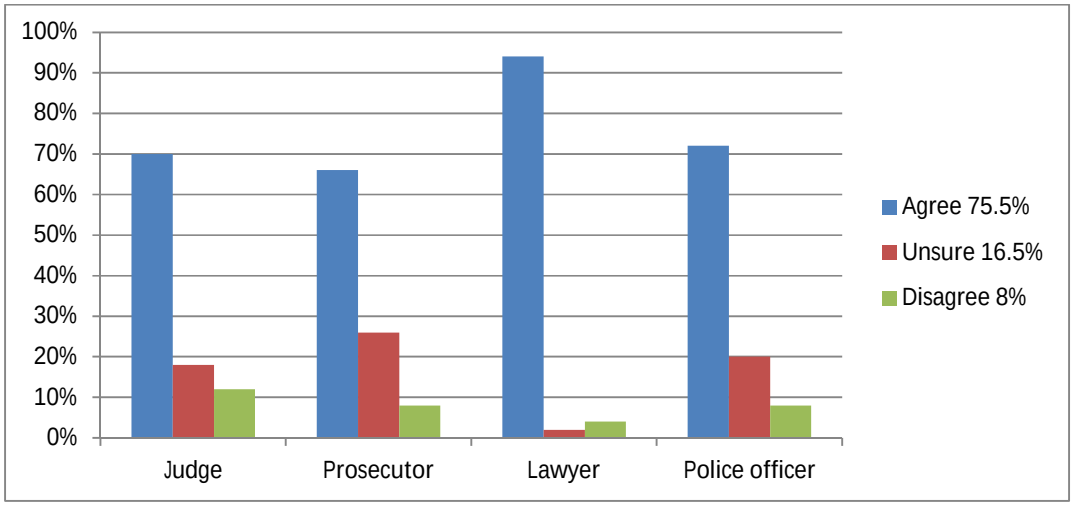
A. Legal term of electronic evidence

There has always been controversy regarding whether to define electronic evidence or not. Respondents were asked their opinions, and the results illustrated that 75.5% thought that there should be a legal set of terms to define electronic evidence (Figure 11). Only 8% of respondents disagreed. Some of the respondents commented by giving some important indicative comments: 'Defining electronic evidence may lead to narrow scope of electronic evidence'. Another one thought: 'Finding rules to regulate electronic evidence process is more valuable than defining electronic evidence'. On the other hand, another respondent thought: 'The definition of electronic evidence should be clear'. Another one agreed, stating: 'To differentiate between electronic evidence and other evidence'.[63]

With reference to the results of the first question 'the difference between electronic evidence and other kinds of evidence', this shows that only 32% were able to distinguish between the two types of evidence, and two-thirds were unable to do so. Therefore, applying a uniform definition to electronic evidence is very important. Some may argue that any definition of electronic evidence will be out of date after a few years, due to technological developments. This point of view may be true, however with such a low level of knowledge, it has become extremely important to provide a broad definition.

[63]See: questionnaire respondent comments (open-ended questionnaire question) in Appendix 4.

Figure 11: There should be legal terms for electronic evidence.



B. Promulgate clear guidelines on how to deal with electronic evidence in the UAE

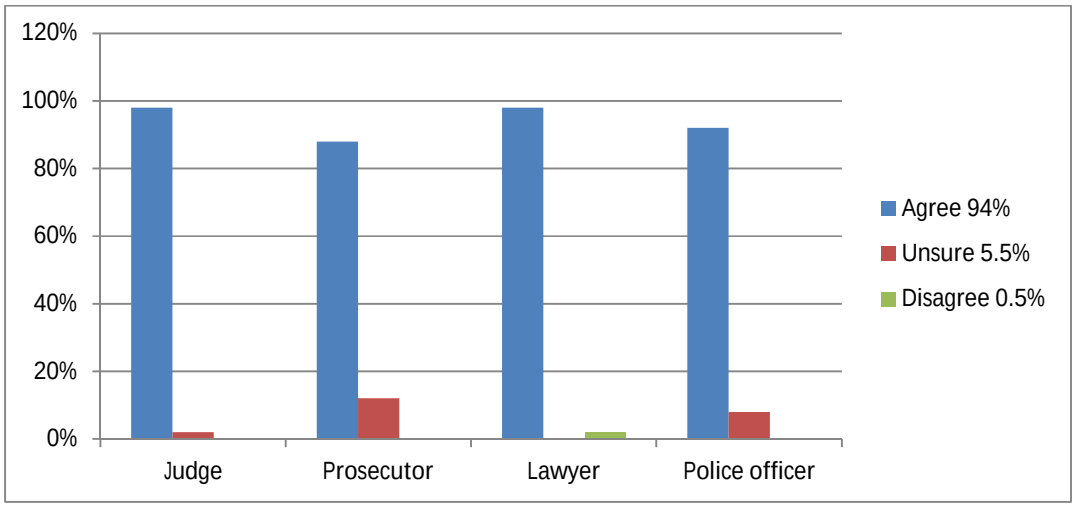
When asked whether we need to promulgate clear guidelines on how to deal with electronic evidence in the UAE, 94% of the respondents agreed. Only 0.5% of respondents disagreed, while 5.5% were unsure (Figure 12). They commented: 'In order to have clear rules', 'In order to perform correct procedures for search and seizure of electronic evidence', 'To ensure that all process of search and seizure for electronic evidence is correct', 'So we can easily check all procedures'.[64]

Those who were interviewed also argued this point (regulating electronic evidence by applying special rules and stating guidelines). A majority of those interviewed stated that the rules in the CPL are insufficient to regulate electronic evidence. Others believed that we do not need to amend the CPL and apply rules to electronic evidence.[65] This difference in opinion opens up a new area of discussion, as each group has its own arguments. In fact, the UAE has new laws, but these laws have not been tested yet, as few cases have raised procedural problems. However, the Emirates have no statistics on this issue and therefore cannot measure the magnitude of the problems. Other countries are evolving their laws, and so it seems incumbent on the UAE to improve its laws also. Crime has become global. What happens on the other side of the earth can affect those

[64] Ibid.
[65] See: translated transcript of the interview with anonymity police officer and Ali Hamouda in Appendix 5.

living in the UAE. The limited number of such cases should not be a reason for not updating laws. There may be many cases that have not yet been reported or even discovered. An example of this issue is the credit card case affecting the Ras Al Khaimah Bank. The defendants were able to penetrate the electronic system and steal customers' data. They were then accused of fraudulent use of credit cards, changing the withdrawal limit, and stealing 17 million US dollars. This robbery was discovered only after the accused tried to withdraw money from a US bank in Manhattan.[66]

Figure 12: We need to promulgate clear guidelines on how to deal with electronic evidence in the UAE.



C. Gathering electronic evidence

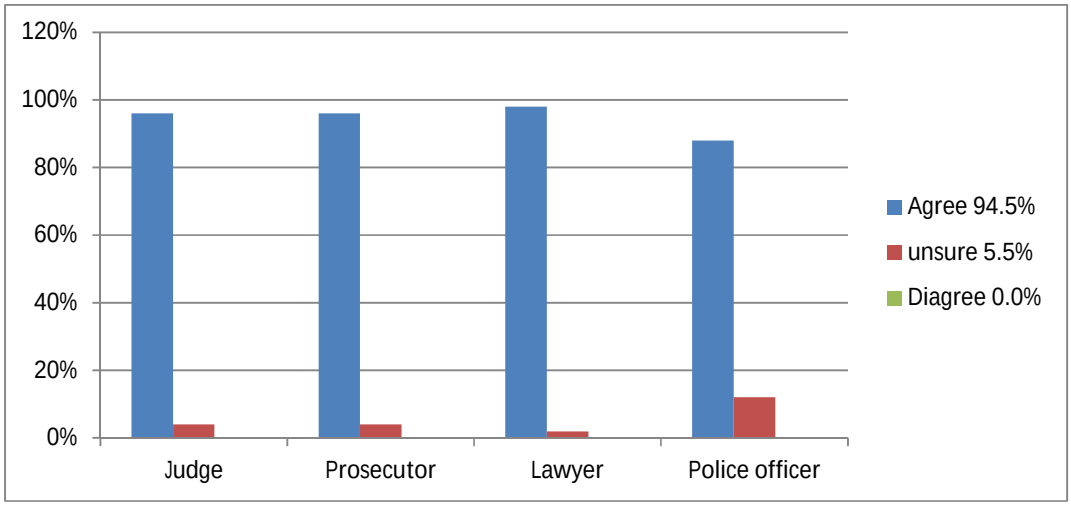
Respondents were asked whether they thought that the collection of electronic evidence should be done by qualified persons. 94.5% of respondents agreed that electronic evidence should be gathered by qualified persons, while only 5.5% were unsure (Figure 13). Respondents commented that: 'When electronic evidence collection is done by unqualified people this can lead to inadmissible evidence', 'Is extremely essential to avoid loss evidence', 'It is inconceivable all police officers have knowledge of how to deal with electronic evidence, so there should be collection of electronic evidence by qualified people'. In contrast, one of them said: 'I agree, but there are unqualified persons (they do not have certificates) having knowledge and experience in the

[66] Amal Al Minshawi, 'RAKBANK confirm penetration credit card balances worth 17 million US dollars' *Emaratalyoum Newspaper* (Dubai, 11th May 2013) <http://www.emaratalyoum.com/local-section/accidents/2013-05-11-1.573717> accessed 11th May 2013.

technical field who may help'.[67]

Although a significant percentage of respondents think that gathering electronic evidence should be done by qualified persons, there are many difficulties associated with putting this into practice. The limited number of technicians, and the extensive time needed for searches may cause difficulties. The UAE government authorities would be wise to classify those cases requiring a technician and those that do not. The authorities would also benefit from putting procedures in place to facilitate access to technical assistance.

Figure 13: Gathering electronic evidence should be by qualified persons.



D. Examining electronic evidence

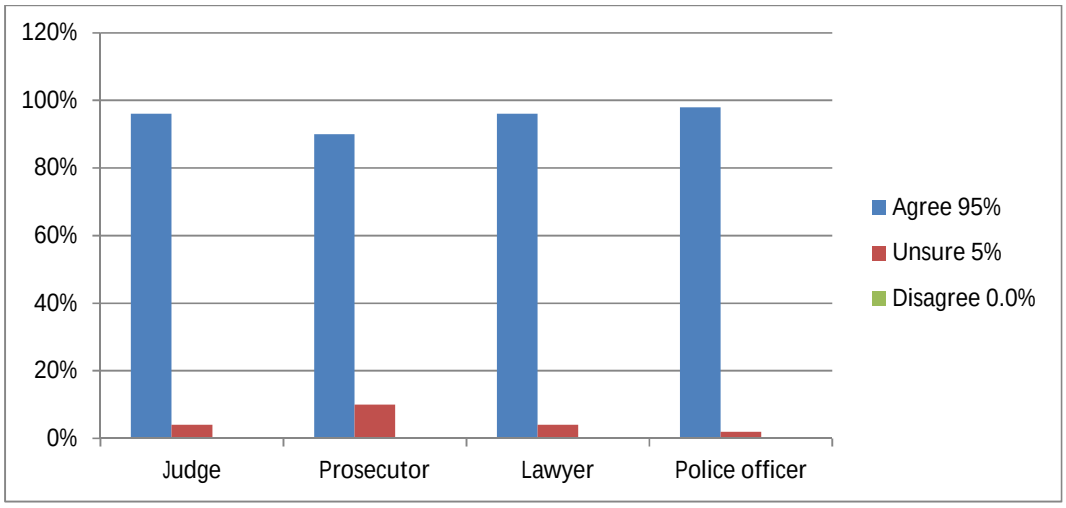
The researcher asked respondents whether the processes associated with the examination of electronic evidence should be documented. Only 5% of respondents were unsure and the majority (95%) agreed (Figure 14). They commented that: 'We need to document all the procedures when examining electronic evidence. As a result, we can guarantee the examination process', 'In order to be referenced and we can refer to it'.[68]

Legal rules have more impact than administrative rules. Administrative rules do not guarantee the proper functioning of proceedings. Thus, we need legal rules to ensure

[67]See: questionnaire respondent comments (open-ended questionnaire question) in Appendix 4.
[68]Ibid.

checks and balances are in place to guarantee reliability. Attaining a result is easy but following proceedings and ensuring reliability is a complicated process. Although most UAE laboratories are internationally recognised, they must set conditions and criteria commensurate with UAE laws.

Figure 14: Examining electronic evidence should be documented.



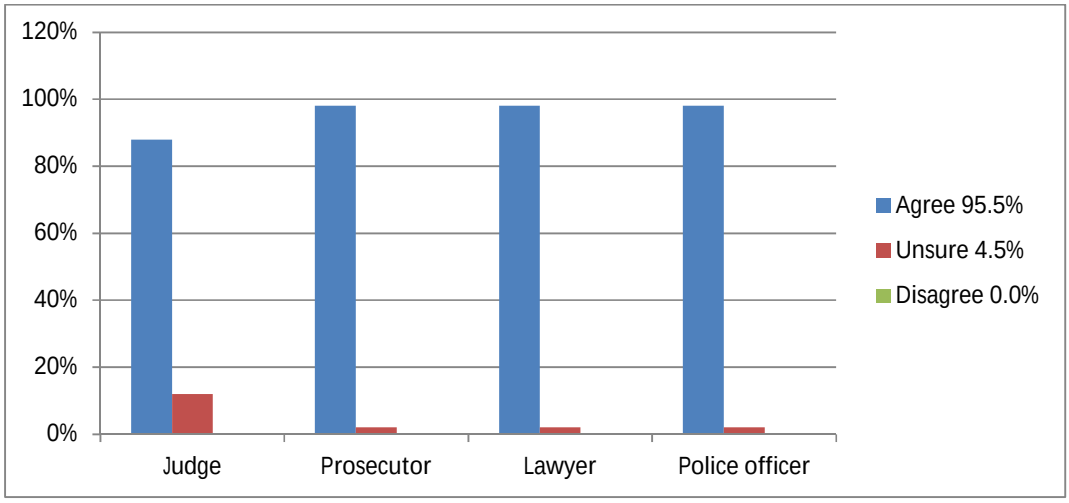
E. Update laboratories for handling electronic evidence

Subsequent to the above question, the respondents were asked: 'should we update laboratories that handle electronic evidence continuously'. The response illustrated that a substantial majority of participants (95.5%) agreed, and only 4.5 were unsure (Figure 15). They commented that: 'There should be updated laboratories to effectively combat criminals', 'To keep up pace with the technological development', 'This field is developing fast.'[69]

Nobody can argue that the development of laboratories is important. However, we should not overlook the adoption of examination devices from competent agencies. It is also important to attach expert reports to certify devices that were used in examinations.

[69]Ibid.

Figure 15: Should we update laboratories of electronic evidence continuously.



F. Professional training on electronic evidence

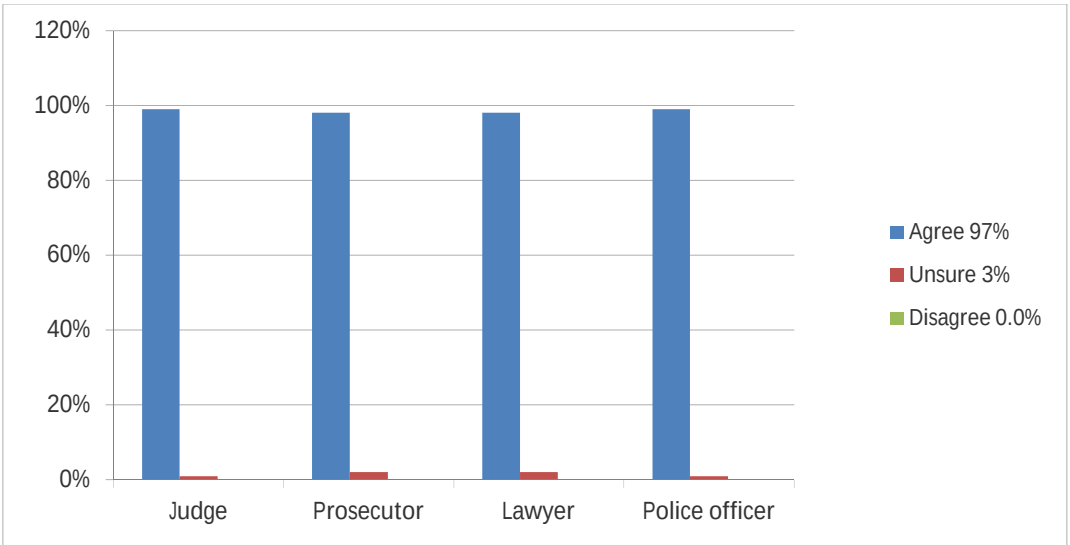
It was extremely important to measure the participants' attitudes towards knowledge and qualifications, in particular whether they needed more training and rehabilitation. The researcher asked the participants to comment on the statement: 'police officers, lawyers, prosecutors, and judges need more professional training on electronic evidence'. The results were as follows: the majority of respondents (97%) agreed, while only 3% were unsure (Figure 16). Those who agreed stated that: 'I think we need to focus on training people especially police officers'; 'Training is beneficial for admissible electronic evidence'; 'We must raise awareness among all people who deal with electronic evidence'; 'There is a government trend towards qualifying prosecutors, and judges on cybercrime'; 'Frankly, there is a delay in preparing forensic reports and level of understanding and awareness is extremely low. Police officers use primitive methods when handling electronic evidence'; 'Training is particularly powerful', 'To raise knowledge level'.[70]

It may be that training and raising the level of knowledge held is the most important consideration when building an integrated system of electronic evidence regulation. If we have the most up to date laws and laboratories, but do not have qualified people, they are of no value. Increasing knowledge is a starting point for effective application of the law. Therefore, the UAE requires more courses and seminars, and more academic

[70]Ibid.

research studies. The UAE also needs media to disseminate awareness programs.

Figure 16: Police officers, lawyers, prosecutors, and judges need more professional training on electronic evidence.



G. International cooperation and coordination

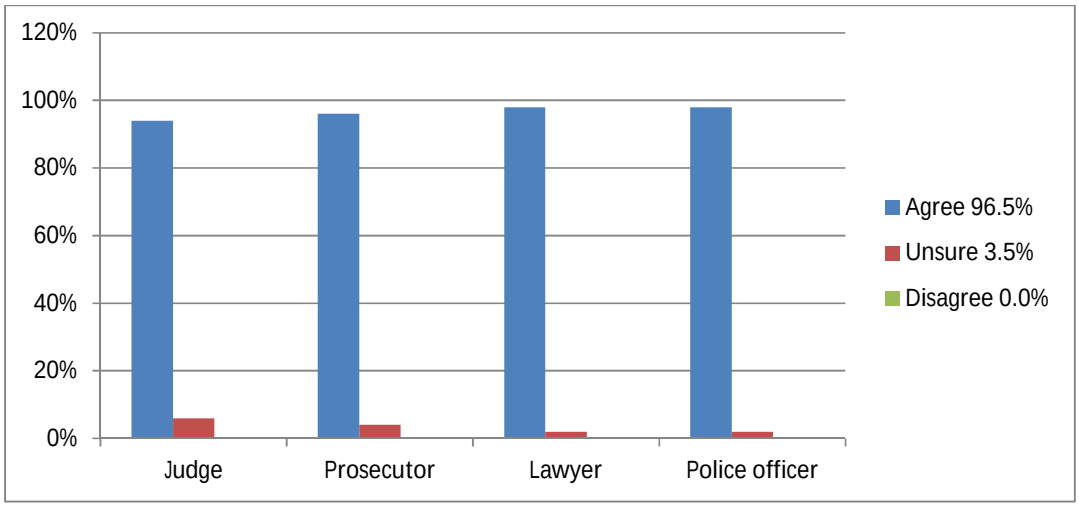
Another significant hypothesis tested by the questionnaire was the need to adopt international cooperation. Participants were asked to comment: 'There must be strong international cooperation and coordination between regulators to succeed in the effective prosecution of cyber-crimes and make full use of electronic evidence'. The analysis of the results revealed that a great proportion of the respondents (96.5%) agreed, and only 3.5% were unsure (Figure 17). The respondents made the following comments: 'Because cybercrime is international crime, we need international cooperation and coordination', 'Cybercrime is intercontinental crime, facilitating the commission and difficulty of reaching to the defendants', 'Electronic evidence can be found outside the UAE', 'To sharing experiences', 'To increase the level of knowledge and sharing experiences'.[71]

One of the problems facing the prosecution of crimes was obtaining evidence. Electronic evidence can be found in different places, either in the State or abroad. Thus, the UAE requires good methods for attaining evidence, that are covered by legal rules,

[71] Ibid.

and which guarantee the safety of procedures. The UAE also needs to acquire effective international cooperation joining international treaties and conventions.

Figure 17: There must be strong international cooperation and coordination between regulators to succeed in the effective prosecution of cyber-crimes and make full use of electronic evidence.



A clear result was provided in section four and this was emphasised by the fact that it was supported by the results in the survey. Indeed, it supports the general attitudes of police officers, lawyers, prosecutors, and judges, who, according to the questionnaire, think that electronic evidence is a problem they face and that regulation should be developed to high standards.

5.4 Conclusion

The most vital part of this study was the applied methodology. A number of questions were highlighted during the course of conducting this thesis. The present chapter attempts to provide answers to these queries with the help of the reasoning and selection of a mixed-method (quantitative and qualitative). To some extent, the results derived from both quantitative and qualitative methods were consistent. To investigate electronic evidence from the viewpoint of legal specialists, two different approaches were employed.

A clear image of the opinions, ideas and attitudes of legal specialists towards electronic evidence was delivered as an outcome of the study. The attitudes and behaviour of the

participants and interviewees, taken as a whole, cohered with the thesis proposition. They confirmed the idea that the regulations that exist for handling electronic evidence are insufficient and generally, this favours the researcher's arguments. These facts were explored in the previous chapters.

In conclusion, it is important to represent the main results of the applied study briefly:

I. The applied study showed that most police officers, lawyers, prosecutors, and judges were not familiar with:

   A. Gathering methods of electronic evidence.

   B. Methods of preserving electronic evidence.

   C. Procedures for examining electronic evidence.

   D. Techniques and tools for electronic evidence examination.

   E. Forensic expert reports.

   F. Challenges and problems associated with cyber-crimes in relation to electronic evidence.

II. The issues which police officers, lawyers, prosecutors, and judges complained about most in the UAE with regard to electronic evidence were:

   A. Lack of procedural guidance for electronic evidence preservation.

   B. Lack of specific rules governing search and seizure of electronic evidence.

   C. Absence of awareness and indicative programs.

   D. Limited specialists to handle electronic evidence.

   E. Absence of international cooperation.

III. Most police officers, lawyers, prosecutors, and judges think that there should be legal terms set that are unique to electronic evidence.

IV. The majority of police officers, lawyers, prosecutors, and judges think there is a need to promulgate clear guidelines on how to deal with electronic evidence in

the UAE.

V. The majority of police officers, lawyers, prosecutors, and judges believe that electronic evidence should be collected by qualified persons.

VI. The majority of police officers, lawyers, prosecutors, and judges believed that examinations of electronic evidence should be documented.

VII. The majority of police officers, lawyers, prosecutors, and judges believed that we must update the laboratories handling electronic evidence continuously.

VIII. Almost all of the police officers, lawyers, prosecutors, and judges think that they need more professional training to evaluate and handle electronic evidence.

IX. The majority of police officers, lawyers, prosecutors, and judges believe that there must be strong international cooperation and coordination between regulators if they are to succeed in the effective prosecution of cyber-crimes and to make full use of electronic evidence.

X. The applied study showed that the level of awareness and understanding of electronic evidence in the UAE is very low. This is supported by the interviews, in which there was found a consensus that awareness and knowledge level of electronic evidence is low.

In brief, both the interviewees and the respondents to the questionnaire explained their views in-depth in regards to the current regulation of electronic evidence. The study supported our proposition that there are overall deficiencies in the regulation of the electronic evidence system, as explained in the previous chapters. The best solution to address this insufficiency is to propose a Federal law that clearly regulates electronic evidence. Those legal experts who were interviewed supported this view; Judge Al kaabi said:

> Proposed Federal law can be a best solution, which should clearly regulate electronic evidence. If we cannot do this, we can adopt guidelines. From a legal point of view, the last solution is partial. A guideline has no power equivalent to the law in front of a court. From my point of view, there should be a completely new law in regard to this.[72]

[72] See: translated transcript of the interview with Judge Al kaabi in Appendix 5.

Another interviewee said:

> There should not only be a law. There should also be guidance under the adopted law covering all procedures for electronic evidence, starting with how to search and seize and in the end how to examine this evidence. Who is must be based procedure, and what qualifications have. In the UAE, there is Federal Law No. 5 of 2012, which covers crimes and penalties, but there is no law regulating the procedures for search and seizure of evidence. Several crimes cannot be able to be proven because of the lack of rules.[73]

Another interviewee stated: 'There is a vast area in electronic evidence that needs to be regulated'.[74]

[73] See: translated transcript of the interview with Professor Elbushra in Appendix 5.
[74] See: translated transcript of the interview with Al ketbi in Appendix 5.

CHAPTER SIX: NEW STRATEGY FOR ELECTRONIC EVIDENCE IN THE UAE

This thesis is an analysis and evaluation of the UAE laws regulating electronic evidence. It is also an investigation into the existing procedures underpinning such evidence. To date, despite reported misuse of electronic evidence, there have been few suggestions concerning the resolving of such issues.[1] The previous chapters have demonstrated that there is currently not sufficient legislation in place for this system of electronic evidence.

