Factors Influencing Digital Evidence Transfer Across International Borders: A Case Study

MICHAEL EDWARD SPENCE
BSc Hons (Sheffield Hallam University, UK)

a thesis submitted to the graduate faculty of Computing and Mathematical Sciences
AUT University
in partial fulfilment of the
requirements for the degree of
Master of Forensic Information Technology

School of Computing and Mathematical Sciences

Auckland, New Zealand
2010

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

.....

Signature

Acknowlegements

This thesis was completed at the school of Mathematical Sciences at Auckland University of Technology.

I would like to thank Dr Brian Cusack for his direction and assistance as academic supervisor during the writing of this thesis. I would also like to thank the following people who contributed their time and invaluable professional insights during this research: Nick Flanagan, Barry Foster, Campbell McKenzie, Michael O'Brien, Andrew Shirnack, Philip Skelton and Brent Whale.

I would also like to express my thanks to Maureen and Eddie Spence whose lifetime's unswerving support of their children in all of their endeavours is more appreciated as the years go by. If given the option, I simply could not have chosen better parents.

Finally I would like to thank Sue Spence my wife, soul mate, editor and chief moral officer without whose help this thesis would not have been completed.

Abstract

Digital Forensics has grown out of the necessity to extract, analyse and present evidence from digital devices in support of an investigation or court case. In its early stages in the 1970' and 80's this would often relate to a computer that was not connected to any networks. The issues were therefore local and dealt with by local law enforcement agencies and prosecuted under local (national) laws. The explosive growth of Internet usage and e-commerce has resulted in a corresponding growth in international e-crime. The perpetrator of this international e-crime can be based in one country with the victim in a second country and the data in a third country. This raises the question regarding in which country the offence has occurred and under which jurisdiction it should be investigated and prosecuted.

This new paradigm now means that the digital forensic practitioner may have to deal with the acquisition and presentation of digital evidence in a foreign country. This raises a whole new level of complexity regarding both the integrity of the evidence that has moved between countries and acceptance of the digital forensics practitioner as an expert witness in a foreign court. The differences in the laws of the countries involved in the investigation and prosecution of the offenders can also have a substantial impact on the digital evidence process.

The purpose of this research is to identify the main factors that influence the successful presentation of digital evidence across international borders. The test of the success of the presentation of digital evidence is usually considered to be that the evidence and the digital forensic practitioner presenting the evidence are accepted by a court of law.

The research commences with a review of the current literature in this area. From the review of the literature a set of 16 hypothesised main factors influencing the transfer of digital evidence across international borders is

formulated. In order to test the 16 main hypothesised issues, and investigate if any other main factors exist, a case study approach is used as part of a series of unstructured interviews with digital forensic and legal professionals. A thematic analysis technique is applied to the interview transcripts to extract common themes in the options of the interviewees.

The result of the research is the identification of 11 main factors that influence the transfer of digital evidence across international borders. These factors are classified in the four areas of Technical, Transportation, Standards/Qualifications/Certification and Legal. The research postulates the main areas in which the solutions to some of the issues raised by these main factors may be found.

The research recognises that the area of digital forensics and the international perspective of the movement of digital evidence across borders is a new and evolving discipline. The thesis concludes with the learnings from the research, the limitations of the research and suggests four areas for future research regarding law enforcement development of digital forensic guidelines, certification of digital forensic practitioners, international standards and harmonisation of international e-crime laws,

Table of Contents

List of Tables

List of Figures

List of Abbreviations

CCFE	Certified Computer Forensics Examiner
CDESF	Common Digital Evidence Storage Format
IARIA	International Academy Research and Industry Association
INTERPOL	International Criminal Police Organisation
ISO	International Standards Organisation
MD5	Message Digest Algorithm 5
NIST	National Institute of Standards and Technology
SHA	Secure hash Algorithm
SWEGE	Scientific Working Group on Digital Evidence

Chapter 1
Introduction

1.0 INTRODUCTION

The opening section of this thesis gives a background to the evolution of the information revolution. This leads on to a review of the growth of e-commerce followed by comment on the evolution of e-crime. The growth in volume and complexity of e-crime has driven a requirement for the collection of digital evidence, required in order to be able to investigate and prosecute offenders. Following this is an explanation of the international aspects of digital evidence collection and presentation leading to a definition of the research question which the thesis will investigate.

The next section then covers the motivation for this research and the reason why this is of considerable importance to the researcher. Chapter 1 then closes with a section on the structure of the thesis.

1.1 THE EVOLUTION OF DIGITAL EVIDENCE COLLECTION

Digital evidence collection has evolved because of the necessity to police the growing area of e-crime. The chronology of the development of digital evidence collection commences with the start of the information revolution which is reviewed in paragraph 1.1.1. This leads to the evolution of e-commerce and e-crime detailed in paragraph 1.1.2. In response to e-crime it has been the necessary to develop e-Laws both national and international, which are reviewed in paragraph 1.1.3. The types of investigations requiring the collection of digital evidence are outlined in paragraph 1.1.4 which also details the emergence of the digital forensics practitioner. Paragraph 1.1.5 discusses the factors that are affecting the transfer of digital evidence across international borders. Section 1.1 then concludes with paragraph 1.1.6 which details the question that will be investigated in this research.

1.1.1 The Information Revolution

Humankind is currently in the throes of an information revolution (Britz, 2008). The impacts can be argued to be as far reaching as those of the preceding Agrarian or Industrial revolutions. However, major differences are the pace with which the information revolution is moving and the number of human beings it is affecting. It is difficult to note when any revolution of this kind ceases, other than with considerable hindsight. Indeed there are many differing opinions regarding the start and end date of the Agrarian and Industrial revolutions. What marks the Information revolution as very different is the pace of the change. Within less than one generation, humankind has moved from the widespread adoption of the telephone through the invention of the electronic computer to the adoption of the Internet. Countries, or more accurately their populations, are now more closely connected than ever before. This widespread adoption of the Internet is a fundamental change to the way humankind accesses and uses information. This has lead to considerable change at both a personal level and in the development of electronic methods to conduct business. E-commerce has been embraced expansively throughout the world.

1.1.2 E-commerce and E-crime

The uptake of computers and access to the Internet has quickly lead to a situation in most developed countries of a high level of penetration of Internet-linked computers in both households and businesses. Indeed there would be very few businesses in developed countries that run without any computer use. The early adoption of computers in business concentrated on computerising existing functions. This very often started in the finance sector and covered functions such as invoicing and payroll. The wider adoption of the Internet has lead to new ways of conducting business electronically, referred to as e-commerce.

Where money is involved crime will tend to follow and the development of e-commerce has lead to the development of e-crime. In its early stages

computer hackers typified this. Hackers tended to be young computer-literate individuals who were predominantly more interested in the challenge of breaking the security of a computer system than any financial gain. However as e-commerce has grown so has the sophistication of e-crime (Tipton & Krause, 2006). An example of a new crime in this area is skimming. In skimming, criminals will attach devices to the outside of Automatic Teller Machines (ATMs) to harvest account details and Personal Identification Numbers (PINs) of individuals in order to steal money from their banks accounts. These criminals, known as skimmers, have become more sophisticated in recent years and now often operate as gangs. They are often located outside the borders of the country in which they are resident. They believe that by operating only in foreign countries they may make it too difficult for local law enforcement agencies to investigate, collect evidence and prosecute them.

1.1.3 Development of E-crime Laws

A number of e-crimes have a component covered by conventional laws within countries. Taking the above act of skimming this can be prosecuted as theft, as money is essentially being stolen from a bank account. However this may not be as clear-cut if, for example, someone obtains the personal information of an individual by hacking into their computer, or places an intimate picture of an individual on the Internet. These types of crimes have seen several countries introduce specific laws regarding digital systems and information. Examples of these types of laws include Privacy laws regarding digital information, Computer Misuse laws and Data Protection laws placing legal obligations on organisations to protect personal information. In order to prosecute someone under a law it is usual that evidence will need to be presented in a court. In the case of e-crime, a significant element of this evidence is likely to be in digital format.

1.1.4 Criminal Investigations Involving Digital Information

Law enforcement agencies throughout the world have had to deal with the emerging problem of e-crime. This has involved them having to invest in skills and tools for staff in order that they can investigate e-crime and obtain the necessary digital evidence to be able to prosecute that crime.

This requirement has seen the development of the Digital Forensics practitioner. It is interesting to note that for the first 15 to 20 years of the existence of the digital forensics practitioner, they were referred to as Computer Forensic practitioners. The growth in digital devices such as mobile phones, cameras, Personal Digital Assistants (PDAs), however, has lead, more recently, to the use of the more encompassing term of Digital Forensics practitioner.

During a court case in most countries, defence legal council is entitled to access the same information and expertise as the prosecution legal counsel in order to ensure a fair trial. The early digital forensic practitioners were almost exclusively member of law enforcement agencies. However, independent digital forensic practitioners, who may work for the prosecution or defence, have now joined these. The number of digital forensic practitioners is likely to grow with the growth in the volume of e-crime.

Digital forensic practitioners, therefore, need to posses investigative skills including such issues as chain of custody knowledge, technical skills as they can be called upon to extract digital evidence from any type of digital device and, finally, an understanding of the legal requirements placed on them in the country in which they operate. This might include requirements under expert witness undertakings.

1.1.5 International Issues Relating to the Transfer of Digital Evidence

In the early stages of computerisation, prior to the widespread adoption of the Internet, e-crime tended to be a local crime. Local law enforcement and local country-based laws would deal with the issue. However the Internet is no respecter of international boundaries and consequently neither is e-crime (Power ,

2001). A criminal can be based in one country, access information in a second country which concerns an individual or organisation based in a third country.

This ease with which e-crime can traverse international borders has lead to considerable complexity regarding laws. Even the question regarding which country the crime was actually committed in can lead to significant difficulty in establishing which country has jurisdiction to prosecute the crime.

A case was outlined above where an offender might be based in one country, the information located in a second country and the victim in a third country. This type of investigation could require a digital forensics practitioner to acquire digital evidence in all three countries. Each country might have very different laws covering this area. If the case were to proceed to court then the question would arise of which country should prosecute the case and consequently in which country the court case should be heard. This would have a consequential effect regarding whether the digital forensics practitioner was considered to have suitable experience, qualifications and certifications to be recognised as an expert witness in the courts of that country and allowed to present the digital evidence found.

1.1.6 The Research Question

As outlined in the above sections, the question of digital evidence being used in an e-crime case with an international component may involve considerable complexity. That said the issue is very real and here and now. Countries are aware that if e-crime cannot be prosecuted over international borders, then the effect on e-commerce would be very considerable. Any criminal would feel safe committing e-crime providing they did not offend in their own country of residence.

The research question needs to cover both the technical and legal issues as a failure in either could potentially taint or exclude digital evidence from a court proceeding. The research question that has been developed is therefore: What are the factors influencing digital evidence transfer across international borders?

1.2 MOTIVATION FOR UNDERTAKING THE RESEARCH

There are a number of motivating reasons for undertaking this research. The researcher has been an IT professional for many years, is a past senior IT Manager with the New Zealand Police and, for several years recently, has acted as a digital forensics practitioner and expert witness. This has lead to the following reasons for the research.

1.2.1 Issue During the Execution of a Search Warrant

In the very recent past the researcher was acting as a digital forensics practitioner during the execution of a search warrant on behalf of a New Zealand Government department. The warrant was being executed at business premises in New Zealand. During the execution of the warrant it became apparent that a significant volume of the company's information was located on a server of the parent company based in Australia. Several staff on a daily basis were accessing this information over a leased line link between the New Zealand entity and the Australian entity.

The New Zealand company was quite hostile to the execution of the search warrant. The key information described in the search warrant was, in fact, located on the server based in Australia. From a technical perspective it was a simple exercise to make a copy of the information held on the Australian server. There seemed little doubt that if the information was not collected at that point it would be removed from the Australian server.

The question this raised was whether, under the terms of the search warrant and Australian law, it was acceptable to make an image of the information held on the Australian server. The wider question raised was what other factors were involved in the collection of digital evidence between countries.

As this situation seemed likely to occur again in the future, it also raised the question of what standards or guidelines were in place to assist in the decision making process.

1.2.2 Avoiding a Criminal Conviction

Many countries have strict data protection and computer misuse laws. New Zealand itself has a number of new computer misuse laws. These laws provide for criminal convictions and lengthy jail sentences for, amongst other things, accessing a computer without authorisation or copying data from a computer without authorisation. Also, in many countries ignorance of a law is not considered an acceptable defence if it is proven that the law was broken.

Clarity in the legality of collecting digital evidence across borders was, therefore, of considerable interest to the researcher as a criminal conviction was unlikely to assist his personal or professional development.

1.2.3 Lack of Existing Research in this Area

The digital forensics specialism is relatively new and the area of the international transfer of digital evidence newer again. There have been relatively few specific academic qualifications available in this area around the world and, consequently, relatively little by way of academic research. It was therefore of considerable interest to add to the knowledge base in the fast moving and fascinating area of international e-crime and digital forensics.

1.2.4 A Mix of the IT and Legal Professions

The acceptance of digital evidence across international borders requires expertise from both the IT profession and the legal profession if it is to be successful. The relatively new and immature IT profession and the old and very mature profession of Law are not natural bedfellows. Indeed quite the opposite. However for an e-crime investigation to be successful the digital forensics practitioner must have some understanding of both of these professions.

This makes this study a fascinating blend of the growth and development of the digital forensics profession. This is being driven by the rapid development of technology and emerging digital laws trying to catch up with the information revolution.

1.3 THE STRUCTURE OF THE THESIS

The thesis covers a very real but broad area. Two main professional groups, the IT profession and the legal profession, drive this area, which is in a considerable state of change. The structure of the thesis is detailed below.

Chapter 2 of the thesis is the literature review. This contains a review of published work in the area of digital forensics. A review is also made of the standards and guidelines that have been published internationally in the area of digital forensics. The current state of qualifications and certification in this area is also reviewed.

In Chapter 3, a methodology is developed to analyse the subject area and identify the main issues affecting it. This covers a review of five previous research papers that have dealt with a similar problem area. Different methods of data collection for the study are also discussed. The expected outcomes of the research are hypothesised and the limitations of the research discussed.

Chapter 4 details the data capture and analysis of that data. The metrics in terms of the data collected, via interviews and diary records, and the results of the analysis are covered. The chapter concludes with a review of the hypothesised factors compared with the actual factors identified by the research.

Chapter 5 is a discussion of the findings. The hypothesised factors will be discussed in relation to the level of support they received as part of the research. Any new issues will also be identified. The chapter will conclude with the main findings of the research which will be a list of the main factors influencing the transfer of digital evidence across international borders. Potential resolution areas for these factors will also be explored.

Chapter 6 is the concluding chapter and will summarise the main findings of the research. The main learning's from the research will be detailed together with potential areas for future research. The chapter will close with a review of the main findings and the individuals or groups who may find them of most interest.

At the end of the thesis a full list of the references is detailed. A series of appendices are also included.

Chapter – 2

Literature Review

2.0 INTRODUCTION

Digital evidence is an emergent phenomenon of the past few decades that is driving change in the legal and technical worlds. Evidence may be anything acceptable to a court of law and Digital evidence is any data that is stored or streamed digitally that may have an evidential value. The information revolution, the universal uptake of computing information systems by all types of enterprise, and the ubiquitous access to information of high value through the world wide web (WWW) has given rise to a growing array of business legal challenges. Core information assets have become more accessible, transportable and volatile in information markets. In an ideal world both the technology and the legal systems would have consistency for the fair imposition of information control. However often the two are moving at different speeds and information rights are distributed unfairly. The purpose of this study is to identify the factors currently affecting the movement of digital evidence across international borders. The problem is a critical issue area of the persecution of e-crime. The development of new technologies (eg. mobile phone texting, iPhone capabilities and USB memory sticks) and global ubiquitous access have brought with them a new set of issues regarding e-crime and the balancing of rights.

The development of digital evidence issues (both domestic and international) is characterised by an uneasy relationship between the technical developments and the legal developments. These two areas, by their very natures, tend to move at different speeds. As is shown in the physical world, if two bodies are moving at different speeds, then friction is likely to occur at the interface. In the technical / legal world interface this means that people's rights are being violated because prosecution of e-crime is being hindered. A consequence is the perpetration of crime using information technology across jurisdictions may not be prosecuted or that prosecution is extremely difficult. This chapter reviews the

current literature to locate and identify the issues surrounding the problem of cross-border movement of digital evidence.

The chapter is divided into four main sections that review the issues affecting the presentation of digital evidence across international borders. Section 2.1 relates to the technical issues, this covers the Acquisition 2.1.1 (including tools, remote acquisition and other digital devices), 2.1.2 Preservation, 2.1.3 Analysis and 2.1.4 Reporting of Digital Evidence. Section 2.2 reviews the Chain-of-Custody issues and Transportation of Digital Evidence across International Borders. Section 2.3 looks at the emerging areas of Standards, Qualifications and Certification in the context of bridge building co-operation. In section 2.4, legal issues are reviewed including the expert witness concept, jurisdiction and developing domestic and international legal issues. Section 2.5 gives a summary of the major issues identified.

2.1 TECHNICAL ISSUES

There are many definitions of Digital Forensics reflecting the speed at which the problem area is evolving.

> "Computer Forensics is a young but rapidly developing discipline. Borrowed from principles that have proven themselves in the physical world, it faces challenges that are unique to the Cyber space domain. (Caloyannides, el al., 2009).

Until recently the area would have been referred to as Computer Forensics. One general definition is "Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence" (Pollitt & Shenoi, 2006). Other definitions also include the concepts of preservation of evidence and chain of custody (Brown, 2006; Casey, 2004). In the following subsections the technical problem areas of acquisition, tools, remote system access, and digital devices are discussed to define the issues and challenges facing Digital Forensic investigators.

2.1.1 Acquisition of Digital Evidence

Acquisition is the act of acquiring the evidence in the first instance. It was not uncommon in the early days of computer forensics for the actual evidentiary computer itself to be used to obtain the evidence (Casey, 2004). Casey goes on to further note (Casey, 2004, p28),

> "It was not until the early 1990s, that tools like SafeBack and DIBS were developed to enable digital investigators to collect all data on a computer disk, without altering important details".

The history of safe acquisition of digital evidence (image) at the time of writing this report is therefore less than 20 years old.

The acquisition phase is also a process that must be clearly documented. The nature of the collection of digital evidence is such that the right person with the right skill sets may not be the person available, at the time when the evidence requires collecting. Hence one approach has been to develop flow charts for the evidence collection process and these charts are disseminated to those who are of a risk level for forensic incident. The approach is planned to mitigate risk by enforcing some systematic quality control.

The following flow chart (Figure 2.1) is from the American Department of Justice and is typical of a flow chart approach to evidence acquisition.

In the early 1990s at the start of digital forensic acquisition techniques, the acquisition of evidence involved the copying of data. The technique effectively limited the digital investigator to acquiring live files. Later the imaging of drives became more common as this allowed for a complete image of a computer's hard drive. In comparing copying and imaging (Sammes & Jenkinson, 2007, p. 298) notes that:

> "In the early days of forensic computing, before imaging was widely available, most recovered evidence was in the form of copied files or raw sectors. When imaging became the norm copying decreased".

However the rapid increase in the size of computer drives and time constraints that can sometimes be placed on making images (as during the execution of search warrants) has seen a return to copying in some instances:

> "Once disks became so large as to cause time constraints on warrants, copying has been re-introduced as a method of capturing data quickly" (Sammes & Jenkinson, 2007, p. 298).

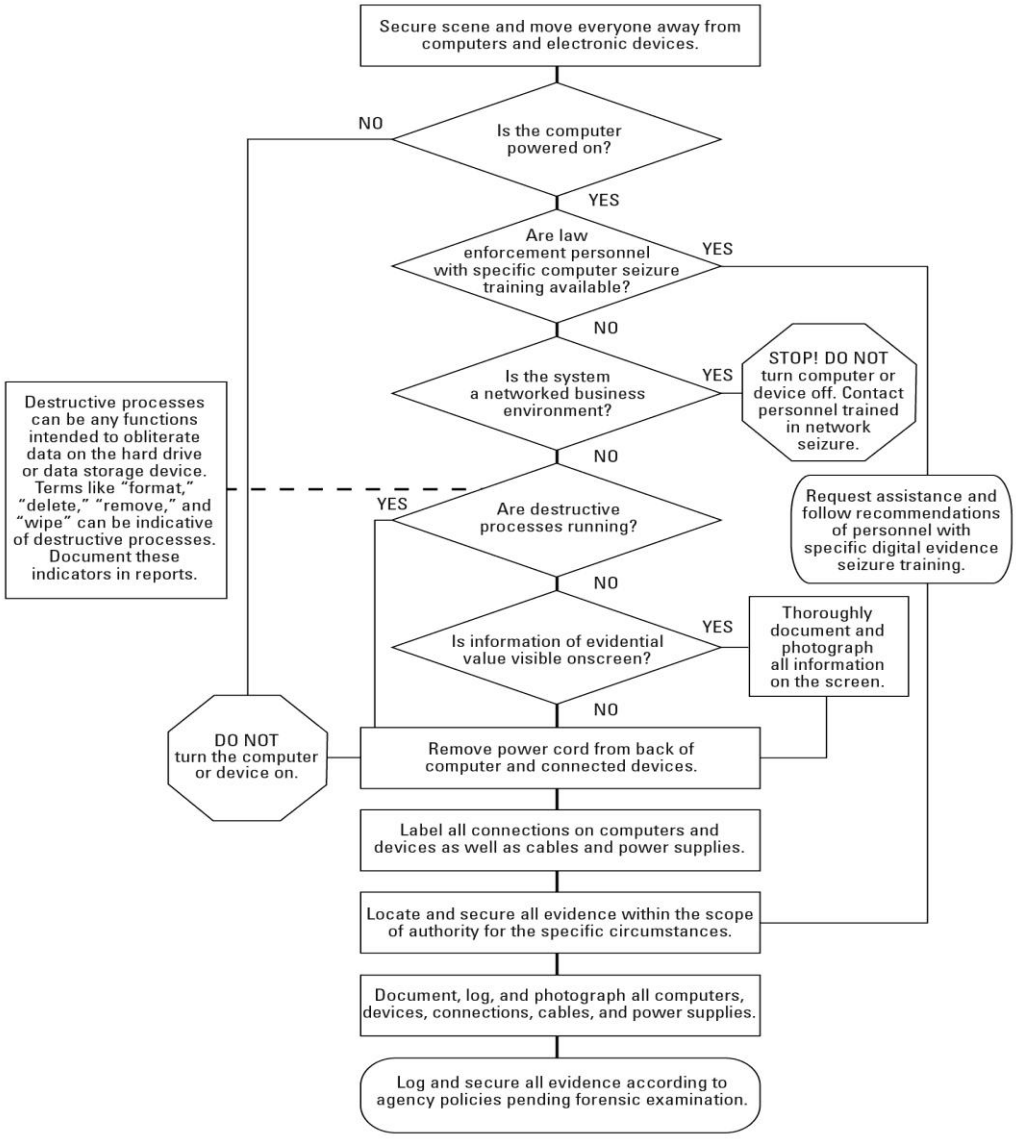

Figure 2.1. Electronic Crime Scene Investigation: A Guide for First Responders (Murkasey, et al., 2008, p.29)

2.1.1.1 Acquisition Tools

An in-depth study of all the acquisition tools is outside the scope of the research. However computer disk imaging is currently the single most common (and most accepted) method of collecting digital evidence. To this extent (Brown, 2006, p. 236) notes that:

> "Disk imaging is such a key component to the evidence collection process that NIST created the Computer Forensics Tool Testing Project (CFTT) in an effort to standardise technologies in use".

