A Code of Conduct for Computer Forensic Investigators.

by

James Ronald Gay

A Thesis submitted in partial fulfilment of the
requirements for the degree of

Professional Doctorate in Information Security

University of East London

2012

Approved by

Chairperson of Supervisory Committee

Program Authorized to Offer Degree

Date

Abstract

The amount of electronic data that is held about individuals and their activities is staggering. Tools enabling data recovery, believed deleted, vary in consistency and reliability of result. Data under review can be fed into investigative tools which also vary immensely in reliability, consistency, quality and indeed price.

Conclusions and inferences drawn from the use of these tools can be morally, socially and commercially damaging for the individuals or entities being investigated. Often not purely because of the lack of experience of the investigator, but also because of the simplistic operation of the toolsets.

Whilst prescriptive guidelines exist in the public sector for the proper handling, analysis and reporting of computer evidence, little commercially independent professional guidance exists in the private sector. This lack of guidance has led to a position whereby actors in the field of data forensics have few challenges as to their expertise or experience. Recent cases of incompetence and crossing ethical and professional boundaries provide strong support for a National, preferably International certification and training scheme for data forensic analysts, supported by clear ethical codes.

This research in light of the above challenges, provides examples of failures in extrapolation, operator understanding and tool use; argues a proposal for a code of conduct to ensure correct and repeatable process is followed; along with a suggested outline for the creation of the supervision of conformity to that code in the private sector. The current forensics community and academic research body of knowledge, supported by the extensive experience of the researcher have been the major inputs to the work. The outputs of this work are intended to form a solid base for the furtherance of the Computer Forensics profession, and as such will represent a significant contribution to the advancement and knowledge base of that profession.

Table of Contents

TABLE OF Figures

The spread of crime using computers was inevitable; the question is how much damage computer crime has caused and still may. (Meyers and Rogers, 2004, p. 1)

Quis custodiet ipsos custodes? (Plato, c380bc.)

1 Introduction

This chapter is designed to set the scene, it will lay out the histories in the professions that are related to the data forensics field as well as some simpler definitions of the needs and challenges of that field. It will outline current and past research calls for similar studies as well as some of the possible parallels between the public and private sector deliveries in the field. Most importantly it summarises the aims and objectives for the research, as a whole.

1.1 Background

The advent of computers into the everyday world has brought with it many benefits. There is hardly a profession that has not gained either efficiency or precision from the use of computers. Early predictions as to the value of computers to the masses and the incursion of the ubiquitous personal computer into our homes seem strange as we now look in retrospect, and these predictions may have helped delay the understanding of need for forensic investigative capabilities. The founder of the greatest computer empire so far, Thomas J. Watson, is reputed to have stated that *"I think there is a world market for maybe five computers"* (Carr, 2008, p. 1). The then second largest manufacturer of computers, Digital Equipment Corporation Chairman and CEO, Ken Olsen in 1977 stood up and announced "*There is no reason anyone would want a computer in their hom*e" (Gatlin, 1999, p. 2), although there is some discussion that Olsen actually meant a computer to *control* a home (Gatlin, 1999; Rifkin and Harrer, 1988).

1.2 Aims and objectives of the research

Whilst prescriptive guidelines exist in the public sector for the proper handling, analysis and reporting of computer evidence, very little supplier independent professional guidance exists in the private sector. This lack of guidance has led to a position whereby actors in the field of data forensics have few challenges laid against them as to their expertise or experience. No formal certification, that is supplier agnostic existed until very recently, nor is there a common criteria even between suppliers. Recent cases of incompetence and crossing ethical and professional boundaries provide strong support for a National, preferably International certification and training scheme for data forensic analysts. Ethical behaviour cannot be described as good or bad if it is not clear what is expected, so there is a need to support any certifications with clear ethical codes.

Much of the referenced data has been drawn from the physical security world, where little tool agnostic guidance on how to properly conduct a data forensic investigation exists, certainly in the United Kingdom commercial sector. A common ethical problem is managing the discovery of confidential data that is irrelevant to the case at hand. Often wrong inferences are drawn not purely because of the lack of experience of the investigator, but also because of the simplistic operation of the toolsets.

This research therefore provides examples of challenges in extrapolation, operator understanding and tool use; argues a proposal for a code of conduct to ensure correct and repeatable process is followed; along with a suggested outline for the creation of the supervision of conformity to that code in the private sector.

1.3 Confidentiality and privacy

The explosion of personal computer use in everyday life around the world has made people complacent and unfortunately usually ignorant, about the amount of sensitive information that is retained about their activities and most secret dealings. There may be an implicit expectation of privacy of that information;

"Do we have an absolute right to privacy, or only an expectation of privacy based on the circumstances?" (Lister, 2004, p. 1).

The trend towards mass information processing and storage growth is most startling in the corporate arena where a complete working day is spent in many cases creating and moving information around corporate computer networks, as well as the ubiquitous Internet. Not all this information is uniquely relevant to that work unit or person, and in many cases can be held to be of danger to that corporate where users abuse their privileges of access. According to Jahankhani (2007) even law enforcement is struggling to cope because of the amount of data involved. Jahankhani suggests a common belief that cybercrime is no different to more traditional types of crime, but does clarify that the perpetrators of cybercrime are increasingly remote to the scene of crime, and more importantly the victim may nowadays not be aware of the crime in progress. In a report in the industry magazine *Security Management* (Berrong, 2009) we are told that research by the University of Glamorgan in the UK, working with peers in the USA and Australia had some disturbing outputs. The research which involved recovering data from discarded hard drives, found data on individuals on 37% of the disks and commercially sensitive data on 46%. This same research also uncovered some very sensitive data surrounding the USA defence program, this particular item on a disk purchased on Ebay.

The growth in calls for certification and peer review in the forensic market is being driven by the amount of litigation and incidents involving computer data (Sheldon, 2011; Goodwin, 2006; Meyers, 2005).

1.4 Dangers

Knowing now, that the majority of homes in the industrialized world not only have access to a computer, but are also almost certainly connected to the Internet, it is easy to see that the aforementioned predictions by Watson and Olsen were so badly formed. What is abundantly clear, is that the phenomenal growth of the use of computers has brought with it some unwanted side effects. It is unfortunately the case that almost every scientific advance brings with it both a positive and a negative side. For example, the splitting of the atom, that absolute wonder of science brought us unlimited free

power, but also brought us weapons of mass destruction that had been unimaginable before the harnessing of atomic fission and fusion. The invention of the combustion engine, a practical solution to the needs of mass transportation, also brought a medium for movement of bigger and more powerful weapons than were previously able to be moved around. Finally, and one could draw upon many more similar examples, examine the wonders of the airplane, so efficacious in moving people and goods around the world, but also a significantly more efficient way to rain death upon remote populations.

1.5 Good and bad

As the power of computers grew, from the earliest tabulators, arguably those produced by IBM in 1924 - the Type IV, that for the first time could actually subtract values as well as add (IBM, 2008), to the Lyons Electronic Office (LEO) (Byford, 1999) which is also arguably the first real commercial business computer system, to the emerging cloud computing services (Knorr, 2009), where the amount of processing power and storage is potentially unlimited, the benefits to the good and the bad were equally predictable (Grimes, 2009).

To understand the potential of a computer to offer itself to both good and bad ends, it is useful to understand the basic make-up of what we all take for granted. The computer is a collection of electronic parts that work together to store and process information in a predictable and repeatable fashion. The nerve centre of the operation is the Central Processing Unit (CPU) which provides calculations on information presented, at its most rudimentary. It does this by manner of a series of decision gates. The information, or input and output (IO) is channelled to and from the CPU down a series of pathways known as IO buses or in the case of personal computers, Basic Input/Output System (BIOS) (Grassrootsdesign, 2009). These buses (in the simplest terms) carry the information to either storage medium, visual display, or network connection. The decision as to where to send the information, and indeed what to do with it when presented at the various decision gates is controlled by operating system software. This software is common across all similar computer hardware setups and is usually maintained by either a systems specialist in a larger enterprise, or by a “user” in the case

of most personal computers. The ability of the maintainer to modify the actual workings of this software is usually very limited. Given a computer, with an operating system, for the machine to do useful work, it is necessary to use an “application”. An application may be for example an Office Management Suite, which provides for word processing, spread sheets, presentations and a simple programming interface. An application can also be more specific and singular in purpose, such as an Internet banking system, or a payroll calculation engine. These specialist types of applications are more likely to be bespoke to the task, and therefore more complicated in their maintenance and usage. All of the activities above, because of the nature of computers, can be expected to make some changes to data input, and therefore produce data output. It is this output that is the basis of value of the computing machine, and the focus of most nefarious activity in the realm of computing.

1.6 Forensics

As well as providing a background to computer systems, it is also worthwhile to provide a brief overview of the discipline of forensic science. Since man first walked the earth, he has used the skills of analysis and reasoning allied to curiosity and experience to better understand and explain the happenings in the world around him. We see representations of early cave men using animal tracks and droppings to understand if an animal was nearby and likely to be good for food (Clements, 2006). We are told of evidential deduction both fictitious and factual that lead to criminals being apprehended in the days long before formal police forces, such as the prefects system in ancient China (Dun, 1978). We see all around us people using facts and experiences to piece together a picture of what has happened in a particular situation, or in other words, forensic analysis. The science of criminal forensics has long been a specialization in the public police force. Forensic science now even has its own public sector regulator in the UK, to ensure the conclusions that are drawn by its practitioners are as sound as possible (Forensic Science Regulator, 2008).

Operating systems and other programs frequently alter and add to the contents of electronic storage (as already outlined above). This may happen automatically, without

the user necessarily being aware that the data has been changed. This is an important aspect of the differences between traditional documentary evidence and computer data.

One of the main advices is that in order to comply with the proper principles of computer based electronic evidence gathering, wherever practicable, an image should be made of the entire target device. Partial or selective file copying may be considered as an alternative in certain circumstances e.g. when the amount of data to be imaged makes this full copy impracticable. This Thesis also explores how the advent of new technologies brings different challenges to the problem in the current "always on" environments.

In a minority of cases, it may not be possible to obtain an image using a recognised imaging device. In these circumstances, it may become necessary for the original machine to be accessed to recover the evidence. The advice of DCL (2009), reflecting general investigator practice, then goes on to provide;

"With this in mind, it is essential that a witness, who is competent to give evidence to a court of law makes any such access. It is essential to show objectively to a court both continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court" (DCL, 2009, p. 5).

1.7 Related Work

There are many methodologies in use to provide basis and background to forensic science, but the one most pertinent here is the "*Daubert test*" (Daubert, 1993). Daubert states that any theory used to provide an opinion or conclusion in forensics must; be generally in use in the forensic community, have been peer reviewed and tested, and where specific, the predicted reliability and error rate is reported. There is also an important additional related theory of crime scenes that will become evident as to its importance as we progress. The "*Locard* principle", (Chisum & Turvey, 2000) argues

that any person entering a crime scene will take something with them, as well as leaving something behind, and that every contact leaves a trace.

"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value" (Kirk, 1953, p. 4).

The American Heritage Dictionary (2000) describes Forensics as, *"the use of science and technology to investigate and establish facts in criminal and civil courts of law"*. Another describes computer forensics as

"… the analysis of information contained within and created with computer systems and computing devices, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved" (Hayley, 2002, p. 1).

Hence from these descriptions we have a rudimentary understanding of the basic profession that this Thesis is attempting to provide a sequence of governance for.

Another author outlines some useful theories into the evolution of the field:

"Computer Forensics is a field that developed from the introduction of new technology which is readily accessible, affordable and heavily depended upon both in the home and businesses. The speed in which this technology has evolved brings both advantages and disadvantages to all. New crime developed which became a main disadvantage especially to law enforcement" (Taal, 2007, p. 62).

Arguably, there is a message that Taal is trying to convey stating that the IT revolution has brought with it new crimes. Clearly this is not a generally accepted argument (Eurim, 2002; Standler, 1999), but may be a useful view to retain when looking at the

manner in which some old crimes are being committed using this new medium. This becomes especially relevant if we are to look, using the lens of the one of the questions the research has considered, that of how to consistently provide forensic support in the investigation of crime and nefarious activity in the private sector.

1.8 History

In the early 1990s, when is it generally agreed that the World Wide Web was in its early development stage, and its creator was working at the Centre for European Nuclear Research (CERN) in Geneva (Berners-Lee, 2010), there were already discussions taking place around the need for training investigators properly. Amongst others, there were calls for

" an educationally sound concept of incremental training in computer crime investigation, together with a suitable syllabus which has application on a national and international basis" (Stanley, 1991, p. 427).

Arguing that the international nature of computing even then made the application of national boundaries a farce in the investigation of computer crime, Stanley then also called for a discussion of what exactly makes up a computer crime, and argued the need for a proper and commonly accepted definition of computer crime. It is worth remembering that this arguing is many years prior to most countries enacting computer crime legislation. Fay (1993) also called for a better definition of computer crime, arguing that the lack of such a definition adds to the difficulty of prosecuting it, suggesting that a starting point would be;

"a computer is used in an act, or an act is committed against a computer to steal money, services, property or information for invasion of privacy, extortion and even committing a terrorist act" (Fay, 1993, p. 154).

Further, this work also logically reminded us that when an investigation is being progressed, it helps to know who the criminals are. Unfortunately, we are offered only the following opinion without any supporting empirical evidence, which is unfortunate

as there were legion stereotypes of the hacker in those days, and the text below is a very neat summary of those beliefs at that time;

"The average computer criminal is a well-educated, skilled professional. Generally the person is respected in the workplace and the community and has no record of criminal behaviour" (Fay, 1993, p. 156).

It should be remembered that Fay is relating generally held public perceptions of computer criminals which were largely based on anecdotal evidence in the early 1990s, given the infancy of the computer crime research at that time, these do though reflect widely held opinion of that era.

1.9 Research background

Within the field of moderating reliability of commercial computer investigations in the United Kingdom there has also been seemingly little academic research. Much of the available published work stems from the United States of America. Meyers (2005) argued then that it is the responsibility of the general scientific community to assist in this endeavour, and yet we still see little progress in the UK. Whitcomb (2007) provides that this discussion has been raging since 1998. In an experience as expert witness in 1989 for Digital Equipment Limited, it was clear to this researcher that the "day in court" was heavily weighted towards the side that had the best technology expert on that day. This is indeed the underpinning of the British legal system, wherein the Magna Carta drove the system to favour due process above fairness (Great Britain, 1297). There was, in the experience of this researcher, in the field of information security and albeit rudimentary data forensics at that point in the nineteen eighties, no expectation that any reproducible process had been followed in the gathering of evidence submitted. A great deal of this lack of expectation of procedure and rigour was arguably because the personal computer had not yet harnessed the power of the Internet via the yet to evolve World Wide Web. There was also a propensity of the senior members of the legal profession involved in such cases towards being less than sophisticated in the technologies being described to them. To amplify using a real example, the concept of a software license key was so complicated to the bench, in the Digital Equipment action

the researcher was supporting, that the case could only properly proceed by using the analogy of a house key and lock to ensure the legal community in the room had a rudimentary understanding of the technical basis of the case (CISCO, 2011). This perhaps lengthy description of one example of the delivery of forensic expertise to a civil action is provided to outline the fairly basic failure of the data forensics profession to actually recognize experience by examination or by certification of forensic practitioners. Whilst in this example, the researcher was arguably amongst the best qualified to provide expertise to that case, this Thesis will show later by use of a conflicting example (Warrren, 2007) that the case could just have easily at that time been informed by someone with absolutely no experience or expertise in forensics whatsoever. The legal profession at that time would have had no better challenge, because of the lack of certification or peer recognition in the profession.

1.10 Commercial slant

Not all computer forensics investigations result in, or are driven by a court appearance, but the methodologies used should be the same (Guidance Software, 2004). Kruse & Heiser (2004) do also affirm that in their view all cases should receive the same care and handling as if each one was intended to be presented in court. Hayley (2002) gives similar advice;

"…regardless of the situation, and whether the evidence will be used in a court of law or as the grounds for a letter of reprimand, the techniques, procedures, and methodologies used should be largely the same" (Hayley, 2002, p. 4).

This Thesis will argue that this advice is often ignored in the private sector, and that evidential, moral, ethical and legal boundaries are sometimes overstepped.

Mendell (1998) suggested that a case needs certain facts in order for it to be successfully pursued, calling these *"solvability"* factors. Listed amongst some of the seemingly more obvious were; knowing the name of a suspect; identifying the characteristics of a vehicle; a description of the suspect; or a known pattern or *"modus*

operandi". Mendell also suggested that although none of the above would be obvious characteristics of a computer crime, the concept of solvability factors is appropriate.

This Thesis specifically uses the word investigation at this point, rather than research as Saunders, Lewis and Thornhill (2003) present an argument that the word *"research"* is overused and as such diluted in its meaning. This researcher is in contention with the argument by Saunders et al., namely that unless there is a systematic process of data gathering, analysis and interpretation, the mere study of that data is not properly described as research. It could be argued, and is the belief of this researcher that by concluding that research is *properly* described as something that people undertake to uncover things systematically, and also arguing that the reasoning behind the research is to increase the knowledge of the researcher, Saunders et al (2003) bound the definition too severely. This Thesis would suggest that often the author has the base knowledge that is being presented for challenge, especially in the areas of professional research by mature researchers. It is, this Thesis contends, the process of considered arguing and analysis that qualifies and cements that knowledge, and therefore not always a systematic path to something that is uncovered.

In simple terms then, the amount of data that is held about individuals and their actions on computer systems can be astounding. The majority of the data that is recoverable is generally believed to have been deleted by that subject. Forensics tools to enable the recovery of this supposedly deleted data are legion and importantly, vary in consistency and reliability of output.

"Computer Forensics Specialists use powerful software tools to uncover data to be sorted through, and then must figure out the important facts…" (Basset et al, 2006, p. 1).

A suggestion therefore that not only technical, but also analytical skills are important. Jahankhani (2007) states that the techniques used by criminals and the knowledge of the technologies that can combat them are essential in the fight. Jahankhani also argues that only by dialogue between agencies, industry and researchers can a global examination of the issues and therefore a solution be found.

1.11 Certification and trust

There were until very recently no tool-agnostic formally recognised private sector qualifications for investigators, computer forensic experts and the like. Even now in 2012, if one is to delve deeply into the few companies offering such certifications, there seems to be little actual professional background to the certifications. The discussions of what are held to be professional and what certification means in the constraints of a professional organisation will be held throughout this Thesis, but for the understanding of the calls being made here at this stage, a professional certification must be one that is based on experience, trust and censure of peers and proven and tested knowledge of the subject being certified. This distinction then hopefully will clarify the feedback received thus far that there are indeed organisations such as GIAC (GIAC, 2012) and EC-Council (EC-Council, 2012) that offer certification. Both of these organisations are offering what can be described as course-based certification, in that if you attend the training course the last day involves certification. There clearly is an uptake for these types of certifications as GIAC claims a certified base of over forty six thousand in their twenty five different certifications since the year 2000, and EC-Council founded in 2001, by 2011 had listed thirty eight thousand in their twenty three wide ranging certificate subjects. Whilst training is certainly important, being certified for sitting in a classroom is not in the basis of the calls being made in this Thesis, for "properly certified professionals". If there is to be trust and sharing between actors with these skills across the public and private sectors, and importantly internationally, there would be immense value in having qualifications that are universally acknowledged and respected. There may be advantage in developing a baseline set of criteria for specific disciplines, possibly at different levels of competence within each, against which knowledge and experience can be measured. A balance needs to be struck between the introduction of formal qualifications, which will take time both to define and to introduce and may be a long-term goal, and the need for measures of practitioner competence to meet the needs for mutual trust and/or admissibility of evidence. It may well be that at least some of the latter can be organised rather more rapidly.

"a Computer Forensic Specialist (CFS) must follow a rigid set of methods to ensure that computer evidence is correctly obtained" (Basset et al, 2006, p. 3).