In Chapter Two, there was a discussion concerning the development of the UAE's CPL and its specific legal system. At the same time, an overview of criminal investigation was undertaken, including a comparison of physical and electronic evidence.

Despite the fact that leading figures from the legislature, politics and the police have agreed the need for regulation in this area, reforms have not yet been implemented.[2] Hence, the author has undertaken a thorough investigation into the legislation, policies and methods of collecting proof in the UAE. Following this research, the situation in the UAE is compared with other locations. Two cases (the UK and China) were compared and evaluated in order to prepare an effective argument for the regulation of electronic evidence.

In Chapter Four, there was an investigation of the difficulties in using electronic evidence in the UAE. This included the various loopholes found in the UAE's CPL and an overview of current regulation.

This study supports the proposition that there are regulatory shortcomings in the electronic evidence system, the most notable being: (1) the regulation of search and seizure; (2) preservation of evidence; (3) international cooperation and coordination.[3] The study also reveals a low level of awareness regarding the use of electronic evidence in the UAE[4] : hence, it can be argued that electronic evidence is problematic. It may

[1] See: pervious example cases in Chapter Four.
[2] See: transcript translated of the interviews in Appendix 5.
[3] See: section 5.3.
[4] Ibid.

also be a problem in other countries, either developed or emerging. Cybercrime, and the obtaining of evidence with which to prosecute, is a global issue. Evidence is frequently lost, either because there are too few rules to regulate electronic evidence, or due to a lack of international coordination and cooperation.[5]

There were a number of aims to this research. Primarily the researcher wishes to identify current shortcomings related to electronic evidence in the UAE's CPL. Secondly, the author aims to examine the key issues surrounding electronic evidence, including the awareness of legal experts concerning this area and improving the knowledge gap regarding electronic evidence in the UAE. Finally, the researcher aims to put forward improved approaches to the use of electronic evidence and suggestions for further areas of research.

This chapter has been split into two parts. The first outlines the evidence uncovered during this study, while the second puts forward suggestions on improvements to the current legislature of the UAE.

6.1 Part one: challenges and problems facing the law enforcers with regard to electronic evidence and gaps in the existing criminal procedures of the UAE

Reliable evidence is essential when undertaking research. Electronic evidence appears in various forms and originates from many different sources.[6] It can therefore be unpredictable and requires protection in order to maintain its credibility.[7]

Law enforcement officers, judges, lawyers and prosecutors are currently unaware of the importance of information attained from electronic sources. As electronic evidence is unique, the system surrounding it requires its own set of regulations and procedures and also demands that investigators understand all of its procedures. The forensic investigator at the Telecommunications Regulatory Authority of the UAE supports this, stating:

[5] See: practical examples given by some interviewees, the transcript translated of the Interviews in Appendix 5.
[6] See: Nigel Jones, Esther George, Fredesvinda Insa, Uwe Rasmussen and Victor Völzow, 'Electronic evidence guide, A basic guide for police officers, prosecutors and judges' (2013) Version 1.0 *Council of Europe*.
[7] See: section 2.3.2.

> I think that we need own procedures dealing with all processes, starting with seizure, preservation and examination of electronic evidence. When it has (been achieved) nobody can argue and also it will be assurance that all procedures have been followed by the investigator.[8]

It is therefore recommended that the investigators secure the original form of evidence and create backups. There follows a discussion of the shortcomings previously mentioned regarding the regulation of electronic evidence in the UAE. Before highlighting the shortcomings in the regulation of electronic evidence, it will be helpful to highlight a number of challenges facing the judges, prosecutors, lawyers and police officers.

6.1.1 Challenges and problems to the investigation and disclosure of crimes in relation to electronic evidence

Criminal judges, prosecutors, lawyers, electronic evidence experts, and investigators face a number of challenges due to crime committed on a global scale and the rapid advance in information technology. It is difficult for the judges handling criminal cases, law enforcement, legal practitioners and computer experts to resolve cases concerned with the misuse of this technology. It is difficult for judges to make a decision when it comes to cybercrime, because the accused are frequently more proficient in information technology than those investigating, prosecuting or judging the case. The issues that arise from the legal side will be discussed later, following an investigation of those faced by the investigators, experts, lawyers, prosecutors and judges.

6.1.1.1 Challenges and problems faced by investigators

The main responsibility of an investigator of these crimes is to identify and preserve computer evidence. When handling crimes that are beyond their geographical borders, the investigators require both expertise and experience. Issues faced by the investigators include:

- Contacting the correct individual within the relevant jurisdiction can prove complex;

[8] See: transcript translated of the interviews with Ahmed Al Ketbi in Appendix 5.

- The investigator may not comprehend the language in which the document is written;
- The investigator might not comprehend the language of the witness [9] and;
- The investigator might not have the skill and experience required to deal with the electronic evidence.[10]

The best means of addressing this problem is to synchronise laws and procedures globally (as this is an issue faced by all countries), alongside improving investigators' technical capabilities. Saeed Al Hajri, Director of the Criminal Investigation Department's-Electronic Crime Section-Dubai Police in the UAE states that in order to obtain improved results, investigators need to obtain professional training in computer forensics in order to improve their approaches to analysing the electronic evidence.[11]

The critical issue faced by the police investigators when dealing with cybercrimes is the identification of the criminal; this is due to the fact that identity in such cases is difficult to establish. Any individual can commit cybercrime by using their own, or any publically available, computer.[12] The result of a study conducted on on-line anonymity concluded that criminals mainly use Internet service providers affording the maximum level of anonymity.[13] To identify and prosecute the suspects thus becomes difficult for the investigator, increasing the time span of the case, because traditional techniques are still used for investigations.[14] It is also difficult to investigate on the basis of an

[9] There are 200 nationalities living in the UAE, according to study presented at the Third Annual Conference 'In the eyes of the communities Emirates' (conference, UAE 20th March 2013) <http://www.alkhaleej.ae/portal/150131e3-9689-42e8-b700-9424c35ccad3.aspx> accessed 25th September 2013.

[10] Toni Makkai, Media Release on 'Effective investigation of high tech crime' (2004) *Australian Institute of Criminology* <http://www.aic.gov.au/media/2004/december/20041202.aspx> accessed 4th March 2012. Toni stated, 'Conducting investigation across national borders raises many practical problems. These include investigators having to contact people on the other side of the globe, documents having to be translated and witnesses speaking other language needing the assistance of interpreters. All of these impediments can be overcome by harmonizing laws and procedures globally, and improving the technical capabilities of investigators'.

[11] Saeed Al Hajri, '4th International Conference on Cyber Crimes' (conference, UAE 14th December 2011).

[12] Beryl Howell, 'Real world problems of virtual crime' (2005) 7, 1 *Yale Journal of Law and Technology* <http://digitalcommons.law.yale.edu/yjolt/vol7/iss1/5/> accessed 14th January 2012.

[13] Russell Smith, 'Impediments to the successful investigation of transnational high-tech crime' (2004) *Australian Institute of Criminology* <http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi285/view%20paper.html> accessed 11th March 2012.

[14] Ibid.

individual's password or PIN (Personal Identification Number), as these can be stolen by criminals from various individuals, making it difficult for the investigators to identify the real criminals. It has been suggested by the Australian Transaction Report and the Analysis Centre (AUSTRAC) that prosecutors should put in place a number of actions to support investigators in solving a case. These include:

- That incriminating information can be obtained by seizing the computer of the suspect to obtain its data; or
- That the investigator can use the information found in the victim's own computer to prove that the victim has been defrauded; or
- That the victim is made aware that his computer has been misused by criminals.[15]

Extra territorial crimes and extradition have to be dealt with by the investigators in the above scenarios. In the UAE, one of the challenges faced by the investigator is the deficiency of appropriate training courses. The UAE is in need of more officers proficient in cybercrime to investigate and obtain electronic evidence. This is to ensure that police officers will always be appropriately prepared to fight the rising number of crimes. The analysis of the applied study illustrates that 77% [16] of police officers in the UAE did not possess sufficient knowledge concerning electronic evidence.[17]

6.1.1.2 Challenges and problems faced by forensic experts

Included in the role of the electronic evidence expert is advising judges (and others who are not experts) information that they can access and easily understand. The expert must also possess the ability to compile evidence in such a way that it can be used by the court. This can be done by retrieving the related information from the system,[18] and to inform the concerned parties (including the judge) of the means of retrieval.

Dealing with technology that is changing rapidly is one of the most complex tasks an

[15]See: Australian Transaction Report and Analysis Centre (AUSTRAC), 'Evidence and the Internet' Action Group into the law Enforcement Implication of Electronic Commerce (AGEC) Issues paper (2010).
[16]The percentage who said I don't know: 28+74+78+80+84+96+96+82×100 ÷8=77.25%.
[17]See: section 5.3.
[18]In the UK, the Forensic Science Service of a Home Office Agency is handling computer forensic examination.

expert has to deal with. This is supported by the forensic investigator of the Telecommunications Regulatory Authority of the UAE, who states:

> Technology is rapidly evolving and it is extremely important to update the laboratory to ensure that the tools are always upgraded. We in the Telecommunications Regulatory Authority update tools continuously.[19]

An example of this is the greatest rapid changes that occur in computer hardware, operating systems and application programs. To ensure that the criminal does not adopt any new technology that will destroy evidence from the past, the expert must remove as much information as possible from the computer. The crucial issue here is when adopting new technology that has not been tested, thereby risking the conviction of an innocent person, or being forced to wait until the new technology is tested.

Issues are also created for experts by the need to upgrade software and computer forensic tools following any kind of development. There is a high cost related to the upgrading of software and procedures to recover the computer. A high cost is also attached when the data recovery service is used by a third party computer.[20] A number of countries face issues due to the fact that experts are not properly trained. An example of this is the fact that electronic evidence can be managed by only 1000 police officers out of the total 140,000 in the UK. Less than 250 personnel have an adequate grasp of forensics.[21] This emphasises the urgent need for training to fill this gap in the UK, which has a much larger police force than the UAE, and therefore it must be presumed that such a need also arises in the UAE. As a result, expert witnesses are usually called to present evidence. In order to ensure the data produced is correct, the lawyer can

[19] See: translated transcript of the interview with Al ketbi in Appendix 5.

[20] In the US, for example, the third party data recovery service depends on a number of variables, namely Resource requirements, Project Lead Times, volume of data, type of storage media, data format, condition of media and operating system.

[21] In addition, Michael Chissick, states that it is a reasonable conclusion that in the 21st century, the UK system can no longer receive forensic examination in computer evidence. The judges and lawyers do not have the ability to undertake this task. There is no ordinary funding to commission experts to accomplish this task. Thus, it is probable that over the years ahead people will be convicted for crimes they did not commit on the basis of incorrect computer evidence or misunderstood computer evidence. See: Michael Chissick and Alistair Kelman, *E-commerce: Law and practice* (3th edn, Sweet and Maxwell Ltd A Thompson Company 2002) 197. For another, slightly more up-to-date argument that supports this, see: Stephen Mason and Nicholas Bohm, 'Banking and Fraud' a written submission to the House of Commons Treasury Committee on 17th January 2011, available at <http://www.publications.parliament.uk/pa/cm201011/cmselect/cmtreasy/430/430vw25.htm> accessed 30th October 2013.

cross-examine these experts and ask them to give their own analysis.[22]

6.1.1.3 Challenges and problems faced by lawyers

It is essential for lawyers to keep up to date with developments in IT, as it is important for them to understand the issues surrounding electronic evidence, particularly from experts, and to be in a position to challenge it, including cross-examining witnesses, etc. In an interview conducted in the UAE, a head of the Electronic Evidence Unit at the Criminal Evidence and Criminology Department of Dubai Police stated that:

> The level of lawyers' knowledge about electronic evidence or expert report is very low. Therefore, he/she cannot discuss the forensic expert's report.[23]

However, it is possible for a lawyer to understand the importance of electronic evidence, dealing with investigative tools and techniques used in the investigation. In order to recognise loopholes in a case involving electronic evidence, it is necessary to understand IT and its related laws. Such knowledge can also help to deal with the means used by police and other experts to obtain electronic evidence.[24] However, many lawyers in the UAE do not possess such relevant knowledge. The current study illustrates that over two-thirds (86%) [25] of lawyers felt that they did not have sufficient expertise when it came to electronic evidence.[26]

It is necessary for lawyers to be aware of the major issues of the IT, where to look for answers and also to be in possession of general background knowledge and therefore aware of the questions they need to put to an electronic evidence specialist.

6.1.1.4 Challenges and problems faced by prosecutors

Framing the charge against the accused is a challenge faced by the prosecutors in such cases, accompanied by lack of all the facts of the criminal investigation.

In cybercrimes, those who abuse the technology must be initially identified by the

---

[22]See: section 4.6.4.
[23] See: translated transcript of the interview with Lootah in Appendix 5.
[24]See: Craig Ball, 'Cross-examination of the computer forensic expert' (2004) <http://www.craigball.com/expertcross.pdf> accessed 11th March 2012. This article could be a good reference for a lawyer who wants to be a trial lawyer as well as an expert in computer forensics.
[25]The percentage who said I don't know: 46+84+96+96+98+98+96+74×100 ÷8=86%.
[26]See: section 5.3.

prosecutor, who will determine if there is any breach of the law. The evidence given by the prosecutor will be challenged by the lawyer. It is therefore vital that the prosecutor is aware of all the facts concerning the evidence, as this will assist in charging the accused with the correct crime according to the relevant law. Most importantly, the prosecutor should be familiar with IT and the relevant evidence gathering techniques. Without this, the prosecutor will be unable to make a solid case against the accused, and will be unable to draw up the charge sheet.

In order to investigate the prosecutors' level of familiarity with electronic evidence, the analysis conducted in the UAE by the researcher reveals that over two thirds (72.25%) [27] of prosecutors did not have sufficient awareness of electronic evidence.[28]

The problem can be highlighted in the case of the UAE's Ministry of Education.[29] Here, the prosecutor was unable to explain the extremely complex IT methodologies and concepts in a court. This tested the skill, knowledge and ability of the prosecutor, the police officer and the judges in handling the electronic evidence, and it revealed their lack of relevant skills and ability in this area. The case demonstrates that unclear procedures and an inability to explain the methods of obtaining evidence lead to different judgments in one case. In the absence of clear rules on electronic evidence, the prosecutor may be subject to rigorous cross examination by lawyers, who may accuse him of mishandling the evidence, or other misconduct.

One of the main issues that a prosecutor has to face when the crime is committed in two countries is one of jurisdiction. Judge Dr. Mohammed Al Kamali states:

> Let's talk first about the problems of jurisdiction within the State. There are problems of jurisdiction between the Emirates. For example, if the case was in Abu Dhabi and the electronic evidence in Fujairah, the police officer could directly get a search warrant issued by prosecutor in Abu Dhabi based on the evidence only, or might need another from Fujairah. There are procedural problems of evidence that must be resolved. At the international level, I think international cooperation takes a long time and the evidence may get lost. I think this is another important point supporting the fact that we need to find procedural laws for electronic evidence.[30]

[27] The percentage who said I don't know: 32+76+74+82+82+88+74+70×100 ÷8=72.25%.
[28] See: section 5.3.
[29] See: section 4.9.
[30] See: translated transcript of the interview with Judge Al kamali in Appendix 5.

This is the case when the criminal resides in the UAE, but the crime has taken place in another country or Emirate, or vice versa. Implementation of international law and obtaining cooperation from the other countries is a complex issue, due to the fact that countries have differing procedures to deal with such crimes. This can cause an issue for the prosecutor when drawing up the charge sheet. Success also depends on the level of cooperation the prosecutor is able to elicit.[31]

6.1.1.5 Challenges and problems faced by judges

A number of conferences have taken place in the UAE regarding cybercrime and electronic evidence.[32] The main agenda of these conferences has been to make judges aware of recent developments and the ways to deal with the crimes in cyberspace. The number of cybercrimes in the UAE has rapidly increased over the past few years. The head of the Electronic Evidence Unit at the Criminal Evidence and Criminology Department of the Dubai Police has stated that the numbers of cases dealt with by the Electronic Evidence Unit in Dubai alone are as follows: 278 cases in 2008; 436 in 2009; 445 in 2010; and 588 in 2011. In 2012, the number reached 772.[33]

The applied study revealed that (78.50%) [34] of the judges, did not possess sufficient knowledge concerning electronic evidence.[35] Judges are therefore in need of regular training on recent developments in cybercrime and electronic evidence, including the implementation of new laws, as they need to be well versed in the knowledge of IT and its uses in such cases.

These issues and challenges lead to a need to rethink the regulation of electronic evidence in judicial proceedings, as the combating of such crimes can be deficient. As a result, there is a requirement to make essential changes to the criminal law. There is no doubt that electronic evidence can play a pivotal role in the investigation of crimes by assisting in establishing the truth. There is a positive aspect to the increased use of technology by criminals that can be exploited. The fact that computers are connected

[31] The First International Treaty to combat crime in cyberspace came into force in 2004. It was prepared in order to achieve mutual co-operation among the countries in the world and to expedite extradition proceedings. See: 'First International Treaty to combat crime in cyberspace' <http://www.assembly.coe.int/ASP/Press/StopPressView.asp?ID=1157> accessed 9th March 2012.
[32] Such as: International Conference on Cyber Crimes.
[33] See: translated transcript of the interview with Lootah in Appendix 5.
[34] The percentage who said I don't know: 22+82+84+98+92+96+82+72×100 ÷8=78.50%.
[35] See: Section 5.3.

together in a crime results in a multitude of electronic evidence that can be used to detect and prosecute criminals. Electronic evidence can also illustrate the way in which the offence was committed, reveal investigative leads, refute or support witness statements, and identify likely suspects.

In the digital era procedure laws need to adopt a broader view when it comes to electronic evidence, in order to identify shortcoming and suggest the best solutions to prosecuting crime. Cybercrime indicate that effective prosecution of crimes at the global level should address not only the penal code, but also follow the more sophisticated methods, of crime detection. Combating crime will prove more effective when there are effective laws and procedures in place to govern the process of detection and investigation. The UAE Government must also take an important role in providing more skilled police officers, lawyers, prosecutors and judges, due to the current low level of expertise.[36]

6.1.2 The rules regarding collecting, preserving, examining and presenting electronic evidence.

The prosecution of a crime requires evidence that is correctly formulated, highly specific and principled. Due to the fact that electronic evidence is not the same as other types of evidence,[37] it must therefore be queried whether or not it requires its own special rules.

According to Paul, electronic evidence demands special attention as it offers an entirely new perspective when it comes to evidence, and therefore advanced hypotheses and methods must be used when dealing with it.[38] Such methods come under the heading of electronic evidence. However, new rules for electronic evidence cannot be established in haste, and it is important to set up an appropriate system of handling. Current regulations for evidence are also applied to electronic evidence. However, in courts where these are practiced they are given little, or no, credibility when the plaintiff is unable to demonstrate how evidence was gained. This has been particularly

[36]Ibid.
[37] See: section 2.3.2.
[38]George Paul, *Foundations of Digital Evidence* (Chicago: American Bar Association 2008) 13-14.

demonstrated in the case of the UAE's Ministry of Education.[39]

There will now follow a discussion of the possible problems faced by using laws written for standard evidence for electronic evidence. In order to simplify the structure of the analysis, the main questions raised in previous chapters will be discussed as follows.

6.1.2.1 Definition of electronic evidence

It is necessary to define electronic evidence concisely and comprehensively in order to provide clear rules for its regulation. However, such a definition is not easy. It is necessary to establish the range of electronic evidence.[40] Introducing a legal meaning satisfies the need for legal certainty, but produces obstacles when put into practice. The phrase 'electronic evidence' is itself not difficult to comprehend, however difficulties arise when its meaning is put into a legal context. With continuous technological advances, it is difficult to establish a single definition in legal terms. Nevertheless, due to the fact there is widespread ignorance of the concept of electronic evidence, it is necessary to establish a definition. This definition is the subject of this research. A loose definition is preferable,[41] however the author also wishes to establish one that has a legal context.[42]

6.1.2.2 Searching and seizing electronic evidence; search warrant issues

Regulations for the searching and seizing of evidences create a number of legal issues, one of which is the search warrant. Searching for electronic evidence differs considerably from searching for traditional evidence. It consists of two phases: pre-digital and digital tracking.[43] Pre-digital is similar to the established search system, where the suspect is found and searched. Digital tracking is consists of a number of steps performed by specialised forensic representatives, who work remotely to where the activity under investigation took place. While these two steps differ, they also have an effect on each other, as actions performed in the first phase may have adverse effects

[39] See: section 4.9.
[40] See: section 1.8.1.
[41] Such as the definition of electronic evidence in the Canada Evidence Act of 1998.
[42] See: section 6.2.5.
[43] Hilali Abdullah, *Inspect Computer Systems* (Dar Nahda Al Arabiah 1997) 125. (Author's translation from the Arabic).
هلالي عبدالله، تفتيش نظم الحاسب الآلي (دار النهضة العربية مصر1997) ص 125.

on the second. For example, as the system of search warrants requires the investigator to reveal their identity and provide the required evidence, it is likely that the suspect may attempt to destroy the evidence. Therefore, the necessity to reveal the investigators' identity needs to be considered in greater detail in order to try and prevent the suspect from deleting any evidence.

In the UAE, the CPL is not permitted to carry out a search warrant without notice and the suspect (or a family member) is required to be present.[44] These regulations need to permit investigators to undertake a confidential search in cases where there is a chance the suspect might delete evidence. While it is important in the UAE to respect the privacy of an individual's home, there are certain instances where officers are permitted to carry out a search without notice, in order to protect lives and property and to search for, and safeguard, evidence, or to arrest a suspect.[45]

6.1.2.2.1 The subject of the search warrant

The data in information technology is electronic. Therefore, evidence being sought can include intangible items, such as electronic pictures, files and data. The search warrant needs to be accurate in order to seize the correct items. Many countries (i.e. Italy,[46] Ireland,[47] France,[48] and Portugal[49]) have updated their evidence rules to include a new means of evidence.

According to the present UAE CPL system, an officer has the right to seize any suspicious item, but it is a legal requirement that the warrant used has been issued for substantial evidence.

Article 61 of the CPL, states that:

> 'The judicial police officers have to sequestrate the objects which may have been used in the perpetration of the crime, resulted therefrom, or if the crime has been committed thereon; in addition to whatever may lead to the truth in the matter'.[50]

[44] The UAE Criminal Producer Law, Article 59.
[45] Ibid, Article 53.
[46] Computer Crime Code of the Republic of Italy 1993, Article 491.
[47] The Irish Criminal Evidence Act 1992, s 2 (1).
[48] Civil Procedure Code of the French Republic Inserted by Law No.230-2000, Article 1316.
[49] The Portugal Criminal Procedural Code DL 324/2003, Article 164.
[50] The UAE Criminal Producer Law, Article 61.

According to current provisions, the broad scope of Article 61 is ineffective when it comes to searching for electronic evidence. Article 61 does not directly mention intangible data or information. However, with the different nature of electronic evidence (which can include intangible or invisible objects) this could lead to the seizure of evidence outside the search warrant.

Therefore the laws of the UAE need to be updated to allow for the examination and confiscation of more insubstantial objects, by providing police officers with the authority they need in order to search and seize 'invisible' evidence.

6.1.2.2.2 The scope of the search warrant

The search warrant must be specific to a location, crime or particular items.[51] The two methods of approach used in electronic investigation are restricted and non-restricted. In the first, the officer is not permitted to copy the original document, while in the second it is permissible to investigate all possible locations and confiscate all possible evidence. While the first safeguards an individual's privacy, it creates difficulties for the officer undertaking the search, as it fails to provide them with all the necessary evidence and limits their ability to differentiate between useful and irrelevant data.[52]

These two approaches have been applied in the UAE. The UAE CPL allows the officer to carry out the maximum possible search on the suspect and make copies of the original documents, if necessary. The system should allow the officer to look at any data, which may prove to be evidence, and avoid the use of data that appears unreasonable and irrational. Simultaneously, the law must clarify the meaning of the word 'things' in Article 51 of the UAE's CPL. The broad scope of word 'things' in Article 51 could lead to different interpretations.[53]

6.1.2.2.3 Location of the search

Moving the electronic equipment in order to carry out the search operation will inevitably create problems for the owners of the equipment. Carrying out an operation at one location for a long period of time can cause problems to both the inhabitants and the staff. A discussion follows concerning two different points of view related to on-site

[51] The UAE CPL outlines several requirements for obtaining search warrant. See: section 4.2.2.
[52] For further details on approaches to electronic investigation see: section 4.2.2.2.
[53] Ibid.

and off-site investigations. The majority of professionals prefer the latter.[54] According to the UAE CPL, investigators are allowed to control all of the steps of an operation.[55] The UAE officers should, however, be given guidance on the search location. Officers should be permitted to carry out the search off-site only when it cannot be undertaken on-site. It must also be decided who should accompany the investigators executing the search.

Investigations are systematic and are required to be carried out by specific individuals, i.e. forensic examiners, technicians, evidence analysts and forensic custodians. In the UAE, it is important for the suspect to be present while such investigations take place. This is difficult to achieve in cases where the search for electronic evidence is done far from the original site. It is therefore important to alter the CPL to allow the search to be carried out in the absence of the suspect. However, this request must also guarantee the suspect's rights.