The current disk imaging tools (which are a collection of hardware and software) all enable the processes of a bitstream image of a drive and a hash value (MD# or SHA# are the current standards). While there is currently no international standard in this area, the legal systems of most countries are striving to achieve consistency. Notably a complete and verifiable image of the computer drive is the aim.

The method in which the forensic image is taken is often referred to as commercial-based imaging and non-commercial based imaging. The two most accepted commercial imaging software packages are Encase and FTK, both of which can be used to produce Encase images. The most popular of the non-commercial image types is the Data Dump (DD) image (Jones et al., 2006). There are also an emerging number of high speed forensic imaging hardware devices appearing. Of more importance to this review is the image type of the output. The image type tends to be either an Encase or DD image. Within the area of computer forensic images, of increasing importance is the acquisition of volatile information:

> "Volatile memory forensics, which can be referred to as a new branch of the classical Digital Forensics discipline, aims as collecting and analysing the whole memory content of a running computer" (Savoldi & Jerks, 2009, p. 3).

2.1.1.2 Remote Acquisition

The acquisition phase is normally conducted with physical access to the digital equipment or storage device. However a relatively recent development is the remote collection (sometimes across international borders) of digital evidence. Specific software is now being marketed for the purpose:

> "Forensic-grade application suites, such as those offered by Technology Pathways in their proDiscover Incident Response and Guidance Software in their EnCase Enterprise Edition have been network enabled to allow live imaging and analysis. These client/server-enabled applications allow investigators to connect to remote systems over local area networks and wide area networks through the use of a remote server application running on the remote suspect system, which redirects low-level sector data as well as other commands to the forensic work station for analysis." (Brown, 2006, p251).

The advent of remote collection has major implications for the use of digital evidence across international borders. It has, and will continue to, raise issues of jurisdiction and when this type of acquisition is acceptable. It is a current example of an area in which the technology is running well ahead of the legislation.

While transportation of digital evidence is discussed in a later section, the 'physically disconnected' remote acquisition brings with it additional problems:

> "The remote and seemingly disconnected nature of disk forensics over networks adds an increased burden of integrity assurance on the investigator. Security steps to be considered when conducting any type of remote disk forensics over a network include the use of the following elements:
>
> Encryption to secure the data channel
>
> Password protected remote agents
>
> Write-protected trusted binaries for remote agents
>
> Digital signatures to attest to remote-agent integrity

Cryptographic hashing to verify completed images

Network segment isolation" (Brown, 2006, p. 252).

2.1.1.3 Acquisition

While the main focus of digital forensics has been the computer, recent years have seen an explosion of other devices holding information and therefore potentially evidence. Amongst the most recent is the rapid development of the mobile phone into a much more complex mobile digital device. Amongst the emerging devices that may hold digital information are car parking meters, fridges, photocopiers, games machines and home management systems. The list cannot be completed as the diversity of devices continues to increase. Each new device all present varying technical issues and emergent challenges during the acquisition phase. Harril and Mislan (2007) suggest the term Small Scale Digital Device Forensics (SSDDF) for this evolving area. They go on to note:

> "The breakdown for each device can be illustrated by the ability to store information magnetically, optically, using solid-state, Flash Memory and by Devices which extend the use of the computer system" (Harril & Mislan, 2007, p. 2).

The conceptualisation is presented in Figure 2.2.

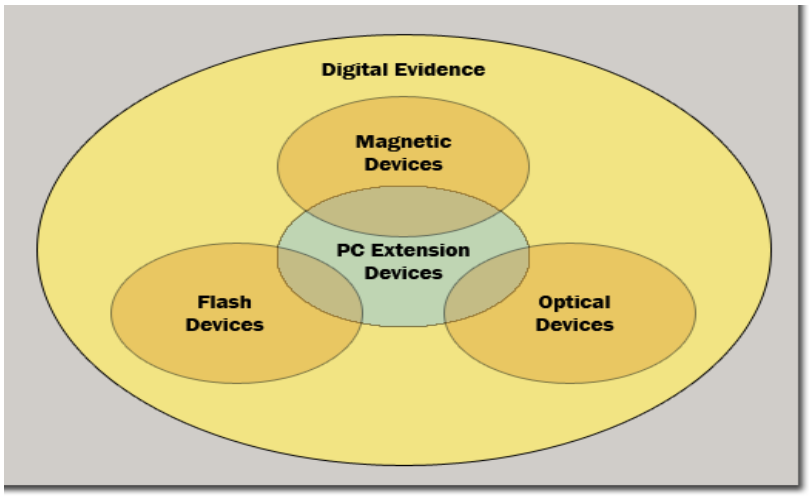

Figure 2.2 Small Scale Digital Forensics (Harrill & Mislan, 2007, p. 3)

A major element of SSDDF is mobile phone digital forensics. It is a fast growing area that presents a number of unique problems. The areas that need to be considered during acquisition include:

> **"**Mobile phones have proprietary file systems.
>
> Mobile phones have proprietary file transfer protocols.
>
> Mobile phone providers lock down certain features of the device.
>
> Different mobile phone providers might install different operating systems on the mobile phone device.
>
> Cables used in the forensic acquisition of a mobile phone can be different.
>
> The mobile phone device's clock changes data continuously on the device.
>
> Different mobile phones have different features.
>
> A mobile phone being used is being provided a service through a carrier, and there are numerous carriers.
>
> Applications can be installed on certain cellular phone models." (Baggili, et al., 2007 p. 2).

Computer Digital Forensics is a different study area from SSDDF and the differences can catch out the unwary investigator (Lim & Khoo, 2009).

2.1.2 Preservation

The preservation of digital evidence is a critical step in a digital forensic investigation. As noted by Casey (2004, p.12), "Once identified digital evidence must be preserved in such a way that it can later be authenticated". The challenge of preservation is further complicated with the acquisition of volatile information. The preservation of volatile information can pose considerable problems for the forensic investigator. In a recent report from the SANs Institute they have taken the issues further and suggest that the order of volatility of digital evidence is:

"CPU, Register and Cache content
Routing table, ARP cache, process table, Kernal statistics
Memory
Temporary file system/swap space
Data on hard disk
Remotely logged data
Data contained on Archival media."
(http://blogs.sans.org/computer-forensics/2009/09/12/best-practices-in-digital-evidence-collection/)

2.1.3 Analysis

Analysis of digital evidence can be undertaken at a number of levels - Physical media, Media management, File system, Application, Network and Memory, (Carrier ,2003). Two of the most well known integrated tools for examination and analysis of digital evidence are EnCase from Guidance Software, Inc and Forensic Tool Kit (FTK) from Access Data Inc. Both products in their latest versions (EnCase version 6 and FTK version 3) automate a number of routine tasks and provide Graphical User Interfaces.

> "As more people became aware of the evidentiary value of computers, the need for more advanced tools grew. To address this need, integrated tools like EnCase and FTK were developed to make the Digital investigator's job easier" (Casey, 2004, p. 28).

Encase is outlined in Brown (2006, p. 200) as follows:

> "Encase was introduced in late 1990s by Guidance Software, Inc. Encase is one of todays most widely used application suits. EnCase uses a case methodology in which users create a proprietary case file to work from that contains information about the project for the generation of reports. In what has become the standard for tools in this class, users can add and

> manage multiple directly attached disks or disk images to a case."

Brown (2006, p. 200) goes on to outline FTK as:

> ".FTK provides an integrated environment that supports collection, Analysis and reporting of computer disk evidence. One of the strengths of FTK is its capability to conduct index searching"

2.1.4 Reporting Results

There tend to be three main methods of reporting results - verbal, written and electronic. This can be complicated for an expert witness in digital forensics, or any expert witness, as they try to convey complex issues in a manner that can be understood by non-experts in the field. If this is being done in relation to an international case then local legal, cultural, and procedural issues may need to be taken into account, as well as language issues. The following subsections define and discuss the problems associated with the different modes of reporting.

2.1.4.1 Verbal Reporting

Under most legal systems throughout the world, witnesses maybe called to a 'court' to give evidence verbally. The evidence may be backed up by written or digital evidence, but the court will expect to see, and be able to question, a witness.

> "The oral testimony of witnesses competes in a sense with documentary evidence to the extent that one may exclude or supplement the other. Under Anglo-American law, almost anyone can be a witness, including the parties and experts; even insane persons, children, and convicted felons may testify. Grounds once used for excluding such persons as witnesses are now used only to impeach their credibility."

(http://www.britannica.com/EBchecked/topic/197308/evidence/28372/Witnesses#ref=ref397439, Jan 2009)

2.1.4.2 Written Reporting

The standard output from most computer forensic investigations remains the written report. The following is a guideline as to what may be expected in a digital forensics report.

"Identity of the reporting agency.

Case identifier or submission number.

Case investigator.

Identity of the submitter.

Date of receipt.

Date of report.

Descriptive list of items submitted for examination, including serial number, make, and model.

Identity and signature of the examiner.

Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.

Results/conclusions." (Ashcroft, 2004)

2.1.4.3 Electronic Reporting

Providing digital evidence in the form of electronic reporting has seen considerable advances in recent years. A limiting factor will always be the availability of suitable equipment to allow display of the evidence in a courtroom environment. It is often preferable to show digital evidence in its native environment such as a multipage spread sheet or a video clip. In New Zealand law the matter is dealt with by the Evidence Act 2006 which in defining a document states "information electronically recorded or stored, and information derived

from that information" (Evidence Act 2006, p. 12). In the wider context, the use of graphics for evidence presentation is not without risk:

> "These can be perceived as a benefit in increasing the understanding of complicated technical information to a generic audience, or as a threat to justice introducing potential bias and prejudice." (Burton, et al., 2005, p. 97)

2.2 CHAIN-OF-CUSTODY AND TRANSPORTATION

Chain-of-Custody is a vital part of the digital forensics process.

> "Chain-of-custody for evidence from the crime scene to the court room is a bedrock principle for both civil and criminal Law. Without a clear and unambiguous chain-of custody there is no way to be sure that an object presented to the court is the same object collected at the scene of the crime." (Garfinkel, 2009, p. 1)

Of critical importance in chain-of-custody is the use of Hashing algorithms. It is common in digital forensics to use the MD5 (128 bit) Hash to provide a method of ensuring that digital evidence has not changed over time. Recently questions have been raised about the security of the MD5# and the debate has lead to the increased use of SHA1 (160 Bit) hash and the SHA -256 (256 Bit). NIST has also started a program to develop a new hash standard (Garfinkle, 2009). The use of MD5# is, however, still widespread in computer forensics and its use is embedded in many tools.

In relation to the international perspective on digital evidence, the most widely accepted hashing standard is of primary importance. "The MD5 algorithm is very well known and useful in digital forensics" (Geoghegan & Gray, 2009). If digital evidence is to be moved across international borders then the integrity and confidentiality of the evidence must be protected.

Steps are being taken to standardise the storage and transmission of digital evidence, such as that by the Common Digital Evidence Storage Format (CDESF) working party. They note that:

" The goal of the Common Digital Evidence Storage Format (CDESF) working group is to define a storage format that is open and accepted by the community.." (CDESF, 2006, p. 1)

A discussion of the current formats is contained in the document 'Survey of Disk Image Storage Formats' (CDESF, 2006). A standard format may however be some way off given the competing agendas of commercial organisations.

2.3 STANDARDS, QUALIFICATIONS, AND CERTIFICATION

The maturing of a profession is usually characterised by three main factors - Professional Standards, Formal Academic Qualifications, and Professional Bodies offering accreditation. These characteristics are apparent in professions spanning several centuries such as Medicine, Law and Engineering. There are recent attempts to gain advances with the development of the IT profession. In the following subsections the matters of standards, qualifications and certification are reviewed to identify ways in which the transfer of digital evidence across borders may be improving. Cooperation, agreements, standardisation and professional consistency are all potential ways the cross border transfer of evidence may be enhanced.

2.3.1 Standards and Guidelines

Standards and Guidelines in the area of digital evidence tend to fall into two categories. Those either aimed at a domestic audience or at an international audience. The following subsections review the major contributors to standardisation of digital evidence.

2.3.1.1 Domestic Standards and Guidelines

Listed below are three of the earliest domestic documents providing guidelines for digital forensics. All three documents have been revised since their initial release. These revisions have been driven both by changing technologies as well as changing practices.

The US Department of Justice (Federal Bureau of Investigation) Digital Evidence Standards and Principles (SWEGE,1999).

The Good Practice Guide for Computer-Based Electronic Evidence produced by the Association of Chief Police Officers (Wilkinson, 2003). This guide states that it is "This good practice guide is intended for use in the recovery of computer-based electronic evidence; it is not a comprehensive guide to the examination of that evidence". It goes on to state that it consistent with the principles of the G8 Lyon Group as a basis for international standards.

The Guidelines for the Management of IT Evidence, Committee IT/012, Standards Australia International.

2.3.1.2 International Standards and Guidelines

Two standards based on international principals are:

The Best Practice in the Forensic Examination of Digital Technology, produced by the International Organisation on Computer Evidence (IOCE). This document contains seven principles that were developed by the IOCE and adopted by the G8 nations.

The most recent development in this area is the emerging International Standards Organisation (ISO) ISO/IEC 27037 -- IT Security -- Security techniques -- Guidelines for identification, collection and/or acquisition and preservation of digital evidence (DRAFT).

The current web site listing states that:

> "This is a new project for ISO/IEC JTC1/SC27. At this early stage, the title and scope are uncertain. It is started developing guidance for gathering and protecting digital forensic evidence, particularly for cross-border crimes where evidence acquired in one country might be presented in the courts of a second. The

standard could also be used within a single jurisdiction". (http://www.iso27001security.com/html/27037.html, Oct 2009).

2.3.1.3 International Organisations Engaged with Digital Evidence

There are a number of international organisations engaged with the issue of digital evidence. Listed below are the four main organisations.

International Standards Organisation (ISO). This is a non-governmental organisation with 162 member countries. It is the world's largest developer and publisher of International Standards. (http://www.iso.org).

International Organisation on Computer Evidence (IOCE). This was formed from the direction of the G8 group of nations proposed principles.. Its principle state that:

> **"**In March 1998, IOCE was appointed to draw international principles for the procedures relating to digital evidence, to ensure the harmonisation of methods and practices among nations and guarantee the ability to use digital evidence collected by one state in the courts of another". state."(http://www.ioce.org/core.php?ID=5)

International Criminal Police Organization (Interpol), was created in 1923 and currently has 188 member countries. "INTERPOL aims to facilitate international police co-operation even where diplomatic relations do not exist between particular countries", (http://www.interpol.int/public/icpo /default.asp). It undertakes this work through a number of working parties.

> "INTERPOL working parties on Information Technology (IT) crime were created to facilitate the development of strategies, technologies and information on the latest IT crime methods. There are regional working parties for Africa, the Americas, Asia and the South Pacific, Europe, and the Middle East and North Africa. (FACT SHEET COM/FS/2008-07/FHT-02 http://www.interpol.int/Public/ICPO/FactSheets/FHT02.pdf)

The United Nations (UN) has addressed the issues of cyber crime and cyber laws in a number of its forums. It recently published "The law of Cyber-Space, an Invitation to the Table of Negotiations" The paper is an explanation of the International issues of Cyber Crime and the creation/ harmonising of laws under the heading Standards of Evidence the paper states that:

> 'This uncertainty is beginning to lead to a proliferation of narrowly focused laws by which various government departments across the countries authorize the use of the records from their own computer systems or in dealings between those departments and the part of the public that they regulate. This creates a serious risk of incompatibility in information systems, even within the same jurisdiction. Some provinces have legislated on electronic evidence, but not consistently with each other. As a result, businesses active in more than one jurisdiction may have to keep records differently for use in different jurisdictions." (Kamal, 2005, p. 206).

2.3.2 Qualifications

Formal academic qualifications in digital forensics are relatively recent, as might be expected. A large number of the early digital forensic investigators came from a general law enforcement background and had no formal tertiary academic qualifications. As with the increase in the volume and depth of academic qualifications in the general computing field in the last 30 years, it can be expected that digital forensic graduate and post-graduate qualifications will increase and become more the norm for digital forensic investigators.

The Electronic Evidence Information Centre web site lists 69 colleges and universities offering tertiary qualifications in digital forensics worldwide. While this number will be growing, it remains a limited and specialist area (http://www.e-evidence.info/index.html).

2.3.3 Certification

Certification programs tend to fall into two categories - the accreditation of the labs and the accreditation of the digital forensic investigators. The following sub sections review these two categories of certification.

2.3.3.1 Digital Forensic Laboratory Accreditation

A number of organisations in different countries offer accreditation for digital Forensic laboratories. These include Acquisition Data Inc in the USA, The American Society of Crime Laboratory Directors Laboratory Accreditation Board and ISO 17025. The latter is the main standard used for Testing and Calibration of Laboratories, as noted in Marcella (2008, p. 179). Within New Zealand the main accreditation body is the International Accreditation New Zealand (IANZ). However as of 3 December 2009 the organisations web site does not list forensics or digital forensics as areas in which it supplies services.

The largest forensics laboratory in New Zealand is the ESR lab. Their web site (www.esr.cri.nz) states that they are accredited by the ASCLD/LAB (the American Society of Crime Laboratory Directors/Laboratory Accreditation Board). The largest digital forensics laboratory in New Zealand is the Police Electronic Crime Lab. The Electronic Crime Strategy to 2010 states that: "Police will implement formalised standard operating procedures, high-quality exhibit management, appropriate lab conditions, and other national practices required to achieve ASCLD/LAB international accreditation".

2.3.3.2 Digital Forensic Investigator Accreditation

The main vendor certification and the oldest on the market is the EnCE (Encase Certified Examiner) from Guidance Software Inc. Guidance software describes the accreditation as follows:

> "Certification candidates must meet professional requirements and pass a rigorous testing program to earn an EnCase certification. The certifications are valid for three years, and require continuing education for renewal".

(http://www.guidancesoftware.com/computer-forensics-training-certifications.htm)

Another vendor-based accreditation program is ACE (Accessdata Certified Examiner) offered by AccessData Inc. They describe their program as:

> "The AccessData Certified Examiner™ credential is obtained by completing a multiple choice exam which consists of Knowledge Based and Practical Based elements. Although there are no prerequisites, ACE candidates will benefit from having the AccessData BootCamp and Windows Forensics - XP courses as a foundation." (http://www.accessdata.com/acePreparation.html).

The difficulty with vendor-based accreditation is that it is tool accreditation. It lacks independent rigour and is naturally driven by the motive of the vendor to sell training courses. It is widely accepted that the major revenue earner for major suppliers of digital forensics software is the training they supply and not the software sales. Although vendor-based accreditation may have its place, it does have its critics. "Certification of personnel is in my opinion counter-productive, one of the more commonly seen certifications is vendor certification". (Reyes, et al., 2007, p.191)

An example of non-vendor based accreditation is the CCFE (Certified Computer Forensic Examiner) which is undertaken by the Information Assurance Certification Review Board (IACRB). IACRB is a not-for-profit organisation that provides certification in the area of Information Security Professionals. They state that they follow ISO/IEC 17024 Standards. They go on to state:

> "The Board will sponsor a world-class certification set, that meets or exceeds the needs of organizations and individuals wishing to hold candidates to the highest possible level of professional certification in the area of information security. As much as it is feasible, the Board will remain independent from any commercial organization. http://www.iacertification.org/

Another independent computer forensic certification is the Certified Information Security Professional (CISSP) administered by the International Information Systems Security Certification Consortium (ISC2). The WorldWideLearn web site notes that:

> "The most widely recognized voluntary credentials available to a computer forensics professional are the Certified Information Systems Security Professional (CISSP) and the Certified Computer Examiner (CCE)." http://www.worldwidelearn.com/online-education-guide/technology/computer-forensics-major.htm

Within digital forensics, as with the early development of computer professionals in general, professional certification is lagging well behind. The difference is that digital forensics is very closely aligned to the legal fraternity, a highly regulated profession, with centuries of history and precedent to call upon. This lack of independent certification to a high standard is causing problems within individual countries. This problem is magnified when evidence and expert testimony are required to cross international borders. The problem has been highlighted in the USA with moves to regulate accreditation of digital forensic investigators. It is noted:

> "We are witnessing a very interesting and disturbing trend in the digital evidence domain. Many states are enacting or amending legislation that will require anyone conducting any type of an "investigation" where a computer is involved to be licensed as a Private Investigator – Michigan being one of the latest examples. This is interesting as it was predicted several years ago that, unless the digital evidence community came up with some sort of gold standard/professional designation with a professional code of ethics, the ability to censure unethical professionals etc. the government would intercede with a less than perfect knee jerk reaction in order to protect consumers of

these services."
(http://deforensics.blogspot.com/2009/01/digital-evidence-investigators-required_14.html.)