In the experience of this researcher, having performed forensics captures and investigations for 20 years around the globe, rarely is the following of a rigid set of methods verified between peers working together on cases, or in the passing data between actors. An important example of where this should indeed have been the case may help in the understanding of the importance of the calls that Basset et al (2006) make. In 2002 this researcher became chief investigator and expert witness in what was then claimed to be the biggest investment or Ponzi (Wells, 2000) fraud on the Internet (USCA, 2006). This case transited the world's courts, albeit mainly centred in the United States of America. At various points, depositions and counter-depositions were laid, against many actors in the case. At the heart of the majority of these challenges lay the data which the researcher personally had recovered from various implicated computer systems. In light of all these legal challenges, there should have been at least a rudimentary cross-examination of how the data was gathered and the tools and methodologies used in recovering and processing the data for the presentation to the various actors. Given that much of the data extracted and presented was extremely specific and incriminating, the fact that no challenge ever materialised was doubly surprising. Indeed even when the agents of the e-crimes section of the Federal Bureau of Investigation (FBI) and Securities and Exchange Commission (SEC) reviewed the case; there was no interrogation of the methodology or integrity of the tools used by the researcher. These two agencies were latterly involved as the case was reportedly deemed to have crossed both state and international borders as well as potentially violating the United States SEC regulations.

This Thesis will attempt to understand and therefore explain why this implied trust exists between so-called experts without any pre-agreed standard of certification or code of conduct.

Meyers (2005) argues that there have been many cited examples of litigation either failing, or being severely dampened by the lack of a formal code of conduct by which commercial investigators actions can be assessed (in the USA).

In contrast, there are many guidelines and restrictions for example within the United Kingdom Public Sector arenas (ACPO, 2007; HMRC, 2006). This confirms that a lack of formal discipline lies mainly in the private or commercial sector. This is recognised at least, for evidential submission, by the publication of a British Standards Institution (BSI) draft for comment in April 2008 on legal admissibility of forensic data (BSI, 2008). The House of Commons Science and Technology Committee similarly made it clear that;

"..training of expert witnesses in the general principles of presentation of evidence to courts and the legal process is essential" (STC, 2004, p. 3).

1.12 Parallel experience

In considering the make-up of a code of conduct, as well as possible certification and peer management against that code, it will be useful to parallel experiences of other professional bodies. Abrahams (2007) argues that certification allows for (in his example) translators to show they have met a certain professional standard. Barbara (2008) suggests that there are two reliability factors that should be explored, certification and accreditation, and devotes a whole chapter to how the two are sometimes confused, but do in fact differ. One organisation offering such a code is the British Institute of Management, which after achieving chartered status in 2002 evolved into the Chartered Management Institute (CMI). The code of conduct, updated in March 2011, is extensive (CMI, 2011). Much of the intent that is in there is certainly a mainstay of the research for the eventual output of this Thesis. There are however, over three pages of words, made up of over thirty specific items that a member must agree to. Important issues like striving for excellence, are diminished by the amount of reading a member must do, including items such as advice on establishing business relationships properly.

In contrast The British Computer Society, produces four concise sections, each containing a maximum of seven bullets, clearly something that would be somewhat easier to have pinned up in a cubicle, or at least within one's subconscious. Rather than expand and wordsmith the code, filling page space and arguably detracting from the

main messages as is suggested the CMI code does, the BCS code offers an appendix to help interpret the code as needed (BCS, 2011). Clearly then more is not always better, and if there is a learning from this, it is surely that concise must be a watchword if a code is to persist and be upheld.

The call for competence, and indeed how to recognise it is one of the basic challenges of this research. This Thesis argues also that, in an area that is so dangerously important to in many cases, the lives and careers of people it touches, that the lack of formal supplier independent education for the proper representation of forensic evidence in the private sector is noteworthy. Whilst this research had not set out to provide discussion on the proper educational processes required, the omission of such discussions from the final Thesis would have left an important part of the problem untouched.

The aims of this research, therefore are clear. What follows is a summary of the objectives that were both designed in the inception of this Thesis, as well as have evolved during the research. These objectives will be revisited further in the Thesis within the appropriate sections.

1.13 Summary of Objectives

- Ensure that the final output provides appropriate background to the subject of Computer Forensics;
- Analysis of related and non-related codes of conduct in similar professional evolutions;
- Review of current similar training / certifications (added during research);
- Provide that actual industry experience not just academic research is included.
- Test viability of code with peers.

This chapter has set the aims and objectives, it has laid out some outline histories in the professions that are related to the data forensics field as well as some simpler definitions of the needs and challenges of this field. It repeats current and past research calls for similar studies as well as some of the possible parallels between the public and private sector deliveries in the field of data forensics.

1.14 Document structure

The Thesis is intended to provide a narrative of both the evolution of the forensics profession and the underpinning professional activities of forensic actors. It is structured to allow an understanding of the profession and the current failings, which build towards the goal of the research, the Code of Conduct (CoC) (Section 8.3; Appendix B).

In this chapter we have related the historical aspects to the perceived failings, we have explored some of the basic activities involved in the profession which will be explored in more depth as the Thesis progresses. We have explored other research and activities which provide impetus for this work, and have set a series of objectives to ensure a solid measurable deliverable at the completion of this Thesis.

In Chapter 2 we will explore the challenges facing this research project. The work draws heavily on extensive evidence from other societies and researchers in the areas of governance and professionalism. It looks at the questions set during the formulation of this project, as well as the indicators we should use to ensure the research was on track. Chapter 2 also sets out a series of commonly held definitions as well as some clarifications to ensure there is a commonality of understanding through the Thesis. Finally the chapter lays out some historical background to ensure we have a properly understandable evolutionary track to guide us forward as the Thesis builds.

Chapter 3 builds upon the definitions and needs of the research project and provides a compendium of the work of a forensic analyst. It discusses and advises on not only the technical but also the governance aspects of the profession. It investigates previous advice to ensure a balanced view is achieved with an traceable outcome. It sets the scene to a review of the tools used in the profession as well as the way in which they can and have been used as well as misused.

In Chapter 4, many of the questions around the use of tools and their make-up from previous chapters are clarified as we explore the world of data forensics tools. Looking at the free tools and commercial tools from sometimes similar but arguably differing requirements of operation, we cement some of the challenges that have been laid against operators in the field. The Chapter also investigates somewhat more in depth some of

the dilemmas professional and indeed non-professional actors are faced with in operating in data forensics sphere.

Chapter 5 uses the previous building blocks to ensure that clear discussion of each of the issues previously presented is had. Much of the review is involved in the previous performance of the profession, and those claiming to be computer forensic operators also. The solid understandings of concepts and terminology provided in the Thesis so far are used to draw out the reasoning and arguing for the profession and later governance model. A forensics model for operation is discussed in detail as a prelude to ensuring any code of conduct, governance and training model proposed would operate properly.

Having referred extensively throughout the Thesis to training being an underpinning of any such governance model, Chapter 6 lays out the outcomes of discussions and research as to what training is needed in the profession. It makes no claims to be unique or revolutionary, merely using the breadth of training currently available in various guises to provide foundation for a structured training curriculum. The value that this research brings therefore is clarity and structure, which draws from the work up to this point. What it does provide in unique terms is the need for certification in a sense of peer review and testing. The Chapter discusses in detail the various opinions and current deliveries in the field that have shaped the Thesis in this area.

Having introduced the requirement for testing and certification to pre-defined level previously, Chapter 7 explores how that could be delivered. It uses other organisations that have delivered similar schemes to test the solutions offered. It discusses indicators of success and indeed failure that could be used to test the effect of implementing a governance model. It also acts as a test for previous chapters to ensure that the issues and challenges we have identified and warned are able to at least be monitored in such a scheme.

Finally, Chapter 8 brings together the warnings, challenges and advices to set out the work of this Thesis, a model for the proper governance of Computer Forensics Professionals. It revisits the discussions on impersonation, censure and peer review

from previous chapters. The Chapter looks at the solutions that have been discussed and how they tie into the overall model. It reviews that calls for structure of previous codes and peer schemes to ensure all the input has been properly respected. Finally it provides the basic structure of the main aim of this research, The Code of Conduct, discussing how the implementation may be designed and critiqued should industry wish to proceed. The objectives, properly, are revisited to ensure we have a reminder of the journey that we took, and how we came to this junction in the road towards the professionalization of the forensics vocation. There are, as always, more questions than answers and the Chapter also lays out some challenges to future research

2 Research challenges

In this chapter, we will review the questions, and direction used to perform the research as well as some of the guidance that has gone before in the area of governance, professionalism, and certification. We will explore the discussions on the emerging field and the various opinions that are shaping its future evolution.

This Thesis is guided by Saunders, Lewis and Thornhill (2003) in the search for supporting and opposing opinion. However, Saunders et al attempt to define research itself are interesting in describing research as *systematic* which is not the experience of this researcher in working on this Thesis. That deviation may relate to the difference in the subject matter of Saunders et al, and the chosen line of analysis for this Thesis. The premise that research is actually about finding out things, and that that this comes from having an initial direct question, or set of questions is one that could be more closely described as the drive behind this research. It also is the driver in joining the Professional Doctorate curriculum. It provides a medium to bring in personal and peer experience to benefit the overall research.

In understanding where the outputs of the research were to be best applied (the profession), it was clear that a systematic review of what had gone before would not provide the strength of argument for the expected output, a code of conduct, of this research. At each significant milestone the research would have to pause and understand if the path was still:

- Relevant
- Timely

During the literature review phase, it was agreed with the supervision team that a paper should be presented to fellow post-graduate researchers on the background and status of the research. This paper was then subsequently presented at the IT Security Conference for the Next Generation, in November 2009 at the University of East London, London, UK. The contents of this first paper are at Appendix A.

Towards the end of the research, the outcomes of the work were clarifying and it was felt appropriate to reach out to a peer audience both in a spoken and written form. Feedback on the viability of a code in the profession would be important if the published Thesis were to provide support to actors in the field. Given that the researcher was a regular speaker on various information security topics at an Executive level Internationally, it was then a matter of choosing a varied set of peers to ensure the feedback would be as valuable as possible. Finally, the decision was made to follow three avenues of formal publication and discussion of the research. Firstly, a presentation on improving forensic capability in the commercial sector was provided to the NetFocus (2012) annual Information Technologists Seminar series.

"*Net Focus UK is the forum where the industry's leading experts help solve the most critical situations facing businesses using the Internet.* " (Netfocus, 2012, p.1).

A supporting text, in the most part reduced from the Appendix A submission was provided for the on-line Netfocus community discussions which continue during the year. Secondly, being asked to speak at both of the MIS Trainers Institute CISO Summits in Prague and Abu Dhabi, (MISTI, 2012), the opportunity was taken to introduce round table discussion on the need for professional certifications and governance in the Computer Forensics profession. Finally, many members of the profession of Information Security have been discussing the need for a more formal way of sharing views than on un-moderated avenues currently available such as Twitter and LinkedIn groups, but arguably less structured and creativity restrained than traditional academic papers or professional journals. Focus of the new avenue is non-commercial and designed to cross between the electronic and the printed medium. Most importantly it is expected to create heated discussions within the community on many controversial topics. A paper, updated from the Appendix A paper has been submitted, and is being editorially revised for inclusion in this new publication (as at 24 November 2012). The funding and backing for this new venture is currently under discussion and as such is not possible to name at this time. Given the timing of this Thesis, it is hoped initial feedback will be available in Q1 2013, as the inaugural edition features the extracts of this research. This cross-section of sharing the data in this work provided much of the

feedback in honing areas such as training need and clarity of code. Much interest has also been shown via these avenues in working with the finalised Thesis, once published, to view how the proposals could be used in the commercial sector by many actors in the field. This interest has provided added impetus in finalising this work.

This research then, initially set out a series of direct questions, laid out a structured path to document the answers, organised an audience prepared to review and challenge any outcomes, and still had a basic failure in the research efforts – where to actually start.

Saunders et al help greatly, specifically in their review of Easterby-Smith, Thorpe and Lowe (2002), in particular

"…the requirements for the research to have some practical consequence. This means it either needs to contain the potential for taking some form of action or needs to take account of the practical consequences of the finding." (Easterby-Smith et al, 2002, p. 94).

Saunders et al (2003) further argue that then recent, in 2003 at least, discussion within the British Academy of Management focused on the trans-disciplinary nature of research. This underlines the premise that this Thesis is driven by, namely that for any research to be useful, it must consider each related area of the subject under question. This Thesis therefore in the process of properly pursuing a course of research for this seemingly narrow topic, has indeed needed to consider many related fields to properly provide a considered and informed response to the challenge the topic has posed. In outlining objectives at the very start of the research, it was clear that many parallels would be needed in order to provide sound conclusions for the code. Many organisations have codes of conduct, and a proportion of those actually censure members for transgressions. Censure then was one of the topics that had to persist through the research, otherwise why bother with a code if it had no teeth.

Tranfield and Starkey (1998), are used by Saunders et al (2003) as examples of the modernist theory that ideas should be developed and related to practice, and that research should *"complete a virtuous circle of theory and practice"* (Saunders et al, 2003, p. 4) in which the practice of a profession informs the research into that

profession. Saunders et al (2003) mesh the academic world and practical delivery in their arguing, which supports the underlying arguments of this Thesis, that Computer Forensics practice, and indeed other information security specializations must drive the need for considered academic research if they are to be considered a profession. It also seems to be the beginnings of the underpinning arguments for what is now being termed, the Professional Doctorate. By ensuring that practical experience of both the researcher and peers was used at various stages of this writing, there always was an underlying test mechanism to ensure that advice or outcomes were relevant and useful. Straying too far into the practical, however, has been an oft repeated mistake, and researching supporting, not opposing data for pre-formed arguments was one area that was difficult to prevent. This has been especially difficult in finding negative views on actually needing a code of conduct and governance, but there are examples in other professions that serve as test data for that code to ensure its usefulness.

Exactly what defines a profession has been argued many times and in particular forms a large part of the writings of the "Security Journal". The Security Journal is affiliated to the American Society of Industrial Society, which is arguably the first independent certifying organisation for security professionals world-wide (ASIS, 2009), providing supplier agnostic professional industry credentials. The specific discussion around computer forensics as a profession, similar to that argued by Manunta (1996) about the security "profession" as a whole, also affects the output of the research. The arguments presented by Manunta, centre around the manner in which traditional professions such as medicine and law have evolved, and what makes them a profession. It is suggested, that to be called a profession it should exhibit certain traits that are common across the peer group. Manunta argues that peer review, in one form or another is critical, stating that the acceptance of practicing professional status depends upon practitioners already in the field, and as such suggests that the quality and skill levels will be naturally maintained. It is not the intent of this Thesis to argue for or against his work here, merely to provide an awareness that in the eyes of Manunta, because of the lack of some basic characteristics of the community, security (in this case as a whole) may not call itself a profession. In providing the means by which, if accepted, the forensics community could be peer reviewed, certified and held to a code of conduct, this Thesis

will hopefully provide input to the discussion. Perhaps therefore suggesting that Manunta would have to look again at least at this particular branch of what indeed is generally called a profession.

Button (2005) interestingly offers the suggestion of a "license to practice", which few of the other calls for standardisation make. This is an important part of the later arguing of this Thesis, for if one were formally licensed, as this researcher strongly believes should be the case, then a license could be revoked for malpractice, as in the legal or medical professions. It would also clarify the semantics at play as discussed earlier as to what the term certification can be taken to represent.

Returning to Saunders et al (2003), they present a conclusion to their chapter on the research process which argues research (in that case on management) needs to advance not only knowledge and understanding, but should help towards providing answers to business problems and practical management issues. This Thesis provides that this is a basic tenet of any research aiming to add value, and indeed the outputs of the research effort here must surely pass that test. By including seasoned professionals in the new Professional Doctorate streams, this experience is brought in naturally to the discussion.

2.1 Practicality

Comte (1877), one of the renowned sociologists of the 18th Century is quoted as having described;

"the progression of knowledge as being one from predominantly theological or supernatural explanations of reality to metaphysical or philosophical ones and finally to scientific approaches" (Hagan, 1997, p. 7).

So, even two hundred years ago, scholars were arguing what is being discussed here, which is that the output of research must have a practical edge for it to be considered complete.

In considering the audience for this Thesis it was important to properly understand the potential effect that a positive outcome would have. As Hagan (1997) points out, an

author has reciprocity of trust with the respondents to any questioning; arguing that it involves an obligation to ensure that the information shared is not used in an inappropriate manner, or in a way which could cause harm or embarrassment to the subject. Hagan also argues that objectivity in the research process is paramount, warning that researchers should refrain from entering into research for which they have deep interest. The danger being they could deliver biased or tainted reports of data gathered or studies completed. Given that this researcher has a significant amount of experience and indeed an expected direction of outcome for this research, this would seem to be good advice. This will bear scrutiny to see if it was not properly considered when the Thesis is published and critiqued by peers. Hagan states a belief also that an author should not misrepresent their research abilities to augment the actual value of their data. It is the duty of the author of the work to ensure that the audience to which the outcomes are presented are professionally capable of judging and forming critical opinions based upon their own experience and theory. This is pertinent advice and does already form part of the delivery methodology of the research of this Thesis. Becker (1986) believes that researchers can become terrorized by the literature, that is there is an absolute mass of information to be pawed through, so much that the author just cannot get started into the dissemination into meaningful pieces.

Hagan (1997) suggests that to limit the amount of information to review, an author should leave out popular literature and the mass media in favour of professional journals and previous research. In this subject, the majority of information actually sits in the popular press. The Thesis discusses practical failure and less than optimum deliveries in the commercial sector, and as such these tend to be reported in a different manner, if actually reported officially at all.

2.2 Matthew effect

One issue which this Thesis wishes needed to consider was the assumed intention of finding fault in other research in order to prove ideas and opinions offered in the research under way. This is presented in a discussion by Hagan (1997) in suggesting one needs not go too far to find some error. Further opinion is provided how various

researchers have focused only on the errors, but then usefully offers the test that errors should only be highlighted when they challenge *grossly* the accuracy of outcomes. Similarly, focusing on the conclusions drawn from the faulty data, is equally remiss. We are advised research should not be scathingly attacked for what can be described as the sake of one-upmanship. Merton, as described in Hagan (1997) identified the *"Matthew effect",* relating to a passage in the Christian Bible. This is loosely described as a tendency of those who are already published, to get further published. This outline of the effect also prescribes that there is a tendency in the research field to cite each other and exclude new ideas from people outside of the clique. This then devolves the scientists or in this case research scientists, into *"a small circle of mutual admiration societies*" (Hagan, 1997, p. 9).

In continuing the comparisons of pure versus applied research, Hagan (1997) argues that pure research is concerned with the acquisition of new knowledge for the development of the field or the sake of science. Conversely, applied research should be used to solve immediate policy problems in that field. Hagan also poignantly informs us that the criminal justice field has always had conflict between the *"common sense"* applied research and the theoretical basis of pure research as can be expected from the academic community. Pure research would usually not be expected to add immediate value to the field but would probably add to the overall knowledge base and contribute to the advancement of the field (Hagan, 1997). James Stuart, previous Director of the US National Institute of Justice (NIJ):

"Criminal justice research and practice is at an important stage in its development. Whilst still in embryonic form, criminal justice could evolve like the fields of health and engineering where those who conduct research and those who practice, essentially share similar paradigms, and look naturally to each other for information and guidance" (Hagan, 1997, p. 14).

2.3 Previous work

One of the most challenging parts of this research has been finding similar attempts to quantify the need for such a stringent code of conduct and ethics in the UK private

sector forensics community. Jankowicz (2000) strives to have us understand that the value of your work is only in relation to others efforts, and that knowledge does not exist in a vacuum. Further discussion results in the introduction of an interesting concept that seems to suggest there is no such thing as original thought. Saunders et al (2003) attribute Jankowicz as saying that the work of an author will only be significant to the extent that it matches or questions previous thinking. Again, could this be more evidence for the existence of the "Matthew effect" (Hagan, 1997), or at least some further arguments to work with. Mortman (2007) challenges that the majority of organisations that claim to have ethical standards actually are only using the word to bolster the apparent quality of the certification, calling this propensity a smoke and mirrors certification. Further, the only International Security organisation that could be claimed to require an ethical understanding is the American Society of Industrial Security (ASIS) as it appears in the curriculum for certification (ASIS, 2009; Mortman, 2007).

Much of the related research that does exist has skimmed around the part that law enforcement, and the law itself has played in the glorification of the forensic profession. Confusion abounds in the industry and indeed in academia whether forensics is a new profession or an extension of older, more established professions (Manunta, 1996; Simonsen, 1996). Even researchers cannot agree whether the activities, more commonly known as computer crimes or infractions are new or old, and therefore should require new professional responses or methodologies. This is quite clearly presented in the following extract:

"There were no new laws to deal with the crimes or guidance as to how to tackle them but most of all the great lack of expertise to understand the intricacies of the crimes, the wide demographics it covered and most of all jurisdiction issues" (Taal, 2007, p. 62).