6.1.2.3 Search and seizure without a warrant

While the UAE does not allow a breach of privacy, there are certain instances where investigators are permitted to enter an individual's home without a search warrant, in order to seize evidence. Exclusions have been seen in the UAE CPL. Article 54 of the CPL states that:

> 'The judicial police officer, even in cases other than red-handed crimes, may inspect dwellings of persons put under surveillance, either according to a law provision or a court decision, should there be strong indications that they may be suspected of perpetrating a felony or a misdemeanour'. [56]

Due to the change in patterns of crime, and the advancements made in technology, it is difficult to use conventional laws effectively. A legal order must be issued to investigators so that they are able to keep all items which may potentially be evidence, particularly if there is a possibility that this may be lost if the electronic equipment is destroyed.

[54] Ibid.
[55] The UAE Criminal Producer Law, Article 53.
[56] Ibid, Article 54.

6.1.2.4 Cross-border searches and seizures

Law enforcement agencies are restricted by physical borders, however there are no physical boundaries in cyberspace. [57] Investigations into cybercrime require multinational cooperation to be effective. However, political, legal and cultural factors can substantially influence investigations. There must be political goodwill and cultural cohesion, as well as a powerful legal system in each jurisdiction. A good working relationship, and the desire to help another country, leads to successful cross-border investigations.

Many factors in cybercrime investigations can impact an investigation, due to the presence of errors in the cybercrime criminalisation policy. The established forms of combined legal assistance (intended for non-electronic crimes) are not as efficient when searching for electronic evidence, where rapid and decisive actions are required. Specific measures have been taken by the Convention on Cybercrime in order to improve cross-border cooperation in cybercrime investigations.[58] The preservation of data from a computer within the territory of a member accelerates the revealing of preserved traffic data, locating and seizing evidence across borders, and the acquisition of traffic data. These are current procedures for cooperative legal assistance with respect to methodology, and are particularly important for rapid and effective cooperation in cybercrime investigations. The involvement of the UAE in international cybercrime investigations is made difficult by its current inadequate legal basis, which is required in order to set up, help and process mutual legal cooperation. The author recommends that the UAE urgently reviews domestic laws which could lead to mutual legal assistance and which are required for a successful cybercrime investigation. Prosecutors should be empowered by a central authority, formed by statute, to issue requests for data normally stored by Internet Service Providers, to be preserved and disclosed as required. Data should be preserved for as long as is deemed necessary.

6.1.2.5 Preservation of electronic evidence

The gathering of electronic evidence for an investigation consists of specific procedures

[57]Ritter Nancy, 'Digital Evidence: How Law Enforcement Can Level The Playing Field With Criminals' (2006) *Journal-National Institute of Justice (NIJ)*.
[58] See: Convention on Cybercrime Budapest 23.XI. 2001.

and expertise, which are unlike the conventional methods of information collection. It is necessary for investigators to be aware of the use of electronic items and also current technological advancements, and therefore appropriate training is important. The UAE Government must provide the necessary funds and time for staff training. There is no specific legal system in the UAE for cybercrime, or for the collecting and storing of electronic evidence. This, alongside the limited information, skills and weak principles, is certain to increase the difficulties created when data is lost.

A number of countries (such as the US,[59] the UK,[60] Romania[61] and Australia[62]) have recognised the importance of developing rules to deal with electronic evidence during a seizure and have therefore established appropriate rules. These aim primarily to preserve electronic evidence and thus reduce the risk of any misconduct by investigators, which may lead to the loss of such evidence. Similar guidelines would be useful in the UAE, particularly given its lack of expertise when it comes to dealing with electronic evidence at a crime scene.

6.1.2.6 Examination of electronic evidence

The examination carried out on electronic evidence is similar to that carried out on any other form of evidence. Electronic evidence presented in court is required to be precise, genuine, comprehensive and believable. Accuracy comes from the information available and it is important to investigate possible loopholes in the evidence, since this determines its reliability. The trustworthiness of a piece of evidence is depends on its source: evidence is deemed comprehensive if all details support each other. As the law of the UAE does not offer any support to the procedure of evaluating electronic evidence, it is important for the UAE to establish laws regarding the efficient working of investigators. Legal rules may be the best option to increase confidence in the safety and accuracy of the procedures followed by the forensic expert.[63]

6.1.2.7 Presentation of electronic evidence

It is important to present expert evidence effectively to lawyers, judges and prosecutors

[59] The US Guide for First Responders. See: section 4.5.
[60]The UK Good Practice Guide for Commuter-Based Electronic Evidence. See: section 3.5.2.
[61] Guidelines: Operational procedure to be followed for search of computers (Romanian Police).
[62]Guideline for the management of IT evidence produced by: Standards Australia.
[63] See: section 6.2.5.

so that its importance is understood. Evidence needs to convey a point clearly or else it is worthless. The manner in which evidence is presented is also important.[64] In order to be effective, the presentation should be coherent and easily understood by a layman. When presenting evidence in criminal proceedings, it should be remembered that electronic evidence and traditional evidence share the same rules. It is the prosecution's obligation in conventional evidence to demonstrate to the court that the evidence has not been changed since it was first seized by the police. Electronic evidence is usually modified in terms of its quantity by operating systems and other programmes. This can happen without the knowledge of the user. It is therefore vital that a sufficiently qualified electronic evidence specialist present electronic evidence. It is important to be objective in a court, while also demonstrating the integrity of the evidence. The manner in which the evidence was obtained needs to be presented step by step. If there were specific rules for the process of electronic evidence it would be a simple matter to explain how, where and when the evidence originated. The President of the UAE's Federal Supreme Court states: 'We need only clear rules, when we have these rules then the judge can check all procedures, not only the judge but also all parties'.[65]

6.2 Part two: recommendations

In this section there will be a discussion of the origins of the recommendations for the reform of the UAE law and regulation of electronic evidence. These recommendations will be supported by the results arrived upon in each of the preceding chapters and by the later findings of the thesis. The theoretical and applied methods employed, along with the recommendations for the regulatory reform of electronic evidence regulation in the UAE, frame the benefits of this thesis.

Prior to conducting a research, the researcher may have certain ideas, which are then moulded into a final shape by the end of the research. Research works in the manner of a factory, i.e. converting raw materials into a product. It can be thought of as a means of supporting a hypothesis, which, if logical, is easily supportable. The role of research is not only to support a hypothesis, but also to demonstrate its strengths and flaws. In its initial phase, this research had very limited scope and few hypotheses. However, a

[64]Burns DC, 'When used in the criminal legal process forensic science shows a bias in favour of the prosecution' (2001) 41.4 *Science and Justice* 271.
[65] See: translated transcript of the interview with Judge Dr. Abdul Wahab Abdul in Appendix 5.

rigorous review of the literature, investigations and analysis have turned these limited thoughts into a body of ideas. Hence, the outcomes of this thesis could not be limited to the original ideas and hypotheses, as they now also embody a number of supporting ideas. The discussion of theories, gathering information and comparing and analysing the data is sufficient to form the basis for appropriate results and recommendations.

While the regulation of the processing of electronic evidence is the subject of this thesis, it also necessarily encompasses the regulation of the proving of such crimes, both in theory and in practice. The wider scientific background cannot be separated from a particular subject.

During the research for this thesis, it became apparent that the general characteristics of electronic evidence regulation are interlinked. This thesis therefore aims to divide the general area of electronic evidence regulation into outcomes and recommendations. It is, however, impossible to separate these recommendations, due to the fact that electronic evidence regulation is a single unit. The outcomes and recommendations of the thesis are therefore divided into the following areas:

6.2.1 Academic findings

This thesis has posed the question of the need for the regulation of electronic evidence. Due to the fact that differing views on the same problem lead to multiple results, a clear approach was adopted in order to approach the subject. On this basis, the main question posed in this thesis has been the potential requirement for the regulation of electronic evidence. This thesis claims that the lack of regulation governing electronic evidence is problematic and requires government by a legal system. There is an ongoing debate regarding support for such regulation. This thesis favours a pragmatic approach, i.e. if in practice the electronic evidence needs to be readjusted, it should be regulated in order to prosecute crimes effectively. This can be seen as an outcome of this thesis.

The next important academic point is related to the applied study. There is an overall lack of research in the UAE into the ways in which electronic evidence can be used to prove crimes, hence it was difficult to set up a pilot study in this area. The result of the applied study must therefore be seen in relation to the limits placed upon it by limited time and resources and also by the lack of any previous studies. Nevertheless, the

applied study can be seen as a progression. It will require the resources of an organisation to research evidence regulation in order to obtain complete comprehension. This thesis therefore recommends that the officials in the UAE give further consideration to studying the regulation of evidence.

The methodology of the thesis should also be noted. It is a hybrid of a theoretical legal study and an applied study. The different methods of the two studies assist in establishing underlying issues and to search for a solution. The art of combining social science and legal methodology is still new in the UAE. The recommendation from this thesis for any academic work in the field is to embody the socio-legal methodology so that increased practical results can be achieved. It is also recommends that UAE law schools consider adding electronic evidence regulation as a module. This will result in an increase of trained specialists in this field and a greater academic contribution. In support of this view, one interviewee stated:

> Cybercrimes and electronic evidence is a new topic at a worldwide level. I think we are still at the beginning in the UAE. At present, the level of understanding and awareness is too low. In the UAE, there is no academic research, training courses or workshops in the field of electronic evidence or cybercrime. There is also no academic module at the universities. Cybercrime is a high tech crime which needs a high level of knowledge.[66]

6.2.2 Coordination and cooperation

It is an undisputed fact that acquiring electronic evidence can be global in nature. Independent states have always needed to request evidence from others for crimes with an international element. In such cases, requests are made for cooperation, including MLA. These involve cross border pleas for assistance, and are particularly important in cases involving electronic evidence, due to the fact that there is a possibility the evidence may be modified or deleted. In order to eliminate this risk, the UAE needs to cooperate with other states and international organisations. In addition, the UAE also needs to approve and establish conventions regarding coordination between states in order to address the problem and deal with a global threat in a unified manner. This claim is supported by Saeed Al Hajiri, who states:

[66] See: translated transcript of the interview with Professor Elbushrain Appendix 5.

> Cybercrime is a global crime. Consequently, electronic evidence is also international. In other words, you can find part of the evidence in one state and other part in another country. We are facing difficulties in gathering evidence from abroad. There are no conventions and effective international cooperation in this field. As an example, our department has been applying for evidence from abroad since 2010 and even now we have not had it. It can take more than 3 years to get evidence. Additionally, suspects could provide other challenges. The suspects nowadays are using 'Anti Forensic Technique' software and hardware which lead to the clearing of evidence.[67]

6.2.3 Training of law enforcers

Cybercrime was not prevalent when the majority of the current lawyers, judges, prosecutors and other law enforcers received their training. The analysis of the applied study illustrates that majority of the participants in the questionnaire did not possess sufficient knowledge of the processes of electronic evidence.[68] Therefore, to ensure justice, it is necessary for them to be trained to the point where they have a basic knowledge of cyber law and its evidence. Training is used to increase the investigator's knowledge of, and handling expertise for, electronic evidence, so that it can be used during a trial.

These programmes should aim for continuous training of officers with regards to law enforcement on collection, analysis and ways in which to effectively present electronic evidence. The programme should also give investigators a working knowledge of the various aspects of electrical evidence. Both the investigators and judiciary should have adequate knowledge of the specific technical details used in cases involving electronic evidence.

6.2.4 Laboratory development

Electronic evidence requires expert assistance from both IT and legal organisations in order for it to be effective. For a successful investigation, the professional concerned with digital forensics is required to be knowledgeable about both the legal and IT professions, due to the rapid growth of technology and developing digital laws, which attempt to deal with the expansion of information technology. It is also important to upgrade the tools used, so that the report on the evidence is accurate and reliable. The

[67] See: translated transcript of the interview with Lieutenant-Colonel Al Hajiri in Appendix 5.
[68] See: section 5.3.

UAE needs to increase the number of laboratories, as it currently has only two. In support of this claim, Judge Dr. Mohammed Al Kamali states:

> We must also not overlook the technical side. The UAE currently has only two laboratories, one in Abu Dhabi and other in Dubai, and the rest of the UAE has no laboratories. As well as having few specialized cadres in the UAE now, these specialists need development and training.[69]

6.2.5 Reforms to the law

It has been put forward that reforms should be made to the system regulating electronic evidence, and to the ways in which it functions. Any changes to the regulations would be deemed insufficient if there were no reforms made to the system as a whole. The researcher has drafted the following recommendations:

Article 1: General: electronic evidence

These rules shall be commonly known as the 'electronic evidence' rules. These rules determine the arrangements for electronic evidence, such as systems, procedures and management.

Article 2: Definitions

'Electronic evidence' is any digital form of information or data,[70] either stored electronically initially or transmitted in this form, which can be used to prove a fact in a court of law.

'Computer system' refers to a device (or group of interconnected devices) which, following a programme, results in automatic processing of data or other functions.

'Computer data' refers to the portrayal of facts, concepts or information in a manner suitable for being processed in a computer system, or is defined as a group of instructions suitable for making a computer system perform a certain function.

Article 3: Search and seizure of electronic evidence

---

[69] See: translated transcript of the interview with Judge Dr. Al kamali in Appendix 5.

[70] There is difference between 'data' and 'information', data becomes information only if it is communicated, received, and understood. 'Data' is therefore potential 'information'. See: Raymond Wacks, *Personal Information, Privacy and the Law* (Oxford: Clarendon Press 1989) 25.

The judicial officer has authority to search a computer system, wholly or partially, and all the computer data stored within, or a medium that can store computer data located where the suspect can exercise their sovereign authority with the desire of avoiding criminal investigation or legal proceedings.

Article 4: According to article 3, if a computer system, or part of it, or data or information from a computer is seized unknowingly in another jurisdiction, the judicial officer conducting the task shall act as if they have been provided with procedures that are to be obtained via mutual assistance requests.

Article 5: The judicial officer has the authority to order, for the process of any criminal investigation, any person who may harbour knowledge concerning the working of the computer system (or measures utilised to keep data hidden), to reveal all the required information and to enable the undertakings of the methods referred to in Article 3.

Article 6: The judicial officer is given power to carry out criminal investigations or proceedings and can (without obtaining a search warrant) go to whatever lengths are required to preserve the data stored by means of a computer system. This is particularly so when they have reason to believe that the information is likely to be retained for a short period or that it could be easily lost or modified. The officer also has power to compel the safeguarding and protecting of the integrity of the data for ninety days, a period that is renewable by the judge.

With reference to paragraph 1, the prosecution office must be notified by the judicial officer within 24 hours from the date of (or information concerning) forceful acquisition of data.

Article 7: In the UAE, police departments must appoint a place of contact available 24 hour a day, 7 days a week, to provide immediate assistance. This is for the purpose of investigating criminal offences related to the use of computer systems and its data, or for the exchange of electronic evidence of a criminal nature. This assistance shall include giving technical advice and preserving data, as well as collecting evidence, giving legal information and locating suspects.

Article 8: Electronic evidence obtained from outside the UAE is to have the same authenticity and evidentiary value as if discovered in the UAE, so long as all the proper

procedures have been followed.

Article 9: The UAE's Minister's Council must prepare guidelines for handling electronic evidence.

Article 10: The Minister's Council should review and update guidelines on an annual basis, for on special events or as required by circumstances.

Article 11: Special documentation for the examination of all electronic evidence is to be carried out and made available for court viewing.

Article 12: It is the examiner's role to ensure that the measures taken on the original or the copy are suitable and correctly documented. The original document must be preserved, and in cases where changes are unavoidable, all of these must be documented appropriately.

Article 13: The judicial officer must be adequately trained with experience and qualifications sufficient to fulfil their role in collecting, analysing and presenting the electronic evidence.

Article 14: The authority and measures referred to in the current articles shall be subject to regulations and safeguards as given by the UAE constitution.

After proposing these rules, it is important establish where they can be inserted: whether in the CPL, Federal Law No.5 of 2012 on Information Technology Crimes or in a special procedural law for electronic evidence. The researcher considers it appropriate to include the new rules in UAE CPL, as insertion in Federal Law No. 5 might lead to a misapprehension that electronic evidence is required and used only for cybercrimes. It is therefore more appropriate to continue with the same legislation policy rather than issuing special procedure laws for electronic evidence.

6.3 Obstacles to applying the previous proposals

When applied, all new proposals are confronted with obstacles. The above proposals are intended as a starting point in attempting to overcome the shortcomings and disadvantages associated with the regulation systems for electronic evidence in the UAE. A number of these obstacles are as follows:

I. **Financial cost**: preparation and qualification of the police officers, prosecutors, lawyers and judges requires an appropriate budget as training has become increasingly expensive. This also needs to cover the cost of specialised courses with qualifications, alongside the development of laboratories with the latest equipment and tools. Finances could be a reason for the lack of development or rehabilitation of most law enforcers, as well as for the lack of modernisation of laboratories.

II. **Law enforcers' training**: UAE is a federal state divided into both local and federal systems. Each state possesses its own administrative and financial jurisdiction. If any UAE state decides to enhance the skills of its law enforcers the project will be run in the state only. This may lead to an imbalance in education levels between the law enforcers of different states. For example, if there is a project to train police officers, prosecutors and judges in Dubai without a similar project in existence in another Emirate, this could lead to a difference in the educational levels between members in the UAE. There is no prosecution or specialised courts for cybercrimes in the UAE, which leads to difficulties in identifying the target group. Development and training entails identifying the group and the purpose of the training, requiring a database currently unavailable in the UAE. It is therefore necessary for the UAE to establish such a database.

III. **New rules for electronic evidence**: new legal rules may create significant procedural problems, particularly at the beginning of the application. A low level of knowledge, understanding and awareness could be the main considerations in deciding whether to introduce new procedural rules. It is very difficult to instigate new rules where the knowledge level of the law enforcers is low. The applied study revealed that a large percentage of law enforcers were unable to distinguish between electronic and other types of evidence. The previous two points (training and new rules) are linked. Education is therefore the first step that needs to be taken. When officers are educated to a high standard, then new rules can be proposed. This is the only means of ensuring that the rules are applied effectively, and therefore the UAE must have both a long and a medium term plan to increase awareness levels.

IV. **Conventions and international cooperation**: strong international cooperation and coordination is extremely important: however, they are also subject to political influence. Although the UAE is currently peaceful state, its government may prefer not to organise or attend international conventions or treaties.

The above obstacles should not, however, become a reason for a lack of regulation of electronic evidence, as for any issue there is usually a solution.

The UAE Ministry of Justice can be offered a financial budget to cover the cost of the above through the ministry resources, or through financial support from local or federal departments, or by private enterprises. When it comes to the training of law enforcers, the UAE Ministry of Justice should have long-and short-term plans for rehabilitation and training across the UAE. The UAE Ministry of Justice must also work to raise understanding and awareness levels of law enforcers when it comes to the new rules for electronic evidence. The UAE Government can pursue the establishment of conventions and international cooperation through attending international conventions, etc., through the Gulf Cooperation Council (GCC).

6.4 Conclusion

Law enforcement faces a number of challenges when it comes to the collection of electronic evidence for criminal procedures. The collection method for electronic evidence is different to that of physical evidence, and so requires the formation of new rules to govern evidence regulation. Reformation will not be confined to the gathering of electronic evidence, but also to the investigative process as a whole. This demonstrates the ways in which technology requires changes to be made to the law. Technology divides the warrant process from its conventional one-step process to a new, two-step process, resulting in the need for new rules to govern the second step. Modifying the rules also gives the legal system an unusual window to experiment with new laws, in order to made the move towards the use of electronic evidence.

The initial findings of this research have considered the research questions. It can be seen that there are defects in the procedures concerning collection, presentation and analysis of electronic evidence. The authenticity of electronic evidence must always be ensured. Law enforcement can ensure that the evidence is allowed in court if guidelines

are followed effectively. It has been noted that law enforcement has difficulties when it comes to dealing with electronic evidence. This stems from the fact that the usual protocol is not followed in the analysis, collection and presentation of electronic evidence. Law officers are not sufficiently trained and there are no programmes to guarantee the development of officials. The problem is aggravated by the fact that standards are lacking when it comes to handling, collecting and presenting electronic evidence. Investigators should be provided with adequate knowledge on how to handle of electronic evidence through the means of standard operating procedures and training.

A number of recommendations have been made on the basis of the findings of this thesis. They aim to improve the methods of collecting, analysing and presenting electronic evidence. Crimes involving computers will become increasingly normalised, and it is time that the effect electronic evidence can have in investigations is acknowledged. More research into electronic evidence is highly recommended in order to keep up to date with developments in cybercrime.

This is the UAE's first investigation into the regulation of electronic evidence and to gain an understanding of the level of knowledge required. It is significant in the field of law and opens the way for further research. This thesis will serve as a basis for future research by providing new information for electronic evidence. It has also demonstrated that judges give their decision regarding electronic evidence based on their current knowledge. Criminal procedure rules must be reworked in the UAE to deal with this new age of electronic evidence. Amendments in rules can affect the prosecution of crimes and set an international standard, and this has the potential to assist other countries facing a similar clash between old rules and new technologies.

CHAPTER SEVEN: CONCLUSION

It is appropriate to conclude by summarising the aims of this thesis and how far it has accomplished its objectives. Specific topics were introduced and there has been an attempt to add to the overall knowledge regarding the regulation of electronic evidence.

The study seeks to find answers to two main questions: (1) whether the UAE's Criminal Procedure Law is sufficient to regulate electronic evidence process and (2) what is the level of knowledge, understanding and awareness of electronic evidence in the UAE? Each question may be linked to, and have an influence on, the other. In order to answer these questions, sub-questions are required, and so the chapters have been designed to answer both questions and sub-questions.

Chapter One aimed to introduce the significance of the research and map out its requirements. The chapter also contained a literature review and established relevant terminology.

It was observed in Chapter One that the subject of electronic evidence has recently gained considerable attention from many authors and institutions. There is a growing body of literature examining the relationship between IT and law. [1]Many of these patterns begin with the classic issue of the crimes being committed and the way they are being dealt with. Nevertheless, cybercrime can be carried out at the touch of a computer keyboard, from any location, and (as a result of globalisation) targeting its victims across the world. This complex problem creates challenges. These include the difficulty of identifying and locating the offender, ensuring that the detection of these crimes is very difficult. This results in the rapid increase in the numbers of criminal cases demonstrating the need to find new ways to combat crime, in order to ensure that the use of electronic evidence can be an increasingly useful weapon. Chapter One further provided definitions of electronic evidence and an interpretation of the term 'computer', neither of which are defined by any UAE statutes. The lack of such definitions could result in diverse outcomes when determining the relevance and authentication of electronic evidence, something that could create opportunities for disagreements during

[1]See: section 1.7.

a trial.[2] It is therefore necessary to use clear and specific terms in order to be successful in the practice of criminal prosecutions, leading to a need to reconsider the law from the point of view of the interpretation of the terminology, rather than to leave such interpretation to the courts. Such an interpretation is required in the UAE states, due to the fact that there are no standard definitions of the terms 'electronic evidence' and 'computer' in their statutes.[3]

Chapter Two provided an overview of the UAE's legal system. This included establishing the development of the criminal procedure law in the UAE and highlighting the role of the judge and each interested party when it comes to evidence. The chapter also covered the type and the nature of electronic evidence and the criminal investigation and distinctions between physical crime and cybercrime.

The main purpose of Chapter Two was to establish a background for the following chapters. It demonstrated the procedural aspects of the UAE's legal system and tracked the CPL development from its introduction in 1992 until its latest amendment in 2005. It also provided a comparison between traditional and electronic evidence, including different types of electronic evidence. In summary, the UAE is a federation of states in which jurisdiction is based on a civil legal system. There is no distinction made between types of evidence in the CPL. However, Chapter Two demonstrated that there are a number of differences in the nature of electronic evidence and traditional evidence. The question then arises as to whether the general rules of CPL are sufficient to cover electronic evidence Chapters Three and Four then aimed to shed further light upon these matters.

Chapter Three provided a 'macro-comparison' approach to the regulation of electronic evidence. The chapter explored the nature and the background of the regulation of electronic evidence in civil and common law systems, through a case study of England and Wales, and China. Significant points of convergence have been noted in respect to the electronic evidence across the system, with a few differences presented either by the respective statutes or general interpretation traditions of the systems. Each system has its unique merits and demerits over alternative systems.

[2]See: section 1.8.1.
[3]See: section 6.2.5.

This chapter established that the issues of electronic evidence can be 'universal'. There are always instances in which 'evidence' has been lost due to the fact that there were no rules with which to regulate electronic evidence, or a lack of coordination and international cooperation. This results in the problem of electronic evidence being a universal one. Chapter Three demonstrated that there is a point of convergence in both regimes, in that their regulatory regimes (particularly the civil procedural laws) have since adjusted their arguments on electronic evidence from admissibility to probative or evidential value. Evidential weight will be higher where such documents can be authenticated. The most important issue relating to the electronic documents, therefore, is establishing their authentication and verification. In common law, the judges wield greater discretion in the establishment of the integrity of electronic evidence, while in a small number of cases business officers and public agencies are permitted to issue authentication certificates. This contrasts with Chinese civil law, where the authentication and verification processes are well defined by the statutes and is a preserve of authentication agencies falling under the executive docket.

Chapter Four provided a 'micro comparison' approach to criminal procedure rules and related issues of electronic evidence. The chapter attempted to support the argument that there are regulatory shortcomings in the UAE's CPL.