Similar moves to regulate are occurring in other countries.

2.4 LEGAL ISSUES

The issue of digital evidence moving across international borders is a particular risk for investigators and also prosecutors. The problem is succinctly stated as:

> "Issues of evidence are firmly grounded in the real world. It is evidence that provides the material upon which a judge or Jury's finding of fact may be made. The admissibility of evidence from new electronic and networked technologies may give rise to complex issues" (Harvey, 2003, p. 241).

Digital evidence presents some unique features and difficulties compared to more traditional evidence. In (Marcella, et al., 2008, p. 298) it is noted under the heading Evidence in the 21st Century that:

> "Traditional evidence in Criminal cases has substance, shape and form. People can see it. In many cases they can touch it. Fingerprints, for example, are often visible on surfaces like table tops. Even where they are latent, simple techniques exist for their retrieval. And fingerprints can last for years or even decades under the right conditions, as can trace evidence like hair or fibres. Computer evidence is entirely different. It cannot be seen, touched or smelled and it often lasts for only very short periods of time."

This International perspective poses challenges and risks for the investigation of cyber-crime:

> "The legal challenges for forensic analysis in cyber-space include:
>
> global liability issues;
>
> jurisdiction – based issues;

risk issues;
data and document retention issues;
response and regulatory issues;
independence, objectivity and expertise issues;
commercialization issues;
regulatory and investigation issues; and
human rights issues"(Wilson, 2008, p. 3).

2.4.1 Expert Witness Status

In his book 'Forensic Science' (Siegel, 2006, p. 510) states that in the USA:

> "The trier-of-fact is the party who has the responsibility of determining the guilt or innocence of the accused. In a jury trial, the jury is the trier-of-fact. In a bench trial, the Judge is the trier-of fact. In all trials the judge has the responsibility of making legal decisions about the conduct of the trial".

He goes on to state (p. 520) that the definition of an expert witness is "a Witness qualified as an expert witness by knowledge, skill, experience, training, or education". He further states:

> "...two important differences between an expert witness and a lay witness are:
>
> An expert witness must be qualified as an expert every time she testifies in court.
>
> An expert witness is permitted to offer opinions, whereas a lay witness generally cannot"

2.4.2 Jurisdiction

In the vast majority of crimes the perpetrator, victim and criminal act will be in the same country and subject to that country's terrestrial laws (Smith et al., 2004). A country will prosecute a case if it believes the crime falls within its jurisdiction. This is an important point regarding digital evidence as it can dictate that a

country may wish to collect (or have collected on its behalf) digital evidence in a second country.

> "In the UK computer misuse Act, 1990 the test for jurisdiction in cases where borders are traversed in the commission of an offense under the Act is whether there is a "significant link with the Domestic jurisdiction. Thus, the UK courts will claim jurisdiction where the perpetrator was in the United Kingdom when he/she caused the computer to perform the offending function or when the computer used was in the United Kingdom or when the victim computer was in the united Kingdom or if the defendant accessed a computer and his/her intention was to commit a further offense in the United Kingdom." (Casey, 2004, p.78).

These jurisdictional issues can however be very 'delicate'. In 2001 the US FBI indicted two Russian nationals for breaking into computers in the US. The pair had been lured to the US by false job offers. In the investigation the FBI used hacking methods to obtain evidence from servers based in Russia, without the Russian authority's knowledge or agreement. In response the Russian Police laid charges of hacking against an FBI agent. The news web site CNET noted:

> "International law experts said a year ago that the operation, the first known incident of international hacking for evidence, created a precedent for indiscriminate cross-border hacking". (http://news.cnet.com/Russia-accuses-FBI-agent-of-hacking/2100-1002_3-950719.html)

2.4.3 Developing Domestic and International laws

In his book Technology and Legal Systems (Cox, 2006, p. 87) states that:

> "international law is more fluid and less certain than the domestic legal systems of most if not all states, as is perhaps

inevitable for a system which has evolved largely through state practice over a considerable period of years"

The speed at which sovereign states are tackling the issue of e-crime varies considerably. "Sovereign States make their own laws and criminalise what they like (or rather what they don't like)" (Smith, et al., 2004).

The Laws impacting or relying on digital evidence are also characterised as 'evolving'. The following are some of the laws and acts in the USA.

"Sarbanes-Oxley Act 2002 (SoX)
Gramm- Leach-Bliley Act (GLBA)
California Security Breach Act (SB 1386)
Health Insurance Portability and Accountability Act (HIPAA) 1996
Basel II Accord
USA PATRIOT and Terrorism Prevention Reauthorization Act 2005
No Electronic Theft Act (NET)
Economic Espionage Act
Child Pornography Prevention Act (2005)
Local Law enforcement Hate Crimes Act (2001)
Computer Fraud and abuse Act (2001)
Digital Millennium Copyright Act (1998)
Identity Theft and Assumption Deterrence Act (1998)
Children's Online Protection Act (1998)
Wire Fraud Act (1997)
National Information Infrastructure Protection Act (1996)
Computer Security Act (1987)
Electronic Communication Privacy Act (1986)" (Albert, et al., 2008)

Each individual state in the USA also has their own computer crime laws. A list of these can be found at the National Security Institutes web site at:

http://nsi.org/Library/Compsec/computerlaw/statelaws.html. The plethora of enactment of recent laws and regulations in the area of digital information is repeated in most countries around the world. Cyber legislation in specific countries is also being copied. The Australian Cyber Crime Act 2001 is based on the UK Computer Misuse act 1990. This is now being extended to cover a number of Pacific Islands (Angelo, 2009).

At an international level there are a number of organisations involved with initiatives related to computer crime and the collection of digital evidence. In an extract from the American law Library entitled 'Computer Crime – International Initiatives it is noted that

> "The Council of Europe (COE), an international organization with more than forty member countries, has been at the forefront in promoting international cooperation regarding computer crime. Mutual assistance in the investigation of cybercrime is also a discussion topic of the Group of Eight (G-8) countries (United States, United Kingdom, France, Germany, Italy, Canada, Japan, and Russia). In May 1998, the G-8 countries adopted a set of principles and an action plan to combat computer crimes.
>
> Other international initiatives also have considered computer-related issues. For example, consumer protection policies have been formulated through the Organization for Economic Co-operation and Development ("OECD"). Computer crime issues have also been discussed in international forums such as the Vienna International Child Pornography Conference. Additionally, the United Nations produced a manual on the prevention and control of computer related crime. The manual stresses the need for international cooperation and global action." (Computer Crime - International Initiatives

http://law.jrank.org/pages/699/Computer-Crime-International-initiatives.html#ixzz0YaCGzpRa)

February 2010 saw a conference entitled 'The First International Conference on Technical and Legal Aspects of the e-Society' this will be run by International Academy, Research and Industry Association (IARIA) They note on their web site that "There is a need for harmonization between national laws for a new era of eDemocracy." (http://www.iaria.org/conferences2010/CYBERLAWS10.html).

2.5 SUMMARY OF ISSUES

As can be seen from the review of the literature there are multiple factors impacting on the movement of Digital evidence across international borders. The factors range from the highly technical to the highly legalistic. Table 2.1 gives a summary of the main factors under each of the 4 primary sections within the literature review.

There are also multiple bodies identified as having 'an interest' in a number of these issues. These range from Individual law enforcement bodies through commercial companies to State legislative bodies. This overlapping of interests adds further to the complexity of the acceptance of Digital evidence.

The 16 Factors identified in Table 2.1 will form the basis for further research. Each issue needs to be analysed in detail and current methods for dealing with the factor and its component issues analysed.

Table 2.1: Factors affecting Digital Evidence crossing International Borders

Technical • Increasing capacity of modern drives • Emerging digital devices • Potential volatility of Digital Evidence • Displaying Digital evidence on paper may not be possible
Chain of Custody and Transportation • Lack of internationally agreed image format • Competing Commercial image formats • No agreed digital evidence verification standard
Standards, Qualifications and Certification • Digital Forensics is a new profession • Domestic standards driven by law enforcement • Limited specific academic qualifications available • Vendor based certification
Legal Issues • Issue is Real, Here and Now • Digital evidence has no substance shape or format. • E-Crime may be multi- jurisdictional • Different countries are legislating at different speeds • Admissibility of evidence is usually the responsibility of an independent judge.

2.6 CONCLUSION

This chapter contains a review of the literature covering the main factors affecting the movement of digital evidence across international borders. It considers the factors from both a technical and legal perspective. These factors together will

influence if digital evidence collected in one country may be accepted in a second country. Of note during the course of the review was how rapidly information in the area of digital forensics becomes out of date for both investigators and prosecutors.

The main finding in the technical portion of the chapter regarded the continued rapid developments. This covered both the development in the digital forensic tools and the development in the digital information devices from which evidence might need to be collected. There are also the development of specialist areas within the digital forensics domain area such as network forensics and small scale device forensics. The main finding in the legal section noted the early guidelines being produced by mainly law enforcement organisations. This has been followed by the development of domestic legislation covering cyber-crime, e-crime and the consequential need for digital evidence standards. While the number of academic courses covering digital forensics is increasing, there remains little international acceptance of accreditation for either labs or digital forensic investigators. There is now some maturing in the area of standards with the work of the International Standards Organisation. However, any harmonisation of legal issues to do with e-crime are still in the early stages.

The next chapter will identify the research methods to be used to investigate the factors in general and the in-depth review of a case study involving digital evidence crossing international borders.

Chapter 3

Methodology

3.0 INTRODUCTION

"If we knew what we were doing we wouldn't call it Research" (attributed to Albert Einstein).

As is seen from Chapter 2, the area of Digital Forensics is evolving from both a technical and legal acceptance perspective. These two areas do not, however, seem to be evolving at the same speed. The difference in the pace is further emphasised at an international level by the different speeds at which individual countries enact their own cyber laws.

The purpose of this chapter is to define the research question and also a methodology for the investigation of that question. As has been seen, this is a relatively new but fast evolving area. There are several human and technical factors interacting to add to the complexity.

The chapter will detail a methodology to analyse the subject area and identify the main issues affecting the transfer of digital evidence across international borders. This chapter comprises five sections. Section 3.1 is a review of five similar types of research approaches. The approach taken by each of the studies to the research methodology has been reviewed. Section 3.2 looks at refining the research question and a hypothesis for the solution of that question. Section 3.3 looks at the detailed research design model and plan. Section 3.4 identifies the data collection method and also the details on how the data will be analysed. This section also includes a data map summarising the data collection and analysis process. Section 3.5 forecasts the outcomes of the study based on the literature currently available.

3.1 REVIEW OF PREVIOUS RESEARCH

Although the area of digital evidence and the issues of it moving across international borders is relatively new, studies of similar areas have been undertaken in the past. In the following sections five studies in the IT area have been reviewed. In each study, the focus concentrates on how the research was conducted, the approach taken to each phase of the study and the outcomes achieved. The section concludes with a short critical analysis of the value of the research conducted.

3.1.1 An ICT Governance Case Study

In referring to the case study approach taken, Tavalea (2009, p.29) notes that:

"According to Benbasat, Goldstein,and Mead (1987, cited in De Haes & Van Grembergen, 2005), case study methodology is suitable for research in ICT fields because researchers always fall behind practitioners in ICT fields in finding out new methods and ideas"

The researcher identified three methods of collecting data - unstructured interviews, document collection and diary recording.

The unstructured interviews were conducted within a single organisation. The target population was executive management and senior ICT staff within the organisation. The interviews were recorded for later transcription. Specific documents were collected which related to the area of interest. Diary recording was also undertaken to preserve ad-hoc comments and observations during the process.

The researcher noted the main 'issues and challenges' as being the inordinate amount of time to gain ethics approval from AUT and the complexity of gaining approval from the authorities in Tonga where the interviews were to be conducted. Interruptions during the interviews were also noted as a distraction.

The outcomes amounted to ten interviews, the retrieval of six documents and the completion of a diary book. From these resources the author was able to draw a number of conclusions regarding the research question.

The research method proved positive in an area with several overlapping factors that blended both technology and people. It was also noted that it is an evolving area of endeavour which adds to the complexity.

3.1.2 The Evolution of Global Intellectual Property

The research question looked at the issues surrounding the evolution of global intellectual property rights. It focused on one single country. The approach taken by Nasir (2008) to the above question was to take two views of the research question. These views were described as a legal humanistics and a case study approach.

Legal humanistics is described as "a method of legal interpretation of a phenomenon while taking into account the considerable social and intellectual surrounding debates." (Nasir, 2008, p.12).

The case study approach was described as:

> "This case study was helpful in developing an in-depth analysis and examination of the policy and policy-making institutions related to Intellectual Property Rights (IPRs) in the third world setting" (Nasir, 2008, p.13)

The researcher also goes on to note the usefulness of the case study approach and that "It helps the novices and equally experienced researchers due to its general design which is "best represented by a funnel." (Nasir, 2008, p.15). Interviews were to be conducted for the case study. It was noted that while the intention had been to record interviews, concerns about privacy and security lead to a change and the interviews were recorded on paper.

Several interviews were conducted with mainly government officials in an overseas country. This twin track approach of legal humanistic and case study to the methodology allowed the researcher to arrive at a number of conclusions regarding the research question.

3.1.3 Security Policy and Forensic Data Collection

In this study the research question concerned the impact of security policy on the collection of forensic data following an incident in an organisation. In his paper Smith (2009) states that "Because digital forensics is a relatively new field, scholarly knowledge is growing and existing cases appear to be available for research and analysis". This lead to a Case study approach in his investigation of the impact of written security policies on the collection of Digital forensics" (Smith, 2003, p.53).

The approach taken to the research was the semi-structured interviews of business units or organisations of large corporate entities.

It was noted that:

> "A semi-structured interview methodology was used for each interview. The questions presented a general guideline to ensure topics are covered while allowing for in depth follow-up as the interview progresses". (Smith, 2009, p.58).

Interviews were conducted with fifteen staff from various organisations. The interviews were taped and then transcribed. The researcher was able to identify two major themes in the response to the research question, based around policy education and first responder expertise.

The case study approach taken was in response to the observation that the practice is running ahead of the scholarly knowledge in this area. This appears to have been confirmed by the research.

3.1.4 Developing a Proactive Digital Forensics System

In his research Ray (2007) reviewed issues relating to a proactive approach to digital forensics systems. Proactive computer forensics is described as an approach whereby processes can be monitored to detect crime at a very early stage. The majority of effort in recent years has been to enhance the capabilities in

more traditional digital forensics. This has been achieved by improved tools and the documenting of processes.

The model for his research was to survey existing systems, both digital forensic models and digital forensic systems. The results of this research were supplemented by a review of some of the basic processes in relation to the windows operating systems in particular. In conclusion a statistical model was developed. The author notes that a statistical model is at the heart of any proactive digital forensics model.

This survey and review approach works well for this proof-of-concept type of research question in an area where established systems can be reviewed and evaluated.

3.1.5 Digital Crime and Investigations Trends

In this paper the researcher is looking at the trends in digital crime investigation, particularly in relation to law enforcement. The purpose of the study is largely exploratory in nature. The researcher states the method to be: "The researcher uses participant observation, a survey, comparison to prior research, and personal interviews to study digital crime Trends" (Murff, 2007, p. 39).

The researcher notes the limitation of the survey approach in particular. She states that there are three main failings in the survey approach (a) surveys can be considered artificial, (b) the use of closed-ended questions and (c) under-reporting due to questionnaires not being returned.

The approach to the research question was seen as having been a success. The output was, in effect, a baseline study of the trends in digital crime in relation to law enforcement.

The findings also seemed to confirm the difficulties of the survey approach. This would seem to be particularly the case if the target participants in the survey are busy senior experts in their field.

3.2 RESEARCH QUESTION AND HYPOTHISES

In defining the research question the results of the literature search in chapter two need to be reviewed. Chapter two paragraph 2.1 noted that the area of Digital Forensics is a new and growing area ((Caloyannides, el al., 2009). This immaturity of the digital forensics profession brings with it many challenges.

Chapter two therefore identified four main areas that encompass the factors that will influence that acceptance of digital evidence that has crossed international borders. The areas were identified as Technical, Chain of Custody, Qualifications/Standards/Certifications, and Legal. Table 2.1 goes on to suggest the 16 main factors that would influence the transfer of digital evidence across international borders. Each of these factors offers considerable complexity in its own right and could offer up many research questions. However as noted by (Harvey, 2003) issues of evidence are real and hear and now.

By way of example of the complexity, in paragraph 2.4 the legal issues were explored. It was noted that in relation to the complexity of forensic analysis in cyber space that

> "The legal challenges for forensic analysis in cyber-space include:
>
> global liability issues;
> jurisdiction – based issues;
> risk issues;
> data and document retention issues;
> response and regulatory issues;
> independence, objectivity and expertise issues;
> commercialization issues;
> regulatory and investigation issues; and
> human rights issues"(Wilson, 2008, p. 3).

This clearly demonstrates that under the legal heading alone there will be many factors that affect the acceptance of digital evidence.

The final test of digital forensic evidence is usually the acceptance of the evidence by a court. The acceptance of the evidence by a court, and the weight that will be given to this evidence, relates to the evidence and the quality of the expert witness giving the evidence As the purpose of the research is to take a holistic approach to the success of digital evidence that that has been transferred across international borders it is necessary to take a high level view of all of those factors. It is recognised that each factor may represent one or more issues all requiring different solutions. The dictionary definition of the word factor states that it is 'A circumstance that contributes to a result'. The result being considered in relation to this research is the success of presenting digital evidence that has crossed international borders.

The research question therefore needs to identify the main factors that will influence the acceptance of the digital evidence and it is defined as:

What Factors Influence the Acceptance of Digital Evidence Across International Borders?

3.2.1 Solution Hypothesis

The United Nations recognises 192 countries around the world. There are also a number of territories and colonies. Each of these countries has national laws and legal systems. Within each of these legal systems are different levels of courts e.g. within New Zealand there are Supreme Courts, High Courts, District Courts and also specialist courts such as the Land Court and Employment Court. Each of these courts may have a different evidential standard. Within each of the legal systems there are several judges with typically a high degree of autonomy to accept evidence within their court.

It should also be noted that within many countries there is a strict division between the executive and judicial systems. This independence of the judiciary is a cornerstone of the structure of many countries.

The researcher hypothesises that the volume, complexity and pace of change of these issues will make the achievement of fully implemented standards difficult to

attain. What may be achieved, however, are international best practice standards in this area which serve to inform judges as to the accuracy and integrity of evidence being presented.

Perhaps a practical approach to this problem would be to 'agree to what can be agreed to' in the first instance and evolve these guidelines over time. This evolutionary approach would be based on the outcome from real world cases. There is some support for this approach within the legal profession as case law is often cited in the absence of codified laws in an area. This is a 'time honoured' approach within the legal profession for dealing with novel questions of law in proceedings.

The draft 27037 ISO standards are probably the most advanced and internationally acceptable emerging standards in this area. The draft is to be considered at the end of 2010 and may become an agreed standard at that time.

Following the literature review detailed in chapter two a list of the hypothesis main Factors influencing digital evidence crossing international borders was suggested. This list detailed in Table 2.1.

3.3 RESEARCH METHOD AND DESIGN

As can be seen from Figure 2.1, the main factors of digital evidence crossing international borders can be grouped into four main areas, Technical, Chain of Custody and Transportation, Standards and Legal. No single professional is likely to have a complete understanding of all these areas. It is therefore necessary to sample a range of views on these Factors.

A case study approach involving Interviews, Document Collection and Diary Recording therefore seems the most appropriate approach to the research.

It is recognized that case study is different from other approaches and has strengths and weaknesses. Case study is weighted towards a qualitative approach whereas a survey is considered to be a quantitative approach (Collis and Hussey, 2003).

The study will involve the collection of information from a number of professionals in both the technical and legal areas. Following the review the literature detailed in chapter 2 and the review of the 5 similar approached research projects in section 3.1 the decided methods for collecting the data will involve interviews, document collection and diary recording.

3.3.1 Case Study

The researcher prefers an interpretive perspective so that the full scope of the problem area may be considered. The professional experiences of people in the case context are investigated and can be reported as evidential to the research concern (Cavana, Delahaye, and Sekaran, 2001; Collis and Hussey, 2003). A case study is to be constructed from interviews and secondary case data. Case study can be defined as the intensive study of a single case where the purpose of the study is to be able to generalize a theory to a population of cases (Gerring, 2007). According to Yin (2003, cited in Dul and Hak, 2008), "a case study is an empirical enquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between object of study and context are not clearly evident". Similarly, Collis and Hussey (2003) define case study to be an extensive study of a single instance of a phenomenon of interest. Collis and Hussey also refer case study as exploratory research. Dul and Hak (2008) simplifies the definition of case study to be a study of a single case or multiple cases in its real life situation and analyze data that are obtained from these cases qualitatively. Case study is an example of qualitative methodology from an interpretive paradigm. Case refers to an individual which can be a group, family, class, office, institution, industry, or profession (Gillham, 2000). Yin (1994, cited in Collin and Hussey, 2003) identifies the following characteristics of case study research:

> to explore certain phenomena and understand them within a particular context;

to conduct the research without a preset of questions and notions about the limits within which the study will take place; and

to use multiple methods for collecting data which can be both qualitative and quantitative.