This research has been unable to uncover any previous academic challenge to these perhaps controversial views expressed above on the lack of expertise in the industry.

2.4 Definitions and clarifications

This section will align some of the basic terms and concepts that will be repeated throughout the Thesis. Whilst in some cases this would be classed as a bibliography, the evolution of the field and its embryonic state requires that we explore some of the discussion around the definitions of basic terms as well as the sometimes conflicting opinion of what definitions should be. Some of the legislations relevant to this Thesis may not be immediately familiar to the non-technical person, it is necessary therefore to provide some direct references for further analysis as needed. These are discussed in Section 7.2, related acts.

2.4.1 Forensics:

" the use of an expert to preserve, analyse, and produce data from volatile and non-volatile media storage. This is used to encompass computer and related media that may be used in conjunction with a computer"(Meyers and Rogers, 2004, p. 1).

Meyers in the following year (2005) further claims that computer forensics is a sub division of digital forensics and partially cites Palmer (2001) for some definitions. Palmer uses a list of specific terms to describe the analysis of digital data: "*network forensics, virtual crime lab, remote forensics and cyberforensics*" (Palmer, 2001, p. 5).

In lay terms, one could regard forensics as the uncovering of data trails and files from information systems. These trails and files may or may not have been plainly evident prior to a forensic effort.

2.4.2 Evidence:

"either the state of being evident; something that makes another thing evident: a sign and a statement of a witness, an exhibit which has bearing on or helps establish a point in question, usually in a court of law" (Sennewald, 1981, p. 117).

Again, in lay terms, this researcher offers a simplistic view that any data that has a bearing on the initial reason for the work in question (recovery or analysis) can be classed as evidence. Many argue that data that has been recreated can not be called evidence, but if voice data from a black box recorder in a crashed aeroplane can be recreated by a synthesiser and termed evidence, then surely similar recreations of computer data can also be thus termed.

2.4.3 Ethics:

"Ethics is the practice of making a principle choice between right and wrong. Such principles are notions of behavior [sic] that are commonly accepted in society although different societies have different notions of what is acceptable" (Chadwick et al, 2007, p. 197).

Ethics, relate to a series of beliefs. Every person has ethics, they stem from personal and societal values as accepted by that person. This makes the commonality of ethics difficult to define as each society and educational system will instil a different set of ethics. Whilst people may all have the same regulation, a common set of rules, their ethical values, that is what they believe rather than are forced to follow will differ. Hagan (1997) cited the need for researchers in the field to subscribe to a code of ethics, claiming that there is an assumption of three things; trust, ethicality and integrity by dedication to such a service or science.

2.4.4 Professionalism:

Hagan (1997) argued that professionalism is looking to show others that there is a reason to be deserving of the prestige and remuneration that comes with such aspirations. The evidence that the occupation has achieved this status can be such as that it will generate its own esoteric and useful knowledge. There are references throughout this Thesis to professional status and what that entails, so it will not be laboured here, suffice that bodies, traditionally understood to be professional, have certain defined characteristics that the Information Security, and therefore subset Computer Forensics

profession may not currently exhibit. Hagan also argued that regulation of conduct must be organized and indeed mandated from within the profession not by legislation or government bodies.

2.4.5 Hacker:

Previously, the term hacker was applied to someone with a patent curiosity in the workings of computer systems and the data that they generated. Usually exploration and access to these systems, albeit unauthorised had a non-malicious intent (Howe, 1995). The following statement of beliefs clearly outlines what was then understood by the term hacker:

"1. The belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing free software and facilitating access to information and to computing resources wherever possible.
2. The belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism, or breach of confidentiality" (Howe, 1995, p. 1).

Later, and it was the opinion between operators in the field when the Computer Misuse Act (Great Britain, 1990) was passed that the nicknamed *Hacking* Act was more a matter of political expediency than a considered path towards effective legislation. This act was to affect the need for expert data forensic testimony more than any other. The passing of the act was generally felt to have been necessitated by the inability to properly prosecute the much publicised outcome of what could now be considered a basic technological and commercial security failure, i.e. the hacking of a voice message box belonging to a member of the British Royal family (Cornwall, 1988). This rapid passing into law, which arguably was indeed overdue, has sometimes been questioned as to whether proper consultative process was followed. Given the visibility of the issue and the personas involved, the prior lack of any relevant legislation to prosecute, clearly brought the term hacker into the greater public vernacular, perhaps for the wrong reasons. Whatever the motivations, the term hacker from that point forward could be regarded to have taken on a new meaning.

If the failure to prosecute in the mailbox hacking case above that which was obviously a criminal act, suggests a lack of expertise was available to understand or tackle the "new" crimes, then the points Taal (2007) presents on this are ratified (Cornwall, 1988). It is however, suggested by this researcher that the expert fight against cyber-crime had actually been running for a long time before that one great burst of publicity both in the public and private sector (Cornwall, 1988). We may however, have to thank this widely publicised Royal security breach for speeding up the larger discussions on computer crime and therefore data forensics.

2.4.6 Hacking

The author of this Thesis was heavily involved in the prosecutions of two similarly high profile, but much more sophisticated computer hacking activities, which by reference should give evidence that expertise was indeed available to prosecute such crimes. Firstly, the Computer Chaos Club of Hamburg, (CCC) which described itself as a *Galactic community of life's beings.* Formed in 1981 it is probably most publicly famous for hacking into the German *Bildschermtext* system, arguably one of the first on-line banking systems (Anderson, 2008). Their published aim was to investigate how computer systems could support the German Greens party. It is generally held they were scavenging around various military and commercial systems, selling secrets to the highest bidder, sometimes hacking into specific systems to order (Anderson, 2008). In 1989 five German nationals related to the CCC were arrested and convicted of espionage on behalf of the Soviet Union. Anderson, goes on to relate that much later in 1995, the CCC attempted to disrupt the national infrastructure in France, in particular the telecommunication provision by hacking and effecting changes to the activities of critical software, this was reportedly in protest to French nuclear testing. Evidence then that by uncovering these attempts, data forensics was even if in a state of relative infancy, actually at play.

2.4.7 Social engineering

The other highly visible activities that support the challenge that computer forensics is not as new a profession as we would be led to believe are those of Kevin Mitnick. Mitnick was probably the first of what we are now calling computer *hackers* in a malicious vernacular. His criminal exploits against Digital Equipment Corporation (DEC) and other companies and agencies are loosely described in a work titled "*The art of Deception*" (Mitnick, 2003). Essentially Mitnick used a subversion technique now generally coined as "social engineering". Social engineering is best described as a technique whereby someone (not necessarily for criminal intent), will use knowledge already gained to either manipulate someone into doing something they would not otherwise have done, or gain more information to enable actions to be performed at a later date to achieve a similar result. A relatively recent, much repeated example of social engineering with malicious intent is to suggest a contract with someone claiming to have something they need, but the sender will not be able to release that item without confirmation from the target of a further item of information. Usually this item will be significantly more useful such as bank details or billing addresses. The newly divulged information can then be used to obtain funds or advantage, criminally. Only by using a process of data forensic investigation can the overall intent of the effort be truly understood. This style of social engineering includes what is now being coined as "Phishing" when done via email, which is a way of getting deeper information from someone than you initially hold, usually purely an electronic mail address. By presenting an initial level of familiarity, phishing is sometimes also used as a means by which to download malware onto a Personal Computer, to be able to gather information at a later stage at will. Again, generally it will require a proper data forensic analysis to be able to truly interpret the intent of the activity in the absence of a guilty party.

2.4.8 Denial of Service

In what is still claimed to have been, somewhat implausibly an accident, Robert Morris, the son of a prominent security expert (who was engaged by the United States Government) released onto the commercial networks of the time, what we now know as

a worm. In 1988 Morris wrote, reportedly as an intellectual exercise, a computer program which would gauge the size of the then Internet, i.e. the number of systems connected by that common network grid. The tool supposedly misfired and essentially brought commercial and, although unconfirmed, some restricted military networks to a standstill. This effectively created the first "*Denial of Service*" attack, or one which fatally interrupts the normal flow of traffic to a network site.

2.5 Network forensics

It is suggested that some knowledge points are to be taken from the experiences of the European Union (EU) (Rosenberg, 2007). To provide some background, we had been presented with claims that the network forensics profession was in need of standards and standardised tool sets. In 2003 the EU released the first global network forensics standards, which it intended at least all EU nations to implement. It argued that these standards were clearly presented and strongly promoted, but claimed that they were unsuccessful, concluding that the computer security community within the EU appeared to have rejected or ignored these forensic tools. Similarly the EU body claimed a complete indifference to the call to use them (Rosenberg, 2007). Unfortunately there is no associated evidence as such, or research presented in the Rosenberg work, or indeed any details of the standards themselves which would support the description of them being *network* forensics standards.

Asking how this happened, Rosenberg suggests, rhetorically, that the answer could lie with the standards themselves, finally providing us a better hint of the standards under review by suggesting:

"The EU's recommended forensic applications were Web-based freeware, written in XML. This design was well intentioned and practical, given the EU member nations' varying rules of evidence. However, XML is slow, and quickly has become outmoded; a Web-based application's value depends on its browser and network connection; and as a way to gather evidence in a high-stakes judicial case, freeware is a dicey solution" (Rosenberg, 2007, p. 1).

What we then gather is that the proposed tool set for network security is in fact what is being termed network forensics standards, and "resounding" call for clarity in the field in that work would seem even is clouded by the arguments therein. There is nothing here that this researcher would suggest is not happening around the industry. Terms and jargon are being reused in many arguments without proper definition, so no one use of a term can be classed as wrong merely because it does not reflect the understanding of the other person. The argument is carried in so much as that without clear definition of terms and expectations, confusion will continue. Neither is this any different from other Information Technology specialisations. In a paper released on the 15th April 2010, the Security Awareness Special Interest Group (SASIG) and the Information Security Awareness Forum (ISAF) launched their paper on convergence, designed to help people in the security profession understand the convergence of risks across traditional and IT security fields. In summary, a paper designed to help clear up confusions (ISAF, 2010). In this paper Information security was then variously called, "*Digital Security, IT Security, Data Security, Intangible Assets*" (ISAF, 2010, p. 1). Clearly, no such promised clarity of definition even in the Information Security profession, and hardly a success in clearing confusions.

Rosenberg expands criticisms of the EU suggestions by discussing the fact that companies may not want to pay for tools when they do not use them, which would seem to be a sensible challenge. The extensive referrals to the United States National Institute of Standards and Technology (NIST) could suggest that there is a bias to present the NIST work as a worldwide standards accreditation body, and therefore no need for any other country to go to the effort. To continue with a further extract of the article;

" Commercial network forensic and analysis tools are common now, and need not be highly elaborate or expensive to provide users with complete and easy-to-understand data. Manufacturers of forensic and visibility tool kits should partner with standards bodies such as NIST, to create functional and lasting standards for network forensics. Network forensics is growing more important. Standardized tools and methods will ease the job for network researchers and expert witnesses, and will be an improvement to the judicial system itself" (Rosenberg , 2007, p. 1).

It is relevant to take the page space to relate exact wording here as it is important for the Thesis to remind that there are also sometimes national interests at stake in the proper functioning of data forensics as a profession.

2.6 Early forensics work

Without expertise in forensically tracing the intricacies of the Morris worm, neither the eradication of its effect or the prosecution of its creator would have been possible. Perhaps the arguments that Taal (2007) presents of not having the expertise available, to understand the intricacies of the crimes, at least in this case, would seem to be opposed by the evidence presented here. Therefore, this Thesis will not rely heavily on the outcomes of that research, but will of course consider some of the very interesting and pertinent challenges presented, along with the respected opinions of that researcher in that paper Taal (2007).

Long before the World Wide Web was in general use, and before most countries had legislation to formally handle computer crime or *hacking*, there was already a need to gather information on nefarious acts in the commercial sector. The need was to understand, and therefore mitigate, weaknesses in the increasingly rapid adoption of newer technologies and methodologies of computer use. The arguments and challenges this Thesis is referencing from earlier research in the 1980s and 1990s are unfortunately therefore just as valid and current as those from this decade, little seems to have changed therefore in the area of commercial sector governance of data forensics.

The further reason for extending the detail of these three early examples of computer forensics here (CCC, Mitnik, Morris) is to rebuff many arguments that computer forensics skills are new and relatively unavailable. By reviewing the cases above, it is clear that we must have had properly experienced experts available. They were able to understand events, gauge the impact of the activities on systems, and importantly decompose evidence found on systems into understandable chunks. Only by this expertise could prevention, remediation and prosecution have occurred. This is then variously known as computer, data, system or network *forensics*. This Thesis contends

that these skills have been available almost as long as the infractions have been occurring, and yet the systematic professionalism of these skills is still under discussion.

2.7 Summary

This chapter has reviewed the questions, and direction used to perform the research as well as some of the guidance that has gone before in the area of governance professionalism, and certification. It has explored the discussions on the emerging field and the various opinions that are shaping its future evolution. The definitions hopefully will serve as the discussion continues and more detail is added to the need for governance in the sector.

3 Crime Scene, Evidence, Laboratory, Presentation

One of the basic challenges outlined in the thinking for this research, and indeed in the experience of this researcher was how to sensibly provide for proper evidential procedure in the private sector during the forensically sound acquisition of forensic data. This chapter explores some of the shortcomings of current practice, outlines some of the more critical mistakes that have been publicised, and importantly considers recent guidance that is growing in how to correct the situation.

"The Association of Chief Police Officers is expected to announce new guidelines informing businesses how they should store and treat information they believe will be used in computer crime cases; and the Institute of Information Security Professionals says that it will be announcing long-awaited plans for a registration scheme within the next two months" (Warren, 2007, p. 2).

This above extract summarises the basis of the evidence section that follows. The private sector, whilst perhaps sometimes being on the forefront of the forensic profession in terms of investment and tools, is almost always behind the public sector in the area of governance and controls. The Thesis explores the rapidly changing computer landscape, and how the forensics profession is having to evolve just as quickly to keep pace, even without the benefit of strong controls and guidance. This chapter also outlines some of the challenges that are presented to investigators, and having laid out the possible errors that can be made, will open up avenues for discussion in later sections as to how to control or rectify these errors.

The laboratory section explores in some depth the actual workings of forensic investigations. It reviews in detail some of the areas that an investigator is required to possess knowledge of, and explores some of the basics of data manipulation on computer systems that forensic investigators rely upon to be successful. It challenges some thinking around the level to which an investigator should be experienced and provides for some suggestions, to be followed up in the training section about how these knowledge requirements could be met.

Finally, the presentation section explores an area that is largely ignored in current technical forensics research, the presentation of outputs. Whilst research tends to be specific and focused on a particular area of forensics such as recovery algorithms, bad disk areas and suchlike, the broad nature of this Thesis requires that the profession of forensics be reviewed as a whole and the integrity of the profession be provided with guidance and suggested controls as part of the conclusions. An investigator must be able in some manner to present the outcome of an investigation in a professional and concise manner in order that the basic challenges against that output, and understanding of the conclusions can be made.

Whilst it has been a repeated statement that this research is aimed at the provision of support to a code of conduct and governance around private sector investigations, it is relevant to detail the excellent prior work in the public sector in documenting their suggested procedures.

The Association of Chief Police Officers (ACPO) is tasked with providing good guidance and best practice in the UK criminal policing sector.

The four ACPO forensics principles (ACPO, 2009) are outlined here to understand the perceived basis of need.

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Figure 1 ACPO Principle 1

Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Figure 2 ACPO Principle 2

Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Figure 3 ACPO Principle 3

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Figure 4 ACPO Principle 4

(ACPO, 2009, p. 6).

Data Clinic Limited (DCL), a commercial forensics service offer what is probably the most succinct explanation of what the ACPO principles are aimed to deliver (DCL, 2009). In presenting an explanatory view of the principles, DCL argue that computer based electronic evidence is no different from text contained within a document. DCL conclude that for this reason, the principles in fact state that the computer forensic evidence is subject to the same rules and laws that apply to documentary evidence.

The ACPO guide, is written to provide guidance on public sector forensics, and DCL explain;

"the doctrine of documentary evidence may be explained thus: the onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of police" (DCL, 2009, p. 3).

3.1 Privacy

Investigators in corporates, in general, rely upon the widely held premise that the company owns, or at least has a right to monitor and manage, all the data on its associated systems. This is an understandable but controversial argument (Livio, 2010; Wesche, 2002; privacy.org, 1993). If an entity hires a painter, provides a canvas and nourishment and remunerates the painter to paint a scene, it can be assumed that the painting belongs to the entity to do with it as it sees fit. Similarly, if a reporter, working for a newspaper provides a ground breaking story, it is usual to assume that the newspaper and not the reporter owns the copyright to that story. These arguments cover the ownership of intellectual property. Similarly, discussions around the coffee machine or in a hallway traditionally have been regarded as private and personal, and rarely would there be an expectation of any commercial enterprise monitoring and recording such conversations. With data on a computer system however, it can be argued that it is not that easy to define the boundaries of privacy and intellectual property. Data has many forms and is gathered in many ways. Because of the nature of computers, and in particular so called Personal Computers, there are activities that are sometimes performed by the employee or office user that may be regarded as personal or indeed secret. Analogies abound, but this Thesis suggests that in an office environment, if an employer were to act upon, or monitor discussions that are held in the canteen or coffee areas, totally unrelated to the work activities then the basics of personal privacy can be held to have been breached.

What is not so clear is the recording of telephone calls for example, to meet legislative requirements. These calls are often difficult to separate from personal calls that are often tolerated to some degree by organisations. Only by opening the call record can the contents be understood, and by then it can be claimed that personal privacy has already potentially been breached. The discussions around why employees should have expectation of privacy in the workplace are legion, and more rigorous than simplified here (Livio, 2010; Boren and Gates, 1994; privacy.org, 1993). Suffice to relate that many companies do hold that any data created on systems provided by them to perform work activities is “fair game” to review in an investigation, irrespective of the

provenance of the data. The most notable challenge to this was by Innamoroto and Krulewicz (2009) in a review of a case in the San Francisco court system, where they successfully challenged the right of an employer to read private, or non-business related email. It is worth noting here that throughout, the Thesis is aimed at the private sector, and its forensic activities. Companies exist to make a profit, and part of that profit making in rounded terms involves the taking of risk. One of the risks that this Thesis suggests is that companies are not always properly advised in the exact boundaries of legal and illegal behaviour in the analysis of systems that may hold personal or private data. In some cases, the experience of this researcher is that even if an investigation crosses legal boundaries, companies may condone the continuance of the activity to ensure an outcome of the investigation, perhaps better paraphrased as *hoping not to get caught*.

3.2 Ethics

Ethics, relate to a series of beliefs. Every person has ethics, they stem from personal and societal values as accepted by that person. This makes the commonality of ethics difficult to define as each society and educational system will instil a different set of ethics. Whilst people may all have the same regulation, a common set of rules, their ethical values, that is what they believe rather than are forced to follow will differ.

As discussed above, once an investigator strays from the narrow focus of the primary investigation, for whatever reason, investigators have been seen to act with questionable moral or ethical boundaries in the pursuit of information gathering against a target. For example, this may involve. the expansion from reviewing what is clearly company data to perhaps personal and private data and therefore straying into potentially unethical or even illegal activities,

"An existing corporate client telephoned our offices late one Friday evening requesting an urgent meeting due to the fact that he suspected that his business partner was using their offices, facilities and finance to launch his own business. International Intelligence Limited were tasked to carry out an in depth investigation into this individual, his

personal finances and to obtain intelligence via investigation and electronic surveillance in order to obtain leverage to force a resignation or face prosecution. We were able to obtain information from our client's computer and telephone system, thus providing recordings of conversations and also emails proving that the target was indeed going into competition with his (at the time) business partner. As a result of our investigations we were able to provide enough evidence to force the Director to resign. He willingly took that option rather than going through lengthy legal channels" (IIL, 2009, p. 1).