Chapter Four thus attempted to shed light upon the processes of all electronic evidence, starting with the search for, and seizure of, electronic evidence, then moving on to the means of its preservation and examination, to the final stage, which consists of its presentation at trial. The following are legal shortcomings revealed by applying the UAE's CPL:

- Since electronic evidence has different criteria from traditional evidence, it is recognised that CPL rules cannot meet the conditions and requirements for search warrants. As seen in Chapter Four, this may affect the search for, and seizure of, electronic evidence and the successful prosecution of crime. The CPL rules therefore need to be modified, due to the fact that using the general rules of CPL has created a procedure that is cumbersome, and is therefore

difficult to use as a successful, regulatory implement.[4]

- Since there are no specific rules, guidelines or any legal framework in the CPL, electronic evidence can be easily lost, damaged or altered, as has been frequently demonstrated. Thus it is important to regulate the processing of electronic evidence in order to avoid any such loss of evidence.

- Due to the fact that there are no rules for documenting the process of examining electronic evidence in the CPL (or any UAE legal framework), it is highly recommended that a legal framework is constructed to ensure that all forensic experts and members of the police follow all the correct procedures, which can also be checked by a third party, and can so ensure a conviction.

- Since there are no rules set down in the CPL concerning evidence obtained from overseas, this evidence would be questioned when presented at court.

- The case of the UAE Ministry of Education (as noted in Chapter Four), highlights the importance of regulating electronic evidence. Evidence that permits different interpretations can lead to different judgments. In addition, the importance of the regulation of electronic evidence was also discussed in other UAE cases, an example of which was given in previous chapters.

Chapter Five examined the issues concerning electronic evidence in the UAE. The applied study highlighted awareness regarding the use of electronic evidence. There was an exploration of views of legal experts and other specialists towards the regulation of electronic evidence in the UAE. Both research methods of social sciences (i.e. qualitative and quantitative) were used, through the analysis of interview findings and the statistical results of questionnaires. The findings revealed by the applied study are as follows:

- The statistical results of the applied study demonstrate that the level of knowledge regarding electronic evidence is generally inadequate.

- There is not sufficient knowledge or awareness regarding the methods used in the search for, and seizure of, electronic evidence, including its preservation,

[4]Ibid.

examination and presentation.

- There is not sufficient awareness concerning the challenges and problems of crime in relation to electronic evidence.

- The issues which law enforcers complain most about in the UAE with regard to electronic evidence are:

A. There is no procedural guide for electronic evidence preservation. This supports the idea that regulation of electronic evidence could reduce the chance of loss of evidence due bad handling.

B. There are no specific rules governing search and seizure of electronic evidence. This claim is supported by the majority of respondents who believe that the CPL rule is insufficient to deal with electronic evidence.

C. Absence of awareness and indicative programs. This claim is supported by the result of the applied study, which demonstrated that the lack of these programs resulted in a decrease in the level of knowledge concerning electronic evidence.

D. Limited specialists in electronic evidence. This supports the view that the UAE needs to increase the number of available specialised training courses.

E. Absence of international cooperation. This supports the idea that the UAE needs to approve and establish conventions regarding coordination between states.

The majority of the interviewees were of the opinion that the CPL rules were insufficient to deal with electronic evidence, and that a solution could be found in a proposed Federal law clearly regulating electronic evidence. However, few interviewees argued that the CPL is capable of dealing with electronic evidence, as demonstrated by Ali Hamouda, who states:

> There is no reason to find a special procedural law. Finding a procedural law for electronic evidence will restrict the authority of the judge. Judges in the UAE legal system have freedom in sentencing. The law will prevent the judge from using this feature, because the judge will apply the legal rules and will not be able to reject the evidence or not apply them.[5]

[5]See: translated transcript of the interview with Dr. Ali Hamouda in Appendix 5.

On the other hand, Judge Abdul Wahab Abdul, President of the UAE's Federal Supreme Court, when asked how Emirates judges can be sure of the reliability and authenticity of the electronic evidence, replied:

> Clearly, because there is a shortage of laws, we depend on the forensic report and for me this represents a weakness in judgment. When the judge rules, based on the opinion of another person not his mind, this could lead to the prejudice of justice. However, if we have clear rules the judge will be able to make a decision.[6]

Judge Abdul Wahab's views are supported during interviews with further specialists, who express the opinion that electronic evidence needs to be regulated. When the researcher queried the Minister of Justice of the UAE on the subject of regulation, the Minister noted:

> Realistically, for this academic controversy, if we need to find a new law we will seek to publish it. The opposing views can be discussed when discussing the issues of the law, but that is not a reason not to publish it. Personally, I tend to support special rules for electronic evidence. The CPL is indispensable. However, if there are some legal shortcomings, it is better to cover them by special laws, especially for some special aspects. The CPL may be able to regulate general aspects, but not special aspects such as electronic evidence or cybercrimes. So it is highly recommended to find special procedural laws.[7]

It will be a positive development if the UAE government chooses to examine the advantages and disadvantages of the regulation electronic evidence.

Chapter Six was divided into two parts. The first raised a number of challenges and problems facing law enforcers with regard to electronic evidence and gaps in the existing criminal procedures of the UAE. The second put forward a number of solutions concerning the regulation of electronic evidence. The recommendations represent the considerations raised by the thesis' academic discussions. The final results of the thesis serve as recommendations for changes to the UAE's regulations. These recommendations will prove invaluable if the investigations regarding the failures of the UAE system prove accurate.

[6]See: translated transcript of the interview with Judge Dr. Abdul Wahab Abdul in Appendix 5.
[7]See: translated transcript of the interview with Dr. Hadef Al Dhahiri in Appendix 5.

7.1 Findings

7.1.1 Is the UAE's CPL sufficient for the regulation of electronic evidence?

This initially appears a straightforward question. As long as there is a difference in the nature of electronic and traditional evidence, the method of dealing with such evidence will inevitably vary. However, when it comes to the legal aspect, the answer is not so straightforward. The procedural problems likely to occur when applying specific legal rules are complex, as the law does not distinguish between types of evidence. Hence, that which is applied to traditional evidence is also applied to electronic evidence.[8]

The lack of academic studies in the UAE has further increased the difficulty of answering this question. A review of the literature is the most effective way to address this issue, as it offers a consideration of differing views, so enabling the researcher to discuss opinions and indicate the strengths and weaknesses of the various approaches.

This researcher therefore referred to an extensive body of literature from other countries in seeking to answer the research question. The 'Admissibility of the electronic evidence in court: a European project' provided by the European Commission was found to be the most useful research project regarding the regulation of electronic evidence. The project covered sixteen European Union Member States in order to investigate whether electronic evidence is regulated in European countries, and to examine the nature of the problems faced in the gathering, analysing and presentation of such evidence.[9]

The difficulties in establishing an answer for this question also lies in the lack of cases in the UAE involving electronic evidence. These issues relate to an interpretation of legal rules, or the implementation of procedural rules, thus implying the existence of legal shortcomings. This is the basis of establishing the effectiveness of the rules for the prosecution of a crime. However, as the Minister of the UAE Justice states:

> The small number of cases does not mean that there is no cybercrime in the UAE. It could be caused by a failure to detect crimes or to not getting evidence.[10]

[8] See: section 2.4.
[9] See: section 1.2.
[10] See: translated transcript of the interview with Hadef Al Dhahiri in Appendix 5.

In order to investigate this matter the researcher conducted a detailed legal analysis. A number of observations can be made from cases presented in previous chapters suggesting that future problems may well arise in relation to electronic evidence.[11]

Thus, the researcher established that the most effective means of finding an answer to the key question is through the use of sub-questions. These sub-questions deal with the four key processes of electronic evidence.

7.1.1.1 What are the difficulties arising as a result of the use of UAE's CPL rules in terms of the search and seizure of electronic evidence?

The previous chapters demonstrated that applying the UAE's CPL in terms of the process of searching and seizure of electronic evidence introduces legal procedural problems, i.e. the need for a search warrant.[12] This has legal conditions. Article 72 of the UAE's CPL provides that:

> 'The member of the public prosecution shall search the dwelling of the accused upon a charge imputed to him of perpetrating a crime or by acting as an accomplice in it. He may, in this respect search any place and seize any papers, arms and all what may likely be used in the perpetration of the crime or resulting there from, as well as anything that may help in revealing the truth'.[13]

As a result, the CPL outlines two conditions for obtaining a search warrant: the crime must have been committed and must be punishable.[14] These requirements must be fulfilled before a search may begin.

Electronic evidence, however, differs from other kinds of evidence. As a result, the UAE's CPL rules may be inappropriate when applied to electronic evidence, which has the ability to exist in more than one place, including outside the state, whereas a search warrant is specified in terms of location and time. The UAE's CPL requires the presence of the suspect or his representative during the search process,[15] something that is difficult to apply when searching for electronic evidence. These conditions are

[11] See: for example the case of the UAE Ministry of Education in section 4.9.
[12] See: section 4.2.2.
[13] The UAE Criminal Procedures Law, Article 72.
[14] For further discussion see: section 4.2.2.
[15] The UAE Criminal Procedures Law, Article 59.

difficult to fulfil. In support of this view, Judge Dr. Mohammed Al kamali, General Director of the Institute of Training and Judicial Studies in Abu Dhabi, UAE states:

> The CPL is not commensurate with cybercrime and crime scene evolution, which is no longer in the past. A crime scene in cybercrime is a default theatre. There are many risks of loss of evidence, and in addition, the electronic evidence may exist in more than one place. Electronic evidence needs expertise in how to acquire and preservative it. Current procedural law has loopholes and does not cover the process of electronic evidence.[16]

7.1.1.2 Is the UAE's CPL sufficient to preserve the electronic evidence?

In the UAE there are no rules or guidance on the ways to preserve evidence, whether traditional or electronic. Shortcomings of the UAE CPL (and a lack of guidance) has the potential to lead to an increase in the loss of evidence, especially as a result of a lack of knowledge on the part of law enforcers. Due to the fact that electronic evidence requires only a single click to be lost, ineffective handling and lack of relevant expertise on the part of law enforcers leads to the need for more stringent rules to regulate the electronic evidence process. A forensic investigator interviewed by the researcher states:

> There are many cases where we lost evidence due to technical or bad handling. Also, the offender is another reason. Sometimes the accused destroys evidence before reaching through programs and tools and so it cannot be obtaining as evidence. The problem is the nature of electronic evidence. Electronic evidence is intangible evidence it's not like other evidence. The difficulty lies in how to find the evidence and get it. The forensic investigator's experience plays an important role in finding evidence and the recovery. If the forensic investigator doesn't have enough experience we will not be able to find the evidence. The error here was not a procedural or criminal intelligence problem, but the forensic investigator's experience.[17]

Hence, an investigation should be conducted into the current situation and to the amendments made to evidence statutes in other countries such as the US, the UK and Australia.

The process of collecting electronic evidence in criminal cases, crime has become

[16] See: translated transcript of the interview with Judge Al kamali in Appendix 5.
[17] See: translated transcript of the interview with Al Ketbi in Appendix 5.

increasingly technical due to the developments in the technology. Investigating such is becoming increasingly challenging when *mens rea* must be proved beyond reasonable doubt. In future, it will become even more complicated, due to everything being stored in a digital format, or some equally intangible form. An investigator must be well prepared and be in possession of the appropriate expertise in order to effectively collect electronic evidence. An investigator requires the expertise to be able to identify which parts of the available material are relevant, while at the same time ensuring that the process of searching leaves the evidence intact. Chapter Four set out the US Pocket Guide for First Responder, which is particularly relevant to this issue, as it details electronic crimes in which computers have been used, and could therefore serve as a basis for creating a standardised operating procedure in the UAE.[18]

7.1.1.3 What are the procedures for examining electronic evidence in the UAE?

The UAE is in possession of the most up to date laboratories and examination devices, but does not have the appropriate legislation. The administrative procedural rules appear to be inadequate and it is necessary to put more effective legal rules in place in order to convince a judge. The best model available for such rules is the Chinese one, in which the authentication and verification processes are well outlined by the statutes and is the preserve of authentication agencies. The Chinese model could prove an advantageous example for the UAE, in particular the introduction of specialised and specific authentication agencies to which neither litigant has access to electronic evidence.[19]

This view is supported by Major Rashid Lootah, head of the Electronic Evidence Unit at the Criminal Evidence and Criminology Department- Dubai Police who, when asked if he considered regulation of the procedures of examining electronic evidence by law as necessary, stated:

> Yes we need to ensure that all procedures were followed properly and all evidence had not been tampered with. The existence of rules will help us to ensure that all forensic experts or police members follow all the correct procedures and can also be checked by a third party.[20]

[18] See: section 4.5.
[19] See: section 3.4.2.
[20] See: translated transcript of the interview with Lootah in Appendix 5.

7.1.1.4 What are the procedures for presenting electronic evidence to a court in the UAE?

Convincing a judge is a means to achieve a ruling. The judge needs to understand all the procedures with regard to obtaining evidence and this will only be achieved when there is effective presentation. UAE laws do not cover the process of obtaining electronic evidence, and thus the prosecutor may be unable to clarify these procedures and thus achieve a conviction. Were such rules in place, the prosecutor would be able to explain and illustrate all the procedures used in terms of search and seizure, and the examination of electronic evidence.

The case of the UAE Minister of Education is a real-life example of the ways in which presentation of the evidence can affect a judge's ruling: when the prosecutor failed to present evidence convincingly and explain the process of obtaining the evidence, different sentences were given.[21]

In the light of this, Judge Dr. Mohammed Al kamali commented in an interview with the researcher:

> If there is a clear rule on search and seizure, and on examining electronic evidence, the judge will convene and therefore will sentence on conviction.[22]

The shortcomings revealed by the answers to the sub-questions illuminate the fact that the UAE CPL is insufficient to deal with electronic evidence in the UAE. A solution therefore needs to be found in order to overcome its failings. The CPL may be suitable in terms of a general framework, but we also need to create a special framework to regulate some of the details.

7.1.2 What is the level of knowledge, understanding and awareness of electronic evidence in practical life in the UAE?

Due to an existing lack of statistics and previous studies, the researcher conducted an applied study in order to measure the awareness and level of understanding of electronic evidence. At the same time, the study highlighted the current issues

[21] See: section 4.9.
[22] See: translated transcript of the interview with Judge Al kamali in Appendix 5.

concerning the regulation of electronic evidence in the UAE from the perspective of both legal experts and other specialists. The results support the proposition that there are overall deficiencies in the regulation of electronic evidence in the UAE, and also in the level of understanding and awareness with regard to electronic evidence in practical life in the UAE.

The results of the applied study reveal that the majority of the participants did not possess sufficient knowledge concerning electronic evidence. [23] Increasing this knowledge is therefore important in removing any uncertainties, and so ensures its effective use. There also needs to be a higher level of understanding and knowledge governing the processes of detection and collecting evidence.

The results of the applied study have been taken into consideration when the researcher established the suggestions put forward in the thesis.[24]

7.2 Limitations of the research

It was important that the thesis was aligned in its approach, working and objectives. An assessment of the thesis is to study its consistency between what was planned and what was achieved. The limitations of the thesis affected its assessment, due to the fact that it was carried out by a single researcher with limited time and money. It would have been beneficial to be able to assess the knowledge of the UAE law enforcement and the potential effect of regulations for electronic evidence on the results of prosecution. However, such unrealistic goals were never part of this work. The applied study is one limited scale study and should be viewed in the light of laying the basis for further work on this subject. It was ambitious to examine the systems in other countries with a similar legal framework as the UAE (such as other Arab countries). Limited academic resources are a barrier to studying such systems, and these systems were found to contain similar shortcomings to the UAE. If this study had examined a developing country then the system would have had the potential to serve as a model. However, studying these systems is difficult due to the language barrier (e.g. French or German).

Constant evaluation of legal rules in a developing country, such as the UAE, is

[23] See: section 5.3.
[24] See: Part two in Chapter Six.

important.[25] This thesis is dedicated to the facts concerning electronic evidence. It might be argued that regulation of electronic evidence is not the most pressing regulatory issue, however, its importance lies in the positive results of such regulations on controlling crime.

As a result of discussions while drafting this thesis, the primary layout was made as malleable as possible so that all issues could be included. The inclusion and exclusion criteria are appropriate to the analysis, and the main body of the thesis is divided into legal theoretical and applied study.

There are many publications relating to the law and IT.[26] A number of writers have chosen to address the law and IT in general, and others have specifically addressed the application of the relevant laws in IT or cybercrime.[27] The issues surrounding electronic evidence have recently become a subject for a number of authors.[28] There are many areas to be considered in terms of detection in the electronic evidence field. This was the starting point for the researcher when it came to selecting the subject for study. Moving from the general to the specific, the researcher then established that an aspect that had not yet been examined was the regulation of electronic evidence. This thesis has endeavoured to establish solutions to the procedural issue of whether the UAE's CPL is sufficient to govern the process of gathering, preserving, examining and presenting electronic evidence and if it requires supplementary legislation. It may, however, require a wider examination in order to obtain a clear picture of the factors that currently influence the legal aspects. This has led to a number of limitations, which are discussed below.

7.2.1 Scope of the research question

The research question sought to cover all procedural issues emerging from the regulation of electronic evidence in the UAE. A number of these (e.g. obtaining evidence from abroad) could not be addressed in detail. However, the researcher chose to take a comprehensive view of the procedural issues, rather than adopt an in-depth

[25]UAE classified as a high income developing country.
[26]Writers such as: Ian Lloyd, *Information Technology Law* (6th edn, OUP Oxford 2011).
[27]Writers such as: Thomas Clancy, *Cyber Crime and Digital Evidence Materials and Cases* (LexisNexis 2011). Susan Brenner, *Criminal Threats from Cyberspace* (Pentagon Press 2012).
[28]See: section 1.7.

research approach focussing on one. The main reason for choosing such an approach is that all the factors are interrelated. What affects the search and seizure stage will affect the examination or presentation stage. Furthermore, as far as can be established, this study is the first in the UAE and it has therefore been necessary to obtain a broad, rather than an in-depth, view. A comprehensive study such as this will encourage in-depth research in the future. This thesis is more focused on cybercrime rather than physical crime, due to the fact that detecting and fighting cybercrime depends a good deal more electronic evidence than does physical crime.

7.2.2 Legal and geographical scope

This research has sought to consider this issue with regard to UAE Federal Laws, in particular Federal Law No. 35 of 1992. However, there are references to other states' laws, which are used as models. While the literature review was drawn from studies globally, the practical elements (e.g. the questionnaires and interviews) have been conducted in the UAE, thus placing a UAE perspective on the responses.

7.3 Opportunities for future research

This study seeks to be the basis of future studies concerning electronic evidence, both at the UAE level and of other countries in the Middle East and elsewhere. However, there may well be many (as yet uncovered) instances of shortcomings in the regulation of electronic evidence. This will be of great value for future research. The researcher recommends the following areas for future work:

- To analyse and evaluate different legal challenges brought about by computer crimes and electronic evidence.
- To examine and evaluate the extent to which UAE laws comply with ICT developments.
- To consider the effect of international laws in accepting electronic evidence.
- To examine and evaluate the extent to which methods associated with search and seizure for electronic evidence can have a bearing on the rights of the suspect.

There are undoubtedly further areas in need of research. Further research into electronic evidence can be structured in such a way as to improve the ability of law enforcers when it comes to the prosecution of crimes. Future research may also apply a number of the methods used in this research, such as combining applied methods and critical analytical methods.

7.4 Conclusion

With the amalgamation of IT and the law, electronic evidence comes into being. The subject of electronic evidence touches on two different professional areas – the law and IT. Electronic evidence has now begun to feature in legal cases and can play an extremely important role in prosecuting crime. However, the judicial process is complicated by the absence of any legal regulation of electronic evidence.

In the light of what this research, it is clear that in the UAE the level of knowledge, understanding and awareness of electronic evidence is weak in practice. This research has also raised the issue that UAE CPL is insufficient for the regulation of electronic evidence. There are a number of areas that need to reform in the CPL due to their current vagueness.

The researcher has put forward a number of recommendations with the aim of helping to overcome the gaps in CPL. In order to reach an integrated regulation for electronic evidence, raising the level of awareness and knowledge among law enforcers is vital at this preliminary stage.

It is hoped that the present work will represent the first step in encouraging a stronger understanding of electronic evidence in the UAE.

Appendices

Appendix 1: A Letters to the Interviewees

Letter of Consent

Dear…….

I am a PhD student at the School of Law, Bangor University, United Kingdom under the supervision of Dr. Yvonne McDermott. I am conducting research to fulfil the requirements for obtaining a PhD in law and am sponsored by the Government of Dubai.

A letter from my supervisor, Dr. Yvonne McDermott from the School of Law, Bangor University, is also enclosed to verify my accountability and reliability.

I would like you to examine the enclosed summary of the study. It is concerned with the subject of 'electronic evidence in criminal procedure' and is entitled "The Regulation of Electronic Evidence in the UAE: Current Limitations and Proposals for Reform". The summary aims to provide an overall insight into the study and highlights the role and importance of your participation.

In this respect, I would like to ask your permission to conduct an interview with you. I assure you this would be conducted under strict ethical research principles. In the interview (which would be expected to take approximately half an hour) you may wish to provide opinions based on your expertise and insight.

Your participation in this study is, of course, voluntary. You have the right to choose not to participate or to withdraw from the study at any time. The results of the research study may be published, but your name will not be used unless you consent. I give you my assurance that all information provided by you in the interview will be used for research purposes only, and will not be conveyed to any third party. It would save both time and effort for us both if the interview could be tape or digital recorded. Otherwise, I will have to transcribe it. Following the interview, you will be given the opportunity to review the transcripts or recordings, and you may ask for alterations to and omissions from your statement. The transcripts will be kept in the privacy of the researcher's home

office and any audio materials containing conversations with the researcher will be erased following completion of the research. Your identity and quotations from the interview will only be mentioned in the research if you give your permission. Each interview will be identifiable only by a random number, and the link between this number and the identity of the interviewee will be kept only in a confidential file in the possession of the researcher and will not be disclosed. The interviewing aims to generate accessible information from your insights and experience, not to access confidential information illegitimately. I would be grateful if you would confirm that your organization will allow you to take part in the interview. If you agree to participate in this study, there are no foreseeable political, legal or economic risks or discomforts. The interview will not involve any self-incrimination or disclosure of confidential information regarding yourself or entity to which you belong. In this regard, you have the right to consent or not to any of the following.

Please tick all of the following boxes to which you agree and leave those to which you do not agree.

- o I understand the purpose of the research being conducted as I have an overview of the study and the role of my participation.
- o I agree to be identified in the research by name and position.
- o I understand that excerpts from my written transcripts and tape-recorded verbal communications with the researcher will be studied and may be quoted in a PhD thesis and in future papers, journal articles and books that will be written by the researcher.
- o I understand that transcripts on paper and tape recordings and digital files, will be secured in the privacy of the researcher's home office and that any audio tapes of my conversations with the researcher will be erased following the end of the research.
- o I understand that my participation is entirely voluntary and that I may withdraw my permission to participate in this study without explanation at any point up to and including the interview.

Yours……,

COLEG BUSNES, Y GYFRAITH, ADDYSG A GWYDDORAU CYMDEITHAS
COLLEGE OF BUSINESS, LAW, EDUCATION AND SOCIAL SCIENCES

PRIFYSGOL
BANGOR
UNIVERSITY

17 January 2013

Re: Khaled Ali Saleh Aljneibi

To whom it may concern,

This letter is to confirm that the above-named individual is a Ph.D. student at Bangor University School of Law, United Kingdom. Under my supervision, he is currently in his third year of doctoral studies on the topic of electronic evidence in the United Arab Emirates.

An important part of Khaled's doctoral thesis is an applied study of opinions and attitudes towards electronic evidence in the UAE. His methodology and action plan have been rigorously tested and approved by Bangor University's Ethics Committee. I hope that you will be willing to participate in this enthusiastic and erudite student's applied study. Your opinions will be invaluable to him in assessing attitudes towards electronic evidence and in formulating recommendations on the use of electronic evidence in the UAE in future criminal proceedings.

Should you have any queries, please do not hesitate to contact me via my direct telephone line: +44 1248 388085, or via email at y.mcdermott@bangor.ac.uk.

With every good wish,

Yvonne McDermott

Lecturer in Law

PRIFYSGOL BANGOR, CANOLFAN WEINYDDOL BANGOR, GWYNEDD, LL57 2DG

BANGOR UNIVERSITY DMINISTRATIVE CENTRE, BANGOR, GWYNEDD, LL57 2DG

RO/PROFESSOR PHIL MOLYNEUX BA, Mphil, PhD
ENNAETH Y COLEG/HEAD OF COLLEGE

Declaration to be attached to the Topic Form
For research degrees (Phd, MPhil and MA by research)

A copy of this declaration accompanied by a copy of the research proposal should be sent to Anwen Evans, Secretary, CBSSL Ethics Committee (CBSSLEthics@bangor.ac.uk)

Prior to undertaking any research project, students and supervisors should familiarise themselves with the University's Research Ethics Policy. The policy document can be found at the website below

http://www.bangor.ac.uk/ar/ro/recordsmanagement/REF.php

Researchers should note that the following research activities would normally be considered as involving more than minimal risk and, consequently, require ethical review by the College Ethics Committee:

i) Research involving vulnerable groups – for example, children and young people, those with a learning disability or cognitive impairment, or individuals in a dependent or unequal relationship.

ii) Research involving sensitive topics – for example participants' sexual behaviour, their illegal or political behaviour, their experience of violence, their abuse or exploitation, their mental health, or their gender or ethnic status.

iii) Research involving groups where permission of a gatekeeper is normally required for initial access to members.

iv) Research necessarily involving deception or which is conducted without participants' full and informed consent at the time the study is carried out.

v) Research involving access to records of personal or confidential information, including genetic and other biological information, concerning identifiable individuals.

vi) Research that would induce psychological stress, anxiety or humiliation or cause more than minimal pain

vii) Research involving intrusive interventions – for example, the administration of drugs or other substances, vigorous physical exercise, or techniques such as hypnotherapy.