The case study selected will be based on its profile, relevancy to remote data collection and the availability of secondary data sources.

3.4 DATA COLLECTION

The primary data collection method will be an unstructured interview. This will be supported by document collection and diary recording. According to Collis and Hussey (2003), interview and archive searching are common data collection methods for case studies.

3.4.1 Unstructured interviews

Six to eight interviews each of 30 - 60 minutes duration are planned. The interviews will ascertain the views of stakeholders on the problem areas of IT and the technical and legal transfer of digital evidence across international borders. To structure and focus the research, one international case that has already been adjudicated will be selected. Those interviewed may not have been involved in the case but are capable of discussing the problem area of remote digital evidence collection, analysis and presentation from their own experience.

Unstructured interviews will be conducted with professionals involved in the digital forensic investigation processes. Collis and Hussey (2003) state that unstructured interviews are likely to be open-ended and probes can be used to explore answers in more depth.

Gillham (2000) uses the term ‘elite interview’ (he also notes that this term is out of favour because it has inegalitarian connotations). It might better be described as Expert Interviewing. All of the individuals to be interviewed will be experts in their field. Gillham (2000) describes the special features of this type of interview as:

> " 1. They will know more about the Topic and the setting than you do; To a large extent they will tell you what questions you should be asking, what you need to know.
>
> 2. By virtue of their authority and experience they will have their own structuring of their knowledge. They will not tamely submit to being interviewed where you direct a series of questions at them
>
> 3. The best you can hope for is that you will raise topics that they will respond to.
>
> 4. Where they can be particularly informative is where (and what) documents and records are to be found; other people you should particularly speak to; what you can and cannot expect to be able to do.
>
> 5. They will expect to have some control over what you do, and will usually demand a level of accountability and reporting back. If you can accept that, they, in return, can be important facilitators". (Gillham 2000, p64)

3.4.1.1 Conduct of the Interviewer

The researcher, and consequently the interviewer for this study, has been involved in computer forensics for fourteen years, has undertaken several international cases and is recognised by the New Zealand courts as an 'Expert Witness'. This situation will have both advantages and risks regarding the interview process.

The advantages will include:

- Depth of knowledge in the subject area.
- Professional relationship with a number of the interviewees.
- Direct experience in the movement of digital evidence across international borders.

The above advantages will assist in obtaining the interviews, establishing trust with the interviewees and in understanding the subject material.

The risks will involve the interviewer projecting personal views or experience to the detriment of the views of the interviewees. This risk will to a large extent be mitigated by the expert status of the interviewees.

3.4.1.2 Unstructured Interview

Unstructured interviews allow the interviewees to talk freely and openly about the research topic with some guidance from the researcher. Collin and Hussey (2003) also suggest that unstructured interview is a good approach to collect qualitative data. Gillham (2000) states that the benefit of interview is the 'richness' of communication. There are three main components to the interview: selection of interviewees, preparing interviews, and conducting the interviews.

3.4.1.3 Selection of Interviewees

As has been detailed in Figure 2.1,the main factors will cover two main professional areas, technical and legal. The Interviewees will be selected on the basis of expertise in the area and direct experience of digital evidence crossing international borders. There is also a distinction between public and private organisations. Under the legal systems of most countries, public organisations will take the lead on criminal cases while private organisations will take the lead on civil cases. The above is a generalisation and there are exceptions.

In several jurisdictions there are some distinctions between the two types of case in relation to the burden of proof. Consider the New Zealand legal system definitions.

Civil cases – balance of probabilities.

Criminal cases – beyond a reasonable doubt.

While from a purely technical standpoint there should be no difference in terms of the presentation of digital evidence, the higher threshold applied in criminal cases may make a difference to the acceptability of digital evidence being presented.

The mix of interviewees will therefore include representations from both the public and private sectors as well as from a technical and legal perspective.

3.4.1.4 Interview Preparation

According to Gillham (2000), there are three main elements of interview preparation. These are interview practice, development of interview topics and questions, and the interview rehearsal. Based on these elements the following approach to the interviews has been developed.

Interview practice will be undertaken to develop the interview. This will ensure that the researcher is familiar with the key topics, prompts and probes necessary for conducting a successful unstructured interview.. In addition, practice will ensure that the interview has the correct flow and retains focus on the research topic. In focusing the interview on the research topic the following items will be identified:

Five to ten open questions will be identified.

A number of prompts will be identified to remind the interviewee about a particular topic.

Probes will be used to encourage interviewees to provide more information on a topic.

The type and use of each question is an important issue. Table 3.1 (Collis & Hussey, 2009, p.145) gives a good example of the types of questions to be asked and the advantages and disadvantages of each type of question.

The interview will be rehearsed in advance. This rehearsal of the interview will help to refine both questions and probes and the style and pace of the interviewer.

Table 3.1. Types of Interview Questions

(Collis & Hussey, 2009, p.145)

Type of Question	**Useful for**	**Not Useful for**
Open Question (e.g. Tell me what happened when...)	Most opening to explore and gather broad information	Very talkative people
Closed questions (what do you consult?)	Getting Factual information	Getting broad information
Multiple questions (more than one in a sentence)	Never useful	Never Useful
Probes (e.g. What happened next ?)	Establishing sequence of events or gathering details	Exploring sensitive events
Hypothetical question (e.g. What might happen that could change your opinion)	Encouraging broader thinking	Situations beyond the Interviewees scope
Comparison question (e.g. do you prefer weekly or fortnightly team meetings)	Exploring needs and values	Unrealistic alternatives
Summary question (e.g. So, am I right in thinking the main issues are...?)	Avoiding ambiguity, validating data and linking answers	Premature or frequent use

3.4.1.5 Recording the Interview

A digital recorder will be used to record the interviews. The recorder has the capability to play, pause, rewind and fast forward and these functions will be used when appropriate. The researcher can press play at the start of the interview and pause the recorder for interruptions such as urgent phone calls, meetings or any other interruptions. Rewind and fast forward can be used to listen to the interview more than once for better interview analysis or to generate more interview points.

The digital recorder will be placed appropriately so that the device can record the conversation of all participants during the interview clearly. For example, the digital recorder can be placed on a table where the interview participants are seated.

3.4.2 Document Collection

Interview alone is not sufficient for data collection. However, relevant documents to this research from the case will be copied and collected for analysis and also be used to verify or clarify some of the points in the interviews. The guiding case for discussion (the secondary data) will be sourced from library and online documents. Documents will also be collected as evidence for this research. Documents will be sorted by category or similar aspect such as organization structure charts and procedure documentation.

3.4.3 Diary Recording

Collis and Hussey (2009) state that diary recording is a good method for collecting qualitative data. The diary is a book which will be used by the researcher to record daily events or issues that may arise during the research in relation to what people do, think and feel which may contribute to the research topic. The diary may also be used to record informal observations, conversations and media references.

3.4.4 Analysis

After collecting data from interviews, documents, and diary recording, they will be analyzed rigorously to find out answers for the research question and also generate some theories for further research.

3.4.4.1 Interview Analysis

The audio recording for each interview will be transcribed following each recording to a separate word processed document. Audio recording is highly recommended for such interviews as they can be replayed many times to capture all aspects from the interviews.

While transcribing, the identity of the speaker will be recorded. The transcribing tool which will be used is Microsoft Word. This process will be done

for each interview and each interview transcription will be saved as a unique filename on the researcher's computer.

A second copy of each transcription will then be made by removing all speech from the interviewer. This will leave copies of the interview with only the words of the interviewee for analysis as detailed below. By undertaking this process, accurate comparisons between each interview on the number of occasions keywords and phrases are used will be possible.

Thematic analysis is one of the methods for analyzing data that will be collected from the interviews. According to Braun and Clarke (2006), thematic analysis is a method for identifying and analyzing themes in the data. Boyatzis believes that thematic analysis is a tool that can be used across different methods. Ryan and Bernard (2000), cited in Braun and Clarke (2006) suggest that thematic coding is a process that is used within qualitative methodology, i.e. grounded theory. Gillham (2000) details a manual process for thematic analysis. With some amendment for this study this analysis would be represented as:

> Take each interview transcript in turn.
>
> Review each one and highlight substantive statements that make a point. Ignore repetitions, digressions, and other irrelevant statements.
>
> Highlight similar statements if they stand out to make a point.
>
> Take a break frequently when necessary to stay motivated instead of becoming dulled.
>
> Revise the transcripts again and the highlighted statements to ensure that you are not missing anything important.
>
> Go through the transcripts and assign appropriate codes for the highlighted substantive statements such as code "STANDARD" for highlighted substantive statement "referring to a documented standard".
>
> Go back to the beginning of the transcript and start deriving a set of categories of themes from the highlighted statements.

Sort these categories and look for any similarities in themes or substantive statements that can be combined.

Go through the transcript again and assign the highlighted substantive statements according to relevant categories. Mark unmatched substantive statements with a question mark and categorize them after assigning the matched highlighted statements.

Create an analysis grid with the theme categories as column headers and substantive statements as row headers. The corresponding cell will be a tick or consist of what the respondents said in the interview.

Transform this analysis grid into writing to describe any relationship, substantive issues, and themes found from the interviews.

3.4.4.2 Interview Analysis Software Tool

There are several textual analysis software packages on the market. There are also two primary digital forensic software packages Encase and FTK that contain the same sophisticated textual analysis features. The researcher has had many years of experience in the use of both of these software packages and holds advanced certification in the use of each.

After reviewing both of these packages, the researcher considers that the FTK software from Access Data Inc. is most suited to the purpose of the thematic analysis of the interview transcripts. FTK forensic software from Access Data Inc. is one of the preeminent software packages for the analysis and report production of digital evidence. This software will be used to conduct the thematic analysis.

The software uses sophisticated indexing and searching methods. Included in the searching algorithms is the ability to undertake searches using Fuzzy Logic, Phonic, Stemming and Synonyms.

It is expected that the stemming option will be of most use allowing for a word such as 'Format' to be searched and returning all derivatives such as Formats, Formatting, Formatted.

This, together with the ability to identify the most common words and phrases used, will allow a thorough comparison of the responses from each interviewee. The software also displays each keyword found and the immediate text around the keyword. This will allow for the immediate identification if a keyword is in context in relation to the issue being analysed at that time.

As a first step, the number of instances of keywords relating to the hypothesised 16 main factors influencing the transfers of digital evidence across international borders will be identified. This will give a broad indication of the number of times that the topic has been raised. Each sentence containing a keyword ‘hit’ will then be reviewed. Sentences that add context or amplification of the point being made will then be extracted and reproduced in the findings chapter.

The second stage will be to review the transcript for issues that are not identified in the above 16 hypothesised factors. The keyword hits and significant sentences for these issues will then be extracted.

While the researcher recognises that this may be a 'novel' use of the forensic software tool it is believed that all of the functionality required is present. A summary of the effectiveness of the FTK tool in the thematic analysis process will be included in the final chapter of the report.

3.4.4.3 Document Analysis

As digital evidence and the international movement of it is a relatively new and fast moving area, the primary method of collecting data for this study is the interviews. A secondary method is document analysis. The process to be used for the document analysis will be from the literature review to identify a small number of key documents that are relevant to the research area.

These documents will then be reviewed in detail in the following manner.

Review each document and highlight statements that support the ones from the interview

Use coding to code highlighted substantive statements.

Compare the results of the interviews with the substantive statements in the documents.

Re-analyse the interviews for any support for substantive statements made in the documents.

3.4.4.4 Diary Analysis

At the conclusion of the interview analysis regarding the 16 hypothesised main issues, the diary will be reviewed in the following manner:

Review for any items that have not been covered by the 16 Main issues identified.

Re-analysise the interview transcripts for information regarding the new item.

Report the findings for any supported issue that is identified.

In this manner any issues of note that have occurred at any time during the study will be identified and additional analysis of the interviews can be conducted.

3.4.5 Data Map

Table 3.2 is a data map of the research model. It gives a summary, in tabular form, of the research question and the subsequent flow of information during the course of the research The map resolves the main issue area into four areas for data collection These are Technical, Legal, Process Integrity and Expert Witness credibility.

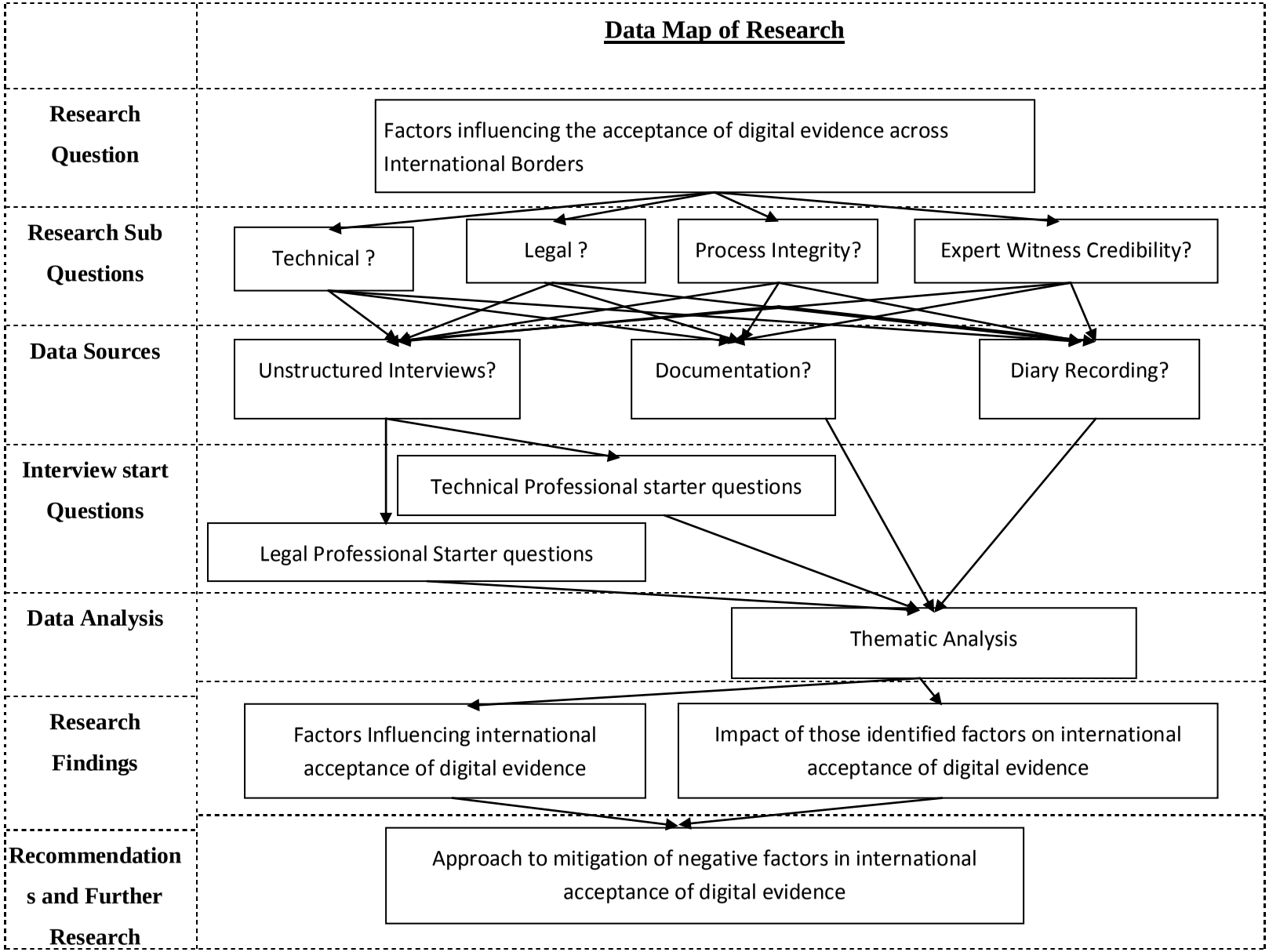

Figure 3.1: Data Map of Research

3.5 FORECAST OUTCOMES

Table 2.1 identified four categories of issues affecting the transfer of digital evidence across international borders. These are Technical, Chain of Custody and Transportation, Standards/Qualifications/Certifications and Legal Issues. Within these four heading 16 specific issues are identified.

It is expected that each of the 16 factors will be noted by one or more of the interviewees in relation to the case study. It is also expected that the focus of the interviewees on the categories is likely to depend on their specialist area - technical or legal.

Digital evidence follows a standard process consisting of four sequential phases. The phases are shown in Figure 3.2. The phases of Preservation, Analysis and Presentation can be repeated if necessary but are dependent on the Acquisition phase. If the processes and technologies used in the Acquisition phase are not robust then all other phases can be challenged. For this reason, it is expected that the importance of the acquisition phase will be emphasised in the study.

It is also expected that other factors will be identified by the interviewees

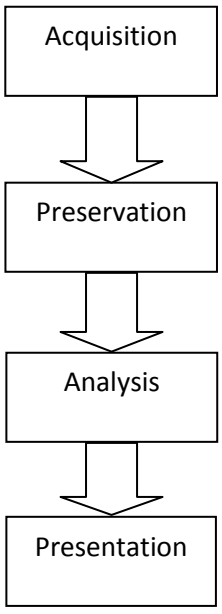

Figure 3.2 Digital Evidence Flow

3.5.1 Limitations

The study will have several limitations. A number of the limitations are typical of a case study approach and several are unique to this research.

3.5.1.1 Case Study Approach Limitations

The qualitative nature of the analysis means that a balance must be drawn between obtaining enough views and perspectives on the issues versus overloading with too much information.

Although it is believed that six to eight interviews will strike the correct balance, the comprehensiveness of the responses will not be known until the interviews are conducted.

There is no definitive method for the analysis of qualitative data. All methods considered rely to some extent on the understanding of the subject matter by the researcher.

3.5.1.2 Limitations Specific to the Subject Matter

The research question is quite broad. It also spans two professional areas that are not natural 'bedfellows'. To this end the results may be influenced by the number of specialists from each group that are interviewed. It would be reasonable to assume that if all legal professionals were interviewed, the results are less likely to highlight the issues in the technical area. To this end it is proposed to attempt to interview an even number of specialists from each area i.e. approximately four technical professionals and four legal professionals.

As a small country, New Zealand may not have the volume of cases involving the transfer of digital evidence across international borders, as e.g. Australia or USA. This in turn will limit the number of professionals within New Zealand with expertise in this area.

3.6 CONCLUSION

The purpose of this chapter was to define the methodology to be used in the research. This has been achieved by reviewing five research papers with similarities to the research to be conducted. This has lead to a refinement of the research question and the hypothesis that the research is meant to explore. A detailed research model has been created. The expected outcomes have then been expressed; these will be used at a later stage to compare against the results of the research. Finally, the limitations of the research method have been explored. These cover both the inherent issues from a case study approach that generates qualitative data to some specific limitations in the topic area.

The main output of the chapter is the detailed method which will be used to conduct the research. As a rapidly developing area of endeavour from both a legal and technical perspective, it is recognised that practice is likely to be running ahead of research in this area. As such a case study approach has been adopted. The output from this case study approach will involve mainly qualitative data. A detailed approach to the analysis of the qualitative data has been outlined.

The research will now be conducted as outlined in this chapter. Chapter 4 will detail the results of the interviews, documents and diary notes taken. The results of the analysis of that data will also be shown.

Chapter 4
Data Capture and Analysis

4.0 INTRODUCTION

In the previous chapter a methodology for the collection and analysis of the data was defined. The primary method of data collection was identified as unstructured interviews. This would be supplemented by document analysis of relevant material and the keeping of a diary of notable events.

This chapter reports the seven interviews conducted as findings. The chapter goes on to analyse and compare the content of those interviews and identify common themes and statements. The second area of findings are the documents that have been reviewed that are seen as most relevant to the research questions. The third area of information concern the items of note that have been recorded in a diary during the life of the research project.

Section 4.1 outlines the major challenges and issues faced in collecting the data in this study. Section 4.2 details the number and volume of information collected during the interviews and also the reasons that the anonymity of the interviewees must be maintained. Section 4.3 discusses the documents collected during the research and identifies the main documents influencing the research topic internationally. The items of note that have been recorded in the diary maintained during the project are detailed in Section 4.4. Section 4.5 shows the findings from the interviews in relation to the 16 main hypothesised factors. Section 4.6 details the findings regarding additional main issues regarding digital evidence crossing international borders that were identified and were not part of the 16 hypothesised factors. The conclusion of the chapter is given in Section 4.7.

4.1 CHALLENGES AND ISSUES FACED IN DATA COLLECTION

There were several challenges and issues faced in the collection of data in this study. These have been classified below.

4.1.1 Breadth of Subject

This is a very broad subject and is an issue in every country in the world. The United Nations recognises 192 countries. All of these countries have their own legal system with different types of judges and different rules regarding the admissibility of evidence. No study could hope to cover every jurisdiction in detail. The study, therefore, will indicate trends and issues seen predominantly from a New Zealand perspective.

4.1.2 Technical and Legal Views

The subject is encompassed by two main professions, the IT technical profession and the legal profession. As might be expected, the tendency of the professionals interviewed was for them to comment more on the issues that related more closely to their profession. These two views from the professional groups tend to give a stereoscopic view of the subject in its entirety. This study brings that stereoscopic view into a single 'focused' view.