Clearly, in the IIL example, there were no expectations of the investigator that the Director of the target company would be granted any privacy on his computer system, or telephone system. As is generally expected in such cases, or at least in the experience of the researcher, instead of reverting to the powers of law, in what could arguably be classed as a case of computer hacking, if not simply a breach of privacy, the target *folded and ran*. Grobler & Louwrens (2006) poignantly argue that not all investigative actions that are clearly legal can automatically assumed to be ethical. Commercial investigations are often based on a hunch, suspicion or sometimes plain curiosity. This Thesis suggests, that this driver is in vivid contrast to a police (magistrates) search warrant in the UK for example, which specifies exactly the boundaries that any investigation must remain within and the justifiable reasons for the search. Any stepping outside the boundaries and scope of the agreed search warrant can, and often has, caused a failed prosecution, even in the face of blatant guilt. Once again, this relates to the British (criminal) justice systems overarching desire to follow due process, sometimes at the detriment of truth and justice, previously mentioned in Section 1.9 (research background).

3.3 Crime scene

In traditional forensics terms, a crime scene is usually able to be physically segregated and cordoned off until the investigating officer is confident that enough evidence has

been gathered, or that there is no further value in segregating the area. We imagine things like shootings, suicides, armed robberies and bombings as crime scenes, all well-defined areas bounded by assumed relevance to the criminal event. The crime scene a computer forensic investigator is faced with is rarely so well defined. Usually an unexpected failure or interruption will cause either a suspicion or claim that data may be available on a computer system, to prove or disprove the particular event, or series of events. A first responder in a computer forensic investigation is generally the computer user or system operator of that system. To provide a parallel, it is not dissimilar to the victim of a violent crime being asked to cordon off their particular understanding of the crime scene in case evidence of the crime be available. In the case of such computer crimes, the first responder (the user) can in some cases also be the miscreant, and this has to be taken into account when managing computer forensics cases. This is the first area that has evolved in this research, namely if proper evidential procedures are expected to be followed, and indeed they must if proper investigative procedure can be depended upon, then it is clear that evidential first responders absolutely must have proper and relevant training, and also must be properly selected. This training would encompass the proper seizure of computer systems, relevant media controls and evidential triage.

3.4 Seizure

Any device that is used to capture data evidence must be certified as free from contamination. Just as in traditional crime forensics where the scene of crime responder would use gloves and sterile receptacles to gather evidence, so should any data devices or containers used in computer forensics also be sterile. In some cases, where electro-magnetic interference is a concern, such as in areas of high voltage or microwaves, then Electro Magnetic Pulse (EMP) shielded carriers may need to be used. Properly trained and aware first responders would be fully *au fait* with the need in such cases. Traditionally, when computer media was delivered from the factory, it was contained in anti-static bags to ensure that any on-board electronics could not be contaminated by static or other electronic discharges. It is accepted good practice to maintain this method

of transport for any media that could possibly be affected by static or other discharge to prevent any such issues.

3.5 Media

In most forensic captures, there will be the potential to make either a search based extraction, for example from a large server farm, or in the case of a single or small system, full disk capture. The media used should be certified clean and malware free, and there are discussions as to what this would entail (Guidance Software, 2004). Whilst this research has not concentrated specifically upon targeted malware, as this is a different subject area, it would be certainly a very useful research area. Brand, Valli and Woodward (2010) presented a paper on the subject in Perth during the Edith Cowan Digital Forensics conference, offering an interesting analysis methodology. The paper concentrated more on the intent of the malware however, importantly the background information and supporting research was very enlightening. Another area of current research is that of looking at methodologies for future use to properly certify media as being as free of contamination as is as reasonable to expect. In discussions with involved researchers, it is apparent that the University of Glamorgan is already doing extensive research into the verification and clarification of these challenges (Glamorgan, 2010).

3.6 Triage

As we will see in the training and certification chapters (Chapter 6, Chapter 7), the aim of the first responder is to categorise evidential capture in the most effective manner. This can be in the form of urgency for example where data is likely to change or be overwritten, or in some cases where the devices are in a state of decay. It also should classify any reasoning for using search techniques to selectively extract relevant data in the cases described above. Triage has the same effect in computer forensics as in any other use of the word. It uses a methodology, usually based on urgency, perceived importance and viability of item to ensure that effort is expended in the most efficient and productive manner possible. Obviously, just as in an emergency accident situation

where an on the scene doctor would triage victims for survivability, then a forensics analyst will triage artefacts during acquisition to ensure the best outcome of the effort.

3.7 Solvability factors

Mendell (1998) offers a comprehensive list of solvability factors. These factors have been in use by many operators in the field, particularly in the USA for a long time and these arguably should be considered before the evidence capture process is begun. In the absence of any other checklist, they form a basis on which an analyst may be given hints as to how and where to triage, if not concentrate search efforts:

3.7.1 Modus Operandi (MO)

"A unique Modus Operandi speaks from the crime scene or from the fact pattern surrounding the scene." (Mendell, 1998, p. 16).

Given that the majority of forensic analysts, presented with a crime scene, or tasked with a data recovery will have had prior experience, it is proper to expect them to apply previous knowledge and experience in assessing the viability of effort. For example, in the relatively early evolution of the Internet, Digital Equipment Corporation (DEC), then the second largest computer manufacturer held user symposiums yearly for their current and prospective purchasers. The Digital Equipment Users Society (DECUS) was provided with the facilities to review new versions of operating systems, try out prototype systems etc., usually under non-disclosure, but in many cases open access to front ends of systems. There were also many presentations by DEC specialists as well as DEC users on various subjects, for example DECUS Cannes, France in 1992 (DECUS 1992). The Digital Equipment Security teams would be supporting the event, ensuring that disruption of these systems by malfeasants was kept to a minimum by monitoring keyboard activities on the floor of the exhibits. Quickly, year after year it became very easy to spot the body language and activity characteristics of those who had come to be other than curious. This is one example where a known MO was used to identify a need for forensic (or other) intervention.

3.7.2 Persons

"Only one person or a limited number of people could have committed the computer crime." (Mendell, 1998, p. 16).

In many situations where closed offices are involved, inexperienced analysts will jump to a conclusion that door entry records or building control records are adequate to assign a specific body to a place and time. In many cases this has been the avenue to total waste of effort, and sometimes wrongful accusations. The factor above is as much around understanding how multiple people could *NOT* have committed as much as *COULD* have. Access cards can be stolen and swapped, passwords shared and compromised, keys forged and doors left open. Certainly the challenge of integrity of passwords and therefore used to prove who had access has long been dismissed as useful by most analysts. In specific situations where physical controls prove that system access was only possible by named individuals, such as in a the case of a disconnected computer, can an analyst use presence as sole indicator.

3.7.3 Physical

"Strong physical evidence found at the crime scene." (Mendell, 1998, p. 16).

This factor in essence speaks for itself. If evidence is appropriate to the investigation and suggests a sound theory of culpability, then it would be appropriate to proceed with the investigation, expecting a solution".

3.7.4 Software

"Software or software tools discovered in unauthorised hands." (Mendell, 1998, p. 16).

In most modern societies, software theft is a criminal offence, if not just a copyright issue. Given that an analyst is aware of software seemingly stolen or misappropriated, it is in most cases reasonable to expect a probability other evidence of non-conformance to societal rules. If the investigation (as most are) involves uncovering miscreant

behaviour, then stolen software would seem to be one good indicator of character either of the user or owner of the system under review.

3.7.5 Honeypot

Activity occurs on trapped files (latterly known as a honeypot). (Mendell, 1998, p. 16).

Honeypots have been in uses since the very earliest attacks, including some of those mentioned earlier (Mitnick, Morris, CCC). There are various types of honeypot, at least in terms of computer security, and most are very well detailed by Spitzner in a 2003 paper (Spitzner, 2003). Essentially the aim of a honey pot is to perform activities using a simulated environment that purports to be a real system or application. It is intended to mimic the actual target of a malicious attack, fool the operator (system or person) enough to continue the effort and gather enough *modus operandi* on the attack to be able to dissuade, prevent or defend in future.

3.7.6 Selling

"Offers to sell proprietary information to third parties. "(Mendell, 1998, p. 16).

Where commercial activities are under threat from loss of intellectual property (IP) or more recently disclosure of personal or financial data, a great deal of forensics investigations are concentrated on data loss investigations. Often companies are less aware of the value of their information than some of their less trustworthy employees, or criminals that *hack* into their systems. An indicator of the potential for an investigation to succeed is if there is real evidence that data has in fact been compromised. One of the most obvious ways to uncover this is if a third party offers indicators that they have been approached. Caution is to be applied though, as many data leak sources are never uncovered, owing to the ubiquitous nature of many elements of corporate, financial and personal information.

3.7.7 Malicious code

"Malicious code or spam that has a traceable return path." (Mendell, 1998, p. 16).

Again, caution could be applied, and it is in that the prevalence of network address spoofing was very much less prevalent when Mendell was writing these factors than today. Essentially any network address in the current Internet protocol (IP) V5 range can be spoofed with relative certainty, and there are discussions of whether even IP V6 in its current form will resolve the issue. Spoofing is a fairly technical concept and is properly outlined by Farrow (2000). Essentially when a packet or message is sent, it carries a sender and return address. That address can be altered either by the sending actor, or intercepted and altered in some cases to point to a location other from which it originated. This can be worked to the extreme where victims can be at both ends of the attack, the spoof address can sometimes be attacked unwittingly by receiver of the primary attack in supposed retaliation, causing an escalation of traffic both ways, making analysis even more difficult.

3.7.8 Code altered

"Unauthorized alteration to code that can be tracked back." (Mendell, 1998, p. 16).

Later, in Section 3.19 we will discuss in more depth, the use of Metadata by programs and some of the challenges hasty conclusions using that data can bring. Suffice at this point to highlight that most modern application suites contain supporting log and snapshot evidence to show when data files have been altered. In most cases, such as word processing and spread sheet programs these are to ensure recovery in the case of accidental or catastrophic deletion of work, they are also there for audit purposes where records are required to be kept for example in a financial services environment. Often successive versions of data files will be resident whether in a visible or forensically recoverable state, to help show certain file changes were made on a specific system.

3.7.9 Cause and effect

"Losses or incidents tied to a specific time or event. A cause and effect relationship exists." (Mendell, 1998, p. 16).

Most commercial forensic tool suites carry a timeline viewer to enable the analyst to set out recovered artefacts in a chronological view. Very rarely is a computer failure or breach the result of one specific action, it is more usual that a succession of failures leads to a failure or breach. By plotting the various failures, activities of actors and recovered artefacts against the timeline, it is often easier to build a proper picture of the event leading to the incident in question. As we will see later in Section 6.9 (data presenter), pictures are very useful in producing compelling evidence of failures for lay persons.

3.7.10 Accounts

"Unexplained system or user account changes." (Mendell, 1998, p. 16).

In many investigations, the best indicators of untoward activities on systems is in the area of user accounts. Malware creators have realised over time that to gain value from their actions, they have to recover or retrieve data (assuming theft, espionage or blackmail). To enable this in the simplest manner, creating an account or modifying access to one already in existence as part of the attack provides this facility. Another avenue is where a password to an account has been altered or revoked, depriving the owner of that account their rightful access, an sometimes providing for impersonation of that person.

3.7.11 Mail traffic

"The sudden receipt of a large amount of abusive mail or spam." (Mendell, 1998, p. 16).

This indicator is one that is not immediately apparent in some aspect. Certainly the most obvious case is where a system is under attack such as a denial of service. Less obvious

is where the user of the system, where that is the suspect actor has been more active on other sites, and as such has attracted attention.

3.7.12 Media contaminated

"Malicious code in media received via a delivery service." (Mendell, 1998, p. 16).

Again, given the dating of the excerpt, media was as likely to be the method of transport for data as the Internet, and as such there was likelihood that media carried malware. This indicator could be modernised looking for malware in the delivery of code via a download service for example.

3.7.13 Internet talk

"Malicious statements on the Internet attributable to particular sources." (Mendell, 1998, p. 16).

As social media permeates almost every part of commercial enterprise and the propensity of people to speak their mind goes on unabated, the number of investigations involved in recovering, analysing and reporting social media infractions against persons or enterprises will surely grow. This is indeed a very topical indicator in 2012 when we look at the furore around people making what they claim to be innocuous asides on Twitter in the Newsnight paedophile accusations.

"The Tory peer has asked users who posted malicious claims in the wake of the BBC Newsnight investigation, and who have less than 500 followers, to apologise and donate to Children in Need" (Evans, 2012, p.1).

3.7.14 Associated intel

"Strong intelligence leads which identify likely suspects". (Mendell, 1998, p. 16).

This is relatively self-explanatory, but does leave the investigator with a choice to make as to what defines "strong". Once again we have to hope that the experience of the investigator and the performance of investigations leave him with a *gut* feel (Ball, 2004), this *gut* feel is discussed later in Chapter 7.

3.8 The Evidence

Traditional forensic (scene of crime) evidential procedures and computer forensic procedures exhibit similar needs. O'Hara (1994) argues that any evidence presented in court should be in practically the same condition as when it was found. This can be properly extrapolated into computer evidence where it should be shown to be reproducible (if copies are used) to the same state as when it was first gathered. O'Hara concludes that evidence should be properly protected from the first gathering to the final production in a case in court or archiving at the end of an investigative process. This is supported by a statement from a governmental committee, the Select Committee on Science and Technology (SCST, 2006) that was set up to oversee the formulation of a watchdog body for public sector forensics in the UK.

"We recommend that the Government establish a cross-departmental group, bringing in experts from industry and academia, to develop a more co-ordinated approach to data collection in future. This should include a classification scheme for recording the incidence of all forms of e-crime. Such a scheme should cover not just Internet-specific crimes, such as Distributed Denial of Service attacks, but also e-enabled crimes—that is to say, traditional crimes committed by electronic means or where there is a significant electronic aspect to their commission" (SCST, 2006, p. 3).

3.9 Legitimacy

O'Hara (1994) argues that courts, whilst not usually predisposed to take into account *opinion*, in the case of specialists such as forensic investigators, are more likely to be swayed by the *opinion* of such a specialist than they would by the average layman. There is considerable discomfort in professional circles around the power that this

brings as well as the accountability that is forced on the investigator by default because of this phenomenon.

Mendell (1998) suggests that computer systems themselves embody authority, and that an illusion of legitimacy is created by the technical knowledge associated with them. Mendell also states that investigators should not let that illusion cloud their judgements, simply because the information is there in a digital format does not make it genuine or authentic. Similarly, the authentication of a message should not be assumed to be genuine without other collaborative evidence as to the originator. Further people often assume new personas in cyberspace, offering further challenges to the provenance of data:

"Cyberspace offers many masks to hide behind" (Mendell, 1998, p. 46).

The popular press has been particularly active in the furthering of ideas that a person can immediately be identified because of data in a particular stream. These current ideas would seem to stem from the so-called experts who have rushed to capitalise on this frenzy of litigation. Take the aggressive press release statements presumably jointly formed between the lawyers and *experts* working on the McAlpine case of 2012.

"*Lord McAlpine has hired a team of experts who have collated a "very long list" of people and their offending messages, even those that have been deleted…More than 1,000 original tweets and 9,000 retweets have already been identified. We have been watching people who have been taking down what they put on Twitter. We already have all the information. We have found a couple of firms of experts who have produced pretweets, post-tweets, the effect of the tweets and the retweets. What starts at one ends up as 100,000 in some cases."* (Evans, 2012, p.1)

At this point (late November 2012) there have been no related civil or criminal cases where an accused person has defended against tweet allegations using arguments such as the *Trojan* claim (Leyden, 2003). This whole discussion around the Newsnight / McAlpine issue may indeed prove to be very valuable for the forensic profession as a whole as it may help to dispel some of the *black magic* reputation of data forensics sometimes held (Evans, 2012; Ball, 2004).

3.10 Identity and persona

This assuming of another identity, or indeed multiple identities on the World Wide Web is a normal activity, and recently greatly extended in the personas found in virtual environments such as *Second Life*. Second Life is a virtual reality world where real people design a complete persona, wardrobe and social background for their chosen virtual character (Linden Research, 2010). Reality and virtual reality blur in many cases, and there are examples that defy comprehension without understanding the depth to which people become attached to their virtual personas. Japanese police arrested a woman in 2008 for reportedly murdering her virtual husband (Parry, 2008). In the USA, a woman murdered her real world partner after finding he was having a virtual affair using his persona with another virtual body (Stanage, 2007). The first *Second Life* dollar millionaire was crowned in 2006 who was selling what is in effect non-existent land that has a temporary state purely in the electronic memory of a computer system somewhere (Hof, 2006). Importantly, none of the Second Life assets are backed by any real world funds. It could be argued that similar activities in trading networks create non-existent funds such as stock markets or forex trades, but these are intended eventually to translate back to real world funds, whereas Second Life assets are not. We must never assume that any persona we uncover in data is bone fide (i.e. believable) or correlates to a real person. As a scientific investigator at a crime scene, we would then be dragged into the world of opinion should we resort to such a conclusion.

3.11 Data gathering

All data gathered during an investigation has value of some kind. It is the duty of the investigator to provide reasonably argued conclusions as to the relevance of the data being presented. Data moves around computer systems in different forms at different times, but usually will be in a reproducible and recordable format when it is on a data storage medium of some type. Dependent upon the type of device, this may be a one-time copy that the investigator is presented with, as in the case of a volatile media such as solid state memory (*PCMAG*, 1996) or even a snapshot stored to disk as in the case of network traffic. It is important to the investigative process that wherever possible, the

original or primary data not be used for any analysis, but an exact copy be used. This has two benefits, if the investigation has to be restarted, to follow a different path, then the slate can be wiped, but also in cases where there is a defence party, the defence investigation team has exactly the same underlying data to work from as the challenger. Again, to be clear here, this Thesis presents the term challenger to try to retain the concept that this work is about the civil or commercial investigative process, not the public prosecutor. Due *evidential process* is central to all the challenges that this research is presenting, no matter which area is the intended outcome, civil or criminal. What constitutes due process has to be properly defined and agreed by interested parties before any evidence collection or triage is performed.

It is widely accepted that any data device prepared for investigative capture should be in the most reasonable state of acquiescence possible (Carvey, 2007a; ACPO, 2007; Guidance Software, 2004). Traditionally this has meant for hard disks or drives that the system in question was either idled, or physically powered off. Systems that have power applied cannot be ever assumed to be truly acquiesced as error management routines as well as system clocks still continue to function. This can be provided by means of batteries on board the machine, or by trickle power such as in a standby state that (as a representative example) most audio-visual devices generally have. Public sector guidelines, as for example, the ACPO guide (ACPO, 2009; ACPO, 2007) or FBI guide (FBI, 2007) therefore have, in the past, instructed first responders to immediately shut off all external power supplies and / or disconnect hard drives from the system motherboard to ensure no contamination or further data loss be possible. As systems have evolved to using more intelligent disks, and indeed memory chip only devices that lose their contents when power is removed, guidelines are having to be revisited. Overall, the advice now must be reformulated to provide triage at first entry, rather than an encompassing all power-off as in the past. Of course, triage takes time, and time is not always available. At the recent (October 2012) IT Security Forum in London where the researcher was presenting alongside the respected Professor P. Sommer described as *Digital Evidence & CyberSecurity Expert* the opportunity was taken to discuss this Thesis. In particular the aspect of acquiescence of systems in the current environment

was discussed and centred around the triage of potential evidence, and of course copious notes on the process of the investigation.

Extreme, but nonetheless interesting visualisations of the gathering challenges faced are the semi fictional movie sequences of computer hackers and evil enemies "zapping" disks in microwave ovens and degaussing (high powered magnetic force to reset the iron filings on data surfaces) pads being run up and down the front of systems in the movie *War Games* (1983), memories being erased by intelligent "bugs" in *The Matrix* (1999) or blasted by electron bombs in *Gamer* (2009). Reality is very often far from that presented in the movies, but the examples are poignant enough to bring the speed of triage point across, action must be taken quickly and thoughtfully. This also properly introduces a challenge that this research is presenting, the validity of evidence presented should be based on physical proof or testimony. In a perfect world, any evidence presented to a deciding authority which is in the case of the private sector as likely to be a business manager as a judge, would be safely stored in Electro-Magnetic Pulse (EMP) protected containers, copied in a bit stream copy that can be replicated as many times as needed without recourse to the original. Corresponding original files or data entities presented would be in their original readable state.