Data Protection

If it is anticipated that human participants will be engaged, duly singed Consent forms and information sheets should be drawn up and a copy lodged with the secretary of the College Ethics Committee. Special attention must be given to compliance with the legal requirement of checks by the Criminal Records Bureau

when dealing with children and vulnerable adults. The College Manager should be able to guide applicants through this process. The student must discuss with supervisors and agree procedures to ensure confidentiality of respondents.

Declaration by student:

The student should sign either of the following declarations, as appropriate, followed by a declaration by the supervisor.

EITHER
I certify that I have read the Research Ethics Policy of the university and my supervisor agrees with me that none of the issues raised there is relevant for this research project because (Maximum of 200 words overleaf)

(Sd).....Date.....

Name of researcher.....

OR
I certify that I have read the Research Ethics Policy of the university and believe that my research proposal requires ethical review. The relevant ethical issues are addressed as follows.(Maximum of 200 words overleaf)

(Sd).....Date 3.10.2012

Name of student Khaled Al.Jneibi.

Declaration by supervisor:

I have read the University's Research Ethics Policy and the College Ethics Policy and, in my professional judgement and on the basis of information given to me by the student (**delete as appropriate**)

EITHER

All the relevant ethical issues have been addressed satisfactorily and I recommend that approval is given subject to these steps being taken (**enumerate**)

OR

All the relevant ethical issues will have been addressed satisfactorily subject to following steps being taken by the student, and I recommend that approval be given by CBSSL Ethics Committee

(Sd) Yvonne McDermott Date 03/10/2012

Name of Supervisor Yvonne Mc Dermott

Declaration on ethical issue raised in the research project

Khaled Ali Aljneibi (PhD Thesis) under Supervision Dr. Yvonne McDermott At School of Law in the College of Business, Social Sciences and Law-Bangor University.

The research title**:** The Regulation of Electronic Evidence in the UAE: Current Limitations and Proposals for Reform.

This statement intends to provide assurance that the above named Ph.D. research program will be conducted in such a manner that it satisfies the requirements of the University's Research Ethical framework. In particular, the research will address the following ethical responsibilities:

- Ensure that valid, informed consent is obtained before individual participate in the research;
- Avoid personal and social harm;
- Protect the confidentiality of information about the research participants and their identities;
- Ensure dignity, respect and privacy are accorded to research participants;
- Review the assessment and management of risk to the researchers and the research participants during the research.

The proposed research requires ethical review and approval from the College Ethics Committee because the research will be conducted in UAE which is outside United Kingdom (as enshrined in section 5.3 of the Bangor University Research Ethics Framework).The research will be conducted in one phase. It will be carried out between December 2012 and March 2013.In addition to this statement, I pledge to comply with any other condition(s) the University may so wish to add that will make the propose research valid and reliable. Enclosed are a copy of signed Declaration for the College Ethics Committee's consideration and approval.

Mr. Khaled Al jneibi

Ph.D. Program (Ref: 5000189834)

School of Law

Appendix 2: Original questionnaire (Arabic)

إستبيان.

يهدف هذا الاستبيان لجمع المعلومات الضرورية لغرض قياس الآراء ومستوي الوعي والإدراك بالمشاكل العملية للادلة الإلكترونية في الواقع العملي لدولة الامارات العربية تحت عنوان " تنظيم الأدلة الألكترونية، القيود الحالية ومقترحات الاصلاح، دراسة قانونية تطبيقية ".

المطلوب منك الإجابة على أسئلة الإستبيان بدقة وموضوعية مع الأخذ بعين الاعتبار أن المشاركة إختيارية ولك الحق في الإنسحاب في أي وقت. كما أود أن أؤكد على أن جميع البيانات والمعلومات الواردة في هذا الاستبيان سوف يتم التعامل معها بسرية تامة بواسطة الباحث ولهدف البحث العلمي فقط. ولكم جزيل الشكـــــــــــر والتقدير....

أولا: البيانات الأولية:

جهة العمل:

القضاء (.....)

النيابة (.....)

المحاماة (.....)

الشرطة (.....)

الخبرة: 3-6 سنوات ☐ 7-10 سنوات ☐ 11-15 سنوات ☐ 16سنه وأكثر ☐

ثانيا:- يرجى وضع علامة (√) في المربع الذي يلائم رأيك.

- ما مدى معرفتك بما يلي:

العبارة	اعلم	لا اعلم
الأدلة الإلكترونية والفرق بينها وبين أدلة الإثبات الاخرى.		

العبارة	اعلم	لا اعلم
طرق جمع الأدلة الإلكترونية.		

العبارة	اعلم	لا اعلم
أماكن تواجد الدليل الالكتروني بمسرح الجريمة الإلكترونية.		

العبارة	اعلم	لا اعلم
كيفية المحافظة على الأدلة الإلكترونية.		

العبارة	اعلم	لا اعلم
الإجراءات الواجب إتباعها عند فحص الأدلة الإلكترونية.		

العبارة	اعلم	لا اعلم
طرق إستعادة الادلة الإلكترونية بعد حذفها والتقنيات والأدوات المستخدمة في ذلك.		

العبارة	اعلم	لا اعلم
التقارير الفنية الخاصة بالأدلة الإلكترونية (كيفية الوصول الى النتائج وطرق عرضها ومناقشتها).		

العبارة	اعلم	لا اعلم
الصعوبات العملية والتحديات الناشئة عن الجرائم الإلكترونية فيما يتعلق بالحصول على الأدلة الإلكترونية.		

ثالثا: فيما يلي مجموعة من السلبيات الشائعه في مجال الأدلة الإلكترونية ،المطلوب من المشارك أن يختار السلبيات التي يرى انها تنطبق على دولة الامارات (يمكن إختيار عدد غير محدد).

م	البـــــند	الاجابة
1	عدم وجود قواعد خاصة تنظم عمليات تفتيش وضبط الأدلة الإلكترونية.	
2	عدم وجود قواعد إرشادية تكفل المحافظة على الأدلة الألكترونية بمسرح الجريمة.	
3	عدم توثيق الإجراءات عند فحص الأدلة الإلكترونية.	
4	جمع الأدلة الإلكترونية من قبل أشخاص غير مؤهلين.	
5	عدم وجود فني متخصص بمسرح الجريمة أثناء ضبط الأدلة الإلكترونية.	

6	قلة عدد المتخصصين في مجال الأدلة الإلكترونية.	
7	عدم تحديث المختبرات الخاصة بفحص الأدلة الإلكترونية بصورة مستمرة.	
8	عدم وجود إتفاقيات وتعاون دولي في مجال الأدلة الإلكترونية.	
9	الأحجام وعدم الإبلاغ عن الجرائم الإلكترونية.	
10	عدم وجود أنظمة إجرائية وبرامج حماية تقنية بالمؤسسات الخاصة والدوائر الحكومية.	
11	عدم وجود تنسيق بين الدوائر والهيئات التنظيمية المختلفة.	
12	عدم وجود برامج تثقيفية و إرشادية لافراد المجتمع.	

رابعا:- يرجى وضع علامة (√) في المربع الذي يلائم رأيك مع إمكانية إضافة أي تعليقات لبيان وجهة نظرك .

- الى أي حد توافق او تختلف مع العبارات التاليه:

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
1	يجب وضع تعريف قانوني محدد للادلة الإلكترونية.			

تعليق:.....

.....

.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
2	يجب وضع قواعد خاصة تنظم طرق الحصول على الأدلة الإلكترونية.			

تعليق:.....

.....

.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
3	يجب جمع الأدلة الإلكترونية من قبل أشخاص مؤهلين فنيا بذلك.			

تعليق:.....

.....

.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
4	يجب توثيق جميع الإجراءات الخاصة بفحص الأدلة الإلكترونية.			

تعليق:.....

.....

.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
5	يجب تحديث المختبرات الخاصة بفحص الأدلة الإلكترونية بصورة مستمرة.			

تعليق:.....

.....

.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
6	يجب وضع برامج تدريبة وتأهيلة لأفراد النظام القانوني (أفراد الشرطة، محامين، وكلاء نيابة، قضاه) فى مجال الأدلة الإلكترونية.			

تعليق:.....

.....

.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
7	يجب إبرام إتفاقيات فى مجال التعاون الدولي لضمان الإستفادة من الأدلة الإلكترونية والحد من تزايد خطورة الجرائم الإلكترونية.			

تعليق:.....

.....

.....

Appendix 3: Translation of the questionnaire (English)

This questionnaire is a method to collect necessary data for the following research:

Title: The Regulation of Electronic Evidence in the UAE: Current Limitations and Proposals for Reform. (PhD Thesis).

Researcher: Mr, Khaled Ali Aljneibi.

Supervisor: Dr. Yvonne McDermott.

University: Bangor University, United Kingdom.

I ask for your participation, in this questionnaire, which aims to measure attitudes and experiences towards electronic evidence in the UAE. Initially, I would like to thank you for accepting to take part in this study. For research purpose, I would need your true and honest answers to this set of questions. All the information provided by you will be used for research purposes only and will be secured in the privacy of the researcher's home office. Your participation in this study is, of course, voluntary. You have the right to choose not to participate or to withdraw from the study at any time. I would be grateful if you would answer this questionnaire fully. The questionnaire will be anonymous.

Section (1): Demographic Information:

Please put a tick (√) in the box that best suits your demographic information

1- Profession Type:

A- Judge ( ).

B- Prosecutor ( ).

C- Lawyer ( ).

D- Police officer ( ).

2-Average Practical Experience:

3-6 Years ☐ 7-10 Years ☐ 11-15 Years ☐ 16 Years and over ☐

Section (2): How would you rate your own familiarity with?

Please put a tick (√) in the box that best suits your opinion.

Statements	I Know	I don't know
The difference between electronic evidence and other kinds of evidence.		

Statements	I Know	I don't know
Methods of gathering electronic evidence.		

Statements	I Know	I don't know
Placement of electronic evidence in the cybercrime scene.		

Statements	I Know	I don't know
Methods of preservation of electronic evidence.		

Statements	I Know	I don't know
Procedures for electronic evidence examination.		

Statements	I Know	I don't know
Techniques and tools for electronic evidence examination.		

Statements	I Know	I don't know
Forensic expert's reports of electronic evidence (how to get the results, presented and discussed).		

Statements	I Know	I don't know
Challenges and problems of cybercrimes in relation to electronic evidence.		

Section (3): The respondent is asked to select from twelve negative aspects of electronic evidence field which they thought were applicable in the UAE (You can select an unspecified number).

NU	Item	respond
1	There is no specific rules' governing search and seizure of electronic evidence.	
2	There is no procedures guide for electronic evidence preservation.	
3	Procedures of examining electronic evidence not documenting.	
4	Unqualified persons collect Electronic evidence.	
5	There is no technician person during a seizure of electronic evidence.	
6	Limited specialists of the electronic evidence.	
7	Do not update laboratories of electronic evidence.	
8	Absence of international cooperation.	
9	Non-reporting of cyber-crimes.	
10	Absence of protection programs.	
11	Lack of coordination between departments and the regulatory bodies.	
12	Absence of awareness and indicative programs.	

Section (4): To what degree do you agree with these statements?

Please put a tick (√) in the box that best suits your opinion.

NU	statements	Answer		
		Agree	Unsure	Disagree
1	There should be legal terms for electronic evidence.			

Comments:.....

.....

.....

NU	statements	Answer		
		Agree	Unsure	Disagree
2	We need to promulgate clear guidelines on how to deal with electronic evidence in the UAE.			

Comments:.....

.....

.....

NU	statements	Answer		
		Agree	Unsure	Disagree
3	Gathering electronic evidence should be by qualified persons.			

Comments:.....

.....

.....

NU	statements	Answer		
		Agree	Unsure	Disagree
4	Examining electronic evidence should be documented.			

Comments:.....

.....

.....

NU	statements	Answer		
		Agree	Unsure	Disagree
5	Should we update laboratories of electronic evidence continuously.			

Comments:.....

.....

.....

NU	statements	Answer		
		Agree	Unsure	Disagree
6	Police officers, lawyers, prosecutors, and judges need more professional training on electronic evidence.			

Comments:.....

.....

.....

NU	statements	Answer		
		Agree	Unsure	Disa gree
7	There must be strong international cooperation and coordination between regulators to succeed in the effective prosecution of cyber-crimes and make full use of electronic evidence.			

Comments:.....

.....

.....

Appendix 4: Questionnaire respondent comments (open-ended questionnaire question

9	الإحجام وعدم الإبلاغ عن الجرائم الإلكترونية.	✓
10	عدم وجود أنظمة إجرائية وبرامج حماية تقنية بالمؤسسات الخاصة والدوائر الحكومية.	✗
11	عدم وجود تنسيق بين الدوائر والهيئات التنظيمية المختلفة.	✗
12	عدم وجود برامج تثقيفية و إرشادية لافراد المجتمع.	✓

رابعا:- يرجى وضع علامة (√) في المربع الذي يلائم رأيك مع إمكانية إضافة أي تعليقات لبيان وجهة نظرك .

- الى أي حد توافق او تختلف مع العبارات التاليه:

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
1	يجب وضع تعريف قانوني محدد للادلة الإلكترونية.	✓		

تعليق:.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
2	يجب وضع قواعد خاصة تنظم طرق الحصول على الأدلة الإلكترونية.	✓		

تعليق:.....

"I think we need to focus on training people especially police officers".

3	يجب جمع الأدلة الإلكترونية من قبل أشخاص مؤهلين فنيا بذلك فقط.	✓	

تعليق:.....

"When collecting electronic evidence is done by unqualified people that could lead to inadmissible evidence".

تعليق: حتى يمكنه الرجوع اليها من قبل الجهات الرسمية
في حال فقدانه او تقرير علاوة الى الحاجة الماسة لشرعية بيانات
نفس الجهات.

"We need documenting of all procedures of examining electronic evidence. As a result, we can guarantee the examination process".

تعليق: لن توجد جرائم حديثة بأساليب غريبة يلزم مواكبتها

"There should be updated laboratories to effectively combat criminals".

6	يجب وضع برامج تدريبية وتأهيلة لأفراد النظام القانوني (أفراد الشرطة، محامين، وكلاء نيابة، قضاه) فى مجال الأدلة الإلكترونية.	✓		

تعليق: حتى يتم وجوب النظر وقبول الأدلة الالكترونية

"Training is beneficial for admissible electronic evidence".

7	يجب إبرام إتفاقيات فى مجال التعاون الدولي لضمان الإستفادة من الأدلة الإلكترونية والحد من تزايد خطورة الجرائم الإلكترونية.	✓		

تعليق: للاطلاع على احدث التقنيات
وطرق علاج او الوقاية من تلك الجرائم في اسرع وقت
قبل وصولها الى الدولة.

"To increase the level of knowledge and sharing experiences".

9	الأحجام وعدم الإبلاغ عن الجرائم الإلكترونية.	✓
10	عدم وجود أنظمة إجرائية وبرامج حماية تقنية بالمؤسسات الخاصة والدوائر الحكومية.	
11	عدم وجود تنسيق بين الدوائر والهيئات التنظيمية المختلفة.	
12	عدم وجود برامج تثقيفية و إرشادية لافراد المجتمع.	✓

رابعا:- يرجى وضع علامة (√) في المربع الذي يلائم رأيك مع إمكانية إضافة أي تعليقات لبيان وجهة نظرك .

- الى أي حد توافق او تختلف مع العبارات التاليه:

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
1	يجب وضع تعريف قانوني محدد للادلة الإلكترونية.	✓		

تعليق: [illegible]

"To differentiate between electronic evidence and other evidence".

تعليق: [illegible]

"In order to have clear rules".

3	يجب جمع الأدلة الإلكترونية من قبل أشخاص مؤهلين فنيا بذلك فقط.	✓		

تعليق: [illegible]

"In order to do correct procedures for search and seizure of electronic evidence".

تعليق: حتى يمكن الرجوع إليه عند الاقتضاء والعلم بدلالة الدليل من حيث الإدانة من عدمه.

"In order to be referenced and we can refer to it".

تعليق: حتى نواكب التطور التكنولوجي حيث نشهد بعض الدول انتهجت خطوات متقدمة في هذا المجال وبالتالي تتقدم إثباتية الدليل الالكتروني.

"To keep up pace with the technological development".

تعليق: حتى نضمن صحة الإجراءات الالكترونية وكذلك الحفاظ على حقوق المتهم بشكل سليم لأن المتهم الذي ليس له دراية لن يستطيع الحفاظ على الدليل في صورته الطبيعية.

"To ensure that all process of search and seizure for electronic evidence is correct".

تعليق: لأن الجرائم عبر الحدود من الجرائم الأخرى خاصة أن الجرائم الالكترونية تعتبر من الجرائم العابرة للحدود وبالتالي فهي أولى بتطبيق هذه الاتفاقيات.

"Because cybercrime is international crime, we need international cooperation and coordination".

9	الأحجام وعدم الإبلاغ عن الجرائم الإلكترونية.	
10	عدم وجود أنظمة إجرائية وبرامج حماية تقنية بالمؤسسات الخاصة والدوائر الحكومية.	
11	عدم وجود تنسيق بين الدوائر والهيئات التنظيمية المختلفة.	✓
12	عدم وجود برامج تثقيفية و إرشادية لأفراد المجتمع.	✓

رابعا:- يرجى وضع علامة (√) في المربع الذي يلائم رأيك مع إمكانية إضافة أي تعليقات لبيان وجهة نظرك .

- الى أي حد توافق او تختلف مع العبارات التاليه:

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
1	يجب وضع تعريف قانوني محدد للادلة الإلكترونية.		✓	

تعليق: المعرفة بالأدلة الالكترونية وكيفية الوصول اليها أفضل بكثير من التعريف القانوني والذي يدخل ضمن الجانب النظري

"Finding rules to regulate electronic evidence process is more valuable than defining electronic evidence".

تعليق: قد تكون هناك قواعد لدى الخبراء والفنيين ولكن يتعين نشرها للتوعية المجتمعية لمن له علاقة بذلك.

"We must raise awareness among all people who deal with electronic evidence".

تعليق: فلا يتصور أن يكون جميع أفراد التحريات مؤهلين فاحيانا يدخل ضمن إجراءاتهم وجود أدلة الكترونية لذلك يجب تثقيفهم

الاحالة

"It is inconceivable all police officer have knowledge on how to deal with electronic evidence, so there should be collection of electronic evidence by qualified people".

9	الأحجام وعدم الإبلاغ عن الجرائم الإلكترونية.	✓
10	عدم وجود أنظمة إجرائية وبرامج حماية تقنية بالمؤسسات الخاصة والدوائر الحكومية.	✓
11	عدم وجود تنسيق بين الدوائر والهنيات التنظيمية المختلفة.	✓
12	عدم وجود برامج تثقيفية و إرشادية لافراد المجتمع.	✓

رابعا:- يرجى وضع علامة (√) في المربع الذي يلائم رأيك مع إمكانية إضافة أي تعليقات لبيان وجهة نظرك .

- الى أي حد توافق او تختلف مع العبارات التاليه:

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
1	يجب وضع تعريف قانوني محدد للادلة الإلكترونية.	✓		

تعليق:

"Defined electronic evidence may lead to narrow scope of electronic evidence".

تعليق:

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
3	يجب جمع الأدلة الإلكترونية من قبل أشخاص مؤهلين فنيا بذلك فقط.	✓		

تعليق:

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
4	يجب توثيق جميع الإجراءات الخاصة بفحص الأدلة الإلكترونية.	✓		

9	الأحجام وعدم الإبلاغ عن الجرائم الإلكترونية.	
10	عدم وجود أنظمة إجرائية وبرامج حماية تقنية بالمؤسسات الخاصة والدوائر الحكومية.	
11	عدم وجود تنسيق بين الدوائر والهيئات التنظيمية المختلفة.	✓
12	عدم وجود برامج تثقيفية و إرشادية لافراد المجتمع.	✓

رابعا:- يرجى وضع علامة (√) في المربع الذي يلائم رأيك مع إمكانية إضافة أي تعليقات لبيان وجهة نظرك .

- الى أي حد توافق او تختلف مع العبارات التاليه:

م	البــــند	الإجابة		
		موافق	محايد	غير موافق
1	يجب وضع تعريف قانوني محدد للادلة الإلكترونية.	✓		

تعليق: مراعاة الانضباط في التعريف ولا تشمل الألفاظ المطاطة التي تدعم [illegible] الأدلة

"The definition of electronic evidence should be clear".

م	البــــند	موافق	محايد	غير موافق
2	يجب وضع قواعد خاصة تنظم طرق الحصول على الأدلة الإلكترونية.	✓		

تعليق:..

م	البــــند	الإجابة		
		موافق	محايد	غير موافق
3	يجب جمع الأدلة الإلكترونية من قبل أشخاص مؤهلين فنيا بذلك فقط.	✓		

تعليق: قيد جمع الأدلة على التأهيل الفني فقط فيه من الجور لأن التأهيل قد يكون [illegible] الشهادات العلمية الحاصل عليها القائم بالجمع [illegible] [illegible] في مجال التقني والمعلوماتي [illegible] [illegible] [illegible]

م	البــــند	الإجابة		
		موافق	محايد	غير موافق
4	يجب توثيق جميع الإجراءات الخاصة بفحص الأدلة الإلكترونية.	✓		

"I agree, but there are unqualified persons (they do not have certificates) having knowledge and experience in the technical field who may help".

تعليق:...
....
....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
5	يجب تحديث المختبرات الخاصة بفحص الأدلة الإلكترونية بصورة مستمرة.	✓		

تعليق:...
....
....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
6	يجب وضع برامج تدريبية وتأهيلة لأفراد النظام القانوني (أفراد الشرطة، محامين، وكلاء نيابة، قضاه) فى مجال الأدلة الإلكترونية.	✓		

تعليق: توجد [illegible] لتأهيل أعضاء النيابة والقضاة على الجرائم الإلكترونية [illegible] ذلك وهو حاليا قيد الدراسة [illegible]

"There is a government trend towards qualifying prosecutors, and judges on cybercrime".

	من تزايد خطورة الجرائم الإلكترونية.	✓		

تعليق: لأن الجريمة الإلكترونية جريمة عابرة للقارات [illegible] سهولة الارتكاب وصعوبة الوصول [illegible]

"Cybercrime is intercontinental crime, facilitating the commission and difficulty of reaching to the defendants".

تعليق:.....
.....
.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
5	يجب تحديث المختبرات الخاصة بفحص الأدلة الإلكترونية بصورة مستمرة.	✓		

تعليق:.....
.....
.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
6	يجب وضع برامج تدريبية وتأهيلة لأفراد النظام القانوني (أفراد الشرطة، محامين، وكلاء نيابة، قضاه) فى مجال الأدلة الإلكترونية.	✓		

تعليق:.....
.....
.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
7	يجب إبرام إتفاقيات فى مجال التعاون الدولي لضمان الإستفادة من الأدلة الإلكترونية والحد من تزايد خطورة الجرائم الإلكترونية.	✓		

تعليق: بصراحة هناك تأخير في اعداد التقارير وعدم الدراية
بتعريف لافراد الشرطة العاملين في المراكز بادلة الالكترونية
وكيفية التوصل اليها والمحافظة عليها وتوثيقها واستخراج الادلة منها حيث ان
الضبطيات الاولى بدائية من قبل افراد الشرطة في المراكز

"Frankly, there is a delay in preparing forensic reports and level of understanding and awareness is extremely low. Police officers use primitive methods when handling electronic evidence".

تعليق: ....

م	البنـــد	الإجابة		
		موافق	محايد	غير موافق
5	يجب تحديث المختبرات الخاصة بفحص الأدلة الإلكترونية بصورة مستمرة.	✓		

تعليق: أن تكون هناك زيارات دورية لأعضاء النيابة للتعرف أكثر على التحديثات بالناحية العملية

"Prosecutors should visiting forensic laboratory for further knowledge on practical issues".

6	يجب وضع برامج تدريبية وتأهيلة لأفراد النظام القانوني (أفراد الشرطة، محامين، وكلاء نيابة، قضاه) فى مجال الأدلة الإلكترونية.	✓		

تعليق: يجب إفراد [crossed out] نيابة متخصصة في مجال مكافحة الجرائم الإلكترونية بها أعضاء وموظفين

"There should be a specialized prosecution of cybercrime".

7	يجب إبرام إتفاقيات فى مجال التعاون الدولي لضمان الإستفادة من الادلة الإلكترونية والحد من تزايد خطورة الجرائم الإلكترونية.	✓		

تعليق: بالإضافة إلى ذلك يجب عقد مؤتمرات واجتماعات مع الدول المتقدمة في مجال الجرائم الالكترونية للاستفادة من المعلومات الحديثة التي توصلت إليها ومحاولة تطوير الأنظمة لدينا بحيث تواكب كل جديد في هذا المجال.

"There should be courses and workshops on cybercrime and we should update laws".