4.1.3 Number of Interviewees and Volume of Data

As the method used was unstructured interviews, a balance has to be struck between the number of interviews conducted and the volume of data those interviews will produce and will then have to be analysed. There is no scientifically agreed method for the analysis of unstructured interviews. The method taken builds on the mainly manual method of thematic inspection outlined in Chapter 3 and uses modern software to extract 'themes' in relation to issues raised by the interviewees.

4.2 DETAILS OF INTERVIEWS

Seven interviews were conducted in total. Each interview was recorded on a digital voice recorder. Of the seven interviews, three were with technical experts and four with practicing lawyers. Of the lawyers, two were specialists in

Employment Law, one was a Commercial Law specialist, and one a Criminal Prosecutor

.

4.2.1 Anonymity of Interviewees

Several of the interviewees work as part of large corporate organisations. In order to ascertain the professional views of each interviewee, and not compromise any potential corporate conflict of interest with their organisation, the identity of all interviewees will remain anonymous. While it would be preferable for the transcripts of the interviews to be included with this report, this is not practical as a number of the interviewees would be readily identifiable from their interview transcript. Therefore the digital recordings of the interviews and the transcripts will remain confidential to the author of this thesis and the academic supervisor. Where necessary in the report, the interviewees will be identified as I1 to I7.

4.2.2 Details of Each Interview

As each interview was digitally recorded the total time for each interview is available. Each interview has then been transcribed. In order to allow for more accurate analysis of words and phrases, the interviewer's words have then been removed from the transcripts to produce a second copy of the transcript containing only the words of the interviewees. Table 4.1 shows the metrics of all of the interviews conducted.

Table 4.1: Details of Interviews conducted

Interviewee	**Total Interview time in Minutes and Seconds**	**Number of words spoken by Interviewee**
I1	19:24	1,339
I2	65:27	8,083
I3	27:46	2,285
I4	56:53	6,777
I5	23:22	2,274
I6	17:57	1,696
I7	29:29	2,902
Total	240.18	25,356
Average	34:20	3,622

4.3 DOCUMENTS COLLECTED FOR DETAILED ANALYSIS

During the course of the literature review undertaken as part of this project, a large number of documents and references were made. Three main documents were identified as being most significant in answering the questions posed within the thesis. They are available internationally and detail the collection, handling and transmission of digital evidence.

The documents are:

1. ACPO Good practice guide for computer based electronic evidence. Wilkinson , S (undated)
2. Forensic Examination of Digital Evidence: A guide for Law Enforcement. Ashcroft, J. (2004).
3. Guidelines for the Best Practice in the Forensic Examination of Digital Technology. IOEC. (2002).

Documents 1 and 2 are guides produced by national law enforcement organisations. The first is from the UK-based Association of Chief Police Officers and the second is From the US Department of Justice.

The third document is by an organisation, the IOEC (International Organisation on Computer Evidence). This organisation is an international forum for Law Enforcement agencies and produces guidelines and templates in the area of digital evidence.

Although there are several local law enforcement guidelines available from a number of countries, the above three are among the more substantial in this area. These guidelines are likely to influence the emerging ISO standard in the area of Digital evidence. ISO/IEC 27037 (2009) -- IT Security -- Security techniques -- Guidelines for identification, collection and/or acquisition and preservation of digital evidence which is currently in the drafting stage.

The documents were analysed as detailed in Chapter 3. All the documents have the status of guideline. As such they are all broadly in agreement regarding the general stages of a digital forensic investigation. The analysis of the documents has focus on those items that impact on the international transfer of digital evidence. Details of the findings from the three documents are shown below.

4.3.1 International Standards

A single reference was found to international standards in the ACPO guide. Within the introduction (p.4), it is stated regarding the guide that 'They are consistent with the principles adopted by the G8 Lyon group as a basis for international standards'

4.3.2 Transfer of Evidence

The IOEC guide (p 11) and the DoJ Guide (p 12) make the similar statement "Activity related to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved and available for review'.

4.3.3 Jurisdiction

The ACPO guide (p 15) noted that 'Consider also the possibility of a computer's access to remote online storage, which may physically reside in a foreign jurisdiction. There will be legal issues in relation to accessing any such material Legal advice should be sought prior to any access retrieval'. The IOEC guide (p 18) notes that ' The style and content of written reports must meet the requirements of the criminal justice system for the country of Jurisdiction.

4.4 DIARY RECORDED ITEMS OF NOTE

A diary was maintained during the course of the study. The diary was used for two main purposes. Firstly to note issues raised during the interviews which were outside the scope of the 16 hypothesised main factors. These could later be analysed to see if the views were expressed by more than one interviewee. The second purpose of the diary was to collect other information that might be considered of interest during the course of the thesis preparation.

4.4.1 Cost of Implementing ISO standards

One interviewee commented that the cost of implementing the ISO standards in digital evidence might be an impediment to their wider acceptance.

4.4.2 Cloud Computing

It was commented on by one of the interviewees that the advent of cloud computing could have a significant impact on the issue of the cross-border collection of digital evidence.

4.4.3 Jurisdiction

Also noted by one interviewee was that jurisdiction is normally based on presence rather than nationality. This point is of note as e-crime is very often committed across international borders and physical location is of very limited significance in committing e-crime.

4.5 FINDINGS FROM INTERVIEWS RE THE HYPOTHESISED FACTORS

Table 2.1 in Chapter 3 summarised the hypothesised 16 main factors facing the transfer of digital evidence across international borders. Each of these factor areas has been analysed using the process detailed in Chapter 3. In summary, this process involves searching on keywords relating to each factor. The stemming option was used in the search software to ensure all instances of a word are identified, for example the word Format will also report instances of Formats, Formatting, Formatted etc. The sentence containing each word is then reviewed to ascertain if it is relevant to the issue under consideration. Any relevant sentences are 'carved' from the transcript and reported in the results.

Table 4.2 is an index of the results found for each identified factor area. This index table is followed by a Table for each of the 16 hypothesised factor area. each results table contains a Lists of the key words that were used in the FTK software to identify key issues across all of the 7 interview transcripts. This is followed by a list of the number of times that keyword was present across the transcripts. The final column is a list of the keywords that were found in context. This is important as a key word can easily give a 'false positive' response if it is out of context in relation to the factors being searched.

Table 4.2: Index of Results Tables for 16 Identified Factors

Technical
Table 4.3 - Increasing capacity of modern drives
Table 4.4 - Emerging digital devices
Table 4.5 - Potential volatility of Digital Evidence
Table 4.6 - Displaying Digital evidence on paper may not be possible
Chain of Custody and Transportation
Table 4.7 - Lack of internationally-agreed image format
Table 4.8 - Competing Commercial image formats
Table 4.9 - No agreed digital evidence verification standard
Standards, Qualifications and Certification
Table 4.10 - Digital Forensics is a new profession
Table 4.11 - Domestic standards driven by law enforcement
Table 4.12 - Limited specific academic qualifications available
Table 4.13 – Vendor-based certification
Legal Issues
Table 4.14 - Issue is Real, Here and Now
Table 4.15 - Digital evidence has no substance shape or format.
Table 4.16 - E-Crime may be multi- jurisdictional
Table 4.17 - Different countries are legislating at different speeds
Table 4.18 - Admissibility of evidence is usually the responsibility of an independent judge.

4.5.1 Increasing Capacity of Modern Drives

The issue identified was that the increasing capacity of modern computer drives causes significant problems in the acquisition of digital evidence. As can be seen in Table 4.3, this is supported by two comments from the interviews. The comments reference the necessity to forensically image multiple terabytes of data.

Table 4.3 Findings - Increasing Capacity of Modern Drives

Keywords	Hits	Hits in context
Capacity	0	0
Drive	38	1
Disk	13	0
Storage	11	2
Terabytes	2	2

Key Sentences

Massively. Both myself and my offsider, well one of our scene kits, just for us here in Auckland, we each carry six terabytes.

We're regularly coming back from jobs with six/seven terabytes of data, because we're regularly encountering corporate level server structures that we're having to image.

4.5.2 Emerging Digital Devices

This factor regarded the complexity attached to collecting evidence from emerging digital devices. It was supported by one of the interview comments which is shown in Table 4.4 overleaf.

Table 4.4 Findings - Emerging Digital Devices

Keywords	Hits	Hits in context
Phone	2	0
Tablet	0	0
Ipod	0	0
Device	26	2

Key Sentences

However, hat's off to Apple and what they've done recently. I think more people should be having a look at their skills around the Apple OS, and if there is any certification that people need to do, because more and more we' re going to have devices that have Mac OS on it.

4.5.3 Potential Volatility of Digital Evidence

Digital evidence can be static as on a computer hard drive or volatile as when data is held in Random Access Memory (RAM). The comment in Table 4.5 supports this as an issue and comments regarding the response needed when imaging live systems.

Table 4.5 Findings - Potential volatility of Digital Evidence

Keywords	**Hits**	**Hits in context**
Volatility	0	0
Digital evidence	4	0
Fragile	0	0
Live	6	3
Key Sentences If you're not applying live response techniques to a server infrastructure, then the FTK imager approach is your last resort.		

4.5.4 Displaying Digital Evidence On Paper May Not Be Possible

Digital information can be designed specifically to be to be displayed on digital devices e.g. multi-page wide spreadsheets, video recordings etc. While evidence has traditionally been presented in court in verbal or written format, some modern evidence must be produced in digital format. As can be seen in Table 4.6 none of the interviewees commented on this being an issue.

Table 4.6 Findings - Displaying Digital Evidence on Paper May not be Possible

Keywords	Hits	Hits in context
Report	8	0
Display	0	0
Video	0	0
Spreadsheet	0	0
Paper	8	0
Key Sentences (no results found)		

4.5.5 Lack of Internationally Agreed Image Format

The collection of digital evidence is predominantly undertaken by the production of a forensic image. This factor relates to the lack of an internationally-agreed format in this area and suggests this could be an issue when digital evidence is moved across international borders. Table 4.7 shows that seven comments were made on this topic during the course of the interviews.

Table 4.7 Findings - Lack of Internationally Agreed Image Format

Keywords	Hits	Hits in context
International	28	0
Image	57	5
Format	23	13
EO1	0	0
Clone	0	0
DD	10	8
Smart	0	0

Key Sentences

I'm actually personally experiencing a regression in digital formats. I'm finding more and more that I am imaging into DD format.

Whereas with an expert witness file image, you've got your 32 bit CRCs, so it's cyclically checking every sector.

The one I use mainly is the DD image. I find it's very compatible with a lot of different tools I use when I'm examining the image, and it's not proprietary at all. But as long as it's a common image type that can be – it can be reacquired into a different image type if required, I don't see it being a problem. A lot of people still like the EnCase E01 image type.

No, I don't think it's an issue. And I don't think we need to even try for a particular format to be the only standard. I think the tools that have the market share will dictate the image formats, and they're gonna be developing future formats that are compatible.

I'm not aware of any standards in terms of digital images. I'm very sure though that if standards were imposed, I would familiarise myself with them, so I'm assuming that there aren't any in force at the moment.

So is the EnCase evidence file gonna be the future format? Probably not. Underlying all of this and it still seems to be happening all the way along through everything and staying stable, DD is still sitting there, and DD format is still in use widely across the world. All of the forensic tools support it. Most of the stand alone imaging devices utilise it, as the raw or the DD image file; it's still in that respect the fastest way of obtaining an image. And it's also the most usable format without proprietary support.

That is one of the benefits that the expert witness format does have over DD, in that it does multiple layers of verification within file format while you've got your overall value for the data set.

4.5.6 Competing Commercial Image Formats

Several digital forensic formats are proprietary to certain vendors. Chief amongst these would be the Encase forensic image format. The responses shown in Table 4.8 show that, although it is recognised that new formats will emerge, a key issue is the ability of formats to be used across multiple tools.

Table 4.8 Findings - Competing Commercial image formats

Keywords	Hits	Hits in context
Commercial	2	0
Image	57	26
Format	23	15

Key Sentences

The Expert Witness File format – it's traditionally been accepted as being a uber reliable imaging source. However you now get issues where it all really depends on which implementation of the EnCase executable has been written into an imaging tool has a direct end state effect on the reliability of the image file.

I'm actually personally experiencing a regression in digital formats. I'm finding more and more that I am imaging into DD format, and utilising tools which enable me to image into DD – purely because it gives me a more workable image.

The one I use mainly is the DD image. I find it's very compatible with a lot of different tools I use when I'm examining the image, and it's not proprietary at all.

I don't think we need to even try for a particular format to be the only standard. I think the tools that have the market share will dictate the image formats, and they're gonna be developing future formats that are compatible – certainly not proprietary, so yeah, I don't think it's an issue and I don't think i t will be an issue. The number of users out there worldwide won't want to adopt a new format that's not compatible with all the existing tools, and so I think we're fairly safe in retaining compatibility between tools.

4.5.7 No agreed Digital Evidence Verification Standard

The ability to verify the integrity of a forensic image is an important part of the process of transporting digital evidence. Table 4.9 shows seven comments on this subject. They broadly support the continued use of the MD5 hashing algorithm as the primary method for the verification of a forensic image.

Table 4.9 Findings - No agreed Digital evidence verification standard

Keywords	Hits	Hits in context
Verification	12	10
Standard	58	0
MD5	7	7
Sha	3	3

Key Sentences

I've had all sorts of less than satisfactory examples of receiving data, but ideally a verification with SHA-1 or MD5 would be fine.

I am quite happy with MD5. I have no issues at all about MD5 for verification, particularly of a file as large as an evidence file. The whole issue over breaking it is an academic issue; it's not a practical one.

That is one of the benefits that the expert witness format does have over DD, in that it does multiple layers of verification within file format

Is there a verification standard? Not really. That may change given the moves by some parties to try and get some ISO standards around digital forensics.

I'm not aware of any standards in terms of digital images. I'm very sure though that if standards were imposed, I would familiarise myself with them, so I'm assuming that there aren't any in force at the moment.

There's the big fear monger that's gone on about MD5 collisions. People forget it took six – I think it was six to 10 years in a lab.

There's still a – yet to be a verified in the wild conflict occur. So MD5 is still, for practical purposes, a useful algorithm.

4.5.8 Digital Forensics is a New Profession

Digital forensics is recognised as a new profession. Table 4.10 shows the interview responses to this issue. The responses recognise that digital forensics is an 'embryonic' profession.

Table 4.10 Findings - Digital Forensics is a New Profession

Keywords	Hits	Hits in context
Forensics	52	1
Profession	2	2

Key Sentences

There is a school of thought that says we should all be scientists, however, that said, I've– and I'm sure you have as well – experienced multiple cases of very competent computer forensic scientists or - sorry, I'll rephrase that – very competent computer scientists who couldn't find the apple on the apple tree if you got them to do a forensic data examination, because they think differently.

So I think some regulation or standardisation around the discipline if you like, of collecting that information, would assist to give that embryonic profession if you like, more credibility.

Locally, because it's such a small profession – there are so few providers – you know, we're in a fortunate position being a small jurisdiction as well, you know who the good providers are

4.5.9 Domestic Standards Driven by Law Enforcement

As law enforcement agencies in various countries were the first practitioners of digital forensics, early attempts at process documentations and guidelines have tended to be driven by these national level law enforcement agencies. Table 4.11 notes that none of the interviewees commented on this topic.

Table 4.11 Findings - Domestic Standards Driven by Law Enforcement

Keywords	Hits	Hits in context
Police	32	0
Domestic	3	0
Standards	58	0
Law	54	0
Key Sentences (No comments identified)		

4.5.10 Limited Specific Academic Qualifications Available

As a relatively new profession, digital forensics has mirrored the start of the IT profession some 40 years ago. This was dominated by a preference for practical experience as there were no widespread specific academic qualifications available. The comments noted in Table 4.12 tend to support the view that academic qualifications are likely to become more important in the digital forensics field in the future.

Table 4.12 Findings - Limited Specific Academic Qualifications Available

Keywords	Hits	Hits in context
Academic	7	0
Qualification	32	3
Degree	11	0
Masters	9	0

Key Sentences

And so like any expert witness, they have to be qualified before they can give opinion evidence on the validity of what they're talking about. But they can be qualified through their academic background and knowledge as well as their practical experience. But it would certainly assist in the credibility of the expert if they've got those sorts of credentials.

I mean the AUT course is probably the only full qualification that's available outside of law enforcement in New Zealand.

I think, realise that at the end of the day the expertise of the witness will speak for itself, because it's quite detailed, dense, complex evidence that's often being given, and it will just simply become apparent if people are not up to the job as they give their evidence. So I don't think actually that qualifications in it will become a de facto standard any time soon

4.5.11 Vendor-Based Certification

The majority of certifications available for digital forensic specialists is via vendor-based programs. In Table 4.13 there are ten views expressed on this topic which are quite varied.

Table 4.13 Findings - Vendor Based Certification.

Keywords	Hits	Hits in context
Vendor	9	8
Certification	67	17

Key Sentences

Well the first certification that was available in this field was offered by IACIS okay. And that wasn't vendor led. That was industry led by law enforcement agents who wanted a bit of paper to say they'd had some training, cos the Americans are very big on that

We were having people attending advanced courses, who met all the prerequisites, who were still intellectually challenged to drive a mouse properly, but they'd attended the courses. So that was when we conceived the idea of developing a vendor base certification.

I've never gained the certification, because it's a vendor-based certification. Yeah, I could go and get it, but do I really need to have it? Probably not. I know how to use EnCase

A vendor-based training eight years ago – is that still applicable now, 10 years on? Well, probably not.

The results or your findings should be the same regardless of which tool you use, and if someone has a certification by a particular vendor, that's great. It would show that they're proficient in their use and their understanding of how that tool works. But I wouldn't see it as a requirement to have a vendor based certification. It would be more of a 'nice to have' than a 'need to have.

So that's what led to the EnCE certification coming out. They're primarily driven out of the States, because there are certain jurisdictions in the States where if they didn't have a certification, then they weren't able to give evidence.

CFCE process is a really good process for someone who wants to get through the basics of it, however, in my opinion, the process is a little bit tarnished. I've seen guys who've attended the two week training course in Florida, purely because they're law enforcement officers and you can only get on that course if you're a serving government employee, who when they'd started the course they didn't know how to drive a mouse – within six

months of that course they're a certified CFCE.

No individual certification's really been challenged in New Zealand.

I think the SANS certification is becoming more and more recognised, primarily because it is a lot more generic.

My recommendation was – which I then pursued – was to obtain EnCase certification because that was the tool we're all using.

4.5.12 Issue is Real Here and Now

This issue revolved around the very practical nature of the presentation of digital evidence. The issue is a here and now issue and will not wait for academic research or the production of agreed standards. Table 4.14 notes that only one of the interviewees commented on this aspect.

Table 4.14 Findings - Issue is Real Here and Now

Keywords	Hits	Hits in context
Real	33	0
New	88	0
Now	45	0

Key Sentences

That's what I mean about the interface with what the New Zealand courts require versus what the local jurisdiction says you have to do in order to provide evidence that can be used overseas. So that's a practical dimension that's a real – makes life rather difficult and very expensive for a party that's trying to bring another party to justice

4.5.13 Digital Evidence has No Substance Shape or Format

This issue concerns the fact that digital evidence in its most base form is not a tangible item. People are not able to read, with their eyes, the presentation of digital evidence on a disk platter or RAM chip. This has tended, internationally, to result in differing laws regarding digital evidence admissibility being enacted in different legal jurisdictions. Table 4.15 notes a number of the views expressed by the interviewees on this subject.

Table 4.15 Findings - Digital Evidence has no Substance Shape or Format

Keywords	Hits	Hits in context
Substance	0	0
Shape	1	0
Digital Evidence	4	1
Electronic Evidence	12	4

Key Sentences

How do I see digital evidence, with respect to evidence? It's evidence.

UK and South Africa are similar, but Argentina a very different concept, where in fact it's a criminal act to look at someone else's, for example, hotmail, even if it resided on a computer owned by a company they worked for without – if you want the information seen, you need to get a judge to basically sort of look at it, so much more hamstrung by use of electronic evidence because their legal system hasn't really sort of moved to keep pace with the changing technology.

The fact that electronic data or electronic evidence is now legally classified as a thing, it's legally classified as something that data can be stolen; data is now officially recognised as evidence in New Zealand under the Evidence Act.

4.5.14 E-crime may be Multi Jurisdictional

Electronic crime known as e-crime can be multi jurisdictional. The advent of the internet has allowed easy electronic access for the average computer user to information and data throughout the world. Following on from this has been the ability for criminals to commit e-crime in distant countries. These crimes are often committed by criminals safe in the knowledge that, even if the crimes are detected, it may be impossible for law enforcement agencies to obtain a conviction in a foreign land. In the comments shown in Table 4.16 the breadth and complexity of this issue are shown.

Table 4.16 Findings - E-crime may be Multi Jurisdictional

Keywords	Hits	Hits in context
e-crime	0	0
jurisdiction	30	6
border	14	2

Key Sentences

The Australians are not subject to the jurisdiction of the New Zealand high court, and received advice that they did not have to comply with the New Zealand court order and they chose not to.

The usual principles are no, that your jurisdiction is territorial. That *you* have jurisdiction over New Zealanders – and jurisdiction is usually based upon *presence* rather than nationality.

It's about identifying in which jurisdiction the criminal activity in this case occurred.

I think the basic New Zealand position is that overseas evidence by way of affidavit needs to be sworn in a manner consistent with the country in which it's sworn. And then you get into the difficulties of ensuring that you comply with it – with the local niceties, which vary from jurisdiction to jurisdiction.

the different rules that come into play around electronic evidence in different jurisdictions.

The only other thing that would be regulatory guidelines would be any restrictions that are put under data transmission by local data protection acts. And there are some restrictions in some jurisdictions on that. Depending on the jurisdiction, they range from: you cannot transit data across the border full stop, to - it has to be protected by certain levels of encryption.