The unfortunate reality is that most systems in the current information era are "always-on", in that the ability to shut them down, or indeed interrupt their operation is very limited. Therefore a first responder has to make an executive decision, whether before the evidence is seen, or at first sight, as to what data could safely (in the legal sense) be gathered to support the case under investigation. Having decided this, the training referred to in Section 6.2, will help that person in becoming singular minded in gathering what data is needed for that task. A qualitative view can be presented of any ancillary data that may be relevant, and most importantly the proper recording of the exact circumstances of the capture will also be necessary. If one accepts that many systems just cannot be physically accessed and therefore acquiesced, usually because they reside in a different town, or in many cases, continent, then the data gathering has to be very carefully bounded with supporting data that can be used to properly frame the circumstances of that capture. To provide an analogy, the first responder, may, in the

case of these newer computing technologies, never be able to produce what is colloquially known as the *smoking gun* or indeed a dead body, to prove the event in question actually took place Doyle (1893). There may however, be enough circumstantial data in evidence to argue a reasonable case that the suspected activity was committed. It is this understanding that is critical for any further discussion on evidence, the problem of placing a person or a computer in a certain series of events with reasonable and arguable certainty. Again, to provide an analogy, with no witnesses to a car hit and run crime, the only evidence that will sometimes be available is that there is a body (the victim), fragments caused by the collision that will point to either a particular type of car, or if the car is found, a specific car. There may also be a reasonable series of circumstantial arguments about the habits of the owner or regular driver of that suspect car. Other circumstantial evidence can then be researched to narrow down the potential of improper conclusion. Computer forensics evidential procedure, and scene of crime triage is moving further towards snapshots of live data. As such these cannot be reasonably reproduced because of their inherent transient nature, therefore any investigation that depends upon the skills of the data gatherer to properly capture and store relevant facts is deeply reliant upon the professional qualities not only of that gatherer, but the training and expertise he brings to bear at that crucial point.

The following comments on relatively recent digital disclosure legislation in the US, suggest that in all civil litigation it is the;

"duty of the parties to preserve the evidence just as police freeze the scene in a criminal investigation" (Kelman, 2009, p. 1).

Kelman also argues that a decade ago, calls for evidence preservation in commercial prosecution or contractual litigation cases used to mean purely looking at computer networks and checking that clients had back-up tapes with a regular back-up cycle. Widening the scope of the challenge is the fact that today, communication can also be using Blackberries, E-mails, Instant Messaging and Texting. Some of the challenges introduced by growing automation are issues such as the fact E-mails may be responded to without user intervention. The advent of routine automation provides that transactions

relevant to the prosecution of a particular case may sometimes be made without actual human intervention – such as automated downloading materials from a website after completion of a web form. Kelman repeats the argument which many investigators know well, that multiple iterations, and therefore versions, of single documents will be captured as they go through their various stages of editing. It is the duty of the investigator to understand which version they are dealing with. Consider the more complicated example of the leaked dossier produced by the Cabinet Office in the Iraq war during 2002 which showed who had contributed to it and where the information came from (*Washington Post*, 2005). This example introduces the concept of *Meta Data* - the underlying signatures and data trails that exist in compound data sets. The arguments presented by Kelman (2009) firmly underpin a major theme that this Thesis is presenting, that evidential capture and preservation is no longer, if it can be argued ever to have been, an exact science. The continuing argument is that it will always be open to challenge as to the voracity of the process in any case involving the production of forensically acquired computer data. Peer review and common criteria then are the basis of moving forward. In the experience of the researcher, the Encase Certified Examiner examination process best mimics what is being called for (ENCE, 2010). The candidate attends a series of courses, or studies against a set curriculum to gain a certain level of expertise against the product set and methodologies. The candidature has to be supported by similarly experienced professionals, and in most cases is allocated an already certified peer as support. The candidate, having qualified against the experience and study requirements is provided with a test environment and a time frame in which to complete a report and a series of predictable forensic discoveries. The report is then submitted to a peer board and if successful the candidate is awarded the Encase Certified Examiner designation (ENCE, 2010). This certification is renewed by proving continuing study and / or experience across a three year period in a related subject, again peer reviewed.

3.12 Contamination

Evidential contamination is the single most worrisome and widely misunderstood trend in computer forensics. Because of the simplistic nature of the various tool sets and the

lack of certification or accreditation of their use, any private sector investigator providing evidence to any degree should be challenged as to the sterility of the evidence work bench that is in use. Data devices can be re-used multiple times to provide work areas for various investigations a practitioner will perform (Curley, 2010). Data that has previously resided on these devices can "bleed" into a newly commenced investigation, and as such seriously contaminate the evidence, potentially invalidating the case. It is good, and indeed arguably required, evidential procedure to reset the target data media contents to a predicted pattern, usually "1010" or "–FFFF", to ensure this contamination cannot possibly occur (DoD, 2006). Good practice further requires a peer investigator, who understands the challenge, to formally confirm the work area is thus cleaned before evidence is loaded for investigative review (Guidance Software, 2004).

3.13 Calibration

Prior to using any tools on the target data, the expected outcome of a series of calibration tests should be applied to the performance of the tool set. This is usually a search on a known environment as well as an extract and recovery of known-state data points. This effort also provides a final check that the tools about to be used are still repeatable in effect. Any outputs of tools that cannot be verified by a secondary check should never be relied upon as the sole means of evidence. Tool users that do not have an understanding of, for example, the file system that the tool set is rebuilding or extracting from should not be allowed to provide evidence that has not been verified by properly experienced peers (Curley, 2010).

So once again we should explore the concept of selective data gathering for first responders, that is the capture of data, that according to their or collective experience, would be relevant and useful to the investigator. It is critical that the investigator understand that process, and also that there is sufficient handover of intent between the gatherer and investigator, to ensure that the methodology of thinking be understood (Curley, 2010; Ball, 2004). The disparity of data devices available to the investigator in the field to capture from and on to requires that a reasoned and methodical thought process has to be applied. This thought process applies both to the eventual need to

verify the integrity of the evidential trails and also to perhaps warrant the reliability of device. This activity will dissuade challenges of unsound practice, and therefore credibility of capture is not brought into question (Curley, 2010; Ball, 2004). Many researchers have quoted the *Nintendo* forensics methods, where analysis of forensic data is done with a Common Off The Shelf toolset (COTS) and conclusions and inferences are drawn by the output of the tool that are arguably outside of the actual knowledge boundaries of the investigator (Jones, 2008; Carvey 2007a; Ball, 2004). Whilst it is clear that an investigator should not rely solely on a tool to draw inferences or conclusions, it is difficult to suggest a more expedient solution in the current commercial investigative environment. Whatever underlying systems and mechanisms are used to provide support to the investigative process, the forensics community will always be on the edge of innovation, performing actions with systems and data that were never in the initial design specification (Marcella and Menendez, 2008). Recovering deleted files for example in the Microsoft Windows environment is a pertinent example. A simple file delete by a user merely shifts the file pointer to the wastebasket, something that we all have given thanks for at least once in our journey with the delete key. To properly erase a file record you need to use the shift delete (or equivalent) function, which destroys the pointer from connection to a directory. Because file operations are expensive, or time consuming in terms of efficiency in computer operations, the recorded data though is simply just left where it is, not actually cleaned or erased.

3.14 File systems

This is by necessity the simplest clinical and non-technical description of file deletion operations on Microsoft Windows and whilst this simplistic description probably begs more questions than answers, this Thesis is not about Microsoft Windows files systems. It is therefore not useful to expand further here on the relative designs of modern file systems, but suggest that for the purposes of discussions around file recovery the description suffices. Continuing, the fact that the actual data within the file is still, at that point in an undisturbed state, we can also expect many artefacts that accompany the file to be also similarly undisturbed, creating a nirvana for the recovery of surrounding events. Again, to refer back into the early stages of computing evolution, hard disks

were originally very small in relative terms, so on disk data areas would be overwritten relatively quickly as they were freed up. As such operating systems programmers did not have to worry about swathes of data being left around to be recovered either maliciously or forensically. As hard drives and other storage mediums grew larger, the expectation of data being overwritten dropped exponentially. As outlined in this example, the Microsoft Windows system is actually designed to use the largest contiguous piece of unallocated disk space for performance reasons. Smaller files, in many cases the very ones we look for as linking evidence, had very low probabilities that they would be overwritten. There is actually a side field of disk forensics that performs the analysis on residual magnetic patterns of hard drive data, or data remanence. This specialisation is generally known as magnetic force microscopy, and experts claim the ability to potentially enable data recovery in some cases after data file areas have been overwritten up to five or more times (Nanoscan, 2006; Gutmann, 1996; Veeravalli, 1987). There are also counter claims that this is purely urban myth, but in either case, this is so specialised it would be a distraction for this Thesis to explore in detail (Feenberg 2011). It is nonetheless important in the knowledge bank or tool chest of anyone attempting a critical recovery. As computer systems followed Moore's law and multiplied consistently in size, the rotational speeds of disks did not keep up (Moore, 1965). The platter densities significantly did not correlate to the need to allow equivalently more data to be written on the same surfaces, therefore the hard disks in computer systems became severe limitations of processing speed (Mellor, 2009). This compound limitation is more correctly termed latency, i.e. the time it takes to bring the required data area on the disk to the read / write mechanism.

Rotational speed [rpm]	Average latency [ms]
15000	2ms
10000	3ms
7200	4.16ms
5400	5.55ms
4800	6.25ms

Figure 5 Table of Latency to Speed Ratios

To give some idea of the relative timings of these innovations, the first 10,000rpm disk was released in 1997 by Hitachi which can read 85Mb a second. Maxtor released their 7000 series disk in 1991, rotating at 3500 rpm, which was then declared to be able to only require 37 seconds to read 26 Megabytes (sequentially). To put these two into context, the latest solid state disks, those that are made purely from solid state memory, typically have read speeds of 250+Mb per second.

3.15 The streaming challenge

Creatively, operating system designers decided that to enable faster writing to disks, instead of continually asking for small reserved chunks of data areas to fill, they would retrieve one large area and just stream data down into it in a contiguous fashion.

The concept of streaming is in itself important to understand, as data can reach the disk surface, or at least the electronics in charge of writing to the surface, at different times from different processes (Bhat et al, 2007). This often means that different pipelines of data have to be held until the next slice of data arrives from each process large enough to warrant a flushing and writing to disk. The concept of that holding area is named

cache, as in an arms cache or suchlike (AMD, 2010). At points in the forensics analysis process it can be very important to understand if cache has been flushed to disk before capture of evidential data or not. Various complex algorithms evolved to optimise the allocated size of pre-arranged free area against the possibility of unwritten, and therefore wasted platter space. An investigator has to understand the workings of such algorithms and accordingly be able to predict whether not only if data belongs to a particular process stream or not, but more importantly if it is new or old (Hamilton, 2009). As in many advances, this optimization and trade off of speed versus unwritten disk areas created what is arguably another basic branch of data forensics and recovery known as *file slack* (Hamilton, 2009). Slack space describes the end unused data area or file, reserved by a program in pre-arranged slices or chunks, but as yet unwritten. Data is written into that reserved area until the program has finished whatever operation it is undergoing. An *end of file* command is then properly dispatched to the writing application or system software (Hamilton, 2009). Immediately (in data pipeline terms) acknowledgement is sent back to the program that the cache for that process has been flushed or written to the device, the file end marker has been properly written and any other unused pre-allocated extents (or chunks) of disk are returned to the operating system for future use. Obviously, in this simplistic description we have not allowed for an error to be returned, but we will assume this is understood here as not particularly pertinent to the description. It is then and only then the file is marked as properly closed. If the program has not completely filled up the file extent allocated, data from the previous use of that disk area is then captured in time until a properly authorised program or application deletes that new reserved file and the pre-allocation cycle is restarted (Hamilton, 2009). Whilst this is a simplistic explanation, similar effects can be found in volatile memory - chip or random access memory (RAM) in other words, and as such the concept of slack space can be applied to any memory usage situation in file systems that exhibit the pre-allocation of fixed size extents (Garden, 2010). The extent to which this Thesis has gone to provide an understanding of this concept, perhaps more than other computer concepts, is because it is an important outline of the deep knowledge an evidence analyst or computer forensic investigator absolutely needs to possess. When an investigator is challenged to describe for example, why a telephone

number found in a seemingly non-connected file directory structure, or memory location, could in fact be contributory proof of a particular event, this expert knowledge will support any such statement. In all probability all a *Nintendo* tool set (Carvey, 2007a) would state is that it found the number in file slack, with no supporting data. If the toolset is particularly advanced, it may also helpfully describe it as linked to a previous incarnation of a file that *may* have been in a relevant area to the investigation. Relevance can only be introduced by the investigator having a very deep understanding of the *dénouement* of the investigation.

"Having preserved all the evidence does not mean that all the preserved evidence is disclosable. Much of it will be duplicated and irrelevant" (Kelman, 2009, p. 1).

Kelman is obviously well versed in computer or data forensics. The professional experience of this researcher strongly underpins the statement from Kelman. A way to explain this in lay terms is by having a general understanding of the methodologies of designers of operating systems attempts to increase the effective operation speed of the data storage device, usually known as, hard disks.

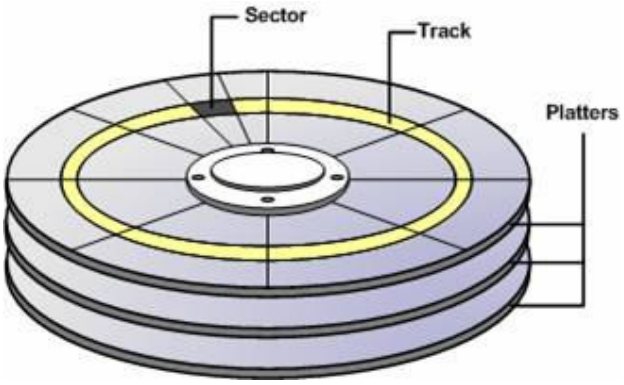

Figure 6 Physical Characteristics of a Hard Disk

Hard disks can in very simple terms be described as mechanical as opposed to optical data storage devices made up of one or more rotating horizontal platters coated in iron filings (Hamilton, 2009). A read/write (R/W) head skims the surface of the platters as they spin, usually at 5600 or 7200 rpm, which have been consistently proven to be the optimum aero dynamic speeds for such applications (Mellor, 2009).

Electrical impulses or signals, timed to coincide with a particular filing passing under the head, set it positive or negative (thus altering the magnetic alignment). The head moves in and out towards and from the centre of the disk to align ready for the next write signal (Mellor, 2009). It is clear therefore that there are without doubt some physical limitations of the equipment that at a certain time become barriers to increased speed of data access.

3.16 Data positioning

It has been shown that rotational speeds cannot be arbitrarily varied with success (although in the first incarnations of hard disks there were attempts) because of the aerodynamics of the mechanical parts. The speed at which the arm moving the head can be operated in and out has some physical limitations but is generally predictable, so pre-positioning the data write heads is possible with extreme accuracy (Hamilton, 2009).

The outcome is that data writes are queued up to be written at the optimum place for the positioning of the head, and the prediction of the next read operation. Clearly, reads are much quicker than writes and as such leave a little spare time for positioning predictions. Add all this complexity to the file extent estimations above, and one can quickly see that the data has very little chance of ending up on a location on the disk close to the related file data written earlier.

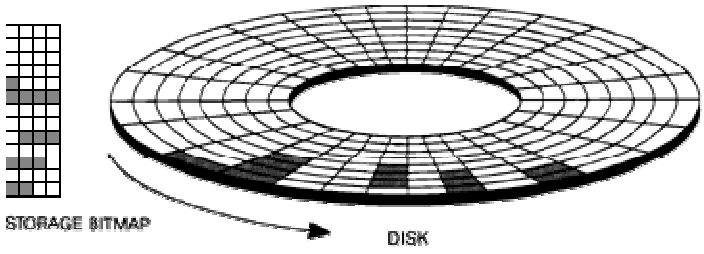

Figure 7 Fragemented files on disk platter

This fragmentation then becomes a challenge when the data is being read back in to a program, as the read and write heads would be jumping all over the platter, and often in

multi platter hard disks, across platters. File system technologists therefore came up with algorithms to optimise the placement of data after it had been written when the system was not busy, and the concept of defragmentation was created (Darcy, 2002).

3.17 Defragmentation

Defragmentation does exactly what it says, it takes separate fragments of files and joins them back together, or more importantly, actually places them in consecutive read areas on disk, which is not always the same. During this optimization operation, defragmentation routines take a copy of the data and move it to its new position (Kleiman, 2006). It is important to remind that file systems do not actually routinely erase expired or released data in modern file systems. Therefore any data that was moved to a new location for performance purposes, the primary copy, or the area on disk from whence it came, still exists until some other process overwrites it. Of course, links to what activity first wrote it are in all probability destroyed, but the data in its raw form still exists as potential evidence. This means that in many cases, a defragmentation exercise can easily create up to four or sometimes more copies of the same data. This for example could be by the defragmentation process using a staging area to rebuild file integrities, whilst upon completion, only one of those copies is actually held to be current and structurally sound by the file system.

3.18 Fuzzy search

If one then postulates on an application driven file operation that for example does something as innocuous as changing the date on a memo and then prints it, the potential for tens of copies of that very similar data to exist is high. The "*not disclosable*" (Leyden, 2003, p. 2) argument is a key driver to calls for proper training in the use of tools in this Thesis. Although the data may exist, and contain something as incriminating as "I stole thousands", unless it exists in a properly recoverable state, with original file links intact and audit trails in use supporting a reasonable suspicion, then at best we can say we have uncovered a string of data that is readable. Again, a *Nintendo* forensics attitude this researcher suggests, would be to run a search utility, mark out a

fuzzy search on such strings, provide a positive result, and the target would be in a very difficult conversation, even with very little actual evidential cause to back up the claimed situation (Jones, 2008).

A fuzzy search could be best described as an estimate of things I would like to be shown, but in this case I am not sure exactly how they would be described in text. Complex algorithms have been developed to deal with the uncertain nature of such searches, (Galil & Apostolico, 1997). In this case the search command could be

{match stole and thousands or words similar with up to two characters missing or transposed, show resultant strings up to four words before and after}.

The search would also therefore potentially return results such as like "*You stops the sands*", or "*I spole thou shards*". The dangers of such powerful search tools is clearly outlined by these examples, simplistic though they must be in nature because of the focus necessary here. Figure 8 shows the simplistic nature of the search string entry screen.

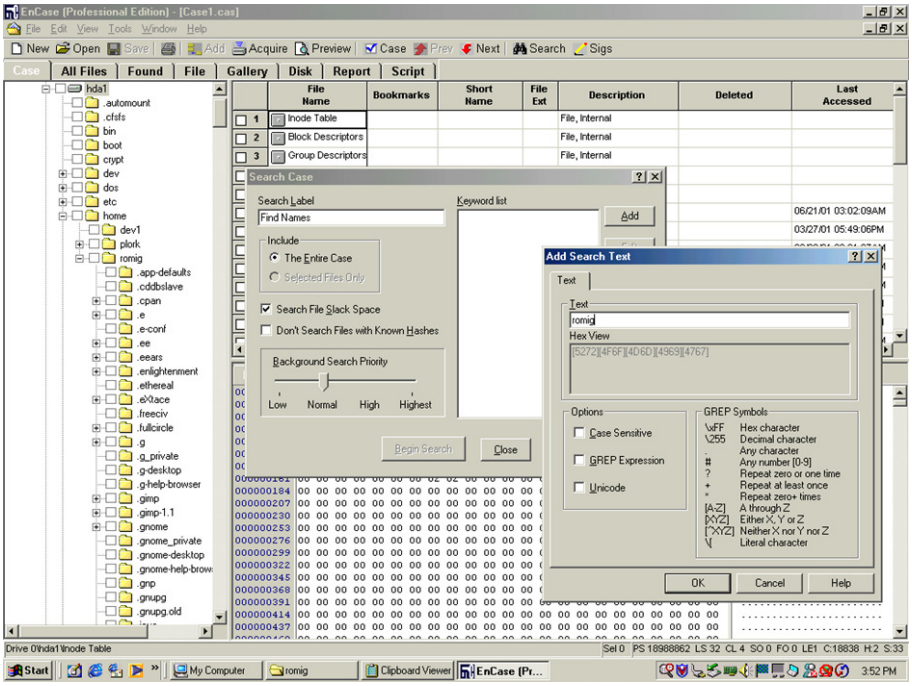

Figure 8 Example of search tool

3.19 Evidence preservation

Anything that is gathered during evidence acquisition should be kept in a proper evidential format, no matter whether it is indeed usable, or used in the case;

*"All preservation means is that the material is available should, at some stage, a court require that it be produced to deal with an issue – such as a costs issue arising after a trial when one party is seeking payment for counsel's fees for approving a draft witness statement" (*Kelman, 2009, p. 3).