تعليق:.....
.....
.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
5	يجب تحديث المختبرات الخاصة بفحص الأدلة الإلكترونية بصورة مستمرة.	✓		

تعليق:.....
.....
.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
6	يجب وضع برامج تدريبية وتأهيلة لأفراد النظام القانوني (أفراد الشرطة، محامين، وكلاء نيابة، قضاه) فى مجال الأدلة الإلكترونية.	✓		

تعليق:.....
.....
.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
7	يجب إبرام إتفاقيات فى مجال التعاون الدولي لضمان الإستفادة من الأدلة الإلكترونية والحد من تزايد خطورة الجرائم الإلكترونية.			

تعليق:.....
.....
.....

"We must also ensure the integrity of evidence".

تعليق:.....
.....
.....

م	البـــــند	الإجابة		
		موافق	محايد	غير موافق
5	يجب تحديث المختبرات الخاصة بفحص الأدلة الإلكترونية بصورة مستمرة.			

تعليق:.....
.....

"Is particularly beneficial to successfully prosecuting cybercrimes".

6	يجب وضع برامج تدريبية وتأهيلة لأفراد النظام القانوني (أفراد الشرطة، محامين، وكلاء نيابة، قضاه) فى مجال الأدلة الإلكترونية.	✓		

تعليق:.....
.....
.....

"To raise knowledge level".

7	من تزايد خطورة الجرائم الإلكترونية.	✓		

تعليق:.....
.....
.....

"To sharing experiences".

9	الأحجام وعدم الإبلاغ عن الجرائم الإلكترونية.	X
10	عدم وجود أنظمة إجرائية وبرامج حماية تقنية بالمؤسسات الخاصة والدوائر الحكومية.	X
11	عدم وجود تنسيق بين الدوائر والهنيات التنظيمية المختلفة.	✓
12	عدم وجود برامج تثقيفية و إرشادية لافراد المجتمع.	✓

رابعا:- يرجى وضع علامة (√) في المربع الذي يلائم رأيك مع إمكانية إضافة أي تعليقات لبيان وجهة نظرك .

- الى أي حد توافق او تختلف مع العبارات التاليه:

م	البـــند	الإجابة		
		موافق	محايد	غير موافق
1	يجب وضع تعريف قانوني محدد للادلة الإلكترونية.	✓		

تعليق: .....

"Electronic evidence is variable evidence".

2	يجب وضع قواعد خاصة تنظم طرق الحصول على الادلة الإلكترونية.	✓		

تعليق: .....

"So we can easily check for all procedures".

		✓		

تعليق: .....

"Is extremely essential to avoid legal loopholes".

4	يجب توثيق جميع الإجراءات الخاصة بفحص الأدلة الإلكترونية.	✓		

تعليق: ..... مهم لتفادي ضياع البيانات الرقمية .....

"Is extremely essential to avoid loss evidence".

		✓	يجب تحديث المختبرات الخاصة بفحص الأدلة الإلكترونية بصورة مستمرة.	5

تعليق: ..... هذا المجال متطور بسرعة .....

"This field is fast developing".

		✓	يجب وضع برامج تدريبه وتاهيلة لافراد النظام القانوني (افراد الشرطة، محامين، وكلاء نيابة، قضاه) فى مجال الأدلة الإلكترونية.	6

تعليق: ..... مهم لتدريب القائمين على الأدلة الإلكترونية .....

"Training is particularly powerful".

		✓	من تزايد خطورة الجرائم الإلكترونية.	7

تعليق: ..... يمكن الأدلة الإلكترونية في أي مكان في العالم .....

"Electronic evidence can be found outside the UAE".

Appendix 5: Transcript translation of the interviews from Arabic

Interview (1)

Interviewee: Ahmed Al Ketbi, forensic investigator, Telecommunications Regulatory Authority of the UAE.

Place and date: Dubai, January 2013.

INTERVIEWER: Can we start with your opinion towards the level of awareness and understanding of cybercrimes and electronic evidence in the UAE?

INTERVIEWEE: "Personally, I think the level is increasing; this is because the media now play an important role in raising awareness of cognitive. Also, the Telecommunications Regulatory Authority of the UAE plays a role in the dissemination knowledge through visiting schools, universities and the parents of students. We face several difficulties such as, how to explain technical issues but in the end we are trying to raise the awareness level".

Can we discuss search and seizure procedures for electronic evidence, please?

"To answer your question we first need to divide the request for the search and investigation; there are two types (covert or overt), covert means that the person does not know about the inspection and overt does; this divide is important because we can select inspection time. When we reach the search and seizer place we must take an overview of the location and imagery. We then Look at the device and determine its condition, is it in running or not. Are there any other devices connected to it or not. Is there a Wireless Access Point or not. All these things and more are important because it affects the search and seizure evidence and any oversight could lead to the loss of evidence".

Are these procedures documented and authenticated as a guide line and must they be followed by an investigator?

"If we want to talk about the Telecommunications Regulatory Authority of the UAE it is accredited by the US ASCLD/LAB and has (ISO 27001:2005) this for quality assurance as well as all procedures undergoing an internal audit".

So I understand that you follow these procedures only for the convention and ISO? Did you have your own procedures?

"No, we only use the procedures accepted by the US ASCLD/LAB but it is a good idea to have our own. I think that we need own procedures dealing with all processes starting with seizure, preservation and examination of electronic evidence. When it has; nobody can argue and also it will be assurance that all procedures have been followed by the investigator".

Did the Telecommunications Regulatory Authority have the cooperation and coordination of other regulatory bodies in the UAE?

"There are some agreements signed with a number of bodies such as, the Abu Dhabi Police. However, this agreement has not become common practice yet. We also seek to sign another agreement with the Dubai Police".

In the UAE, the procedures with regards to the gathering of evidence are provided under general rules of the UAE's Criminal Procedures Law (CPL). In what manner can be said that the CPL is appropriate to cover electronic evidence?

"I am not sure, because I have no legal knowledge. But, I believe electronic evidence needs special care, because electronic evidence has a different nature and criteria. For example, if we need to seize a computer which is a tool of crime we can use general rules of search and seizure. However, if the evidence cannot be found on that computer it could be in another place, so we need take other procedures. As a result, I think it becomes extremely difficult to seize electronic evidence by general rules. At this point, I would note that the electronic evidence can be found in different places".

This is an essential point, as you mentioned that the electronic evidence can be found in different places, it could be in the UAE or outside, have you encountered difficulties in obtaining evidence from outside the UAE?

"Yes, there are difficulties in obtaining evidence outside the UAE, this issue needs international cooperation".

What is the procedure with regard to this?

"We first look if there is an agreement with the state or not. If yes, we contact them

officially. If not, we contact them cordially. The difficulty is if the act was done by the defendant who is not a criminal in that State, the request will be rejected".

Could you please explain how to deal with electronic devices after seizure?

"There is something important to know at this point, if the device is running, you must take data from the RAM directly before shutting down, because if you do not do this there is a possibility of losing evidence. There are many cases where we lost the evidence due to bad handling. After seizing the device, all data is copied on a hard disk; numbering devices and codification data case, date, names…etc. Then we put all the devices in a bag and seal it and sent to the laboratory".

Could you please give us a practical example of bad handling?

"Without naming names, one of the authorities in the UAE told us that one of its staff dissemination and misused a body of information. After investigation we found that the authority had formatted the computer. As a result, we were unable to get the evidence. It was due bad handling from the authority".

Electronic evidence can be altered, lost or destroyed. In practice can we retrieve all data? If not, have there been cases in the UAE? What is the reason? Is it technical or bad handling?

"Can be both, yes there are many cases where we lost evidence. Also, the offender is another reason. Sometimes the accused destroys evidence before reaching through programs and tools and so it cannot be obtaining as evidence. The problem is the nature of electronic evidence. Electronic evidence is intangible evidence it's not like other evidence. The difficulty lies in how to find the evidence and get it. The forensic investigator's experience plays an important role in finding evidence and the recovery. If the forensic investigator doesn't have enough experience we will not be able to find the evidence. The error here was not a procedural or criminal intelligence problem, but the forensic investigator's experience".

Could you please give us a practical example?

"Yes, one of the cases is when the analyst deletes evidence when handling the case and we cannot get it back again".

Are there specific conditions of storage?

"Certainly, there are conditions for storage such as, humidity and temperature of the place etc. Electronic devices need special care".

What techniques and tools are used to examine electronic evidence?

"Electronic evidence can be examined and analysed through several techniques. This can be divided into two main tools; tools for copying and tools for analysis. All these tools must be accredited by organisations and bodies. If not, we must test the tool internally".

Do you take a backup of the evidence before it's examined?

"Sure, where the original evidence is retained and analysed we use the copy only. But there are cases where you cannot take a backup of the evidence then we examine the original evidence".

Is a laboratory for electronic evidence updated continuously?

"Of course, technology is rapidly evolving and it is extremely important to update the laboratory to ensure that the tools are always upgraded. We in the Telecommunications Regulatory Authority update tools continuously".

Could you please illustrate how to write forensic reports?

"After examining devices we write the report, which includes details of the case, description of devices etc. Then we write details of the analysis process and tools used in the examination. Finally, we state the result which does not include the names of people, because you cannot prove that, you only can prove the computer did the action".

Do you think this matter can lead to unsuccessfully prosecuting cyber-crimes?

"I think so yes, it is very easy for a suspect to deny a related device or he can claim that his device was penetrated".

Is there any way to prove a suspect's connection to the device?

"Yes, but it is difficult".

How can you check result reliability? Is there any guarantee?

"There is a guarantee for the examination process, for example; in the examination process the device is checked by more than one person. Furthermore, there is an internal audit. In contrast, there is no guarantee of a valid conclusion".

We can check the examination process by internal auditing, however, how can you prove the guarantee of all these processes if requested by a third party? The reason I asked this question is that I think there is no rule for examining electronic evidence in the UAE. Do you agree with me that we need to regulate electronic evidence?

"I agree. There is a vast area in electronic evidence that needs to be regulated. Also we need to have specialised (UAE) bodies such as courts, prosecutions …etc".

Interview (2)

Interviewee: Judge Dr. Mohammed AL kaabi, President of UAE Federal First Instance Court-Fujairah.

Place and date: Fujairah, January 2013.

INTERVIEWER: In your opinion; what practical problems are faced by judges with regard to electronic evidence in the UAE?

INTERVIEWEE: "We face many challenges, the main challenges I think is a lack of experience judges, and a low level of understanding and awareness. The reason for this could be the limited number of cases that contain electronic evidence and the age of the judges, as well as, the lack of training and specialised workshops".

What do you think are the main problems? Is it a lack of regulation procedures for electronic evidence or the limitations of the laboratories and the lack of specialists?

"In general it can be said both. However, I think a lack of regulation procedures is a real challenge. Without rules or regulations how can we check the reliability and credibility of electronic evidence?".

In the UAE, the procedures with regards to the gathering of evidence are provided under general rules of the UAE's Criminal Procedures Law (CPL).In what manner can be said that the CPL is appropriate to cover electronic evidence?

"In reality, we used the general rules; in some cases it is difficult to apply these rules for electronic evidence. Electronic evidence is different from other evidence, so we face some challenges when used these rules".

What can be a proposed solution?

"A solution can be through a proposed Federal law which should clearly regulate electronic evidence. If we cannot do this, we can adopt guidelines. From a legal point of view, the last solution is partial. A guide line has no power equivalent to the law in front of a court. From my point of view, there should be a completely new law in regard to this".

Emirates judges appreciate the pertinence of the evidence. In relation to electronic evidence, how can the judge be sure of the reliability and authenticity?

"In an application we depend on the forensic laboratory report".

Do you think questioning the credibility of a forensic laboratory report could lead to unsuccessfully prosecuting cyber-crimes?

"Not really, because in the UAE legal system, the judge has power to take any evidence; the judge has the discretion to take the report or to refuse it".

What do we need to make an effective presentation of electronic evidence?

"At this stage, I think we need only a brief presentation, most of the judges are not interested in hearing details. Also it is hard for judges to understand the technical terminology".

One of the challenges of the electronic evidence is a regional issue. Do you think that the UAE laws can deal with this issue?

"In terms of crimes committed outside the country, there are rules governing this issue. But, in terms of evidence I think there is a gap in the laws in this field, there is no rule regulating this issue. I guess this can be dealt with by standard international criminal

procedures".

Is it extremely hard to achieve standard international criminal procedures for all countries due to a lack of global consensuses?

"At the level of the Gulf Cooperation Council (GCC) there is a proposal to regulate cybercrime and electronic evidence by special criminal procedures. On the international level, we need at least more international cooperation and coordination".

Interview (3)

Interviewee: Professor. Mohamed Elamin Elbushra, Managing Director at African Centre for Criminal Justice Researches and Studies, Legal Advisor at UAE Ministry of Interior, Dean of the Studies and Research Center at Arab League – Naïf Arab University.

Place and date: Abu Dhabi, January 2013.

INTERVIEWER: We can start with your opinion towards the level of awareness and understanding of cybercrimes and electronic evidence in the UAE?

INTERVIEWEE: "Cybercrimes and electronic evidence is a new topic at a worldwide level. I think we are still at the beginning in the UAE. At present, the level of understanding and awareness is too low. In the UAE, there is no academic research, training courses or workshops in the field of electronic evidence or cybercrime. There is also no academic module at the universities. Cybercrime is a high tech crime which needs a high level of knowledge. Many members of the society are victims of cybercrime; those members do not know how to handle this type of crime or even maintain the evidence. A lot of people are stealing their account, and the crimes are discovered only accidentally. So, I believe we need more focus on such topics, which will help to raise the level of knowledge and find solutions to legal loopholes".

Do you think the non-reporting of crimes has lead to an increase?

"Of course, most companies prefer not to report because it fears losing the customers confidence and it prefers to cover losses by insurance companies. Also, a lack of knowledge of such a crime may be another reason. There are many reasons for the increasing spread of this type of crime".

In the UAE, the procedures with regards to the gathering of evidence are provided under general rules of the UAE's Criminal Procedures Law (CPL).In what manner can be said that the CPL is appropriate to cover electronic evidence?

"There was no law covering cybercrime in the UAE's Criminal Procedures Law prior to the coming into force of the Federal Law No. 2 in 2006 concerning the Prevention of Information Technology Crime. As a result, all rules of the CPL were designed to cover the offenses of the Penal Code. So, I believe it is notable to cover cybercrime or regulate electronic evidence".

Concerning this point of view is the best thing now to discuss if we need to propose a Federal law to regulate electronic evidence?

"Yes, there should be not only a law. There should also be guidance under the adopted law covering all procedures for electronic evidence starting with how to search and seize and in the end into how to examine this evidence. Who is must be based is procedure, and what qualifications have. In the UAE, there is Federal Law No. 2 of 2006 which covers crimes and penalties, but there is no law regulating the procedures for search and seizure of evidence. Several crimes will not be able to be proven because of the lack of rules".

So, there is a gap in the laws in this field. Have you got an idea why legal procedures were not issued for cybercrimes?

"In the UAE, federal legislation requires a considerably longer time and is more difficult to be adopted. The reason for this is complicated legislative procedures and bureaucracy. The Prevention of Information Technology Crime Law was issued in 2006, whereas the draft of this law was placed in 1999. I was one of the participants of the development of this law. At that time, there was no awareness of procedural problems of cybercrime, but now with the practical application the procedural problems have emerged".

Could you please mention some of these procedural problems?

"Until recently the courts have not allowed the use of electronic evidence and have questioned its credibility. We use traditional methods when dealing with technology; we use no update rules when evidence is seized, we do not use databases to ensure

preservation of evidence etc. All of this could lead to lots of opportunity to prove crimes and discovered. For example, switching off the electricity when seizing a computer can lead to the loss of evidence".

Do you think we need qualified people when handling electronic evidence?

"Definitely we need that; the person must have qualifications and must pass a number of courses. There must be also specialized courts and specialized departments of prosecutions and police. In the future, all crimes will become cybercrime".

One of the challenges of the electronic evidence is a regional issue. Do you think that the UAE laws can deal with this issue?

"This is one of the issues which must be deal with by a new law. Also, there should be a legal definition of the electronic evidence; in this law we should clarify all procedures for electronic evidence".

Interview (4)

Interviewee: Major Rashid Lootah, head of the Electronic Evidence Unit at the Criminal Evidence and Criminology Department- Dubai Police.

Place and date: Dubai, January 2013.

INTERVIEWER: In your opinion; what practical problems are faced with regard to electronic evidence in the UAE?

INTERVIEWEE: "There is no doubt that electronic evidence has a different nature from other evidence. As an example, fingerprints indicate the offender's presence in a place and do not need an explanation or analysis. However, it is not easy to determine electronic evidence locations. It needs more searches and analysis, as well as, the needs from the forensic knowledge, not only about the technical aspects but general knowledge. For example, when a forensic expert is handing an economic case, he must also have a basic knowledge on economic subjects. He must also be able to act as an expert witness. We face challenges in the UAE such as, insufficient number of forensic experts".

Do you think that electronic evidence has more procedures issues than other evidence concerning the search and seizure of evidence?

"Certainly, traditional evidence does not need more procedures, it end at the seizure time, while electronic evidence it doesn't; we need to know whether there are other devices connected to the computer or not. In some cases the search could be on servers and that needs more effort and time. All these factors and others, make the searching processes and procedures for electronic evidence more difficult".

Is there a technician present during a seizure of electronic evidence?

"In practice, no".

Why?

"Comparing a numbers of reports and a number of forensic experts it is difficult to send a technician for every case. Currently police members conduct the seizure process".

But police members may not have enough experience!

"There is coordination between our department and the electronic crime section. If there are any difficulties they will contact us and we will send a technician. There are also procedures on what they have to do when seizing evidence".

Are the rules which must be followed concerning the search and seizure of evidence?

"Yes, there are guidelines on how to search, investigate and the preservation. We aim to be followed by all police members when handling cybercrime".

Are these rules or guidelines accredited by law?

"By law no, they are only internal procedures".

Do you think we need to regulate electronic evidence by law?

"Yes, to ensure that all procedures were followed properly and all evidence had not been tampered with. The existence of rules will help us to ensure that all forensic experts or police members follow all the correct procedures and can also be checked by a third party".

Electronic evidence could be found in the UAE or overseas, does this matter represent any challenges?

"Yes, if there is no convention and international cooperation we will not be able to get the evidence. For example, if the suspect has stored evidence in the 'Dropbox' program how can we get it? In which server can it be found? 'Dropbox' has servers in Europe, Asia, and America".

Are there any practical examples?

"Yes, there are many cases where we cannot get the evidence because there is no cooperation".

Do you think if there is international convention in this field it will help us to get evidence easily?

"Yes, if we can resolve procedural issues the technical matters can be easily solved".

Electronic evidence can be altered, lost or destroyed. In practice can we retrieve all data?

"All evidence can be lost, not only electronic evidence. Fingerprints can be lost as well as electronic evidence. For example, each device has a storage capacity and if data has been cleared the possibility that we are not able to retrieve data is extremely high. Also, if evidence is cleared we cannot decide if there was evidence on the device or not. Even if I find the evidence I cannot decide that the person has already done the action or not; I can only decide that the computer was used as a tool to do the action. Malpractices such as the use of a device by more than one employee with no pass word etc. There is no strategy for companies to protect themselves from crime".

So, how can we ensure the result if we cannot decide that the person has already done the action?

"The results from the forensic expert's report are only a personal view of the expert. We can ensure by internal audit that all procedures were followed are correct, but we cannot ensure the conclusion".

Are there any objections or the conclusion questioned when presenting at court?

"In fact no, the judge is only looking for the conclusion not for the procedures. In contrast, the level of lawyers' knowledge about electronic evidence or expert report is very low. Therefore, he/ she cannot discuss the reports".

How many cases were dealt with by the Electronic Evidence Unit in 2012?

"In 2008 there were 278 cases, in 2009 the number increased to 436, in 2010 the number reached 445, and in 2011 there were 588 cases. In 2012 the number reached 772 cases, this figure in Dubai only".

Interview (5)

Interviewee: Lieutenant-Colonel Saeed Al Hajiri, Director of the Criminal Investigation Department's-Electronic Crime Section- Dubai Police.

Place and date: Dubai, January 2013.

INTERVIEWER: In your opinion; what practical problems are faced with regard to electronic evidence in the UAE?

INTERVIEWEE: "Cybercrime is a global crime. Consequently, electronic evidence is also international. In other words, you can find part of the evidence in one state and other part in another country. We are facing difficulties in gathering evidence from abroad. There are no conventions and effective international cooperation in this field. As an example, our department has been applying for evidence from abroad since 2010 and even now we have not had it. It can take more than 3 years to get evidence. Additionally, suspects could provide other challenges. The suspects nowadays are using 'Anti Forensic Technique' software and hardware which lead to the clearing of evidence".

Can you give us practical examples?

"Our department received a report that there is hacking on the government website, after proving this status and during our taking of action, the suspects were deleting the evidence and we cannot prove the crime".

Could you please explain the search and seizure procedures for electronic evidence?

"Firstly, we investigate a complaint and then collect enough information. After ensuring the complaint is valid we ask prosecutors for a search and seizure warrant. The second step is to carry out the search and seizure process. When evidence is seized we mark identify and send it to the 'Forensic Laboratory' for examination, this is a brief summary of search and seizure procedures".

Is there a technician present during a seizure of electronic evidence?

"Not for all crimes, only when we need that. There is a division of cases in our department, if the complaint needs a technician then we accompany. In brief, all hacking cases are accompanied by a technician".

In the UAE, the procedures with regards to the gathering of evidence are provided under general rules of the UAE's Criminal Procedures Law (CPL).In what manner can be said that the CPL is appropriate to cover electronic evidence?

"We are now applying UAE's Criminal Procedure Law rules; I think it is appropriate to cover electronic evidence".

But there are some challenges when applying this rule to electronic evidence!

"I agree with you".

Do you think if we proposed Federal law to regulate electronic evidence we could overcome these challenges?

"I agree, we can overcome them, but I disagree to propose Federal law".

Why?

"If we have rules, we must follow them. Technology is evolving very quickly, it could be impossible to use these rules five or ten years in the future".

But at least we have rules and we can update them!

"Updating rules in the UAE is very slow".

We completely updated Federal Law No. 2 of 2006 concerning the Prevention of Information Technology Crime after 6 years. How do you think we can resolve electronic evidence issues?

"As it exists in some countries, by guidelines or best practices and we can easily updated them".

So, you agree that the UAE's Criminal Procedures Law cannot only cover the electronic evidence and we need guidelines?

"Yes".

Do you think the non-reporting of crimes leads to an increase?

"Yes, most people do not have knowledge on how to deal with cybercrime and others are afraid about their reputation".

In your opinion, what do we need in order to effectively combat criminals and fully use the electronic evidence?

"I think we need to focus more on training, we need qualification courses. The person who carries out the search and seizure process must have accredited certificates".

Interview (6)

Interviewee: Judge Dr. Abdul Wahab Abdul, President of the UAE's Federal Supreme Court.

Place and date: Abu Dhabi, February 2013.

INTERVIEWER: In your opinion; what practical problems are faced by judges with regard to electronic evidence in the UAE?

INTERVIEWEE: "I agree with you that we face many challenges and difficulties with regard to electronic evidence, the Emirates is an advanced technology States and must have legislation, laws, and judges adapted with this development. I believe that we face procedural problems related to electronic evidence. There are no rules covering search and seizure processes, we don't know how to preserve electronic evidence or how to examine it. The judges now apply general rules of evidence which I think is not commensurate with the nature of electronic evidence and Criminal Justice. I have a

viewpoint in this respect; the UAE must have procedural law which regulates electronic evidence. We have penal law on cybercrimes but we don't have procedural law. The judge faces many challenges when handling electronic evidence, it is very difficult to understand procedures or how to deal with this kind of evidence, a judge is trying to apply general rules, but I think they do not apply. On the other hand, the cognitive level of judges concerning electronic evidence is low because of the lack of courses and lack of law regulates this field. Finally, I must restate my opinion that we need the creation of a new law dealing with electronic evidence".

Emirates judges appreciate the pertinence of the evidence. In relation to electronic evidence, how can the judge be sure of the reliability and authenticity?

"Clearly, because there is a shortage of laws we depend on the forensic report and for me this represents a weakness in judgment. When the judge rules, based on the opinion of another person not his mind, this could lead to the prejudice of justice. However, if we have clear rules the judge will be able to make a decision".

Do you think questioning the credibility of a forensic laboratory report could lead to unsuccessfully prosecuting cyber-crimes?

"Yes, I agree with you".

What do we need to do for the effective presentation of electronic evidence?

"We need only clear rules, when we have these rules then the judge can check all procedures. Not only the judge but also all parties".

One of the challenges of the electronic evidence is a regional issue. Do you think that the UAE laws can deal with this issue?

"In practice, as far as I know, this issue did not pose a problem before at the UAE Federal Supreme Court. Also the UAE laws did not deal with this issue, so we are facing a gap. I think this issue must deal with the new law of electronic evidence".

Is there any proposal in the UAE to regulate electronic evidence?

"As far as I know no, but there are claims with regard to this".

Interview (7)

Interviewee: Younis Al Balushi, Chief Prosecutor–Dubai Public Prosecution.

Place and date: Dubai, February 2013.

INTERVIEWER: In your opinion; what practical problems are faced with regard to electronic evidence in the UAE?

INTERVIEWEE: "There are a number of issues and challenges. There are issues relating to how to get the evidence, challenging on the search, seizure, and preservation processes. Most of these procedures are understood by police officers, lawyers, prosecutors, and judges. There is no technician present during a seizure of electronic evidence. There is no law to regulate electronic evidence. There is no effective international cooperation and coordination".

You mentioned a number of procedures and challenges. Do you think the main problem is a lack of regulation concerning the procedures of electronic evidence more than the technical challenges?