I've done quite a bit actually of cross border enforcement and the general approach is utter cooperation, because everybody understands that what we're trying to regulate is cross border and there's no way to deal with it other than pretty full cooperation. And increasingly New Zealand the regulatory agencies are signing up formal cooperation agreements with their counterparts overseas.

4.5.15 Different Countries are Legislating at Different Speeds

Legal jurisdictions around the world are legislating in relation to crimes involving digital evidence at different speeds. This disconnect in national legislation for crimes which may cross international borders is problematic. Table 4.17 show seven comments that were made regarding this topic.

Table 4.17 Findings - Different Countries are Legislating at Different Speeds

Keywords	Hits	Hits in context
Legislation	9	1
Country	44	3
Jurisdiction	30	9

Key Sentences

Japan, China, France etc. So depending on the current legislation what the rules are, their rules may state that no data stored in China should be removed from China for the purposes of investigation.

There are certain countries in the world though, that have a – it's a tighter control policy over their data

The EEC directives to comply with. And I think there's an informal schedule of countries outside Europe that Europe has informally agreed are safe havens for transmission of information, so in other words, jurisdictions which have good data protection/privacy protections in place.

The Australians are not subject to the jurisdiction of the New Zealand high court.

So one of the issues that strikes me is if the – it's about identifying in which jurisdiction the criminal activity in this case occurred.

We're much more used to our courts accepting that evidence. UK and South Africa are similar, but Argentina a very different concept, where in fact it's a criminal act to look at someone else's, for example, hotmail, even if it resided on a computer owned by a company they worked for.

if you want the information seen, you need to get a judge to basically sort of look at it, so much more hamstrung by use of electronic evidence because their legal system hasn't really sort of moved to keep pace with the changing technology.

4.5.16 Admissibility of Evidence is usually the Responsibility of an Independent Judge.

In most legal jurisdictions in the world, the admissibility of evidence is the responsibility of the presiding judge. In the absence of any legislation, case law or legal guidelines, the judge may have wide discretion regarding admissibility of evidence. Table 4.18 shows the two views that were expressed on this topic.

Table 4.18 Findings - Admissibility of Evidence is Usually the Responsibility of an Independent Judge

Keywords	Hits	Hits in context
Admissibility	3	0
Judge	14	2
Independent	45	0

Key Sentences

The High Court rules set out a code of conduct for expert witnesses, so the witness has to be qualified in terms of that. But there's no set of standards that they must meet. It's just a matter for the judge to decide whether or not the person is truly an expert.

like any expert witness, they have to be qualified before they can give opinion evidence on the validity of what they're talking about. But they can be qualified through their academic background and knowledge as well as their practical experience

4.6 ADDITIONAL IDENTIFIED FACTORS

Identification of factors not covered by the 16 hypothesised factors was also undertaken. The initial identification of these additional factors was undertaken in the following ways:

Following each interview a brief note had been made in the diary regarding any issues which were not in line with the 16 identified factors but might be worthy of further investigation.

Each transcript was read and any issues not covered by the 16 identified factors were noted in the diary. During analysis of the 16 identified factors any issues of note were also entered in the diary.

As with the analysis of the 16 identified factors, each additional factor was probed further using the keyword technique identified in Chapter 3 and summarised in Section 4.5.

One factor was identified that falls outside the scope of the 16 hypothesised factors. This factor, shown in Table 4.19, relates to the importance of academic

qualifications for a digital forensics investigator. The comments from the interviewees show that, although academic qualifications are an asset for a digital forensics investigator, a lawyer or judge will take experience into consideration also.

Table 4.19 Findings - Importance of Academic Qualifications for Digital Forensic Investigators.

Keywords	Hits	Hits in context
Academic	7	3
Degree	11	4
Masters	9	2

Key Sentences

But they can be qualified through their academic background and knowledge as well as their practical experience

So you have to combine the level of academic exercise in a degree or a master type programme, up against what technical skills they have as well, because in the role of forensic computing expert, technical skills are right up there with anything else.

I don't think you need to have a master's degree to be able to conduct computer forensics. Obviously everyone's gotta start somewhere and with the right guidance and supervision and training, I think the job can be done, and it would be dangerous to suggest someone has to be qualified in a particular way to be involved.

I don't look at particular qualifications or what degrees they have. I go largely off word of mouth, experience in dealing with people who have been involved in this area

That said, you could have a person who's got a doctorate degree who's attended one course 10 years ago, or eight years ago. Is that training now still valid?

The main thing I know though, is that these qualifications don't necessarily teach

technical – a degree or a masters. So you have to combine the level of academic exercise in a degree or a master type programme, up against what technical skills they have

Whether you had a master's in Forensic IT, for me personally, wouldn't make too much of a difference. It would be your vast experience of having been involved in this type of exercise

4.7 CONCLUSION

This chapter has reported the findings of the data collection that has been undertaken. The primary method of data collection has been the interviewing of seven professionals with knowledge in the area of digital forensics. These professionals were from both the IT and legal professions. Main documentation regarding the evolution of digital evidence procedures has also been identified. Finally, the notes made in the diary of recordings have also been referenced in order to further the analysis.

The findings from the above three areas have been documented. In the case of the interviewees, tables have been produced documenting the comments made by the interviewees for each of the 16 hypothesised main factor areas. The interview transcripts have been further reviewed and together with the diary notes have resulted in the production of an additional table documenting a main factor area not identified in the 16 hypothesised factors. A review of the major documentation has also been undertaken which has resulted in the identification of two principal documents in relation to the development of the digital forensics profession and also the transfer of digital evidence across international borders.

Chapter 5 is a discussion chapter and will comment on the findings from all sources. A critical analysis will be made of the findings and potential explanations for some of the findings will be produced. The current state of the digital forensics profession will also be discussed. This will provide informed comment regarding the impact that developments in the area of digital forensic evidence crossing international borders is likely to have on the direction of the profession. Finally, comment will be made regarding the main factors identified

as influencing digital evidence crossing international borders and how these relate to the 16 main factors that formed the hypothesis for the research.

Chapter 5
Discussion of Findings

5.0 INTRODUCTION

In Chapter 4 the results of the research were reported. The research was conducted based on the methodology detailed in Chapter 3, which followed the literature review in Chapter 2. 16 main factors were hypothesised regarding digital evidence crossing international borders.

Chapter 5 discusses the hypothesised main factors in dealing with digital evidence crossing international borders to the results of the research that has been completed. Based on this discussion, the chapter concludes with a response to the research question and details the findings regarding the main factors in dealing with digital evidence crossing international borders.

The chapter commences with Section 5.1 which is a discussion regarding each of the 16 hypothesised factors that were identified in Table 2.1. This is followed in Section 5.2 with a discussion regarding the new factors identified as a result of analysing the interviews. Section 5.3 details the main findings of the research regarding the identification of the main factors affecting the transfer of digital evidence across international borders. Section 5.4 is a comparison of the hypothesised main factors against the main factors that have been identified during the research.

5.1 DISCUSSION ON HYPOTHESISED FACTORS

The following is a discussion regarding the findings for each of the 16 hypothesised factors. At the end of each discussion is a conclusion as to whether the hypothesised factor is supported or not. In several instances the result of the discussion is that the factor is put in a revised format.

5.1.1 Factor - Increasing Capacity of Modern Drives

Table 4.3 details two responses from the interviews dealing with the issue of the capacity of modern computer hard drives. In both responses, the interviewee is commenting on the increasing difficulty in the acquisition of digital evidence caused by increasing drive capacities. It is well known amongst digital forensic practitioners that the major reduction in the cost per gigabyte of computer hard drives together with the requirement for more storage space, is resulting in ever increasing hard drives in all computers. This has resulted in significant change in the requirements relating to the amount of drive capacity to store the forensic images of those computers. The practicalities of this are that in some instances (during the execution of a search warrant is a typical instance) it may not now be practical to forensically image all drives. This is leading to a change in practice from imaging entire physical drives to previewing a drive's contents and then selectively imaging only the data from the drive considered 'most likely' to contain the evidence.

The approach of forensically imaging entire physical drives has been described in relation to the execution of a standard search warrant of a house. An analogy would be that, during the standard execution of a physical search of a house, the most accessible hiding places will be searched - cupboards, drawers, under beds. It is not typical practice to take the house apart brick by brick and look inside each brick for evidence. A forensic image of an entire physical computer hard drive allows for a search down to the bit level of all information on the drive. In future this may simply not be practical in all instances of very large drives.

As identified in the results of the research in paragraph 4.5.1 the increasing data storage capacity of digital devices is leading to a change in accepted practice by forensic practitioners. It may not now be feasible to forensically image the entire permanent storage (either mechanical drives or other storage devices) of a digital device in all cases. It is this change in accepted practice to imaging of part of a computer's hard drive, and how it is catered for in different jurisdictions,

which may affect the acceptance of the digital evidence across international borders. By way of an example, the decision of a digital forensic practitioner to forensically image only part of a computer's hard drive could be argued by either a prosecution or defence legal counsel as having the potential to have failed to collect important evidence. The effect of this change in practice is also likely to see the introduction of additional tools for identifying the data areas most likely to contain evidence. These areas can then be targeted for forensic imaging.

The issue of increasing capacity of modern drives in relation to the international acceptance of digital evidence could be expanded to be stated as 'Increasing drive capacities are leading to a change in current accepted practice of forensically imaging an entire drive to imaging only selected data from the drive'.

5.1.2 Factor - Emerging Digital Devices

This was supported by a comment from one of the interviewees which is detailed in Table 4.4. The comment reflects the fact that the Apple operating system is becoming more prevalent and that more forensic practitioners will require skills with this system.

Probably the most dramatic area of change in digital devices in the last five years, which is also likely to continue over the next five years, is in the mobile phone area. Indeed the devices in this space have changed to such an extent that to call them simply a mobile phone is probably an understatement. These devices now routinely contain keyboards, complex software applications and even GPS and navigational aids.

There are a multitude of highly proprietary operating systems and the move towards fewer and more open operating systems is likely to be slow as this can be in direct conflict with the commercial aspirations of the device manufacturer.

Although digital evidence taken from a mobile device is in essence the same as digital evidence taken from a computer, the manner of accessing this digital evidence is in a much more embryonic state.

The availability of rapidly developing applications to forensically image and analyse mobile phones will vary very considerably between jurisdictions. The availability of the forensic applications is in contrast to the access to the emerging devices themselves, which may be widely available. This area is likely to be an ongoing issue in terms of the digital evidence being acceptable in a second jurisdiction.

5.1.3 Factor - Potential Volatility of Digital Evidence

That this is an factor was commented on by one of the interviewees (Table 4.5). The response comments on the emerging need to apply live response to systems, especially server infrastructure.

Live response techniques have become more important as RAM within systems has changed together with developments of operating systems to make best use of this available RAM. This has resulted in significant amounts of data being held in volatile RAM. As the tendency for servers is now to run 24 by 7, certain types of information may only be available in RAM.

The access to the applications and skills required to image live systems may not be present in all jurisdictions. This can pose an issue in finding local expertise to evaluate digital evidence that may have been imported to that jurisdiction.

This factor may be better clarified as 'Techniques for the acquisition of live, volatile data are a developing area.'

5.1.4 Factor - Displaying Digital Evidence on Paper May Not be Possible

As is shown in Table 4.6, none of the interviewees considered this to be a significant issue in relation to digital evidence crossing international borders. This may have been due to the high level of sophistication of the interviewees in relation to modern computing.

Taking New Zealand as an example, the introduction of placing computer screens throughout courts remains a relatively recent occurrence. While access to

this type of IT infrastructure within courts may not be present in the majority of the countries of the world, none of the interviewees or the reviewed documentation considered this a major factor.

It is therefore reasonable to assume that this should not be considered as a major factor in the context or this report.

5.1.5 Factor - Lack of Internationally Agreed Image Format

This factor solicited significant comment from the interviewees. Table 4.7 details the seven comments made. A broad range of comments were raised in relation to the factor. In summary, they suggest that the type of forensic image chosen is not important from an evidential standpoint. Supporting this view are the statements that a regression to the DD image format appears to be occurring. This is one of the oldest and most basic of the image formats. This is in spite of the release of the more sophisticated formats being available such as the Advanced Forensic Format, Encase Formats and Expert Witness Format.

The main reason suggested is that the DD image is seen as a 'neutral' format as compared to the more sophisticated and proprietary formats available. This neutrality has lead to the majority of forensic software application being able to read DD format images.

This is a very interesting debate and demonstrates the practical nature of digital forensics in providing solutions to problems now versus the more theoretical approach of developing an agreed international standard for forensic image formats that contain all of the more sophisticated attributes of security, embedded metrics and error checking. The reality is that a digital forensic practitioner may need to view forensic images in a variety of different applications from different vendors depending on what is required. This could be in relation to expanding a compound file, reading a specific database or retrieving passwords.

The broad acceptance of the DD image may see it accepted as a de-facto standard across different jurisdictions. Should an alternative image format be

proposed, such as in the emerging ISO digital forensic standards, then the wider acceptance of this standard may well be dependent on the breadth of support for it within the competing forensic software applications and the wider digital forensics community.

Perversely, the lack of an international standard image format at present may actually be an advantage as any of the widely used image formats is likely to be acceptable in another country. If an international standard format was adopted acquisitions made using a different format may be less acceptable in court.

As such it would seem that the lack of an internationally agreed forensic image format is not a major issue.

5.1.6 Factor - Competing Commercial Image Formats

Four comments were made regarding this subject which are shown in Table 4.8. The comments are similar to the comments made in the previous section.

The Encase standard from Guidance Software was for many years the de-facto standard for forensic images, especially among law enforcement agencies. While this is a proprietary image format that has been revised on many occasions, a large number of forensic software applications have the ability to read the Encase format.

Seeing the advantage gained by Guidance Software from having a widely accepted forensic image format, other software vendors have endeavoured to release their own formats, albeit for specific instances of forensic images. These include AccessData's logical image format and an image format from Paraben Forensics.

It would seem that the factor 'Lack of internationally agreed image format' and the factor ‘Competing Commercial image formats' are closely linked factors. However, neither issue would seem to be significant in terms of digital evidence being accepted across international borders

5.1.7 Factor - No Agreed Digital Evidence Verification Standard

The ability to verify the integrity of a forensic image is an important part of the process of transporting digital evidence. Table 4.9 shows seven comments on this subject made by the interviewees.

The responses support the MD5 (Message-Digest algorithm 5) hash standard as well as the stronger SHA (Secure Hash algorithm) standard. It is noted in one comment that there has been one compromise in the laboratory of a MD5 hashed document. However, the perception was that is a lab-based academic breach rather than a practical breach.

In reality there are a number of well documented compromises of the MD5 hashing algorithm. One was shown at the 25th Chaos Communication Congress when a group of researchers showed how they had used MD5 collisions to create an intermediate authority certificate. This certificate appeared to be legitimate when checked via its MD5 hash.

It could be argued that these are not of a high significance for the digital forensic practitioner because, within digital forensics, MD5 hashing is used to verify both forensic images and files within them. For all practical purposes the ability to amend a forensic image or document and then for the MD5 value to remain unchanged is impractical.

A key element in the security of moving digital evidence across international borders is the ability to verify that the information that was despatched has not been altered in transit. This is done by the use of hashing algorithms. Statements that the MD5 algorithm is insecure may provide a perception that using the algorithm to verify forensic images is also unsecure.

For this reason, several forensic software applications also provide the ability to undertake SHA hashing. This is likely to be seen as more secure and its use, especially when evidence is being moved between jurisdictions, as a more acceptable method of verification. This is an area where an international standard would certainly help to remove any doubt about which hashing algorithm should be employed.

5.1.8 Factor - Digital Forensics is a New Profession

In Table 4.10, three comments are shown regarding digital forensics being a new profession. Digital forensics in many ways mirrors the development of IT as a profession.

IT as a profession can trace its start back to the 1970s. At this time it was populated mainly by individuals with no academic qualifications or unrelated qualifications. This was because academic qualifications were not widely available. The profession was in a high growth, high demand period. There were no widely accepted specific professional bodies for IT, unlike the more established professions of engineering, law or medicine for example. In the past 30 to 40 years IT has grown as a profession with academic qualifications and professional bodies with entrance criteria, codes of conduct and requirements for ongoing professional development.

As a new profession, digital forensics has no agreed professional bodies and digital forensic practitioners very often have no academic qualifications and may be working in, or had their initial training in, law enforcement agencies. If as seems likely the digital forensics profession follows the same pattern as the wider IT profession, then the emergence of requirements for academic qualifications and membership of professional bodies is to be expected.

In the interim, the issue of digital forensics being a new profession is likely to impact on the acceptance of digital evidence moving across jurisdictions. Judges will need to make decisions on the 'expert witness' (or equivalent) status of digital forensic practitioners from other jurisdictions where the local standards for an expert witness may be significantly different. This decision is currently made more difficult by digital forensics being a new profession.

5.1.9 Factor - Domestic Standards Driven by Law Enforcement

This issue relates to the fact that, to date within the digital forensics profession, the standards have been driven by law enforcement agencies. These standards are in fact all labelled as guidelines. Of the three documents that were considered

most influential in this area and are detailed in Section 4.3, two are produced by law enforcement agencies and the third is produced by an international committee whose membership is made up predominantly of law enforcement officials.

Table 4.11 shows that none of the interviewees considered this to be an issue in relation to digital evidence crossing international borders.

Within New Zealand well in excess of 95% of digital forensic practitioners are either based in law enforcement agencies or are working in the private sector but have had a law enforcement background in digital forensics. While figures for other countries are not available, it is reasonable to suggest that they would follow a similar pattern to New Zealand.

It would seem reasonable to assume that as the digital forensics profession matures, and with the advent of more advanced and specific academic qualifications being available within this area, then more practitioners without a law enforcement background are likely to emerge.

A number of judicial systems throughout the world are based on the adversarial principle. It is also the situation that in most criminal cases the prosecution is represented by an appointee of the state and the defence is represented by an individual from the private sector. It is recognised that the defence may also be funded by the state where economic circumstances would otherwise make the application of justice unfair.

It is interesting to note that in the case of the production of digital evidence, the standards/guidelines that have been developed locally within jurisdictions are almost exclusively produced by law enforcement agencies. These standards and guideline are then, in the majority of instances, implemented by individual digital forensic practitioners who either work within law enforcement or have a law enforcement background.

None of the interviewees or documentation reviewed as part of this research has raised this as an issue. However there may well be a question worthy of additional research as to whether the development of the digital forensics profession (both guidelines and implementation), to date, predominantly by law

enforcement trained officials has produced a bias towards the prosecution rather than the defence.

5.1.10 Factor - Limited Specific Academic Qualifications Available

In Table 4.12 the three comments made by the interviewees are shown. The comments support the view that only limited academic qualifications in this area are available. It is widely recognised that this situation is changing at different speeds in a number of countries as academic course become available.

The requirement for law enforcement agencies throughout the world to respond to the issue of digital evidence caused the majority of digital forensics practitioners to be employed from within law enforcement. The lack of any specific academic qualifications at the commencement of digital forensics as a profession meant that the majority of these practitioners were without a specific academic qualification.

As the early digital forensic practitioners have progressed in their careers, many have been promoted to management/supervisory positions within the profession. Coupled with the growth of academic courses relating to digital forensics, this has resulted in a position, at this stage of the development of the digital forensics profession, where Digital Forensic Managers many have very considerable experience but no an academic qualification. These managers are appointing and managing Digital Forensic practitioners who may have significant academic qualifications but very limited experience.

While the above dynamic is interesting to note, the expectation is that, over time, academic qualifications for digital forensic practitioners will become more prevalent or a requirement.

5.1.11 Factor - Vendor-Based Certification

Vendor based certification has been a fact of digital forensics since its inception. Table 4.13 details the 10 responses from the interviewees on this topic.

One of the earliest and most widely recognised of the vendor based certification is the Encase Certified Examiner (EnCE). Most suppliers of digital forensic software offer some form of certification in its use. This will usually involve attendance at training courses run by the vendor and some form of ongoing commitments to training with the vendor. During the early stages of the development of digital forensics, these certifications provided a degree of conformation that a digital forensics practitioner had some skill in the use of a specific tool and some understandings of the fundamentals of digital forensics. The profession was called Computer Forensics at this time and it is only in the relatively recent past that the more accepted term has become Digital Forensics.

There are a number of non-vendor based certifications in existence. One of the major ones mentioned by the interviewees is the certified Forensic Computer Examiner (CFCE) offered by the International Association of Computer Investigative Specialists (IACIS). Membership of this organisation has to date been limited to current and past members of law enforcement organisations. In 2010 the membership voted to open the membership more widely but would place additional, as yet unspecified, criteria on members from outside law enforcement. At the time of this research, these criteria have not been finalised. This law enforcement bias may limit the acceptance of the certification outside of the law enforcement community.

Another non-vendor based certification noted by the interviewees was the SANS Institute certification. This is the Certified Forensic Analyst (GCFAs) certification. SANS (which stands for SysAdmin, Audit, Network, Security) was established in 1989 as a cooperative research and education organisation.

There are a number of these non-vendor based certifications available across a number of local and international organisations. None at this stage can be said to have gained major acceptance across the whole digital forensic profession. All however have something to offer.

Although vendor based certification in digital forensics can be criticised as a commercial offering from the vendor in order to sell training courses, any

certification in digital forensics, especially in the absence of specific academic qualifications in the area has to be better than none.

While the issue that was hypothesised was that vendor based certification was an issue in relation to digital evidence crossing international borders, the research would seem to suggest that the issue might be more broadly stated as 'The number of competing vendor and non vendor certifications available in the digital forensics space may cause more confusion than clarity in the eyes of a judge or legal professional trying to establish the expertise of a digital forensic practitioner'.