Kelman firmly outlines the arguments that the triage of evidence is critical and also the capture and storage should be properly documented, both requirements called out later in Sections 6.2 and 6.3 as part of formal training.

3.20 Presentation

Whatever the skill level of a forensic investigator, analyst or researcher, it is highly probable that the results of their efforts will have to be presented either to a peer community or a panel of deciding actors for example, judge, manager or public prosecutor. The strength of their conclusions, analysis and reasoning of their outputs will be a critical factor in the value of their work and indeed the positive conclusion of their intended goals. Most, but not all investigations are begun because there is a reasonable suspicion or circumstantial evidence of a nefarious event that is having, or has had negative effects on the current desired state (Guidance Software, 2004). Most data forensic investigations involve many hours of painstaking analysis of data, long question sessions with peers around alternative theories, and most importantly, challenges both in the defensive sense as well as the credibility of methods used to provide a conclusion to some authoritative body (Jones, 2008; Daubert, 1993). It is unfortunate then that there is not a common methodology or even a prescribed format for presenting private sector forensic investigative outputs in the UK. This may be because the profession has grown in separate efforts from each company seeing a niche in the market and delivering services against a perceived need. Arguably it may be that the formalisation and governance that is experienced in the public sector is not

appropriate to the entrepreneurial spirit that abounds in the private sector information security arena. Even more worrisome is that there is no agreed data forensics industry standard to describe the investigative process in use, or indeed support the varied methodologies used. This research has found that many supposedly watertight conclusions of relatively simple evidential analysis have been properly dismissed. This has variously been because of improper presentation of facts, less than professional drawing of conclusions, or blatantly simple misunderstanding of the proper investigative process (Curley, 2010; Livio, 2010; Ball, 2004). To explore the concept of potential misunderstanding, an example is the description of the use of Metadata.

"Metadata is data about data – hidden data which provides information which about other data [sic]" Kelman (2009, p. 1).

Kelman offers the somewhat technically questionable, but nonetheless useful example that if a barrister says that he took three hours to review and revise a draft witness statement supplied in Microsoft Word, a check of the metadata stored within the document can show precisely how long the activity actually took. An experienced forensic investigator would of course be able to support only the argument that the document was open for a length of time and that during the editing session some changes were made. Whether the reviewer went off for a coffee, or took a train home from the office and reopened the laptop at home (assuming this was a portable computer), could both be challenges any opposing party could make as to the actual length of time that review and revisions actually took.

Another example of the use of Metadata;

"in confidential information cases the examination of the metadata in a Blackberry handed in by a leaving employee may reveal that it has been backed up to a home personal computer, showing that the employee has kept a complete list of his employer's confidential contacts and correspondence which he has not divulged at his leaving interview" (Kelman, 2009, p. 1).

Normally, at in presenting such evidence gathered, a forensic investigator could not make such conclusive statements at least not without some form of additional data log

to support such assumptions providing corroborating evidence from other sources. Whilst Kelman is obviously using the example in isolation to make this point, such statements are unfortunately commonplace from many supposed forensic experts, and because of an assumed mantle of expertise, are believed as to actually have been produced from the evidence (Curley, 2010). The salient point here being that in the absence of counter discussion, such statements become matters of record and without challenge can severely affect the outcome of an investigation. Even by inclusion here, if the statements were quoted from this Thesis out of context, it could be argued that this string was agreeing with the statements made above by Kelman as to how much *may* actually be uncovered from a Blackberry activity log, which it certainly is not intended to. As an important lesson, presentation is about focusing audience attention, but for a forensic investigator, it absolutely must be done with a supportable argument if it is to remain credible (Daubert, 1993).

To provide a further analogy, there is, in most areas of post graduate study, a formal course requirement to undergo research and presentation or report writing modules before a student can be admitted, or indeed begin study. At best, evidence must be provided of proper academic arguing previously completed or past academic outputs that have been peer reviewed. This ensures that the student is at least aware of the power of argument as well as the requirement to properly attribute arguments and document facts (UEL, 2010). Even in light of this compelling argument, the presentation skills training module proposed in Section 6.6, will however, be best offered as an optional module, being given its' own certification. It should be considered that not every investigator will either be comfortable or be required to actually present or argue results. This area is the one piece of research that has strikingly different aims to that of the forensic regulator (Forensic Science Regulator, 2008). For the public sector investigator, the presentation of evidence is rarely a work of persuasion. Public sector cases are almost always a pure presentation of facts, which will be interpreted, in most cases by another expert. This interpretative expert can sometimes represent the defence, but more often prosecution (Leyden, 2003). The private sector investigator however, is usually in a position where they are expected to produce a factual recount of the activities performed, a factual description of the data

recovered or reviewed, and then provide an expert opinion as to the relevance and importance of items presented.

Activity / Delivery	Public	Private
Gathering of data	The data can only be gathered under warrant	Data can be gathered with permission of system owner.
Analysis of data	Data must be analysed under strict procedures, with specific suspicions.	Data can often be analysed in a general manner with no specific suspicion.
Presentation of data	Full evidence trails and methodologies must be presented. Any data extracted must be presented to the defence also.	Presentation can range from a simple email to a full commercial report, but rarely requires evidential procedure to be presented.
Opinion of data extracted.	Opinions are usually restricted to the reliability if data, not the event under investigation.	Often an opinion of the probable "guilt" of the subject is provided, based on "experience".

Figure 9 Comparison of Delivery Styles

The training for presenting then is by necessity massively diverse, and detailed further in Chapter 6. Formal presentation of detailed facts and the ability to answer questions based purely on those facts and not embellish with any level of opinion is a difficult skill to teach. This research suggests it is one that is not generally available as a taught module anywhere in the related private sectors. This then is an area that has required detailed experience and case analysis before the research was able to confidently predict that the methodologies and skills chosen to drive the training will have the desired outcomes. Further, being able to offer an analytical walk-through of artefacts in an investigation, draws upon not only presentation and oratory skills, but also underlying technical knowledge or at least understanding of the system or application under review. This research has determined that this is one area that, whilst critical to the proper execution of an investigative process, measurement and teaching of these skills can be best handled elsewhere. For example through Microsoft system training (Microsoft, 2010) Oracle database administration training, (Oracle, 2010), ISC^2 information security training (ISC^2, 2010) etcetera.

"The next issue to be determined is format for disclosure. Should information be disclosed in static electronic formats (Adobe PDF files and TIFF files) or in a native format such as the format of an e-mail client like Microsoft Outlook" (Kelman, 2009, p. 3).

This extract suggests that there are arguments to support both directions. Kelman first proposes that static formats exactly match the conventional lever-arch file systems and therefore documents can easily be organized in folders. A suggestion that this maybe more palatable or understandable for someone more used to a traditional filing system, conceding though that in a very short time the volume of data usually overwhelms the disclosure process in static format. Kelman further suggests that disclosure in a computer email format is much more complicated since special software has to be used to access the disclosed documents, allowing that it provides very neatly for reviewers to electronically search the disclosures and also provides some additional MetaData (which we have already discussed). The conclusion presented is that it is a relatively speedy effort then to produce accurate time based analysis. Whilst the example of the Blackberry earlier in this section does not automatically support his final conclusion, given that it may be in need of other supporting information, it serves as a good outline of the reporting expectations for forensics. This specialised formatting and presentation is suggested to be the only way in which information can be intelligently handled. We are also offered an extended example of trial in the fuller text. Although public sector prosecution is not a stated avenue of this research, it is useful to review those thoughts on how the court and trial judge, in the case cited, must also be prepared to accept and use the data in the native format. Kelman does concede that this may however require special software to be loaded onto the laptop or desktop of the presiding judiciary. This change in the artefacts in use in the courtroom brings with it the assumption that the actors in and around the case have a modicum of information technology training, and access to the specialist tools and systems that the presenters of facts do (Ball, 2009). The research for this Thesis suggests this is a dangerous assumption (*Yorkshire Post*, 2007). One compromise position Kelman offers is that it has been suggested that the presenters of fact disclose in native formats and some middle man function use this to produce digital bundles in static formats for the trial. This Thesis also supports the

arguments that not all investigators would need presentation skills and strongly supports this conclusion with detail in Section 6.6.

O'Hara (1994) reminds us that when we are discussing evidence, crime scenes differ, and in particular those involved with information crime. An experienced (fraud) investigator knows that crimes such as forgery and embezzlement need no particular physical activity in their commission so usually allows that traditional evidential methods would not be appropriate. It is suggested also that this has to be taken into account when presenting evidence as traditional methods may indeed be expected, such as in a court trial (O'Hara, 1994).

"The investigative report is no place for speculation, hypothesis or opinion (the investigator's judgment or prejudices). If the reader of the report engages in any of the above, as a result of the facts presented, that is his prerogative" (Sennewald, 1981, p. 159).

The research underpinning this Thesis suggests that this is excellent advice. Arguably in the commercial sector, there is in many cases an expectation that the investigator will present an expert opinion. As long as this opinion is clearly annotated as such, then it is right and proper to include as part of a formal report of the outcomes of particular piece of investigative work.

"This is not to say that the investigator should not have opinions or engage in speculation. But any such subjectivity should not be included or reflected in the report itself" (Sennewald, 1981, p. 159).

This is one area of this seminal work where this researcher and others find a disagreement with the fixed style suggested. It is not possible to have a one size fits all in the commercial world, but it is advised where opinion is presented it should be clear that it is that, an opinion given as a basis of experience and expertise applied to the data and artefacts reviewed (Ball, 2009).

O'Hara (1994) reminds us that evidence should satisfy certain requirements of quality, trustworthiness and logical sufficiency. Further in the work we are presented with a

description of the whole evidential procedure in exacting detail, which is not timely to relate here, but does indeed support the claim of familiarity with the process. A conclusion is given that the whole must be presented in an orderly and logical fashion. This clear closing argument supports the stream of this chapter, that is; without an orderly delivery of the relevant data and a logical argument of the facts surrounding the data, it would not be possible for any like-minded person to examine the conclusions presented and challenge any part of that arguing process. O'Hara (1994) finally suggests that we establish the basic elements of the offence in order to round off the process of proof.

One of the basic challenges that was outlined in the thinking for this research, and indeed in the experience of this researcher was how to sensibly provide for proper evidential procedure in the private sector during the acquisition of forensic data. This chapter explored some of the shortcomings of current practice, highlighted some of the more critical mistakes that have been publicised, and importantly reported recent guidance that is growing in how to correct the situation.

The private sector, whilst perhaps sometimes being on the forefront of the forensic profession in terms of investment and tools, is almost always behind the public sector in the area of governance and controls. The chapter described the rapidly changing computer landscape, and how the forensics profession is having to evolve just as quickly to keep pace, even without the benefit of strong controls and guidance. The chapter also described some of the challenges that are presented to investigators, and having laid out the possible errors that can be made, suggested avenues for discussion later as to how to control or rectify these errors.

3.21 Review

We reviewed in some depth the actual workings of forensic investigations. We looked in detail at some of the areas that an investigator is required to possess knowledge and explored some of the basics of data manipulation on computer systems that forensic investigators rely upon to be successful. We challenged some thinking around the level

to which an investigator should be experienced and gave some suggestions, to be detailed later in Chapter 6, about how these knowledge requirements could be met.

The presentation skills argument traversed an area that is largely ignored in current technical forensics research, the delivery of outputs. Current forensics research tends to be specific and focused on a particular area of forensics such as recovery algorithms, bad disk areas and suchlike. The broad nature of this Thesis requires that the profession of forensics be reviewed as a whole and the integrity of the profession be provided with guidance and controls as part of the conclusions. An investigator therefore must be able in some manner to present the outcome of an investigation in a professional and concise manner in order that the basic challenges against that output, and understanding of the conclusions can be made.

4 Tools

A large part of the research and discussion in the public sector has been towards the provision of and verification of supporting forensics tools. There are many examples of tools being used without proper forensics knowledge, and as shown earlier in this Thesis mainly in Section 1.3, the outputs provided have sometimes been frankly fabricated in real terms. Derogatory terms such as *Tyke* and *Nintendo* have been variously used to describe these tendencies, as well as some very public challenges to the integrity of the industry leading tool sets. The chapter attempts to balance these concerns with the activities that the tools are being asked to perform. It attempts to show that by working at the "bleeding edge" of computer systems data recovery, these tools can be expected to have higher failure rates than traditional robust computer applications.

4.1 Evolution

Previous research concludes that of all the common forensic tools they reviewed, none were without failings that could easily impede and sometimes disqualify the basis of an investigation (Arthur et al, 2004). This is a most worrying conclusion, but is surprising to anyone practicing in the forensics field (Livio, 2010; Sapphire, 2007; Ball, 2004). Take for example the product Encase (figure 10), one of the market leading tools in the commercial and public sector, arguably *the* market leader (Guidance Software, 2004).

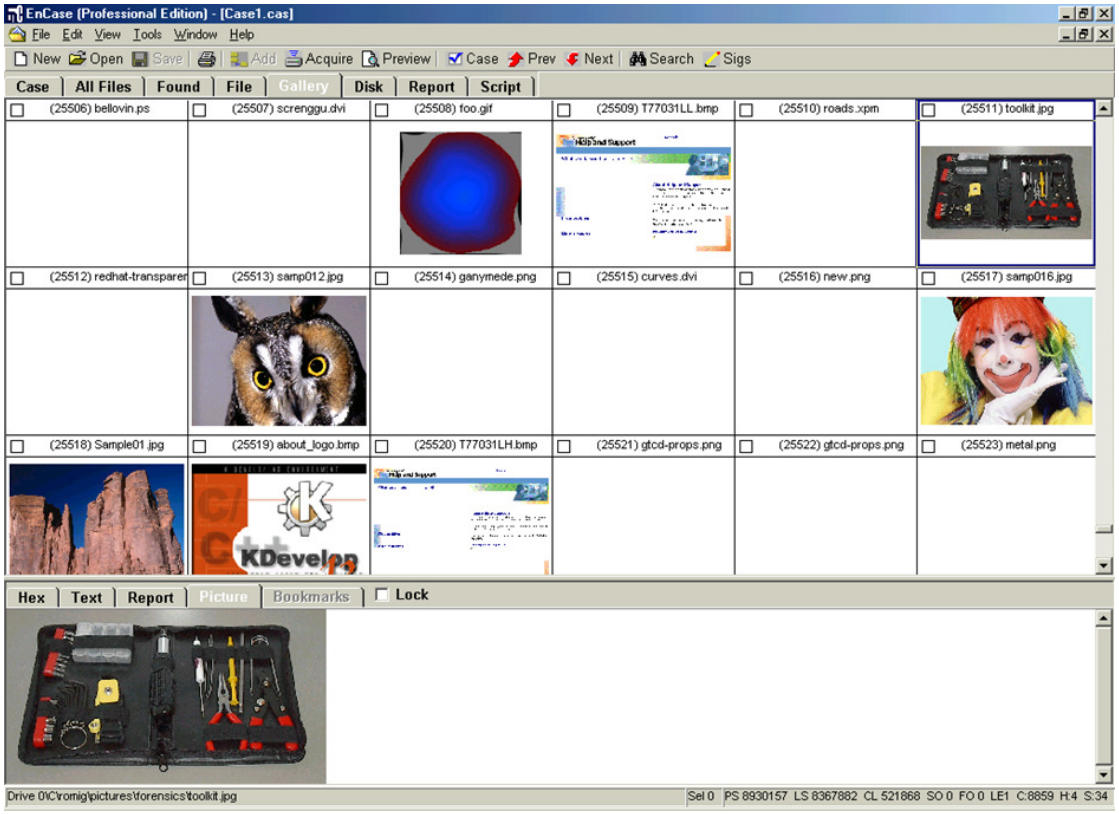

Figure 10 Encase Tool

The tool was born from an evolutionary process preceded by many other similar tools, and in this case a call from serving police officers in the USA for a better tool set, than ILookPI (figure 11), the proprietary and copy protected forensics tool of US law enforcement (Perlustro, 2010).

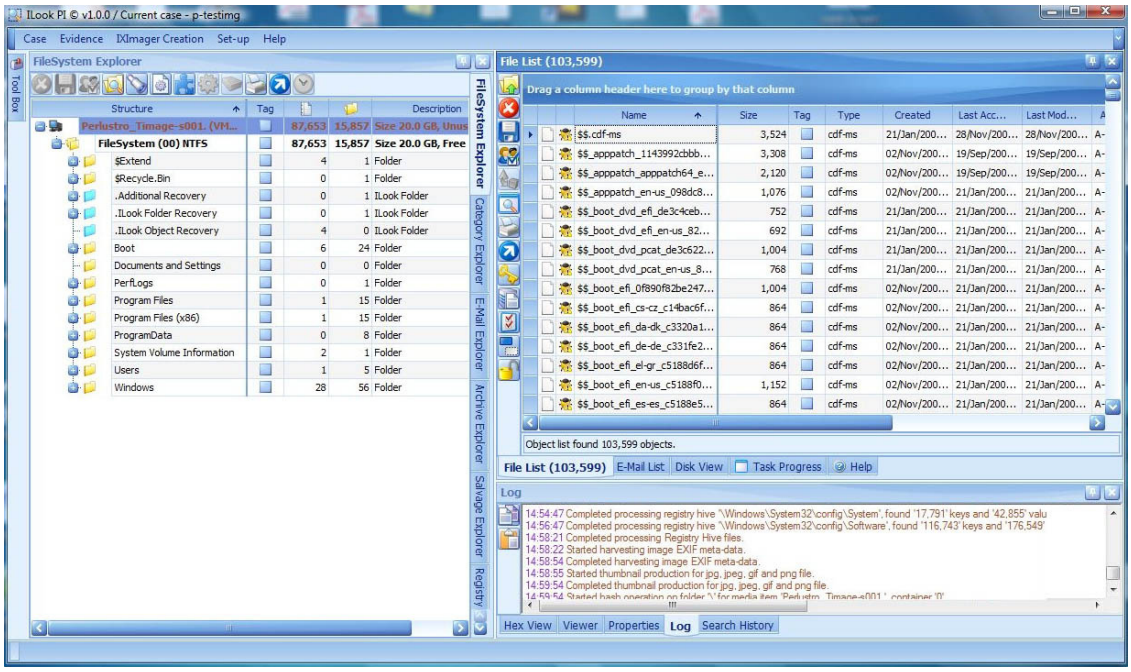

Figure 11 IlookPI tool

The closeness of the Guidance Software delivery organisation to the user community has been both the success as well as an arguable future commercial survival challenge, one that forces continual decision between a structured and defendable business plan, against a need to support the changing landscape that the current user base are working in. Most mature software applications on the market today go through extensive testing and structured development processes to ensure that they both meet the needs of the buyers as well as removing as many failures from the underlying application code as possible (Crispin & Gregory, 2009). In such commercial environments software goes through multiple iterations until the producers are confident that optimum, but not necessarily perfect service level has been achieved and then the software is released as a thoroughly tested product. Forensics software applications in general do not always have this luxury of time or quality, and Encase is a prime example.

The release schedule for a mature software product, in the experience of this researcher is aimed at quarterly or half yearly update. Conversely, on 30th March 2010 Encase version 6.16 was released, on 6 April version 6.16.1 was released, then quickly followed on 14th May by version 6.16.2. Both of these subsequent releases fixed significant flaws

in the major version 6.16 release. Version 2 of Encase was debuted at the IACIS conference in 2000 (Prince, 2000), so it is evident that even after more than ten years of evolution the product is not what could be called stable. Indeed, as late as 2007 there were serious arguments being played around the Internet after iSEC, a respected US security forum reported fundamental integrity and reliability flaws in the Encase version at that time (Sheldon 2011; Prince, 2007).