"We can say it's the most influential. If there are rules or regulations for electronic evidence that will lead to raised levels regarding professionalism and knowledge. As a result, there will be no technical problems".

In the UAE, the procedures with regards to the gathering of evidence are provided under general rules of the UAE's Criminal Procedures Law (CPL). In what manner can be said that the CPL is appropriate to cover electronic evidence?

"I think there is gap. Criminal Procedures Law cannot cover the electronic evidence processes. We must have procedural law for cybercrime and regulate electronic evidence".

How can we be sure of the reliability and authenticity of electronic evidence?

"Now we look at the extent of the application of the general rules. For example, we look at the search and seizure warrant, had it been applied or not? In brief, we look at the framework of procedures".

Do you think questioning the credibility of a forensic laboratory report could lead to unsuccessfully prosecuting cyber-crimes?

"So far we have not faced any appeals".

Can I say the level of understanding and awareness could be the reason?

"It could be also qualitative of cybercrimes. In the UAE there is no organised crime. Although I think crime has increased in recent years. There are many cases of electronic fraud and hacking. Also the commit crime methods have evolution".

One of the challenges of the electronic evidence is a regional issue. Do you think that the UAE laws can deal with this issue?

"This issue can be dealt with by effective international cooperation and coordination, and rogatory documents which I think it is not effective. The rogatory needs an extremely long time to get help".

Are there any practical examples?

"There are many applications and we are still waiting for a reply".

In your opinion, what do we need in order to effectively combat criminals and fully use the electronic evidence?

"For effective prosecution we need to raise understanding and awareness levels, we need effective international cooperation and coordination, and we need strategies to combat crimes. In contrast, for electronic evidence we need laws to regulate it".

Interview (8)

Interviewee: Anonymous, lawyer.

Place and date: Sharjah, February 2013.

INTERVIEWER: In your opinion; what practical problems are faced with regard to electronic evidence in the UAE?

INTERVIEWEE: "The main challenge is the understanding of the electronic evidence. I think the level of understanding concerning electronic evidence and how it is collected and analysed is low, as well as, the lack of specialists and lack of academic research in

this field".

What do you think are the main problems? Is it a lack of regulation procedures of electronic evidence or the limitations of the laboratories and specialists?

"Both, there is no rule to regulate electronic evidence, as well as, the limitations of the specialists".

In the UAE, the procedures with regards to the gathering of evidence are provided under general rules of the UAE's Criminal Procedures Law (CPL).In what manner can be said that the CPL is appropriate to cover electronic evidence?

"We now apply the general rules of evidence, which I think we can use as a framework. However, the nature of electronic evidence requires us to look beyond these rules. Undoubtedly, electronic evidence needs more attention concerning search, seizure or examination. The general rules cannot cover this process".

Emirates judges appreciate the pertinence of the evidence. In relation to electronic evidence, how can the judge be sure of the reliability and authenticity?

"There is no standard for that. As you know that the judicial system of the UAE allows the judge to take evidence or reject it".

How do you view the understanding and awareness level of lawyers with regard to electronic evidence?

"Frankly, low".

One of the challenges of the electronic evidence is a regional issue. Do you think that the UAE laws can deal with this issue?

"There is no problem as long as the evidence is taken from the official body and meets conditions. The problem with cooperation bodies is in obtaining evidence and the time it takes to get the evidence".

What can the solution be?

"I think the best solution is the existence of mandatory agreements".

In your opinion, what do we need in order to effectively and fully use the electronic evidence?

"We have to look at both sides; law and humanity. We should have laws to regulate electronic evidence or at least guidelines and we must rehabilitate and train people".

Interview (9)

Interviewee: Judge Dr. Mohammed Al kamali, General Director of the institute of training and Judicial Studies in Abu Dhabi, UAE.

Place and date: Abu Dhabi, July 2013.

INTERVIEWER: In your opinion, what practical problems are faced with regard to electronic evidence in the UAE?

INTERVIEWEE: "I believe that the UAE is currently experiencing legal problems resulting from the lack of special procedural rules governing electronic evidence rather than from technical problems. Emirates have the financial ability to establish and develop laboratories. A current obstacle you may encounter is the inability of the Emirates' existing laws and regulations to deal with the special nature of electronic evidence. You must also not overlook the technical side. The UAE currently has only two laboratories, one in Abu Dhabi and other in Dubai, and the rest of the UAE has no laboratories. As well as having few specialized cadres in the UAE now, these specialists need development and training. The CPL is not commensurate with cybercrime and crime scene evolution, which is no longer in the past. A crime scene in cybercrime is a default theatre. There are many risks of loss of evidence, and in addition the electronic evidence may exist in more than one place. Electronic evidence needs expertise in how to acquire and preservative it. Current Procedural law has loopholes and does not cover the process of electronic evidence".

So you believe that current law has gaps and cannot cover the process of electronic evidence. In your opinion, what is the best solution?

"There are two groups. The first group believes that we only need to improve the current laws. The second group believes that we need to create a special procedural law for electronic evidence. I think it would be most suitable for the UAE to create a special procedural law".

But there are people who do not accept this opinion and who believe that creating a special procedural law may conflict with the UAE legislative policies.

"I disagree with this opinion. There are many examples of special laws that include procedural rules, such as UAE Federal Law No (28) of 2005 concerning Personal Status, which include a number of procedural rules. Yes, the Code of Civil Procedure organizes all procedural matters. However, the Personal Status law regulates some recent procedures, which were not mentioned in the civil code. These new rules of the Federal Law No (28) cover the gaps in the Civil Code rules. Cybercrimes both in the UAE and globally have increased significantly at the present time. In addition, the perpetrators of such crimes are experienced and clever. These criminals can commit crimes without leaving any trace and it may be difficult to prove such crimes using traditional laws. The current CPL has many defects, and the UAE need to reconsider the law. Emirates have released many of the penal laws: there are special penal laws, as for example the Information Technology Act. However, they have not updated the CPL, especially the evidence rules".

There are some who believe that the current CPL is capable of handling electronic evidence, so that there is no need for a special law or rules.

"With all due respect, I do not support this view at all. If we do not need special laws governing some of the issues which are not covered by the general laws, then the penal code law is enough for the criminalization of all crimes and we do not need for a special law regulating cybercrimes".

But some people believe that with the development of technology, issuance of special procedures of law or rules for electronic evidence will become out-dated after a short period. Thus we will need to amend the rules continuously, and amending laws in the UAE takes a long time.

"There is simple solution to this problem. Firstly, amending laws does not need to take a long time in the UAE: many laws have been amended or issued in a short time. There have been laws issued in a month. The solution can be found in new laws such as the Corporate Governance Code, which includes rules allowing the Council of Ministers to amend the law when the need arises. And this becomes the decision of the Council of Ministers as a law. This can also be applied to electronic evidence rules. The existence

of such rules in the law gives us flexibility and speed in the amendment of the law".

Some countries have resorted to finding guidance without seeking to change law rules. In your opinion, is it better to find such guidance as a first stage before changing the rules?

"I belief finding rules is better than finding guidance. Some countries, such as the UK and the US, have taken this guidance as a definite common law system. The legal system of these countries allows for the existence of such guidance. Judicial judgments in the common law system are considered as laws, while we in the UAE follow your civil system. Therefore we need legal rules, and we can stipulate the guidance in the law as rules".

As you pointed out, the UAE is a civil legal system, thus the verdicts are issued upon the conviction of the judge. In your opinion, do you think that finding such rules will contribute to convincing the judge?

"I agree with you that if there is a clear rule on search and seizure, and on examining electronic evidence, the judge will convene and therefore will sentence on conviction".

How do you explain the existence of a special penal law (Cybercrime Act) without any procedural rules?

"I do not know the reason for that. It may be that the committee that prepared the law believed it necessary to keep working on CPL, or that this question was not up for discussion".

Does nothing prevent finding rules or laws covering electronic evidence?

"There is no reason. It is important and necessary to find these rules in the UAE, just as it is necessary find a specialized judge and prosecutor. The lack of laws and specialized judges is the problem. Significant numbers of existing judges are unfamiliar with the technological aspects. How can a judge who does not have a basic knowledge of computer cybercrime cases or understand the electronic evidence? In the absence of any rules, the judge compares other similar things and this may create problems. For example, UAE law does not allow unsealed letters without the consent of the General Attorney, and that also applies to email. There are also many procedural problems. My question is whether a search warrant with its own terms can be set forth in the CPL as

appropriate for searching electronic evidence. Searching for traditional evidence differs from searching for electronic evidence. There are many issues that must be regulated. The world evolves, so we must develop our laws. Judicial interpretation differs from one judge to another. This difference could lead to significant problems, and may lead to the loss of the opportunity to prove crimes. Personal Status Law before its release was conditional jurisprudence, and has varied judgments despite the similarity of the facts. But after the issuance of the rules there is no jurisprudence".

As General Director of the institute of training, what is your opinion regarding the level of awareness and understanding of cybercrimes and electronic evidence in the UAE?

"I think the level is low. Judges, especially in the higher courts, are elderly. There have been only one or two courses or seminars held in the UAE. The saying that 'the judge is the highest expert' may not be true, especially in cases of cybercrime and electronic evidence. Judges currently build judgments on the experts' reports, without being able to discuss the reports. We need specialized courses; we need to raise the level of knowledge".

One of the challenges of electronic evidence is a regional issue. Do you think that the UAE laws can deal with this issue?

"Let's talk first about the problems of jurisdiction within the State. There are problems of jurisdiction between the Emirates. For example, if the case was in Abu Dhabi and the electronic evidence in Fujairah, the police officer could directly get a search warrant issued by prosecutor in Abu Dhabi based on the evidence only or might need another from Fujairah. There are procedural problems of evidence that must be resolved. At the international level, I think international cooperation takes a long time and the evidence may get lost. I think this is another important point supporting the fact that we need to find procedural laws for electronic evidence".

Interview (10)

Interviewee: Dr. Ali Hamouda, Head of the Dubai Police Academy.

Place and date: Dubai, September 2013.

INTERVIEWER: In the UAE, the procedures with regards to the gathering of evidence are provided under general rules of the UAE's CPL. In what manner can it be said that the CPL is appropriate to cover electronic evidence?

INTERVIEWEE: "I think it is appropriate. We only need to rethink the Penal Code and Cybercrimes Law, not all procedure law. Cybercrime is advanced crime. We must improve the penal law so that the procedural law is able to cover and deal with all evidence and prove the crimes. If we improve our laws we can prosecute crimes easily, we can prosecute crime by penal law not by procedural law".

So you think that the UAE does not need to find procedural law to regulate electronic evidence. Is there any reason for that?

"We will need to develop and train personnel, and to develop the judiciary, police and prosecutors. In addition, amending laws in the UAE takes a long time. There are many stages law must pass in order to change. There are specialized courts and prosecutors for cybercrimes in the UAE. Accordingly, there is no reason to find a special procedural law. Finding a procedural law for electronic evidence will restrict the authority of the judge. Judges in the UAE legal system have freedom in sentencing. The law will prevent the judge from using this feature, because the judge will apply the legal rules and will not be able to reject the evidence or not apply them".

In practice, we find that the judges build decisions on the laboratory reports without the ability to discuss the report, so the judge's rule is not based on his conviction.

"This may be true, but judge has the right to accept or reject the expert report".

Some people believe that the CPL has some procedural problems, especially when dealing with electronic evidence, such as the use of search warrants, and that we need to find new rules.

"The UAE has modern laws, and the CPL is also a modern law and always being reviewed. In 2005 the CPL was reviewed and there were many rules changed, but there was no change in evidence rules, so this rule is adequate and there is no need for change. Finding special rules requires special people to apply them, which is currently not available in UAE".

One of the challenges of electronic evidence is a regional issue. Do you think that the UAE laws can deal with this issue?

"I do not think there is problem. If the evidence was obtained legally and the procedures were documented the judge, can take evidence without any problems".

In your opinion, why has electronic evidence not been adopted as a model for academic study until now?

"When teaching proof in general as an academic model, you cannot focus on a specific type of evidence, and leave the rest. Also, electronic evidence is used simply in practical life".

Interview (11)

Interviewee: Dr. Hadef Al Dhahiri, Minister of the UAE Justice.

Place and date: Abu Dhabi, September 2013.

INTERVIEWER: There are two groups: one believes that the CPL is appropriate and sufficient to deal with electronic evidence and the other believes it is inefficient due to the special nature of electronic evidence and that we need to find special rules for electronic evidence. Which group do you support?

INTERVIEWEE: "Realistically, for this academic controversy, if we need to find a new law we will seek to publish it. The opposing views can be discussed when discussing the issues of the law, but that is not a reason not to publish it. Personally, I tend to support special rules for electronic evidence. The CPL is indispensable. However, if there are some legal loopholes, it is better to cover them by special laws, especially for some special aspects. The CPL may be able to regulate general aspects, but not special aspects such as electronic evidence or cybercrimes. So it is highly recommended to find special procedural laws".

In practice, have there been any claims to find rules for electronic evidence or special procedural laws?

"So far, there have been no claims. There is a demand on behalf of Dubai Prosecution just about the adoption of electronic signatures".

Is there anything to prevent the finding of such rules? Are they inconsistent with the legal system of Emirates?

"Legally there is nothing to prevent finding such rules. But as I mentioned there have been no claims. In the past, some people have objected to the suggestion of special laws for cybercrimes, and believed that the Penal Code is enough to cover all crimes. But when there is a claim there will be a need to find a law concerning it. It is only due to absence of a claim. There is no reason for the UAE Ministry to look at any claim. In the UAE there are legislative sessions to review the laws every three years. If there is no request to find rules for electronic evidence before the date of the session, the Ministry will ask to discuss the finding of procedural law for cybercrimes, or rules for electronic evidence. Then the ministry can utilize the results of your research when discussing the question".

In your opinion, why have there been no claims to find rules for electronic evidence even though there are people who believe in the importance of finding these rules?

"I think the main reason is the lack of the number of cases at present. I think you encountered the same thing when you were searching for cases".

Some people believe that the slow pace of issuing and amending laws in the UAE is the main reason.

"I do not think this argument is correct. Laws in the UAE are reviewed on a continuous basis. The cybercrimes Law was passed in 2006 and amended in 2012. There are laws which are reviewed on an annual basis, such as the Drugs Act. If new types appear, we amend the law and add this type. The Cybercrimes Law is also a sophisticated law, thus we review it on an on-going basis, in the same way as when we have a special procedural law. The statistics show that cybercrime has increased in the UAE recently. The small number of cases does not mean that there is no cybercrime in the UAE. It could be caused by a failure to detect crimes or to not getting evidence".

There was a project on establishment of specialized courts for cybercrimes in the UAE. Why was this not applied?

"We have created criminal circuits as a first stage, until there arises a need to establish

special courts".

In your opinion, do you think that the courses and seminars on cybercrimes and electronic evidence which are currently held in the UAE are enough to raise the knowledge level?

"I do not think they are enough. We need to have more, just as we also need scientific research such as your research. Academic research is currently limited to studying the penal code or crimes, and there is no academic research on procedure law. I think that your research will be of importance for the UAE, especially as there are no academic writings on procedural problems in the UAE. Your research on electronic evidence and result findings will be of interest and will be discussed by the Ministry".

Interview (12)

Interviewee: Anonymous, Police officer.

Place and date: Abu Dhabi, September 2013.

INTERVIEWER: In your opinion, is CPL appropriate to cover the process of electronic evidence or not?

INTERVIEWEE: "Yes, I think it is sufficient to cover all process of electronic evidence".

However, there are some who believe that there are some practical problems when applying CPL.

"I do not think so. On the contrary, if we have special rules for electronic evidence, that could lead to practical problems".

Could you explain please?

"In practice, the application of specific rules is trickier than the application of general rules. If we have specific rules for electronic evidence, that means we must follow up all these rules and this is very difficult. The police officer must follow all the rules, and if he violates this order, the evidence will not have any value. The police officer must take action fast in order to seize evidence, and fast action could lead to not following some rules, and therefore make the proceedings null and void. General rules give police

more freedom in search and seizure".

Do you think that the conditions and rules of search warrants in the CPL are sufficient to cover electronic evidence?

"I think so, yes".

But a search warrant must be specified as to time, place and people, and electronic evidence could be found in one or more places and maybe networks, in the suspect's house or somewhere else.

"Yes, this could happen but it will not happen very often".

So there are loopholes in the CPL and we should find solutions.

"I do not believe these problems are sufficient to issue a special law or rules for electronic evidence. Retaining the current law is best, and we can overcome the practical problems".

How?

"The practical experience of the police officer will help in finding solutions to the practical problems".

Do you think the police officers have enough experience to overcome the practical problems resulting from electronic evidence?

"Yes, a large percentage of them have enough experience".

Which method you, as a police officer, use to seize electronic evidence when the evidence is outside the State?

"We try to get it by remote searches first, and if that is impossible, we request international assistance".

But remote searching is not allowed in the UAE legal system?

"Yes, when get the evidence then we confront the accused, if it is admitted then the evidence is the recognition".

In case of denial?

“We discuss the matter and either memorize the issue or send them to the court”.

Is not better to find a legal way to regulate all these matters?

“At the moment I do not think we need it”.

Bibliography

Books

Allen R. and Kuhns R., *Eleanor Swift and, Evidence: Text, Cases and Problems* (5th end, Aspen Publishers 2011).

Anderson J., Williams N. and Clegg L., *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2nd edn, Sydney: LexisNexis 2009).

Anderson R., *Security Engineering* (2nd edn, Wiley Publishing Inc. 2008).

Anson S. and Bunting S., *Mastering windows network forensics and investigation* (Indianapolis: Wiley Publishing Inc. 2007).

Anthony R., *Cyber Crime Investigations* (Rockland MA: Syngress Pub 2007).

Arcaro G., *Basic Police Powers: Arrest and Search Procedures* (4th edn, Emond Montgomery Publications 2009).

Arkfeld M., *Arkfeld on Electronic Discovery and Evidence* (3rd edn, London: Lexis 2011).

Arnold C., *The Companion to British History* (3rd edn, Loncross Denholm Press 2008).

Bainbridge D., *Introduction to Computer Law* (6th edn, Ashford Colour Press Ltd. 2008).

Bantekas I. and Nash S., *International Criminal Law* (2nd edn, Cavendish Publishing 2003).

Bergman P. and Berman S., *The criminal law handbook: Know your rights, survive the system* (12th edn, Nolo 2011).

Bologan J., *Fraud auditing and Forensic Accounting: New tools and techniques* (John Wiley and Sons 1987).

Brace I., *Questionnaire Design: How to Plan, Structure and Write Survey Material for Effective Market* (2nd edn, London; Philadelphia: Kogan Page 2008).

Brenner S., *Criminal Threats from Cyberspace* (Pentagon Press 2012).

Brown C., *Computer evidence: Collection and preservation* (2nd edn, Rockland MA: Charles River Media 2009).

Bryant R., *Investigating digital crime* (John Wiley and Sons Ltd. 2008).

Byrne J. and Rebovic D., *The New Technology of Crime, Law and Social Control* (Criminal Justice Press 2007).

Casey E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn, Waltham Mass: Academic Press/Elsevier 2011).

……*Handbook of Computer Crime Investigation (Academic Press 2010).*

Chase O. and Hershkoff H., *Civil Litigation in Comparative Context* (Thomson West 2007).

Chissick M. and Kelman A., Electronic Commerce: Law and Practice (3rd edn, Sweet and Maxwell Ltd 2002).

Clancy T., *Cyber Crime and Digital Evidence Materials and Cases* (LexisNexis 2011).

Clifford R., *Cybercrime: the Investigation, Prosecution and Defense of a Computer-Related Crime* (3rd edn, Carolina Academic Press 2011).

Cohen A. and Lender D., *Electronic Discovery: Law and Practice* (2nd edn, London: Aspen Publishers 2011).

Cohen F., *Digital forensic evidence examination* (4th edn, Fred Cohen and Associates 2012).

Cross R. and Tapper C., *Cross and Tapper on Evidence* (12th edn, Oxford 2012).

Crotty M., *The foundations of social research: meaning and perspective in the research process* (Thousand Oaks Calif.; London: SAGE 1998).

Cruz P., *Comparative law in a changing world* (3rd edn, New York NY: Routledge-Cavendish c2007).

Damaška M., *Evidence law adrift* (New Haven; London: Yale University Press 1997).

…… *The faces of justice and state authority: a comparative approach to the*

legal process (New Haven; London: Yale University Press c1986).

Daniel L. and Daniel L., *Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom* (Syngress 2011).

Daymon C. and Holloway I., *Qualitative Research Methods in Public Relations and Marketing Communications* (London: Routledge 2002).

Denscombe M., *The Good Research Guide* (Buckingham: Open University Press 1998).

Dobinson I. and Johans F., *'Qualitative Legal Research' Research Methods for Law* by McConville M. and Chui W., (eds) (Edinburgh University Press 2007).

Dreyer J., *China's Political System: Modernization and Tradition* (8th edn, Pearson 2011).

Feldman J., *Essentials of Electronic Discovery: Finding and Using Cyber Evidence* (New York: Glasser Legal works 2003).

Fink A., *How to Sample in Surveys* (2nd edn, Thousand Oaks [Calif]; London: SAGE 2002).

Finn P., *The common law in the world: the Australian experience* (Centro di studi e ricerche di dirittocomparato e straniero 2001).

Franklin C. and Diliberto K., Investigating Computer Crime (CRC Press; 1996).

Franklin C., *The Investigator's Guide to Computer Crime* (Charles C Thomas Publisher 2006).

Gahtan A., *Electronic evidence* (Carswell Thomson Publishing 1999).

Gardner R., *Practical Crime Scene Processing and Investigation* (2nd edn, CRC Press 2012).

Gilbert N., *Research Social Life* (2nd edn, Sage Publication 2001).

Gillham B., *Case Study Research Methods* (London: Continuum 2000).

……. *Developing a Questionnaire* (London: Continuum 2000).

……*The Research Interview* (London: Continuum Press 2000).

Gilmore W., *Mutual Assistance in Criminal and Business Regulatory Matters* (Cambridge University Press 1995).

Gissel R., *Digital Underworld: Computer Crime and Resulting Issues* (Lulu.Com 2005).

Grabosky P., Smith R. and Dempsey G., *Electronic theft: unlawful acquisition in cyberspace* (Cambridge: Cambridge University Press 2001).

Harvey D., *Internet.law.nz: selected issues* (3rd edn, LexisNexis Wellington 2011).

Hrycko O., *Electronic discovery in Canada: Best practices and guidelines* (2nd edn, CCH Canadian Limited 2007).

Jacobson J., *Antitrust Law Developments* (6th edn, American Bar Association 2007).

Jane Fu, *Corporate Disclosure and Corporate Governance in China* (Kluwer Law International 2010).

Joubert C., (eds), *Applied law for police officials* (3rd edn, Juta Legal and Academic Publishers 2009).

Kanellis P., *Digital crime and forensic science in cyberspace* (Idea Group Publishing 2006).

Kent A., Williams J. and Holzman A., *Encyclopedia of Computer Science and Technology* (Marcel Dekker Incorporated 1987).

Kipper G., *Wireless crime and forensic investigation* (Taylor and Francis Group LLC. 2007).

Klamberg M., *Evidence in International Criminal Trials: Confronting Legal Gaps and the Reconstruction of Disputed Events* (Martinus Nijhoff Publishers 2013).

Kvale S. and Brinkmann S., *Interviews: Learning the craft of Qualitative Research Interviewing* (2nd edn, Los Angeles; London: SAGE 2009).

Lange M. and Nimsger K., *Electronic evidence and discovery: What every lawyer should know* (2nd edn Chicago: ABA Publishing 2009).

Lentini J., *Scientific protocols for fire investigation* (Taylor and Francis Group LLC. 2006).

Lloyd I., *Information Technology Law* (6th edn, OUP Oxford 2011).

Malek H., Auburn J. and Bagshaw R., *Phipson on Evidence* (17th edn, Sweet and Maxwell 2010).

Marcella A. and Menendez D., *Cyber Forensics: a field manual for collecting, examining, and preserving evidence of computer crimes* (2nd edn, Auerbach Publications 2008).

Mason S., *Electronic Evidence* (3rd edn, LexisNexis Butterworths 2012).

…… *International Electronic Evidence* (British Institute of International and Comparative Law 2008).

McLean J., 'Homicide and Child Pornography' in Eoghan Casey (eds), *Handbook of Computer Crime Investigation* (Academic Press 2010).

Millard C., *Legal protection of computer programs and data* (Sweet and Maxwell 1985).

Mohay G., Anderson A., Collie B., Vel D. and Mckmish R., *Computer and Intrusion Forensics* (Artech House Inc. 2003).

Moore R., *Search and Seizure of Digital Evidence: An Examination of Constitutional and Procedural Issues* (University of Southern Mississippi 2003).

Mueller C. and Kirkpatrick L., *Evidence* (4th edn, Wolters Kluwer Law and Business 2009).

Mueller S., *Upgrading and Repairing PC* (20th edn, Que Publishing 2011).

Murphy P. and Glover R., *Murphy on evidence* (12th edn, Oxford University Press 2011).

Nelson S., Olson B. and Simek J., *The Electronic Evidence and Discovery Handbook: Forms, Checklists And Guidelines* (New York: American Bar Association 2006).

Oppenheim A., *Questionnaire Design and Attitude Measurement* (London: Continuum 2001).

Paperback B., *Hacking exposed Linux* (3rd edn, McGraw-Hill Osborne Media 2008).