5.1.12 Factor - Issue is Real Here and Now

This issue attempted to express the practical problem that the issue of the acceptance of digital evidence is a here and now problem. Table 4.14 details a single opinion from one of the interviewees on this area. The point comments on the requirements of New Zealand courts regarding evidence and that the requirement from overseas courts could be different.

Digital forensic practices have evolved over the last 10 to 20 years and they continue to evolve as technology evolves. The movement of digital evidence across international borders has also grown and will continue to grow with wider penetration internationally of the internet and the growth in e-commerce. But the question faced by a judge in a court case today regarding the admissibility of evidence from an external jurisdiction requires a decision today.

In the absence of internationally agreed standards, or certification for digital forensic practitioners, judges and legal professionals will make decisions based on the best information they have and the rules regarding the admissibility of evidence within their jurisdiction. The interviews and documentation do not support this as a main issue.

5.1.13 Factor - Digital Evidence has No Substance Shape or Format

Three comments were made regarding this topic and are shown in Table 4.15. Two comments reflect the fact that digital evidence is now specifically recognised under New Zealand law. The third comment concerns the significant difference between how digital evidence is treated under New Zealand law and the Argentinean legal system.

Several countries have initiated legislation to clarify the position and admissibility of digital evidence. One of the issues in a 'connected world' is that if the sovereign laws are not harmonised then digital evidence from one jurisdiction regarding a crime in a second jurisdiction may not be admissible.

This requirement for new legislation to classify digital evidence comes about because the class of digital evidence does not fit into any of the existing classes. As such it poses a significant issue in the movement of digital evidence across international borders.

The issue might be more clearly defined 'As digital evidence has no substance shape or format, countries are enacting new laws to deal with it'. This, therefore, is not considered to be an issue on its own but may form part of the issue to do with the enactment of e-crime legislation detailed in Section 5.1.14.

5.1.14 Factor - E-crime may be Multi Jurisdictional

The advent of the internet has allowed easy electronic access for the average computer user to information and data throughout the world. Table 4.16 details seven responses from the interviewees on this topic. In addition, the ACPO Guide (p.15) comments that remote storage in foreign jurisdictions can pose difficulties in acquiring evidence.

Of note in one of the comments is that 'jurisdiction is usually based upon presence rather than nationality'. This has been a basic tenant of sovereign laws. The advent of the internet however moves outside this definition. Individuals will often now not know in which country the server, which holds the information they

are viewing, is located. This indifference to physical presence makes the jurisdictional questions around e-crime much more complex to agree.

The growth in e-crime is likely to continue as penetration of the internet throughout the world grows and with it the increasing uptake of e-commerce.

5.1.15 Factor - Different Countries are Legislating at Different Speeds

Table 4.17 lists the seven comments made by the interviewees on this topic. The comments recognise the different speeds and approaches being taken by different countries to enact laws relating to digital evidence .

Of note are also the references to Data Protection and Privacy Acts. These laws, which will often prohibit the transfer of personal information outside the borders of the country, can have the effect of hindering the transfer of digital evidence. There are also laws to protect a countries sovereignty issues such as currently in China where the export of electronic data for the purposes of an investigation is specifically prohibited. This has resulted in a number of organisations working in the digital forensics space having to open offices in China in order to carry out digital forensic investigations in that country.

There are also differences between laws in countries that can cause problems to an investigation spanning borders. For example, in New Zealand any information an employee creates on a company's computer can be viewed by the company, whether it is considered private or not. In Argentina, however, viewing an employee's private information, such as a hotmail email, on a company's computer would be considered a criminal act.

While is could reasonably be argued that it is very common to find different laws in different countries what causes an issue with digital evidence in this respect is that the nature of the information and the activities of the individual can cross borders with complete ease.

5.1.16 Factor - Admissibility of Evidence is Usually the Responsibility of an Independent Judge.

As noted by (Siegel, 2006) in most legal jurisdictions in the world, the admissibility of evidence is the responsibility of the presiding judge . In the absence of any legislation, case law or legal guidelines, the judge may have wide discretion regarding admissibility of evidence. Two comments are made in Table 4.18 regarding this issue.

The independence of the judiciary in a country is a cornerstone of the legal system in many countries. Indeed in many countries the distribution of authority between the executive, legislative and legal arms of the state is a documented and basic principle.

It is often described as the role of the judiciary to interpret the laws of the state. Within this framework, judges can have considerable powers of discretion on the admissibility of evidence.

This situation was noted by one of the interviewees when discussing expert witness status within New Zealand courts and is noted in Table 4,18.

> ‘The High Court rules set out a code of conduct for expert witnesses, so the witness has to be qualified in terms of that. But there’s no set of standards that they must meet. It’s just a matter for the judge to decide whether or not the person is truly an expert'.

While international standards for digital evidence may be created, such as the emerging ISO/IEC 27037, they will in most, if not all instances, be used as a 'good practice guide' by judges who will decide on the admissibility of digital evidence or, in the cases of many countries, the acceptance of a digital forensic practitioner as an expert witness. This situation differs markedly, for example, with an international standard on telecommunications where member countries will sign up to agreed detailed standards in order to be able to transfer telephone calls in and out of their country.

While the international standards on digital evidence may not have the definitive acceptance and implementation of other standards of a more engineering flavour, they will give judges a benchmark on which to base

decisions regarding digital evidence issues. Table 4.7 supports this point when it was noted by one of the legal interviewees regarding digital evidence standards that:

> 'I'm not aware of any standards in terms of digital images. I'm very sure though that if standards were imposed, I would familiarise myself with them, so I'm assuming that there aren't any in force at the moment'

As standards develop judges might well feel less inclined to admit digital evidence from a foreign jurisdiction, if that jurisdiction had adopted the ISO digital evidence standard, but the digital forensic practitioner had not complied with that standard in the collection storage and analysis of that evidence.

This remains a highly complex issue for digital evidence. The completion of an international standard in this area will be a major step forward regarding digital evidence moving between countries in particular.

5.2 DISCUSSION ON ADDITIONAL IDENTIFIED FACTOR

As part of the thematic analysis of the interview transcripts described in paragraph 3.4.4.2. one additional factor, to the 16 hypothesised factors, was identified. This additional factor involving academic qualifications is discussed in the following paragraph.

5.2.1 Factor - Importance of Academic Qualifications for Digital Forensic Investigators

The issue that was identified related to the fact that qualifications are not currently a prerequisite in order to practice digital forensics. Table 4.19 lists the seven comments that were made by the interviewees on this topic.

The comments note the importance of practical experience for a digital forensics practitioner. That both prospective employers and the courts will take considerable note of a practitioners experience in their deliberations, comment is

also made that academic qualifications do not necessarily teach the technical skills required to practice digital forensics.

It could be argued that this is a transitional issue and perspective for digital forensics practitioners. Paragraph 4.5.10 notes that specific academic qualifications have not been available until relatively recently, digital forensic practitioners on the whole have not had these qualifications. The courts and employers with a 'here and now' requirement have relied to a large extent on experience. As discussed in paragraph 4.5.11, certifications because of either being vendor based or not well recognised, have been of limited assistance in assessing the ability of the practitioner in the field.

In contrast, if one considers the situation of a Medical Pathologist it would be almost unthinkable that a court would admit evidence regarding an autopsy from someone who was not a qualified doctor. At some point in history, before medical qualifications were available, no doubt the expertise of unqualified practitioners would have been sought.

The advent of more numerous digital forensic academic qualifications will undoubtedly raise the standards of digital forensics as a profession. As the profession matures in each country, it would seem highly likely that the importance of a specific academic qualification in the digital forensics field will become a requirement for attaining recognition by a court as an expert witness. As the process regarding a medical doctor’s qualifications has developed over many centuries, it may be reasonable to assume the similar process for digital forensic practitioners may take several decades or longer

This poses an interesting question regarding the previously identified issues of lack of specific digital forensics academic qualifications. Are the courses offering the qualification not there because the courts (and employers) are not demanding them? Or are the courts and employers not demanding academic qualifications because they are not widely available. Time will undoubtedly answer this supply and demand question.

In relation to digital evidence crossing international borders, the issue that will face judges will be a complex balancing act between the typical academic qualifications and experience of a digital forensics practitioner in the country submitting the evidence and the typical academic qualifications and experience of a digital forensics practitioner in the country in which the evidence is going to be heard.

This transitional issue regarding qualifications for digital forensic practitioners will change at different paces in different countries. It will be a difficult issue to 'codify' in any emerging international standards or any international certifications that are established.

The issue of foreign digital forensics practitioners and academic qualifications might be better clarified as ' The prevalence of relevant academic qualifications amongst digital forensic professionals will vary considerably from country to country'

The practical outcome of this issue could be clarified as ' In establishing the credentials of a digital forensics practitioner a judge or legal professional may need to take into account the prevalence of academic qualifications amongst digital forensic professionals in the country in which the practitioner works'.

5.3 THE MAIN FACTORS AFFECTING THE TRANSFER OF DIGITAL EVIDENCE ACROSS INTERNATIONAL BORDERS

Based on the literature search in Chapter 2, the research methodology in Chapter 3, the results of the research in Chapter 4 and the discussion in Chapter 5, Table 5.1 is a summary of what are considered to be the main factors affecting digital evidence crossing international borders. This summary table is followed by a table for each factor. These tables contain a statement regarding the impact of the factor and a series of bullet points covering the resolution areas which may provide the solution to the factor from an international perspective.

Table 5.1 Main Factors Affecting Digital Evidence Crossing International Borders

Factor Number	Factor
1	Increasing digital device capacities
2	Emerging digital devices
3	Acquisition of live (volatile) data is a developing area
4	No agreed digital evidence verification standard
5	Digital forensics is a new profession
6	Lack of specific academic qualifications
7	International variations in the importance of digital forensic academic qualifications to courts and employers
8	The number of competing vendor and non-vendor certifications available.
9	Laws covering e-crime are country based while the crime can be international
10	Different countries are legislating regarding e-crime at different speeds.
11	Admissibility of evidence is usually the responsibility of an independent judge

Table 5.2 Factor - Increasing Digital Device Capacities

Impact	Resolution areas
Increasing digital device capacities are leading to a change in the current accepted practice of typically forensically imaging an entire physical drive to one of imaging only selected data from the drive. This discretion on the part of the digital forensic practitioner during the acquisition process will be questioned by legal professionals.	• Emerging best practice procedures • Documentation regarding decision process on the part of the digital forensic practitioner • Emerging international standards

Table 5.3 Factor - Emerging Digital Devices

Impact	Resolution Areas
Forensic software lags behind device development. Access to this software may vary considerably between countries.	• Increasing access to digital forensic applications • International cooperation between jurisdictions in the joint investigation of an e-crime if expertise is not available in one of the jurisdictions

Table 5.4 Factor - Acquisition of Live (volatile) data are a Developing Area

Impact	Resolution Areas
Techniques for the acquisition of live (volatile) data are a developing area. This is likely to cause a more pronounced imbalance of expertise between jurisdictions than might otherwise be the case.	• Increasing access to live acquisition tools and expertise • International cooperation between jurisdictions in the joint investigation of an e-crime if expertise is not available in one of the jurisdictions

Table 5.5 Factor - No Agreed Digital Evidence Verification Standard

Impact	Resolution Areas
The integrity of digital evidence transferred between jurisdictions can be questioned	• Availability of unquestioned verification algorithms in digital forensics applications • A single 'open' international standard for the verification of digital evidence would provide transparency and certainty when digital evidence was moved between jurisdictions

Table 5.6 Factor - Digital forensics is a New Profession

Impact	Resolution Areas
As a new profession digital forensics is not widely understood. Standards certifications and qualifications are all emerging areas and will take time to establish themselves internationally	• Continuation in the development of professional standards. • Wider understanding of digital forensics within the legal profession

Table 5.7 Factor - Lack of Specific Academic Qualifications

Impact	Resolution Areas
Lack of specific academic qualifications will hinder the development of digital forensics as an accepted profession. Legal professionals are not able to demand academic qualifications because of a lack of digital forensic practitioners holding the qualifications. This situation makes it more difficult for judges to conclude on the expert witness status of a foreign digital forensics practitioner.	• Increasing number of specific academic qualifications available internationally • Greater weight given in the digital forensics profession and legal community to academic qualifications

Table 5.8 Factor - International Variations in the Importance of Digital Forensic Academic Qualifications to Courts and Employers

Impact	Resolution Areas
As academic qualifications become more available, courts are more likely to take them into account when deciding on the expertise of a witness and the admissibility of the evidence which they are presenting.	• More widely available digital forensics academic qualifications • Judges taking into account the availability of digital forensics academic qualification in a foreign jurisdiction

Table 5.9 Factor - The Number of Competing Vendor and Non-vendor Certifications Available

Impact	Resolution Areas
The number of certifications, both vendor and non-vendor based makes it difficult for both members of the digital forensics profession and the legal community to evaluate these certifications when making decisions about the expertise of a digital forensics practitioner	• Defining the certifications into training certifications and professional certifications • Rationalisation of the number of certifications available leading to a wider recognition of fewer certifications

Table 5.10 Factor - Laws Covering E-crime are Country Based While the Crime can be International

Impact	Resolution Areas
Growth in the volume and complexity of e-crime would seem inevitable with worldwide growth in the internet. To a large extent physical borders between countries are meaningless to an internet user. This growth will lead to increasing demands on the digital forensic profession.	• Increase in volume of digital forensic practitioners • Increasing the quality of digital forensic practitioners • Increase the ability of legal professionals to assess the expertise of a digital forensics professional from an overseas jurisdiction

Table 5.11 Factor - Different Countries are Legislating Regarding E-crime at Different Speeds

Impact	Resolution Areas
Differences in national laws can impact on the harmonisation of the collection and presentation of digital evidence. The speed at which countries are legislating in this area can cause difficulties when the crime crosses the border.	• International harmonisation of laws regarding e-crime • Cooperation between law enforcement agencies in different countries in e-crime investigations • Agreed international standards on issues to do with digital evidence

Table 5.12 Factor - Admissibility of Evidence is Usually the Responsibility of an Independent Judge

Impact	Resolution Areas
In most jurisdictions judges have a high degree of autonomy within their court regarding the admissibility of digital evidence. This can naturally produce variances within a country and even more so between countries.	• Increasing ability of legal professionals to quantify the expertise of a digital forensics professional from an overseas jurisdiction. • Development of international standards in digital evidence issues to 'guide' judges in making decisions on the admissibility of digital evidence from a foreign jurisdiction

5.4 COMPARISON OF HYPOTHESIESED FACTORS AND IDENTIFIED FACTORS.

Table 2.1 identified the 16 hypothesised factors in relation to the research question of the main issues in regarding digital evidence crossing international borders. Following the discussion in this chapter these has been reviewed and refined. Of the 16 hypothesised factors, 10 were supported, some with minor revisions to the way the factor is worded. Six factors were not supported and have been discarded. One additional factor has been

added this is listed as number 7 in table 5.1. This has resulted in 11 main factors being identified and these are summarised in Table 5.1. Table 5.13 maps the initial Hypothesised factors to the factors identified following the research.

Table 5.13: Comparison of Hypothesised Factors Against Finding of Research

Hypothesised factors	**Research outcome**	**New factor number table 5.1**
Increasing capacity of modern drives	Supported	1
Emerging digital devices	Supported	2
Potential volatility of Digital Evidence	Supported	3
Displaying Digital evidence on paper may not be possible	Not-supported	
Lack of internationally-agreed image format	Not-Supported	
Competing Commercial image formats	Not-Supported	
No agreed digital evidence verification standard	Supported	4
Digital Forensics is a new profession	Supported	5
Domestic standards driven by law enforcement	Not-Supported	
Limited specific academic qualifications available	Supported	6
Vendor-based certification	supported	8
Issue is Real, Here and Now	Not-Supported	
Digital evidence has no substance shape or format.	Not Supported	
E-Crime may be multi- jurisdictional	Supported	9
Different countries are legislating at different speeds	Supported	10
Admissibility of evidence is usually the responsibility of an independent judge.	Supported	11

5.5 CONCLUSION

In this chapter the results of the findings in Chapter 4 have been discussed. This has been undertaken by reviewing the 16 hypothesised main factors concerning digital evidence crossing international borders identified, as detailed in Table 2.1. To this has been added the additional factor that was identified after the review of the interviews and identified in three main documents on this subject.

As a result of the discussion in this chapter, six of the hypothesised factors were discarded as not being supported by the research as qualifying as main factors in this area. 10 of the hypothesised factors were supported by the research and one additional factor was identified. This has resulted in the identification of 11 main factors relating to the transfer of digital evidence across international borders. These are summarised in Table 5.1. Tables 5.2 to 5.12 show more detail about each of these factors and note the areas that may hold the resolutions for some of these factors.

Chapter 6 is the concluding chapter of the thesis and will review the effectiveness of the research and the identified strengths and weaknesses of the research model and techniques used. A brief review of the use of FTK software from Access Data in the thematic analysis of unstructured interviews will also be included. The chapter will conclude with recommendations for further research in this area.

Chapter 6
Conclusion

6.0 INTRODUCTION

In Chapter 1 it is noted that the growth in access to the internet is leading to a growth in e-crime. This has occurred as the technology revolution has impacted to a greater or lesser extent on every country throughout the world. Access to the internet and the adoption of e-commerce continues to grow. This new dynamic in communication and undertaking business has naturally seen a growth in the individuals who would exploit it for criminal purposes.

In the past few decades law enforcement agencies have had to developed skills and procedures to deal with the investigation of e-crime and the associated collection of digital evidence. Running alongside this effort has been the development of laws within countries to try and define this new class of offending and clarify the factors around the acceptance of digital evidence in courts.

In addition to these substantial challenges, the complexity of the offending across international jurisdictions has added to the difficulties. As an example Maritime Law and Air Transport laws are two major areas that deal with cross border issues. In both areas considerable responsibility is often vested in the captain of the ship to uphold the laws, The internet on the other hand has no captain, and the speed and size of the worldwide population 'travelling' on the internet is a very new dynamic.

The concluding chapter of thesis will look in Section 6.1 at the learnings gained form undertaking this research. Section 6.2 will look at the limitations of conducting the research. Future potential research topics in the area of digital forensics crossing international borders are discussed in Section 6.3. Finally, Section 6.4 identifies the main research findings and outlines those individuals and groups who may find the research of some assistance.

6.1 LEARNINGS FROM RESEARCH

As noted in Chapter 1, this research was sparked by the researcher being faced with a very real issue during the execution of a search warrant. The question regarded the acquisition of potential evidence , via a company's network link, of data located in a second country. The question this raised was ‘Would the action of acquiring this data from a foreign country be considered legal in the local and remote countries?’ Failure to acquire the data at that time would more than likely have resulted in the data being deleted. Accessing computer systems and copying information without authorisation is a criminal offence in many countries. The learnings from the research cover a number of areas which are detailed below.

6.1.1 Pace of Technological Change

The pace of technological change continues and is likely to continue to run ahead of the digital forensics tools and practices. The practical result of this is that there will continue to be variances between countries as access to newly emerging tools and practices for the acquisition of digital evidence from emerging technologies will always vary. This will lead to the need for judges and legal professionals to evaluate the expertise of overseas digital forensics practitioners who may be using tools and techniques not available in their own country.

6.1.2 The Maturing of the Digital Forensics Profession

The digital forensics profession is in the process of maturing in the same way that the IT profession has matured over the last 40 years. This maturing will involve increasing numbers within the profession. Those individuals are more likely to have specific academic qualifications and more internationally recognised certifications from professional bodies. As the profession matures it should become easier for judges to be able to evaluate the expertise of digital forensic practitioners form a foreign jurisdiction. This should assist in the transfer of digital evidence across international borders.

6.1.3 International Standards and Independent Judiciaries

There is a conflict between the 'scientific/engineering' approach to introduce international standards in the acquisition, analysis and presentation of digital evidence with the international practice of an independent judiciary.

While international standards, can to a great extent be mandatory, in areas such as telecommunications the interaction within the digital evidence issue between the technical aspect and the legal aspect is likely to result in any international standards being viewed as guidelines by Judges and members of the legal profession. These guidelines will however provide judges with an international baseline on which to make decisions around the admissibility of digital evidence or the expert status of a foreign based digital forensics practitioner.

6.1.4 Cross Border Acquisition of Digital Evidence

While the technical tools are available to allow for the cross border acquisition of digital evidence, this area is fraught with legal issues. These issues start with the question of whether the digital forensic practitioner is authorised to collect the evidence. This authority needs to be applicable both in the country they are working from and in the country where the digital evidence is located, the remote location. In countries around the world, laws such as Privacy Acts, Data Protection Acts and Computer Misuse Acts are emerging. Although these are being put in place for valid reasons, they can restrict the ability to collect digital evidence remotely. Legal professionals in one country cannot be expected to have a full knowledge of all laws, including emerging laws, in a second country. This may result in the requirement to undertake legal consultation in the remote country. During the execution of a search warrant this time delay could be very problematic in terms of ensuring that evidence is not deleted.

A second area may regard the requirement in a remote location for digital forensics practitioners to hold certification or, as is required in several US states, for digital forensics practitioners (outside of law enforcement agencies) to be

registered Private Investigators. These specific requirements regarding the certification of the digital forensics practitioner must also be taken into account.

6.2 LIMITATIONS OF THE RESEARCH

As discussed in Chapter 1 the subject of the research was very broad. The subject covers technological and legal areas relating to digital forensics and both national and international laws. Paragraph 3.2 notes the decision by the researcher to take a 'Holistic' approach to the issue of Digital evidence crossing international borders and not to narrow the focus. From a practical perspective the 'acid' test of the integrity of digital evidence is when it is accepted in a court. The test is when a digital forensics practitioner is in a court with lawyers and a judge testing the admissibility of the digital evidence and the standing of the digital forensics practitioner. It would be impossible to look at just the technical side or just the legal aspects and obtain a coherent picture of the factors that are influencing the outcome. This breadth of the research question has, however, lead to a number of limitations that have been identified in the research which are discussed in this section.