To provide some background as to why this may not be so serious as it first seems it is important to understand the challenges faced by forensic tool writers. Many operating system manufacturers will not release the exact details of how software is built, what the links and hooks are to various system areas, and importantly how user activities are recorded. In 1998 for example, Microsoft Corporation was challenged by a US District judge to release source code for its proprietary operating system Microsoft Windows. It challenged that action and made an analogy that if Coca-Cola were made to reveal its secret syrup formula, then its business would be destroyed. Similarly if Microsoft were forced to reveal its intellectual property then it would be severely disadvantaged (Newman, 1998). Therefore, because there is no requirement to release source code, the forensic software writers are at a disadvantage in understanding exactly how applications and operating systems really work. Exact data tolerances and interfaces are never shared for the system architectures, so any software that is trying to automatically analyse these areas will be testing the limits of the software and hardware it is using and reviewing. It is clear that there is still a logical propensity for the Encase developers to provide timely solutions to problems that government agencies in the US may be encountering (the largest customer base). It is therefore predictable that the Encase product and others like it will be constantly evolving and potentially never stable. This would seem to be a challenge for the Daubert “repeatable” test as mentioned earlier in Section 1.4, as well as the stability that would be expected from newer versions of software (Prince, 2007). Within the forensics community, instability of software and chance unreliable results all compound the challenge of professional production of cases (Sheldon 2011; Livio, 2010; Jones, 2008; Ball 2004). Simply, if a defence challenge in a civil suit was to ask if, in this case, Encase was a reliable and stable tool, and could be depended upon to produce the same results on the same input data from different release

versions, arguably then the case would be under threat, or at least the results from the investigation severely in question. Is Encase any different from any other tools - in the experience of this researcher, definitely not, and Encase is in all probability, what could be called the leading edge tool in terms of reliability and quality of result. The important conclusion here is that any case or opinion that depends solely on the output of a tool is by the arguments above, probably flawed (Jones, 2008; Ball, 2004). The need for a forensic analyst to be able to show how the same results can be produced manually, albeit on a sampling basis for expediency, is paramount to the credibility of that expertise, and should go a long way to challenge the *Nintendo* or *Tyke* tags (Sheldon, 2011; Carvey, 2007a; Ball, 2004).

4.2 Free tools

To go some way in understanding the complexity and extent of the growing *Nintendo* or *Tyke* environment, it is useful to list here a plethora of free from subscription tools available to the forensics community (as well as anyone with access to the Internet). Continuously updated versions of this list can be found at ForensicControl (2012), many other sites carry similar lists. The ForensicControl version of the list has been split into areas of interest. Before exploring the boundaries of this significant list of tools, it is important we maintain a caveat to our review. Whilst in itself, the use of as free tool is not an irrefutable indicator that the operator be coined a *Tyke* or be known as someone operating in the *Nintendo* forensics medium, the sole use of free software to perform forensics has inherent dangers, as discussed later in Section 5.5 (tool reliability).

Disk and imaging tools (figure 12) are used in either setting up the forensic work areas, or in mounting or recovering file systems and disks that are to be used in data analysis. Some of the more specialised abilities include repairing otherwise unreadable data areas and rebuilding fragments of files as recovered by the operator.

DumpIt-Generates physical memory dump of Windows machines, 32 bits 64 bit. Can run from USB keys

Encrypted Disk Detector-Checks local physical drives on a system for TrueCrypt, PGP, or Bitlocker encrypted volumes

FAT32 Format-Enables large capacity disks to be formatted as FAT32

FTK Imager-Imaging tool, disk viewer and image mounter

Guymager-Multi-threaded GUI imager under running under Linux

HotSwap-Safely remove SATA disks similar to the "Safely Remove Hardware" icon in the notification area

P2 eXplorer*-Virtually mount drives & forensic images

Tableau Imager*-Imaging tool for use with Tableau imaging products

VHD Tool-Converts raw disk images to VHD format which are mountable in Windows Disk Management

Figure 12 Disk and Imaging Tools

Email analysis tools (figure 13) are useful to enable structured and unstructured analysis of Email files that may otherwise need connection to the master file server, or in some cases require password access in their native form.

EDB Viewer-Open and view (not export) Outlook EDB files without an Exchange server

Gmail Parser-Parses various Gmail artefacts from cached HTML files

Mail Viewer-Viewer for Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird message databases and single EML files

OST Viewer-Open and view (not export) Outlook OST files without connecting to an Exchange server

PST Viewer-Open and view (not export) Outlook PST files without needing Outlook

Figure 13 Email Analysis Tools

The general tools section (figure 14) includes various utility tools that forensic analysts (and others) have found useful over time to support the analysis process.

Agent Ransack-Search multiple files using Boolean operators and Perl Regex

EvidenceMover*-Copies data between locations, with file comparison, verification, logging

FastCopy-Self labelled 'fastest' copy/delete Windows software. Can verify with SHA-1, etc

File Signatures-Table of file signatures

Forensic Test Images-Collated forensic images for training, practice and validation

HashMyFiles-Calculate MD5 and SHA1 hashes

MobaLiveCD-Run Linux live CDs from their ISO image without having to boot to them

Mouse Jiggler-Automatically moves mouse pointer stopping screen saver, hibernation etc

Notepad ++-Advanced Notepad replacement

NSRL-Hash sets of 'known' (ignorable) files

Quick Hash-A Linux & Windows GUI for individual and recursive SHA1 hashing of files

USB Write Blocker-Enables software write-blocking of USB ports

Windows Forensic Environment-Guide by Brett Shavers to creating and working with a Windows boot CD

Figure 14 General Tools

File and data analysis tools (figures 15-16) are by far the most populated set of tools in use. This genre of tools could be argued, especially in their free of charge guises to be the greatest provider of *Nintendo* forensic analysts. This list includes some tools that are real time in nature, that is, data can be recovered as it is being produced, in most cases with no visible effect on the systems under review. The display is split for readability only.

Advanced Prefetch Analyser-Reads Windows XP,Vista and Windows 7 prefetch files

analyzeMFT-Parses the MFT from an NTFS file system allowing results to be analysed with other tools

Audit Viewer-Viewer used with Memoryze (see below)

DCode-Converts various data types to date/time values

Defraser-Detects full and partial multimedia files in unallocated space

eCryptfs Parser-Recursively parses headers of every eCryptfs file in selected directory. Outputs encryption algorithm used, original filesize, signature used, etc

Encryption Analyzer-Scans a computer for password-protected & encrypted files, reports encryption complexity and decryption options for each file

Forensic Image Viewer-View various picture formats, image enhancer, extraction of embedded Exif, GPS data

Highlighter-Examine log files using text, graphic or histogram views

Live Detector*-Collects volatile data; account & password identification; browser artefacts, user behaviour; and Microsoft Windows System info

LiveContactsView-View and export Windows Live Messenger contact details

RSA Netwitness Investigator-Network packet capture and analysis

Figure 15 File and Data Analysis Tools -A

Memoryze-Acquire and/or analyze RAM images, including the page file on live systems
MFTview-Displays and decodes contents of an extracted MFT file
NetSleuth-Network monitoring tool, with covert “silent portscanning”
PsTools-Suite of command-line Windows utilities
Shadow Explorer-Browse and extract files from shadow copies
Simple File Parser-GUI tool for parsing lnk files, prefetch and jump list artefacts
SQLite Manager-Firefox add-on enabling viewing of any SQLite database
Strings-Command-line tool for text searches
Structured Storage Viewer-View and manage MS OLE Structured Storage based files
TimeLord-Time utility; timezones, BIOS times, decode computer time formats, etc

16 File and Data Analysis Tools - B

The MacOS operating system (OSDP, 2012a) has many differences in operation and architecture to the Microsoft Windows operating system (OSDP, 2012b). As such, there is a genre of tools (figure 17) that are specific to the recovery and analysis of data in that sphere.

Disk Arbitrator-Blocks the mounting of file systems, complimenting a write blocker in disabling disk arbitration
Epoch Converter*-Converts epoch times to local time and UTC
FTK Imager CLI for Mac OS*-Command line Mac OS version of AccessData’s FTK Imager
IORegInfo-Lists items connected to the computer (e.g., SATA, USB and FireWire Drives, software RAID sets). Can locate partition information, including sizes, types, and the bus to which the device is connected
Mac Memory Reader-Command-line utility to capture physical RAM from Mac OS systems
PMAP Info*-Displays the physical partitioning of the specified device. Can be used to map out all the drive information, accounting for all used sectors

Figure 17 MacOS Tools

A relatively new area of data forensics is that of mobile devices. Earlier mobile phone analysis tools concentrated on SIM cards, call records and text messages sent and received by handsets that were simplistic (in terms of models available latterly) in operation. As Handsets evolved into devices designed to receive and transmit structured messages, such as electronic mail, and also to send and receive data files, tools were needed to analyse this data (figure 18). Proprietary operating systems designed for these devices had to be reverse engineered in the same way that PC operating systems had been to allow the analysis of that new source of forensic data.

iPhone Backup Browser-View unencrypted backups of iPad, iPod and iPhones
iPhone Analyzer-Explore the internal file structure of Pad, iPod and iPhones
Rubus*-Deconstructs Blackberry .ipd backup files

Figure 18 Mobile Device Tools

In the list of data analysis suite tools (figure 19), we find the type of tools that would be used, generally in a non-commercial investigation to speedily access data and recover information. Commercial tools that have significant cost in most cases, usually include the majority of the facilities listed below in a combined package. These commercially available (at cost) tools are discussed later.

Autopsy-Graphical interface to the command line digital investigation analysis tools in The Sleuth Kit (see below)

Backtrack-Penetration testing and security audit with forensic boot capability

Caine-Linux based live CD, featuring a number of analysis tools

Digital Forensics Framework-Analyses volumes, file systems, user and applications data, extracting metadata, deleted and hidden items

OSForensics-Windows application to carry out wide range of forensic tasks.

P2 Shuttle Free*-Remote disk mounting, network RAM capture, search tools. Limited version of P2 Shuttle Pro

Paladin*-Ubuntu based live boot CD for imaging and analysis

SIFT*-VMware Appliance pre-configured with multiple tools allowing digital forensic examinations

The Sleuth Kit-Collection of UNIX-based command line file and volume system forensic analysis tools

Ubuntu guide-Guide to using an Unbuntu live disk to recover partitions, carve files, etc.

Volatility Framework-Collection of tools for the extraction of artefacts from RAM

Figure 19 Data Analysis Suites

File viewers, in the main are produced by commercial software vendors so that receivers of file produced using their tools (figure 20) can successfully read the data in those files in the format as written. As the mobile media devices increase, it is generally expected that native viewers of proprietary application sets in use on those devices will also be released.

Microsoft Excel 2007 Viewer-View Excel spreadsheets
Microsoft PowerPoint 2007 Viewer-View PowerPoint presentations
Microsoft Visio 2010 Viewer-View Visio diagrams
Microsoft Word Viewer-View Word documents
VLC-View most multimedia files and DVD, Audio CD, VCD, etc

Figure 20 File Viewers

One of the most rapidly growing set of freeware tools is that of Internet and Web Browser history data retrieval and viewing (figure 21). This is not surprising, given that the majority of personal electronic mail and communication is arguably now taking place across the Internet.

ChromeAnalysis -Analysis of internet history data generated using Google Chrome

ChromeCacheView -Reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache

FoxAnalysis -Basic analysis of internet history data from Firefox versions 1, 2 and 3.

IECacheView -Displays various details of files in Internet Explorer cache; number of hits, last accessed times, etc

IECookiesView -Extracts various details of Internet Explorer cookies

IEHistoryView -Extracts recently visited Internet Explorer URLs

IEPassView -Extract stored passwords from Internet Explorer versions 4 to 8

MozillaCacheView -Reads the cache folder of Firefox/Mozilla/Netscape Web browsers

MozillaCookieView -Parses the cookie folder of Firefox/Mozilla/Netscape Web browsers

MozillaHistoryView -Reads the history.dat of Firefox/Mozilla/Netscape Web browsers, and displays the list of all visited Web page

MyLastSearch -Extracts search queries made with popular search engines (Google, Yahoo and MSN) and social networking sites (Twitter, Facebook, MySpace)

PasswordFox -Extracts the user names and passwords stored by Mozilla Firefox Web browser

OperaCacheView -Reads the cache folder of Opera Web browser, and displays the list of all files currently stored in the cache

OperaPassView -Decrypts the content of the Opera Web browser password file, wand.dat

Web Historian -Reviews list of URLs stored in the history files of the most commonly used browsers

Figure 21 Internet History Analysis

Registry and user analysis tools (figure 22) tend to focus on the more popular operating systems such as Unix and Windows, and can be used to understand changes made to systems. They also can be used to understand the make-up of a particular system environment at the point the data was captured.

ForensicUserInfo -Extracts user information from the SAM, SOFTWARE and SYSTEM hives files and decrypts the LM/NT hashes from the SAM file
Process Monitor -Examine Windows processes and registry threads in real time
Registry Decoder -For the acquisition, analysis, and reporting of registry contents
RegRipper -Registry data extraction and correlation tool
Regshot -Takes snapshots of the registry allowing comparisons e.g., show registry changes after installing software
USB Device Forensics -Details previously attached USB devices on exported registry hives
USBDeview -Details previously attached USB devices
UserAssist -Displays list of programs run, with run count and last run date and time

Figure 22 Registry Analysis

The application section (figure 23) tends to cover chat, file share and messenger applications.

KaZAlyser -Extracts various data from the KaZaA application
LiveContactsView -View and export Windows Live Messenger contact details
SkypeLogView -View Skype calls and chats

Figure 23 Application Analysis

On most tools listing sites there is an area where tools that have been useful in the past, and may or may not now work as expected are kept. Some of these can be useful in helping investigate older operating systems or applications.

CaseNotes* -Contemporaneous notes recorder
Exif Reader -Extracts exif data from digital photographs
Fragview* -View recursive HTML, jpg and Flash files
GigaView* -Parses exported GigaTribe chat logs, results can be imported into Excel
Live View -Allows examiner to boot dd images in VMware.
VideoTriagee* -Produces thumbnails of video files so that the whole video doesn't need to be watched

Figure 24 "Abandonware" (old / unsupported)

4.3 Commercial Tools

Encase, produced by Guidance Software, is an internationally available tool and is generally acclaimed to be the market leader. It exists in stand-alone form (figure 25), as well as a multi node, central command console form, known as Encase Enterprise Edition (figure 26).

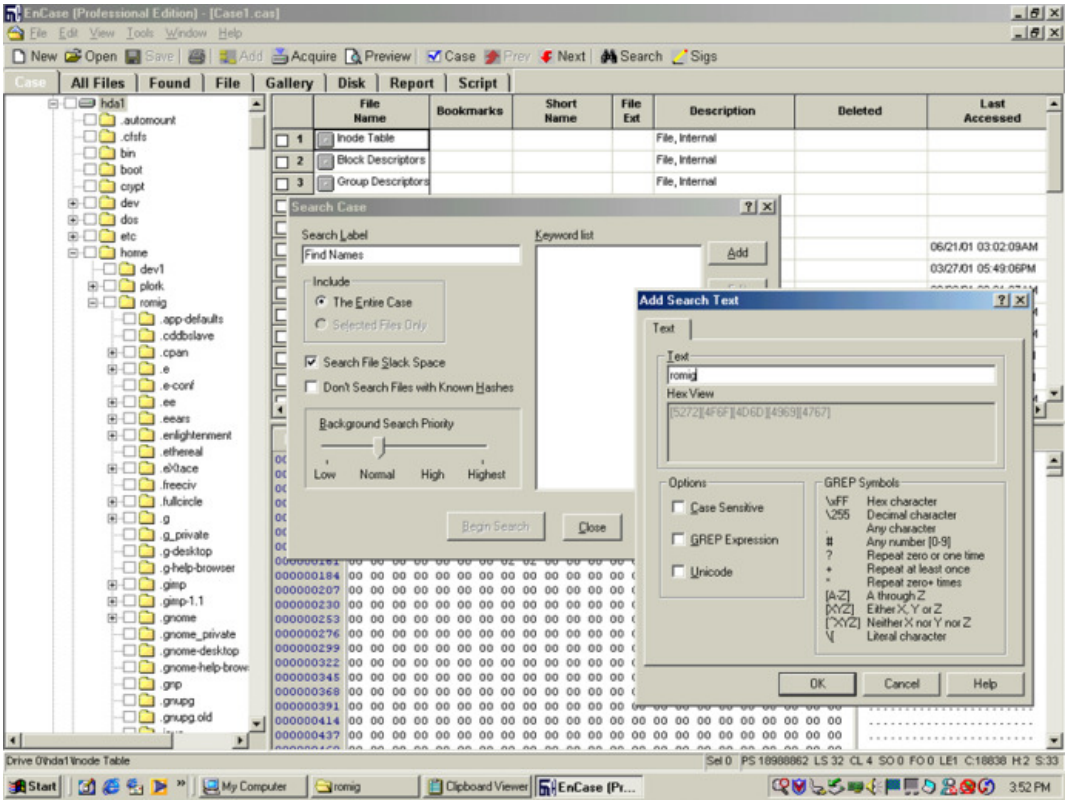

Figure 25 Encase Professional (field) Edition

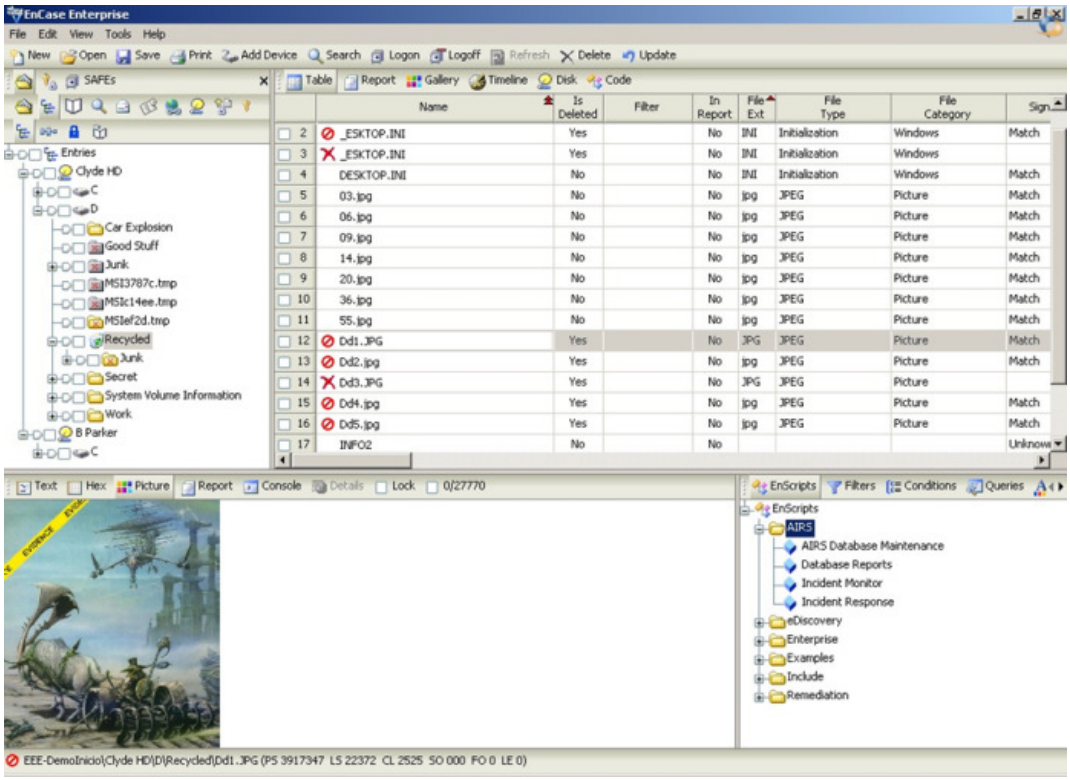

Figure 26 Encase Enterprise Edition

There are also optimised versions available for agencies operating in specialised fields, but these are generally unavailable to non-agency actors so not listed here. Guidance Software offer the *Encase Certified Examiner* course and certification.

ILOOK, (figure 27) is a tool available only to agencies in the Public Sector (Military, Police, Intelligence etc.). It is included here as the extent of use over the evolution of forensics mean that many forensics professionals have at least come across it, or derivatives produced to enable Public-Private sector cooperation in investigations.