Paul G., *Foundations of Digital Evidence* (Chicago: American Bar Association 2008).

Pfleeger C. and Pfeeger S., *Security in Computing* (4rd edn, Pearson Education Inc. 2006).

Punch K., *Introduction to Social Research: Quantitative and Qualitative Approaches* (London: Sage Publication 2004).

Reimann M. and Zimmerman R., (eds.) *The Oxford Handbook of Comparative Law* (Oxford University Press, 2008) .

Reyes A. and Wiles J., *The Best Damn Cybercrime and Digital Forensics Book Period* (Syngress 2007).

Reyes A., O'Shea K., Brittson R. and Steele J., *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors* (Syngress 2007).

Rivest R., *The MD5 Message Digest Algorithm* (MIT Laboratory for Computer Science 1992).

Robson C., *Real World Research: A Resource for Social Scientists and Practitioner Research* (3rd edn, Chichester: Wiley 2011).

Rooyen H., *The A-Z of investigation: A practical guide for private and corporate investigators* (Crime Solve 2004).

Saferstein R., *Criminalistics: An introduction to forensic science* (10th edn, Prentice Hall 2010).

Scheting E., Green K. and Carlson J., *Internet site security (*Addison- Wesley 2002).

Shinder D. and Cross M., *Scene of the cybercrime* (2nd edn, Arlington: Syngress Publishing Inc. 2008).

Siegel J., *Forensic Science: The Basics* (Taylor and Francis Group 2007).

Slapper G. and Kelly D., *The English Legal System* (9th edn, London: Routledge-Cavendish 2009).

Smith R., Grabosky P. and Urbas G., *Cyber criminals on trial* (Cambridge University Press 2004).

Stephenson P. and Gilbert K., *Investigating Computer-Related Crime* (2nd edn, CRC Press 2013).

Tapper C., *Computer Law* (4th edn, Longman 1989).

Tashakkori A. and Teddlie C., *SAGE Handbook of Mixed Methods in Social and Behavioral Research* (2nd edn, Thousand Oaks, Calif.; London: SAGE 2010).

Toren P., *Intellectual Property and Computer Crimes* (Law Journal Press 2003).

Vacca J., *Computer Forensic: Computer Crime Scene Investigation* (2nd edn, Charles River Media Inc. 2005).

Volonino L. and Robinson S., *Principles and Practice of Information Security* (Prentice Hall 2004).

Wacks R., *Personal Information, Privacy and the Law* (Oxford: Clarendon Press 1989).

Walden I., *Computer Crimes and Digital Investigation* (Oxford University Press 2007).

Wall D., *Crime and the Internet* (Taylor and Francis Group 2001).

Westby J., *International Guide to Combating Cybercrime* (American Bar Association 2003).

Yin R., *Case Study Research: Design and Methods: Third publication: Applied Social Research Methods Series* (4th edn, SAGE Publications 2008).

Zhong J. and Yu G., *Establishing the Truth on Facts: Has the Chinese Civil Process Achieved This Goal*? (Florida State University College of Law 2004).

Zweigert K. and Kötz H., *An Introduction to Comparative Law* (3rd edn, Oxford University Press, 1998).

Articles and Papers

Allen R. and Pardo M., 'Juridical Proof and the Best Explanation' (2008) 27 *Law and Philosophy*.

…….. 'The Problematic Value of Mathematical Models of Evidence' (2007) 36 *Journal of Legal Studies*.

Allen R., 'Rationality and the Taming of Complexity' (2011) 62 *Alabama Law Review*.

Allinson C., 'Audit Trails in evidence: Analysis of Queensland case study' (2003) 2 *The Journal of Information, Law and Technology*.

Austen J., 'Some stepping stones in computer forensics' (2003) 8, 2 *Information Security Technical Report* 37-41.

Ball C., 'Cross-examination of the computer forensic expert' (2004) <http://www.craigball.com/expertcross.pdf>.

Bilz K., 'We Don't Want to Hear It: Psychology, Literature and The Narrative Model of Judging' (2010) *University of Illinois Law Review*.

Boddington R., Hobbs V. and Mann G., 'Validating digital evidence for legal argument' (2008) *Edith Cowan University Australia* p3 <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1041&context=adf >.

Brenner S. and Frederiksen B., 'Computer Searches and Seizures: Some Unresolved Issues' (2002) 8, 39 *Michigan Telecommunication and Technology Law Review*.

Brenner S. and Schwerha J., 'Cybercrime Havens: Challenges and Solutions' (2007) 17, 2 *The American Bar Association -Business Law Today.*

Brenner S., 'Is There Such a Thing as "Virtual Crime"?' (2001) 4, 1 *California Criminal Law Review* 1.

Brill A., Pollitt M. and Whitcomb C., 'The Evolution of Computer Forensic Best Practices: An update on Programs and Publications' (2006) 1, 1 *Journal of Digital Forensic Practice* 2-11.

Burns D., 'When used in the criminal legal process forensic science shows a bias in

favour of the prosecution' (2001) 41.4 *Science and Justice* 271.

Buskirk E. and Liu V., 'Digital evidence: Challenging the presumption of reliability' (2006) 1, 1 *Journal of Digital Forensic Practice* 19-26.

Carrier B. and Spafford E., 'Getting Physical with the Digital Investigation Process' (2003) 2, 2 *International Journal of Digital Evidence*.

Carrier B., 'Defining digital forensic examination and analysis tool using abstraction layers' (2003) 1, 4 *International Journal of Digital Evidence* 3-5.

……'Open Source Digital Forensics Tools' September (2003) p2 <http://www.digital-evidence.org/papers/opensrc_legal.pdf>.

Casey E., 'Error, Uncertainty and Loss in Digital Evidence' (2002) 1, 2 *International Journal of Digital Evidence*.

Cheng E. and Yoon A., 'Does Frye or Daubert Matter? A Study of Scientific Admissibility Standards' (2005) 91 *Virginia Law Review* 471.

Cheng E., 'A Practical Solution to the Reference Class Problem' (2009) 109 *Columbia Law Review*.

Chukwuemerie A., 'Affidavit Evidence and Electronically Generated Materials in Nigerian Courts' (2006) 3, 3 *Social Science Research Network* 185.

Clermont K., 'Standards of Proof in Japan and the United States' (2004) 37*Cornell International Law Journal* 273.

Cockfield A., 'Towards a Law and Technology Theory' (2004) 30, 1 *Manitoba Law Journal* 383-399.

Corne P., 'Creation and Application of Law in the PRC' (2002) 50 *American Journal of Comparative Law* 369- 396.

Cox H., 'Recent Developments and Trends in Searching and Seizing Electronic Evidence' (2011) 59, 6 *United States Attorneys' Bulletin* 72-73 <http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf>.

Dearne K., 'Cyber sleuths on e-crime trail' (22nd May 2001) *Australian IT*

<http://www.australianit.news.com.au/articles/0,7204,2024114%5E15306%5E%5Enbv%5E,00.html>.

Deborah D. and William F., 'Rethinking the Probative Value of Evidence: Base Rates, Intuitive Profiling, and the "Postdiction" of Behavior' (2002) 26 *Law and Human Behavior*.

Duerr T., Beser N. and Staisiunas G., 'Information Assurance Applied to authentication of Digital Evidence' (2004) 6, 4 *Forensic Science Communications*1.

Epstein L. and King, G., 'Rules of Inference, The Exchange Empirical Research and the Goals of Legal Scholarship' (2002) 69, 1 *The University of Chicago Law Review* 122.

Finkelstein M. and Levin B., 'On the Probative Value of Evidence from a Screening Search' (2003) 43 *Jurimetrics Journal*.

Fischer S. and Wilke D., 'Electronically signed documents: legal requirements and measures for their long-term conservation' *Digital Evidence and Electronic Signature Law Review* 3 (2006) 40 – 44.

Freiberg A., 'Non-Adversarial Approaches to Criminal Justice' (2007) 16, 4 *Journal of Judicial Administration* 205.

Galves F. and Galves C., 'Ensuring the Admissibility of electronic evidence forensic evidence and enhancing its probative value at trial' (2004) 1, 19 *Criminal Justice Magazine*<http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html>.

Giordano S., 'Electronic Evidence and the Law' (2006) 6, 2 *Information Systems Frontiers* 161.

Goodman M. and Brenner S., 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 3 *Journal of Law and Technology* <http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php>.

Gordley J., 'Comparative Legal Research: It's Function in the Development of Harmonized Law' (1995) 43, 4 *The American Journal of Comparative Law* 555.

Haack S., 'The Embedded Epistemologist: Dispatches from the Legal Front' (2012) 25,

2 *Ratio Juris*.

Hans V., 'Introduction: Citizens as Legal Decision Makers: An International Perspective' (2007) 40, *Cornell International Law Journal* 303-304.

Henry P., 'Best Practices in Digital Evidence Collection' (2009) <http://computer-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/>.

Hosmer C., 'Proving the integrity of digital evidence with time' Spring (2002) 1, 1 *International Journal of Digital Evidence* <http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf>.

Howell B., 'Real world problems of virtual crime' (2005) 7, 1 *Yale Journal of Law and Technology* <http://digitalcommons.law.yale.edu/yjolt/vol7/iss1/5/>.

Insa F., 'The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—results of a European Study' (2007)1, 4 *Journal of Digital Forensic Practice*.

Irons A., Stephens P. and Ferguson R., 'Digital Investigation as a distinct discipline: A pedagogic perspective' (2009) 6.1and 6.2 *Digital Investigation* 82-90.

Jansen W. and Ayers R., 'An overview and analysis of PDA forensic tools' (2005) 2.2 *Digital Investigation* 120-132.

Johnson B., 'Toward a definition of Mixed Methods Research' (2007) *Journal of Mixed Methods Research* 112.

Johnson D., 'Crime and Punishment in Contemporary Japan' (2007) 36, 371 *LexisNexis* 385.

Jones N., George E., Insa F., Rasmussen U. and Völzow V., 'Electronic evidence guide, A basic guide for police officers, prosecutors and judges'(2013) 1.0 *Council of Europe*.

Kenneally E. and Brown C., 'Risk sensitive digital evidence collection' (2005) 2, 2 *The International Journal of Digital Forensics and Incident* 101-119.

Kernutt K., 'Civil Law V Common Law Systems: Are They So Different?' (1999) *Oregon Review of International Law* 31.

Kerr O., 'Digital Evidence and the New Criminal Procedure' (2005) 105, *Columbia Law Review* 279.

…….. 'Search Warrants in an Era of Digital Evidence' (2005) 75 *Mississippi Law Journal* 85.

King M., 'Security, Scale, Form, and Function: The Search for Truth and the Exclusion of Evidence in Adversarial and Inquisitorial Justice Systems' (2001) 12 *International Legal Perspectives* 185-192.

Koch C., 'Envisioning A Global Legal Culture' (2003) *Social Science Research Network.*

Koehler J., 'When Do Courts Think Base Rate Statistics Are Relevant?' (2002) 42 *Jurimetrics Journal*.

Krings A., 'A Formalisation of Digital Forensics' (2004) 3, 2 *International Journal of Digital Evidence*.

Krotoski M., 'Effectively Using Electronic Evidence Before and at Trial' (2011) 59, 6 *United States Attorneys' Bulletin* <http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf>.

Kuhn A., 'Societe Nationale Industrielle Aerospatiale: The Supreme Court's Misguided Approach to The Hague Evidence Convention' (1989) 69 *Boston University Law Review LexisNexis*1011-1014.

Kwiatkowski J., 'Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images' (2002) 10 *Journal of Law and Policy* 267.

Langbein J., 'Historical foundations of the Law of evidence: A view from the Ryder sources' (1996) 96, 5 *Columbia Law Review* 1168-1194.

Llewellyn K., 'Behind the Law of Divorce' 32 *Columbia Law Review* 1284.

Makkai T., 'Media Release on 'Effective investigation of high tech crime' (2004) *Australian Institute of Criminology* <http://www.aic.gov.au/media/2004/december/20041202.aspx>.

Mason S, 'Electronic evidence: A proposal to reform the presumption of reliability and hearsay' (2014) 30 *Computer Law and Security Review* 80-84.

Mason S. and Bohm N., 'Banking and Fraud' a written submission to the House of Commons Treasury Committee on 17th January 2011 available at <http://www.publications.parliament.uk/pa/cm201011/cmselect/cmtreasy/430/430vw25.htm>.

Mehren A., 'An Academic Tradition for Comparative Law?' (1971) 19 *American Journal of Criminal Law* 624, 628.

Moore R., 'To View or not to View: Examining the Plain View Doctrine and Digital Evidence' (2004) 29, 1 American Journal of Criminal Justice 57.

Nancy R., 'Digital Evidence: How Law Enforcement Can Level The Playing Field With Criminals'(2006) *NIJ Journal-National Institute of Justice*.

Palmer G., 'Forensic Analysis in the Digital World' (2002) 1, 1 *International Journal of Digital Evidence.*

Pan L. and Batten L., 'Robust performance testing for digital forensic tools' (2009) 6.1and 6.2 *Digital Investigation* 71-81.

Pardo M., 'The Field of Evidence and the Field of Knowledge' (2005) 24 *Law and Philosophy*.

Paul G. and, Baron J., 'Information inflation: Can the legal system adapt?'(2007) 13, 3 *Richmond Journal of Law and Technology* 1-41.

Peerenboom R., 'The X-Files: Past and Present Portrayals of China's Alien Legal System' (2003) *Global Studies Law Review* 47.

Pizzi W. and Marafioti L., 'The New Italian Code of Criminal Procedure: The Difficulties of Building An Adversarial Trial System on A Civil Law Foundation' (1992) 17, 1 *The Yale Journal of International Law (YJIL).*

Pladna B., 'Computer Forensics Procedures, Tools, and Digital Evidence Bags: What They Are and Who Should Use Them' *East Carolina University* <http://www.infosecwriters.com/text_resources/pdf/BPladna_Computer_Forensic_Proc

edures.pdf>.

Platsas A., 'The Functional and the Dysfunctional in the Comparative Method of Law: Some Critical Remarks' (2008) 12.3 *Electronic Journal of Comparative Law*.

Quigley J., 'Socialist Law and the Civil Law Tradition' (1989) 37 *American Journal of Comparative Law* 781-792.

Rathinasabapathy G. and Rajendran L., 'Cyber-crimes and information frauds: Challenges for LIS professionals' (1991) *National Research Council Computer at Risk*. <http://www.docstoc.com/docs/30582538/Cyber-Crimes-and-Information-Frauds-EMERGING-CHALLENGES-FOR-LIS>.

Risinger M., 'Inquiry, Relevance, Rules of Exclusion, and Evidentiary Reform' (2010) 75 *Brooklyn Law Review*.

Robinson J., 'The Admissibility of Computer Printouts under the Business Records Exception in Texas' (1970) 12 *South Texas Law Journal* 291.

Samaha A., 'Law's Tiebreakers' (2010) 77 *University of Chicago Law Review*.

Schwartz D., 'A Foundation Theory of Evidence' (2011) 100 *University of Wisconsin Legal Studies Research Paper*.

Smith R., 'Impediments to the successful investigation of transnational high-tech crime' (2004) *Australian Institute of Criminology* <http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi285/view%20paper.html>.

Sommer P., '*Computer Forensic: An introduction*' *vial virtual city* <http://www.virtualcity.co.uk/vcaforens.htm>.

……. 'Downloads, logs and captures: Evidence from Cyberspace' (1997) 5, 2 *Journal of Financial Crime* 138-162.

Teppler S., 'Digital data as hearsay' (2009) 6 *Digital Evidence and Electronic Signature Law Review* 9-24.

Volonino L., 'Electronic Evidence and Computer Forensics, Canisius College' (2003) 12, 27 *Communications of the Association for Information Systems* 2

<http://faculty.usfsp.edu/gkearns/Articles_Fraud/Fraud_Deterrence.pdf>.

Whitcomb C., 'An historical perspective of digital evidence: A forensic scientist's view' (2002) 1, 1 *International Journal of Digital Evidence* 2.

Wilson J., 'My Space, Your Space, or Our Space? New Frontiers in Electronic Evidence' (2008) 86, *Oregon LawReview*1205.

Woo M., 'Law and Discretion in the Contemporary Chinese Courts' (1999) 8, 3 *Pacific Rim Law and Policy Journal* 588-589.

Yong P., 'New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime' (December 2011) *Wuhan University China* 5 <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/Cyber_cp_china_Pi_Yong_Dec11.pdf>.

Zhang M., 'International Civil Litigation in China: A Practical Analysis of the Chinese Judicial System' (2002) 25, 59 *Boston College International and Comparative Law* 93.

Thesis

Bakri J., 'A Holistic Approach for Managing ICT Security in non-Commercial Organization' (DPhil Thesis, Stockholm University Sweden 2007).

Ngomane A., 'The Use of Electronic Evidence in Forensic Investigation' (DPhil Thesis, University of South Africa 2010).

Websites

Association of Police Chief Officers (ACPO), 'Good Practice Guide for Digital Evidence'<http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf>.

Australia High Tech Crime Centre (AHTCC), via Australia Federal Police (AFP) <http://www.afp.gov.au/>.

Civil Procedure Law of the People's Republic of China <http://www.china.org.cn/english/government/207343.htm>.

Criminal Procedure Law of the People's Republic of China

<http://www.unhcr.org/refworld/docid/3ddbcd4e7.html>.

First International Treaty to combat crime in cyberspace <http://www.assembly.coe.int/ASP/Press/StopPressView.asp?ID=1157>.

IOCE; 'G8 Proposed principles for the procedures relating digital evidence' (2000) <http://www.ioce.org/fileadmin/user_upload/2002/G8%20Proposed%20principles%20for%20forensic%20evidence.pdf>.

KPMG,<http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/digital-evidence-recovery-0906.pdf>.

Singapore Techno Forensic Branch, Technology Crime Division, Criminal Investigation Department (CID) <http://www.spf.gov.sg/abtspf/cid.htm>.

SWGDE <https://www.swgde.org/>.

The US Federal Law Enforcement Training Centres <http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/downloads/other/bestpractices.pdf/view>.

TWGECSI, 'Electronic Crime scene investigation: A guide for first responders' (2001) <https://www.ncjrs.gov/pdffiles1/nij/187736.pdf>.

UNDOC, <http://www.unodc.org/unodc/en/expert-group-to-conduct-study-cybercrime-jan-2011.html>.

Conference

Al Hajri S., '4th International Conference on Cyber Crimes' (conference, UAE-Dubai 14th December 2011).

Al Mazeina K., Major General Dubai Police, 'New Criminal Phenomena' (conference, Dubai-UAE 22nd February 2012).

Grabosky P., Cybercrime and Information Warfare (conference, Australia 9-10 March 2000) <http://www.aic.gov.au/events/aic%20upcoming%20events/2000/~/media/conferences/transnational/grabosky.ashx>.

Sherman S., 'A digital forensic practitioner's guide to giving evidence in a court of law' (conference, Australia 2006) <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1032&context=adf>.

The Third Annual Conference, 'In the eyes of the communities Emirates' (conference Dubai-UAE 20th May 2013) <http://www.alkhaleej.ae/portal/150131e3-9689-42e8-b700-9424c35ccad3.aspx>.

Additional References

Al Minshawi A., 'Local exchange companies exposed to foreign penetration operations via the "Western Union"' *Emaratalyoum Newspaper* (Dubai 22nd July 2013) <http://www.emaratalyoum.com/business/local/2013-07-22-1.593094>.

…….. 'RAKBANK confirms penetration credit card balances worth 17 million dirham' *Emaratalyoum Newspaper* (Dubai 11th May 2013) <http://www.emaratalyoum.com/local-section/accidents/2013-05-11-1.573717>.

Allard T., 'New Secret Search Powers' (the Sydney Morning Herald 'Sydney' 1st August 2007) <http://www.smh.com.au/articles/2007/07/31/1185647903263.html>.

Australian Transaction Report and Analysis Centre (AUSTRAC) 'Evidence and the Internet' Action Group into the law Enforcement Implication of Electronic Commerce (AGEC) Issues paper (2010).

Bell R., Internet Assisted Suicide - The Story of Sharon Lopatka, Crime Library <http://www.trutv.com/library/crime/notorious_murders/classics/sharon_lopatka/5.html>.

Cameron S., Digital Evidence (FBI Law Enforcement Bulletin August 2011) <https://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/august-2011/digital-evidence>.

Coates S., 'Rader Gets 175 Years for BTK Slayings' The Washington Post (Washington, 19th August 2005) <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/18/AR2005081800201.html>.

Convention on Cybercrime Budapest 23.XI.2001.

Coren M., 'Digital evidence: Today's fingerprint, Electronic world increasingly being used to solve crimes' (Cable News Network CCN 31 January 2005) <http://edition.cnn.com/2005/LAW/01/28/digital.evidence/>.

Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors (2007) *US National Institute of Justice* <http://www.law.du.edu/images/uploads/library/evert/DigitalEvidenceinTheCourtroom.pdf>.

Explanatory Report to the Convention on Cybercrime (ETS 185) 2001 <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

Fodah M., 'Gang stolen credit card data of banks customers' *Emaratalyoum Newspaper* (Dubai 19th September 2013) <http://www.emaratalyoum.com/local-section/accidents/2013-09-19-1.607865>.

Greenhouse L., 'The Nation: Judicial Intent; The Competing Visions of the Role of the Court' (New York Times 7th July 2002) <http://www.nytimes.com/2002/07/07/weekinreview/the-nation-judicial-intent-the-competing-visions-of-the-role-of-the-court.html.

Handbook of Forensic Services revised 2007 US Department of Justice *FIB Laboratory Division* <http://www.fbi.gov/about-us/lab/handbook-of-forensic-services-pdf>.

Hilotin J. and Bagsair L., 'Cyber gangs on the prowl in UAE' Gulf news (Dubai 3rd February 2011) <http://gulfnews.com/news/gulf/uae/crime/cyber-gangs-on-the-prowl-in-uae-1.756268>.

How much information? (2000) *University of California at Berkeley*<http://www2.sims.berkeley.edu/research/projects/how-much-info/>.

Jahnke A., 'Alexey Ivanov and Vasiliy Gorshkov: Russian Hacker Roulette' (1st January 2005) CSO Security and Risk <http://www.csoonline.com/article/219964/alexey-ivanov-and-vasiliy-gorshkov-russian-hacker-roulette?%3E=>.

Lemos R., 'Russia accuses FBI agent of hacking' *The news web site* CNET (16th August 2002) <http://news.cnet.com/Russia-accuses-FBI-agent-of-hacking/2100-

1002_3-950719.html>.

Norton Cybercrimes Report 2012<http://www.norton.com/2012cybercrimereport>.

O'Brien M., Computer Crime: The UN Manual <http://www.unlimitedinvestigations.com/computer_crime.htm>.

Oxford English Dictionary (electronic edition) (3rd edn, 1997 and Additions).

Report to Congressional Requesters, Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats US Government Accountability Office (2007) <http://www.gao.gov/assets/270/262608.pdf>.

Standards Australia Handbook: HB- 171: Guidelines for the Management of IT Evidence.

The cybercrime convention committee, cybercrime and the European Union (2007) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>.

The UK Code of Practice, Academy of Experts <http://www.academyofexperts.org/>.

The US Secret Services' Pocket Guide for First Responders <http://info.publicintelligence.net/usssbestpractices.pdf>.

United Nations, International review of criminal policy – United Nations manual on the prevention and control of computer-related crime (1999) Global Centre for Information and Communication Technologies in Parliament <http://www.ictparliament.org/node/2128>.

Arabic References

Abdull Mohsen M., *Protection of the Private Life and individuals Rights facing computer crimes* (Alsalasel for printing and publishing 1992).

محمد عبدالمحسن، حماية الحياة الخاصة للافراد وضماناتها في مواجهة الحاسب الالي (ذات السلاسل للطباعة والنشر).

Abdullah H., *Inspect Computer Systems* (Dar Nahda Al Arabiah 1997).

هلالي عبدالله، تفتيش نظم الحاسب الآلي (دار النهضة العربية مصر 1997).

Al Saqer J., *The Procedural Aspects of Internet crimes* (Dar Nahda Al Arabiah 1998).

جميل الصغير، الجوانب الاجرائية للجرائم المتعلقة بالانترنت (دار النهضة العربية مصر 1998).

Hijazi A., *principles of the criminal proceedings in the computer and Internet crimes* (Dar Al Fikr Al jami 2006).

عبدالفتاح حجازي، مبادي الاجراءات الجنائية في جرائم الكمبيوتر والانترنت (دار الفكر الجامعي مصر 2006).

Jihad J., *Brief explaining of the UAE Criminal Procedure Code* (2nd edn, Dubai Police Academy Publications 2008).

جوده حسين جهاد، الوجيز في شرح قانون الاجراءات الجزائية لدولة الامارات (مطبوعات أكاديمية شرطة دبي الطبعة الثانية 2008).

Mustafa M., *Explain Criminal Procedure Law* (Dar Nahda Al Arabiah 1998).

محمود مصطفى ، شرح قانون الاجراءات الجنائية (دار النهضه العربية مصر1998).

Osman A., *Criminal Evidence and Scientific means of Investigation* (Dar Nahda Al Arabiah 1975).

أمال عثمان، الاثبات الجنائي ووسائل التحقيق العلمية (دار النهضة العربية مصر1975).

Rustom H., *The Procedural Aspects of Cybercrimes* (Modern machinery 1994).

هشام رستم، الجوانب الاجرائية للجرائم المعلوماتية (مكتبة الالات الحديثة مصر 1994).