6.2.1 Breadth of the Research Question

The breadth of the research question, covering the emerging technical issues of digital forensics and the emerging legal issues of e-crime and digital evidence, meant that some issues could not be researched in detail. While it is possible to make this criticism, the researcher was more intent on achieving a broad view on all of the main factors rather than an in-depth study of a single factor or set of issues. The attempt to deal with the issue in its entirety has limited the amount of time and resources that could be devoted to individual areas.

6.2.2 Topic is a Moving Target

By its nature the research has produced a 'picture in time' of the factors related to digital evidence crossing international borders. E-crime is an emerging issue

which is changing as technology and applications available on the internet change. The laws, both national and international, are also in various stages of development. Two significant areas that demonstrate this change are qualifications discussed in paragraph 5.1.10 and the fact that different countries are legislating in the area of e-crime at different speeds which is discussed in paragraph 5.1.15.

6.2.3 Topic Spans Two Very Different Professional Areas

The topic spans the two very different professional areas of IT and Law. IT is a relatively new profession; the digital forensics discipline within it is even newer. It is also, to a very large extent, an unregulated profession. The legal profession on the other hand has centuries of development behind it and is a highly regulated profession. It would seem unlikely at this stage in the development of digital forensics that any single person would have a detailed knowledge of both professions. As was mentioned in an earlier chapter, this tends to produce a single view of the issues depending on the professional group of the individual being interviewed. The research has attempted to bring these two views together to produce a single view and set of factors covering the whole problem area.

6.2.4 Variations in Legal Systems of Different Countries

The United Nations currently has 192 member countries plus several dominions and independent states. Each of these countries has their own legal system. Within each of these legal systems there are usually several different types of courts e.g. Criminal, Civil, Employment, High Courts and Supreme Courts etc. The term judge has been used throughout the thesis to describe the head of the court. In some instances a religious figure, one or more lay people or indeed several judges may be in charge of the court. This produces considerable variations between the courts in different countries. It was outside the scope of this research to produce a summary of the court systems in each country. It has therefore been necessary to generalise about the term judge and court.

6.2.5 All Interviews Conducted in New Zealand

While the literature review was able draw on literature from around the world the practicalities of the research meant that all interviews were conducted in New Zealand. This naturally puts a New Zealand perspective on the responses. The laws within New Zealand are to a large extent based on British laws which means that the majority of experience of the interviewees is based around the New Zealand/British legal system.

6.3 FUTURE RESEARCH OPPORTUNITIES

Such an evolving and important area as digital forensics will provide considerable scope for research in the future. As has been commented on in the discussions regarding qualifications in paragraph 5.1.10, there has been very limited specific qualifications available until recently. This has meant that very little academic research has been completed in the area of digital evidence traversing international borders. Listed below are a number of areas which may be of interest for future research.

6.3.1 Digital Forensic Guidelines Developed by Law Enforcement

As has been noted in paragraph 5.1.8, the vast majority of digital forensics guidelines produced to date have been developed by law enforcement agencies. In addition, the vast majority of digital forensics specialist around the world also currently work in law enforcement agencies or have a law enforcement background (paragraph 2.3.2). A major function of law enforcement agencies is to investigate crime and collect evidence, including digital evidence. The naturally undertake this work as part of a wider law enforcement team and from a prosecution perspective. The questions could be asked is ‘has this 'one-sided' development of the guidelines for the digital forensics profession slanted the profession towards the prosecution perspective?’

6.3.2 The Acceptance and Relevance of Digital Forensics Certification

As has been discussed in the research at some length, there are a wide variety of both vendor based and non-vendor based certifications available for the digital forensics practitioner. A number of these certifications are tied to the attendance at a number of highly priced training courses regarding a single product. There is also little evidence that any of the certifications has achieved widespread acceptance by the legal profession. Most professions are characterised by highly regarded professional bodies that mandate entry requirements, good character requirements and an ongoing requirement to professional development for their members. The professional bodies may also have a right to prevent an individual from practising in the profession if they do not meet the standards. It might be expected that in digital forensics there will be a move towards a recognition of vendor based training certification and the wider independent professional certification. There may also be a rationalisation in the area of professional certification to fewer and more recognised professional bodies. The development of digital forensics as a recognised profession will provide an interesting area for future research.

6.3.3 Impact of ISO Standards on the Movement of Digital Evidence Across Borders

The digital forensics practitioner has grown out of a necessity by law enforcement agencies to investigate e-crime and collect and present digital evidence in courts. The development of the current Draft ISO standards on digital evidence will, to a large extent, be the first attempt outside of law enforcement guidelines to produce an independent set of standards. It will also be the first major attempt to produce a set of internationally agreed standards in this area. The take-up and impact 'on the ground' of these standards will be an area of considerable interest. Key amongst these will be the questions of will the standards be adopted by the wider digital forensic community. There is also the question of, will the use of the standards be 'expected' by the courts where digital evidence is being moved between countries

that have both adopted the standards'. The impact of the standards, after a suitable timeframe, on the movement of digital evidence across borders may form an interesting area of research.

6.3.4 Harmonisation of International Laws Regarding E-crime

The harmonisation of international laws regarding e-crime and e-commerce is a highly complex area. There may be competing national and international priorities for states to deal with. There may also be priorities for states regarding protection laws in the areas of privacy and computer misuse which will directly impact the ability of digital forensics practitioners to remotely collect digital evidence from a foreign country. During the 19th and 20th centuries many countries agreed to international maritime laws. The driver for these laws was that international trade would suffer if ships could not be granted free passage. In many ways this is mirrored by emerging laws regarding the digital world. The main difference may be that courtiers at present are enacting laws to protect the conduct of e-commerce within their own country and the move to protect e-commerce between countries is at a very early stage. A key to the future of international e-commerce is the ability to investigate and prosecute e-crime. A key element of prosecuting e-crime is the ability to collect and present digital evidence in a court of law.

6.4 MAIN RESEARCH FINDINGS

The main findings of the research are the 11 main factors affecting digital evidence crossing international borders. These factors are shown in Table 6.1.

As noted in paragraph 6.2 from a practical perspective the 'acid' test of the integrity of digital evidence is when it is accepted in a court. In the literal sense of the word factor all of these identified main factors will influence a successful out come for the presentation of the digital evidence. In the closing paragraphs of this thesis I discuss the key points within the broad headings of Technical, Chain of custody/transportation, Standards/qualifications/certifications and Legal.

6.4.1 Key Findings - Technical

Two of the factors identified in the technical area of digital forensics that will cause continuing issues both nationally and international are the Increasing size of the capacities of digital devices discussed in paragraph 5.1.1 and the continuing emergence new types of digital devices discussed in paragraph 5.1.2. Both of these technological developments can be seen as part of the natural progress of the information revolution. There effect is to provide constant new challenges for the Digital Forensics practitioner and the courts which will have to deal with new processes and technologies to deal with these two issue. As noted in Table 5.2 the resolution areas for dealing with the issues raised by increasing digital device capacities are likely to be emerging best practice and documentation of the decision processes of the digital forensics practitioner when acquiring a sub-set of data. The area of emerging digital devices is likely to find resolution in the areas of cooperation between digital forensics practitioners and constant skills updating of the digital forensics practitioner regarding the extraction of evidence from new digital devices

6.4.2 Key Findings - Chain of Custody and Transportation

The key factor identified in this area regards the lack of an agreed digital evidence verification standard which is discussed in paragraph 5.1.5. This is a key factor in moving digital evidence across international borders to be able to ensure that the integrity of the digital evidence can be shown at all stages. While the MD5 hashing algorithm is still widely used by digital forensics practitioners around the world the widely publicised compromises of the algorithm would suggest that its future use will be brought into question.

6.4.3 Key Findings - Standards Qualifications and Certifications

It is noted in paragraph 4.5.10 that in many way the emergence of the Digital Forensics profession is mirroring the early stages of the development of the wider IT profession. At the start of the IT profession there were no specific academic

qualifications or professional bodies so organisations make employment decisions based on experience. As the IT profession has matured both specific academic qualifications and membership of professional bodies have become more important. As noted in paragraph 5.2.1 As the digital forensics profession mature and specific academic qualifications in the area of digital forensics become more prevalent, courts are likely to take more note of academic qualifications in establishing an individual as an expert witness. This process may however take many decades to evolve.

6.4.4 Key Findings - Legal

The key area identified amongst the legal issues was discussed 5.1.16 in this paragraph it is noted that the admissibility of evidence in a court of law is usually the responsibility of an independent judge. It is at this interface between the digital forensics practitioner and a judge that the science of digital forensics meets the practicalities of the legal profession. From an evidentiary point of view it makes no difference how scientifically accurate the process of producing the digital evidence is if it is not accepted in a court of law. Table 5.12 notes that the resolution areas for this issue are likely to reside in increasing the ability of legal professionals to quantify the expertise of an expert digital forensics witness from a foreign jurisdiction. Another key factor will be the development of International standards in the digital forensics process, these will give judges a guide as to the digital forensics best practice that might be expected in jurisdictions which adopt the standards.

Table 6.1 Main factors Affecting Digital Evidence Crossing International Borders

Factor Number	Factor
1	Increasing digital device capacities
2	Emerging digital devices
3	Acquisition of live (volatile) data is a developing area
4	No agreed digital evidence verification standard
5	Digital forensics is a new profession
6	Lack of specific academic qualifications
7	International variations in the importance of digital forensic academic qualifications to courts and employers
8	The number of competing vendor and non-vendor certifications available.
9	Laws covering e-crime are country based while the crime can be international
10	Different countries are legislating regarding e-crime at different speeds.
11	Admissibility of evidence is usually the responsibility of an independent judge

References

AccesData Inc. (2009). *ACE Preparation*. Retrieved 5 December 2009, from http://www.accessdata.com/acePreparation.html.

Angelo, H. (2009) *Cyber Security and Legislation in the Pacific*. Retrieved 8 December 2009, from http://www.upf.pf/IMG/pdf/06-TIC-Angelo-Cyber-Security.pdf.

Ashcroft, J. (2004). *Forensic Examination of Digital Evidence: A guide for Law Enforcement*. Retrieved 25 May 2010, from http://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Baggili, I., Mislan, R., Rogers, M. (2007). Mobile Phone Tool Testing – A Database Driven Approach. *International Journal of Digital Evidence*. 6(2),

Brand, S. (1985). *Whole Earth Review*. New York: Viking Penguin.

Braun, V., Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology. 3(2), 77-101.*

Britz, M.T. (2008). *Computer Forensics and Cyber Crime*. New Jersey: Prentice Hall.

Brown, C. (2006). *Computer Evidence: Collection and Preservation*. Hingham, Mass.: Charles River Media.

Burton, A., Schofield, D., Goodwin, L., (2005*) Gates of Global Perception*. Paper presented at the 13th Annual ACM International Conference on Multimedia, 19 April , Singapore.

Caloyannides, M., Memon, N., Venema, W. (2009). Digital Forensics. *Computing in Science and Engineering. 7(2), 16 – 17.*

Carrier, B., (2003) Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, *International Journal of Digital Evidence*. 1(4), 1 – 12.

Casey, E. (2004). *Digital Evidence and Computer Crime*. London; San Diego, California.: Academic Press.

Cavana, R., Delahaye, B., Sekaran, U. (2001). *Applied Business Research: Qualitative and Quantitative Methods*. Queensland, Australia: John Wiley & Sons.

Collis, J., Hussey, R. (2003). *Business Research* (2nd ed.). New York: Palgrave Macmillan.

Cox, N, (2006). *Technology and Legal Systems*. London: Ashgate Publishing.

Cyber Forensics (2009). *Should Federal, State, Local and Tribal governments play a role in overseeing the Forensic Science*. Retrieved 5 December 2009, from http://deforensics.blogs pot.com/2009/01/digital-evidence-investigators-required_14.html

Douglas, J.E., Burgess, A.W., Burgess, A.G., Ressler, R.K. (2006). *Crime Classification Manual*. New Jersey: John Wiley and Sons.

Dul, J., Hak, T. (2008). *Case Study Methodology in Business Research*. Oxford: Elsevier Ltd.

Encyclopedia Britanica. (n.d.) *Evidence – Witnesses.* retrieved 5 December 2009. http://www.britannica.com/EBchecked/topic/197308/evidence/28372/Witnesses#

Garfinkel, S. (2009). Providing Cryptographic Security and Evidentuary Chain-of-Custody with the Advanced Forensic Format, Library and Tools. *International Journal of Digital Crime and Forensics*. 1(1), 1 – 28.

Geoghegan, L., Gray, T. (2009). The Evaluation of MD5 Hash Tools as a Digital Forensics Class Experiment**.** *Journal of Computing Sciences in Colleges*. 24(5), 50 – 56.

Gerring, J. (2007). *Case Study Research: Principles and Practices*. Cambridge: Cambridge University Press.

Gillham, B. (2000). *Case Study Research Methods*. London: Continuum.

Guidance Software Inc (2009). *Certification Program*. Retrieved 5 December 2009. from http://www.guidancesoftware.com/computer-forensics-training--certifications.htm

Harrill, D., Mislan, R. (2007*). A Small Scale Digital Device Forensics ontology*. *Small Scale Digital Forensics Journal* 1(1), 1 – 7.

Harvey, D. (2003). *Internet.law.nz : selected issues*. Wellington, N.Z.: LexisNexis.

International Criminal Police Organization (INTERPOL) (2008). *Cybercrime Fact Sheet COM/FS/2008-07/FHT-02*. Retrieved 8 December 2009, from http://www.interpol.int/Public/ICPO/FactSheets/FHT02.pdf

International Organisation on Computer Evidence (IOCE) (2009). *G8 Proposed Principles For The Procedures Relating To Digital Evidence*. Retrieved 8 December 2009, from http://www.ioce.org/core.php?ID=5

IOEC. (2002*). Guidelines for the Best Practice in the Forensic Examination of Digital Technology*. Retrieved 28 June 2010, from http://www.ioce.org/fileadmin/user_upload/2002/Guidelines%20for%20Best%20 Practices%2 0in%20Examination%20of%20Digital%20Evid.pdf.

ISO/IEC 27037 (2009) -- *IT Security -- Security techniques -- Guidelines for identification, collection and/or acquisition and preservation of digital evidence (DRAFT).* International Standards Organisation.

Jones, K., Bejtlich, R., Rose. (2006). *Real Digital Forensics*. USA New Jersey**:**Addison Wesley.

Kamal, A. (2005). *The Law of Cyber Space*. Geneva, Switzerland: The United Nations Institute for Training Research.

Law Library – American Law and Legal Information. *Computer Crime - International Initiatives*. Retrieved 28 March 2009 from http://law.jrank.org/pages/699/Computer-Crime-International-initiatives.html

Lemos, R. (2002). *Russia accuses FBI agent of Hacking. CNet News*. Retrieved 9 December 2009, http://news.cnet.com/Russia-accuses-FBI-agent-of-hacking/2100-1002_3-950719.html

Lim, N., Khoo, A. (2009). Forensics of computers and handheld devices: identical or fraternal twins?. *Communications of the ACM*. 52(6), 132 – 135.

Marcella, A.J. Jr., Menendez , D. (2008). *Cyber Forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*. New York: Auerbach Publications.

Mukasey, M. Sedgwick, J. Hagy, D. (2008*) Electronic Crime Scene Investigation: A Guide for First Responders.*US Department of Justice.

Murff, K. N. (2007). *Digital Crime Investigation Trends in State and Local Law Enforcement*. Texas:Sam Houston State University.

National Institute of Justice (2008). *Collecting Digital Evidence Flow Chart*. Retrieved 3 December 2009, from. http://www.ojp.usdoj.gov/nij/publications/ecrime-guide-219941/ch5-evidence-collection/collecting-digital-evidence-flowchart.htm

Nasir, S. (2008). *The evolution of Global Intellectual Property instruments into trade related Intellectual Property Rights (TRIPS) and its ineffective in developing world :a case study*. NZ: AUT University

New Zealand Government (2006) *Electronic Evidence Act*, Wellington NZ: Parliamentary Services.

Power, R. (2002). 2002 CSI/FBI Computer Crime and Security Survey. *Computer Security Journal*. 18(2), 7 – 30.

Ray, D. (2007). *Developing a Proactive Digital Forensics System.* USA:The University of Alabama.

Reyes, A. (2007). *Cyber Crime Investigations*. Rockland, MA: Syngress Pub.

SANS Institute (2009). *Best Practices in Digital Evidence Collection*. Retrieved 9 December 2009, from http://blogs.sans.org/computer-forensics/2009/09/12/best-practices-in-digital-evidence-collection/

Sammes., A, Jenkinson., B, (2007). *Forensic Computing*. London: Springer.

Savoldi, A., Gubian, P. (2009). Volatile Memory Collection and Analysis for Windows Mission-Critical Computer Systems. *International Journal of Digital Crime and Forensics*.1(3), 4 – 61.

Siegel, J.A. (2006). *Forensic science: the basics*. Boca Raton, FL: CRC/Taylor & Francis

Smith, R. (2009). *The influence of written information Security Policy on Forensic data Collection: A case Study.* USA:Capella University

Smith,R., Grabosky, P., Urbas G (2004). *Cyber Criminals on Trial*. Cambridge: Cambridge University Press.

Standards Australia (2003*). Guidelines for the Management of IT Evidence*. Sydney: Standards Australia Limited.

Stephenson, P., (2000). *Investigating Computer-Related Crime*; Florida: CRC Press.

SWEGE (Scientific Working Group On Digital Evidence (1999). *Digital Evidence Standards and Procedures:*US:FBI

Tavalea, K. (2009) *The Factors Influencing ICT Governance Implementation in the Organisation: A case Study*. NZ:AUT University.

The Common Digital Evidence Storage Format Working Group (2006). *Survey of Disk Image Storage Formats*. Paper presented at the Digital Forensic Research Workshop, 1 September, Lafayette, Indiana.

The Electronic Evidence Information Center (n.d). *Digital Forensic Education. Retrieved 5 December* 2009. http://www.e-evidence.info/education.html

The First International Conference on Technical and Legal Aspects of the e-Society (2009). *Cyberlaws 2010*. Retrieved 12 December 2009, from http://www.iaria.org/conferences2010/CYBERLAWS10.html

Tipton, H.F., Krause, M. (2006). *Information Security Management Handbook*. Florida: CRC Press.

Wiles, J. (2007). *Techno Security's Guide to E-Discovery and Digital Forensics*. New York: Syngress Publishing.

Wilkinson, S. (2003). Good Practice Guide for Computer-based Electronic Evidence. Retrieved 21 June 2010 from http://www.acpo.police.uk/asp/policies/Data/ACPO%20Guidelines%20v18.pdf.

Wilson, N., (2008). *Forensics in cyber-space: the legal challenges*. Proceedings of the First International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia, 21 – 23 January, Adelaide, Australia.

WorldWideLearn (n.d*). Guide to College Majors in Computer Forensics.* Retrieved 5 December 2009. http://www.worldwidelearn.com/online-education-guide/technology/computer-forensics-major.htm

Appendix A - Ethics Approval

MEMORANDUM

Auckland University of Technology Ethics Committee (AUTEC)

To:	Brian Cusack
From:	**Madeline Banda** Executive Secretary, AUTEC
Date:	21 April 2010
Subject:	Ethics Application Number 10/38 **Factors influencing digital evidence transfer across international borders: A case study.**

Dear Brian

Thank you for providing written evidence as requested. I am pleased to advise that it satisfies the points raised by a subcommittee of the Auckland University of Technology Ethics Committee (AUTEC) at their meeting on 18 March 2010 and that I have approved your ethics application. This delegated approval is made in accordance with section 5.3.2.3 of AUTEC's *Applying for Ethics Approval: Guidelines and Procedures* and is subject to endorsement at AUTEC's meeting on 10 May 2010.

Your ethics application is approved for a period of three years until 20 April 2013.

I advise that as part of the ethics approval process, you are required to submit the following to AUTEC:

- A brief annual progress report using form EA2, which is available online through http://www.aut.ac.nz/research/research-ethics. When necessary this form may also be used to request an extension of the approval at least one month prior to its expiry on 20 April 2013;
- A brief report on the status of the project using form EA3, which is available online through http://www.aut.ac.nz/research/research-ethics. This report is to be submitted either when the approval expires on 20 April 2013 or on completion of the project, whichever comes sooner;

It is a condition of approval that AUTEC is notified of any adverse events or if the research does not commence. AUTEC approval needs to be sought for any alteration to the research, including any alteration of or addition to any documents that are provided to participants. You are reminded that, as applicant, you are responsible for ensuring that research undertaken under this approval occurs within the parameters outlined in the approved application.

Please note that AUTEC grants ethical approval only. If you require management approval from an institution or organisation for your research, then you will need to make the arrangements necessary to obtain this. Also, if your research is undertaken within a jurisdiction outside New Zealand, you will need to make the arrangements necessary to meet the legal and ethical requirements that apply within that jurisdiction.

When communicating with us about this application, we ask that you use the application number and study title to enable us to provide you with prompt service. Should you have any further enquiries regarding this matter, you are welcome to contact Charles Grinter, Ethics Coordinator, by email at ethics@aut.ac.nz or by telephone on 921 9999 at extension 8860.

On behalf of the AUTEC and myself, I wish you success with your research and look forward to reading about it in your reports.

Yours sincerely

Madeline Banda
Executive Secretary
Auckland University of Technology Ethics Committee