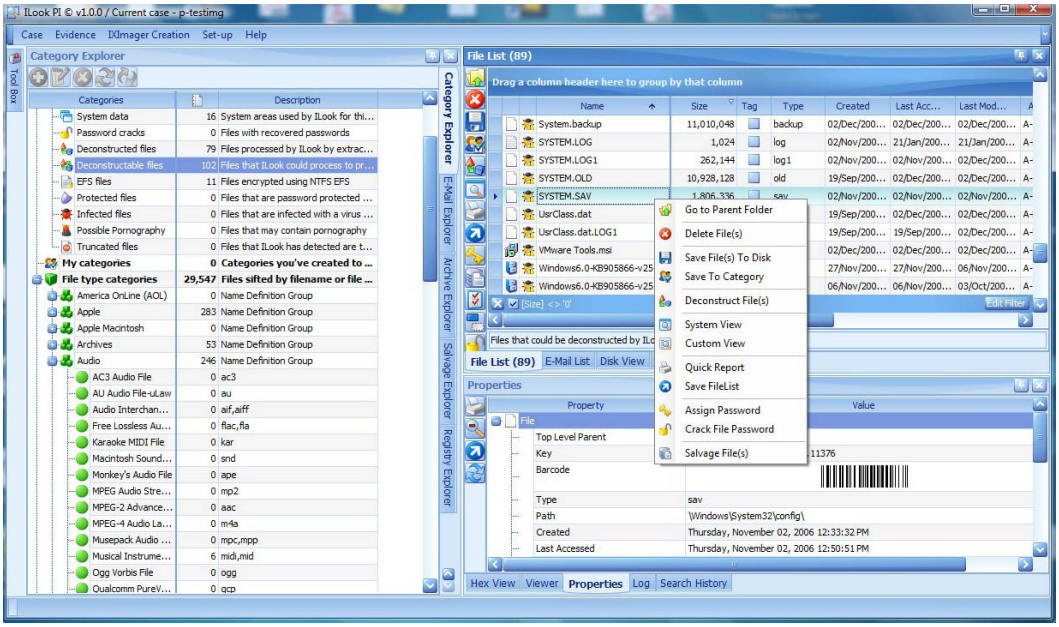

Figure 27 IlookPI Tool

FTK, or Forensics Tool Kit, produced by AccessData is claimed by many to be the second and sometimes equal, in terms of performance to Encase. Many experienced forensic investigators will use FTK (figure 28) as a second opinion on critical evidence analysis performed by other tools such as Encase. Accessdata offer the *AccessData Certified Examiner* training and certification.

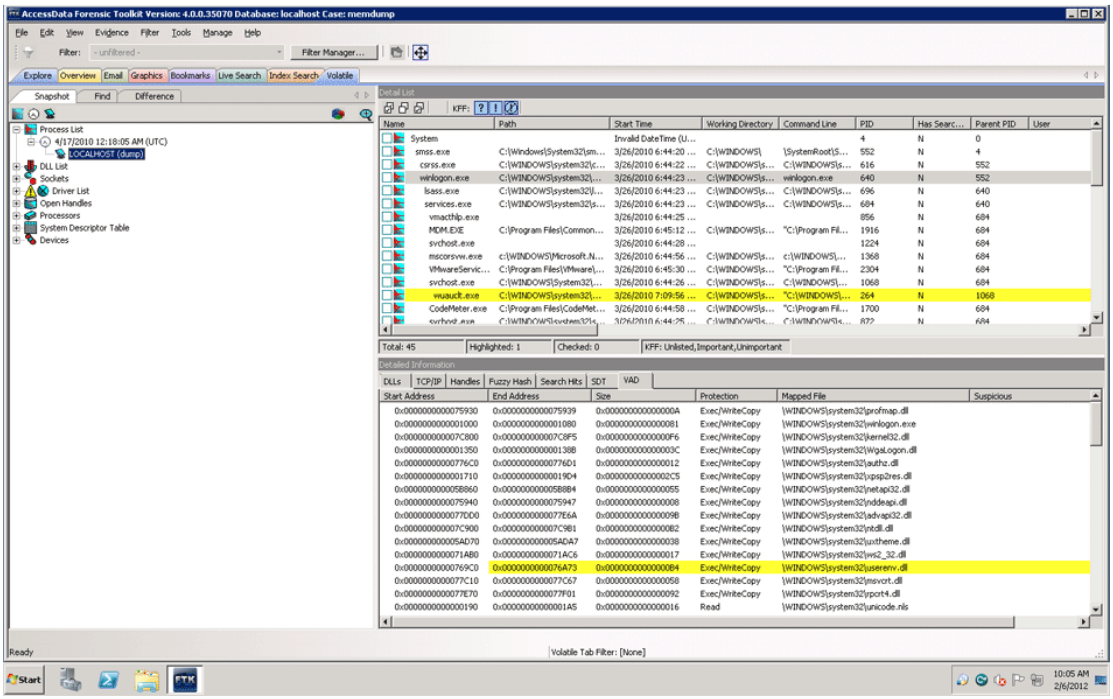

Figure 28 FTK Tool

Paraben's P2 commander software (figure 29), is claimed by many to be a more readily useable reporting tool for providing easily readable outputs needed on routine data analysis. It also maintains a price point that makes it affordable a san entry level commercial product for forensic analysts. Paraben offer a *Paraben Certified Forensic Examiner* course and certification.

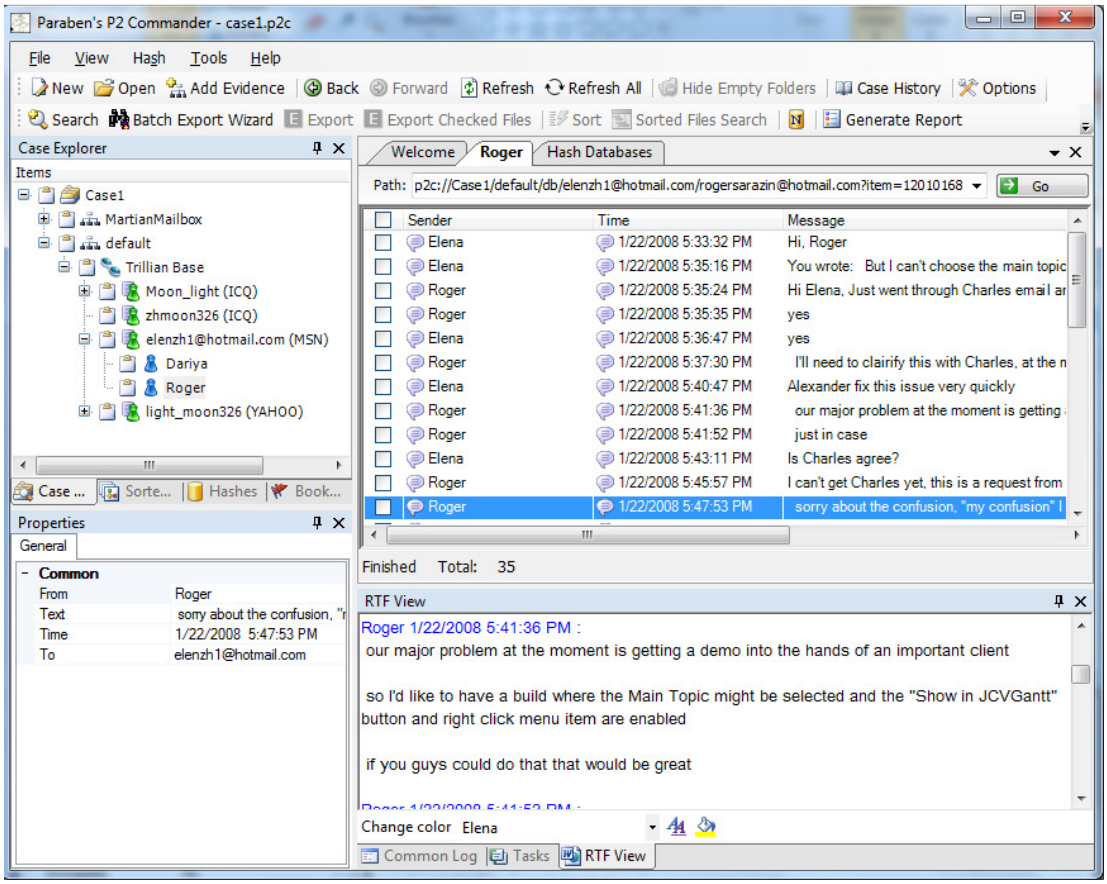

Figure 29 Paraben P2 Commander Tool

COFEE is a set of tools that have been gathered together, in the main by Microsoft Corporation fraud engineers, and until very recently was a proprietary tool kit (that is the make-up rather than the ownership of all the tools). This tool kit was made available under strict license to enforcement agencies by Microsoft, but in 2009 copies of the tool set were leaked onto various sharing sites on the Internet. There was much discussion about the set containing back door access to Microsoft software, but in the main, opinion seems to have been that the set was just a gathering of tools that anyone could

have provided, in this case the work of gathering together and providing a simple menu had already been performed. Given that there are some discussion still running as to the legality of opening the leaked toolset, even to produce a screenshot, only the distribution package outer screenshot is able to provided here as verified by the researcher (figure 30).

Figure 30 COFEE Tool Distribution

Included additionally, (figure 31) to clarify perhaps the arguments that this secrecy may, as claimed by Cohen Associates (Cohen 2009), merely be an attempt to keep private the outdated and basic nature of the tool is an unverified screen shot supplied during training courses in 2009 by J. Wykes of the National White Collar Crime Centre [sic] in the USA.

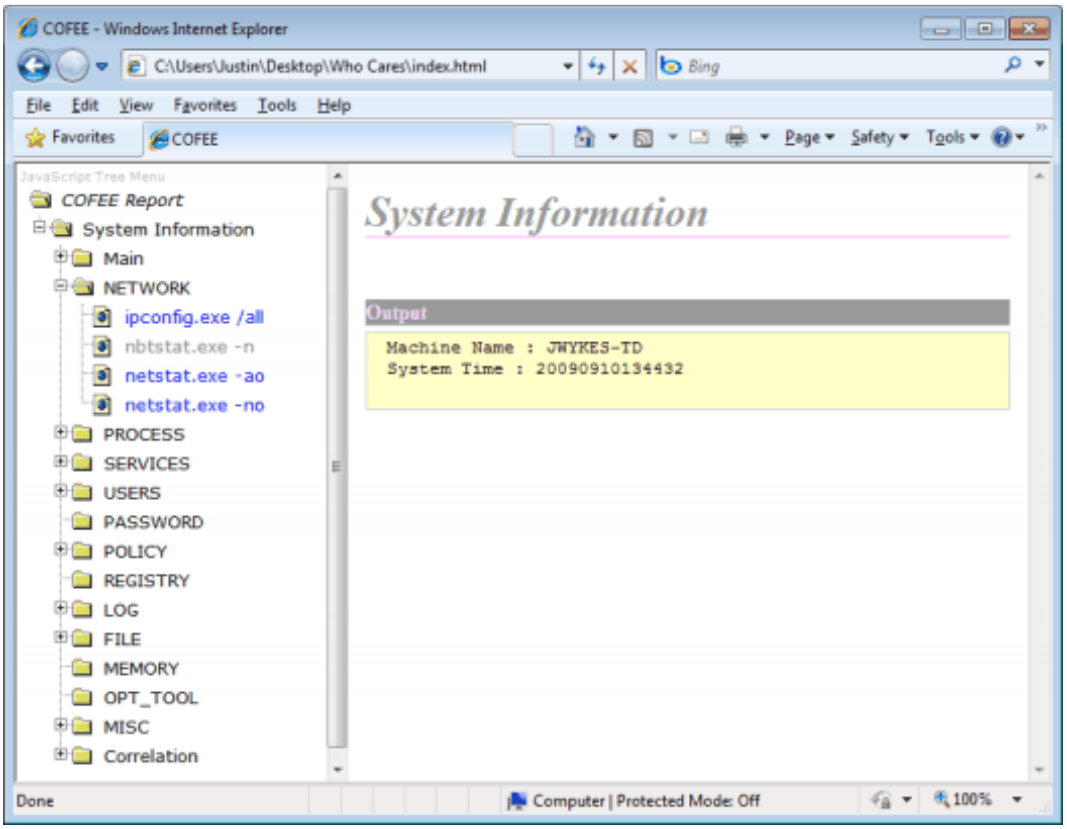

Figure 31 COFEE Forensics Tool

FIT (Forensics Investigation Toolkit) is produced by Decision Group, a Taiwanese PC option card manufacturer. It is a specialised option of a multi-product toolkit that has following in the industry specifically for its ability to analyse network level traffic and network related artefacts (figure 32).

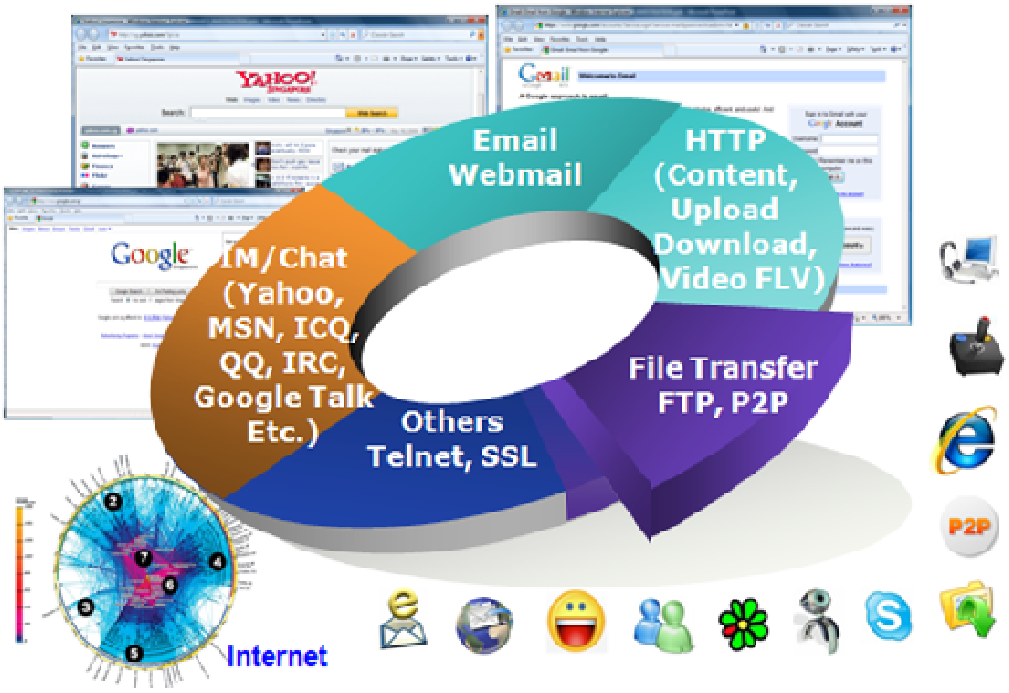

Figure 32 FIT Tool

4.4 Use of tools

The lack of experience and expertise challenges are supported in the main by Thomas et al (2008) in their claim,

"It is essential not only to have the required knowledge when completing a computer forensic case, but also the necessary toolkit in order to assist you in providing reliable evidence. A computer forensic investigation needs stable tools that offer versatility, flexibility and robustness. A forensically sound tool is intended and designed to make the work of a forensic examiner a lot easier by allowing them to perform structured investigations and improve the quality of their results" (Thomas et al, 2008, p. 5).

To further outline the absolute ease that one can set out on a discovery process with little or no experience or expertise, we should consider the review of an IT journalist, published in electronic form on "TechRadar.com", a well-read IT community forum and magazine. The review was of a tool named "BackTrack", described in the article and screenshots (figure 33) as containing "*a formidable array of hacking tools*" (Thompson, 2010, p.1).

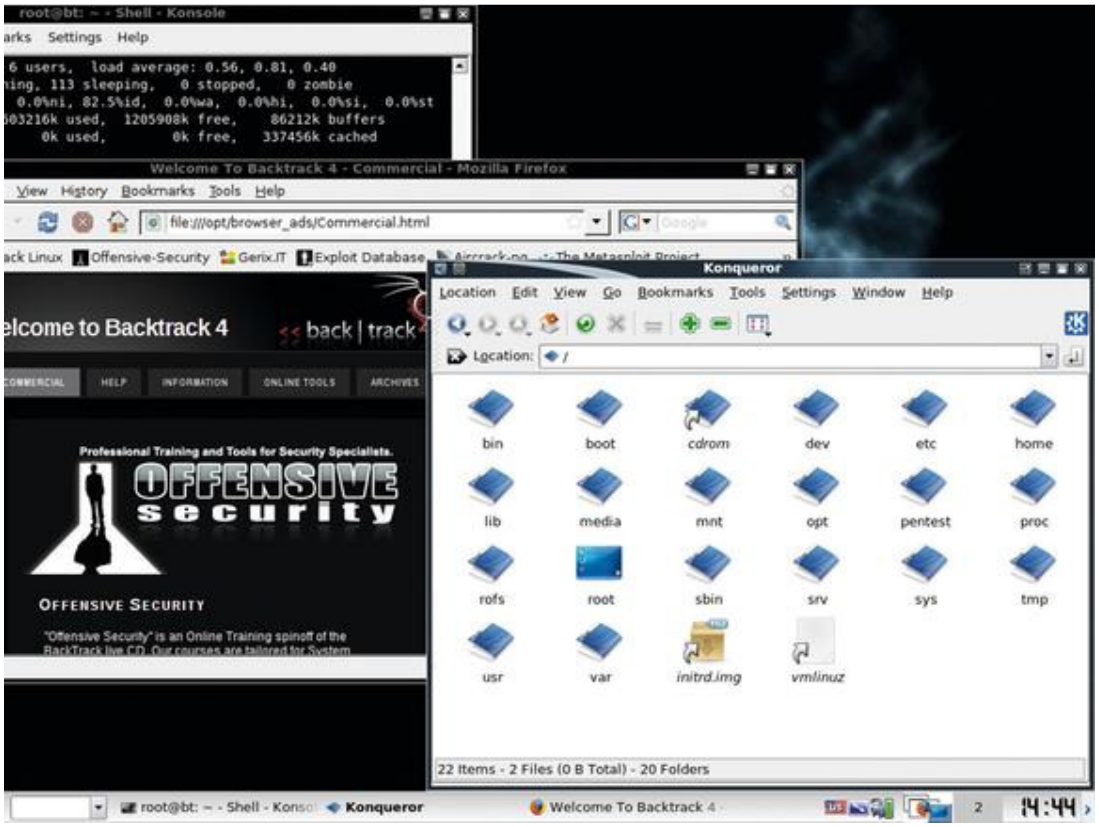

Figure 33 BackTrack Forensic Tool

"Logging into a Windows system is easy using Backtrack, even if you don't know any of the usernames or passwords that have been set up. That's because you can use a utility bundled with Backtrack to remove the password on any Windows account, including administrator accounts." (Thompson, 2010, p.1)

The statement that the tool can remove any password from any account is troubling at best. Some could see this as a treatise to break into an account without permission, thus

contravening the hacking laws of most countries. It is a clear indicator, of at least the seeming understanding of the author of this article, the forensic capabilities of the tool set are to be primarily used to bypass system controls. To provide balance, there are occasions, as all experienced analysts are fully aware, that require the copy of a system to be used in a native, or running state to try to retrieve data otherwise unreadable (encryption, solid state disks and other).

The article also presents another indicator that inexperience does not necessarily mean that tools cannot be used for data analysis, and again perhaps in an illegal manner, in this case potentially breaching privacy as well as accessing without permission;

"….These make it extremely useful to network security specialists and police forces, as well as anyone interested in knowing exactly what's happening on their own networks and any second-hand machines they've bought." (Thompson, 2010, p.2).

Finally, the call to arms of the Tyke community, another extract from the article;

"Backtrack is loaded with all the obscure little utilities used by professional security consultants. Many of them are fiddly command-line programs, but a lot have graphical front ends that make them simple to use….. There are plenty of commercial computer forensics systems around these days, but many of them cost serious money or are only available to the police. However, the open source community has a solution in the form of a special Linux distribution called Backtrack 4." (Thompson, 2010, p.3).

Given such widespread distribution of such articles, as well as the simplistic installation and use of the free tool distributions above, it is not difficult to see how the expansion of forensics into uncontrolled territory has taken place. Control is a strong word to use in describing the difference between a professional environment and one without boundaries, but it is the very element of peer pressure and criticism that defines the credibility of professions. Again, to maintain a balanced argument, merely because a tool has been purchased, rather than acquired for free, does not mean that the purchaser has any better skills merely by virtue of those invested monies.

Hayley (2002) presents a vivid example of how a prosecution expert used a simple tool to provide evidence of hundreds of searches from a browser. The defence then successfully totally dismissed the evidence, purely by exposing the prosecutions lack of knowledge of the tool used. In that case that the defence found "reams" of mail that the prosecution did not, purely because the prosecution did not know how to use the tool properly (Hayley, 2002). The challenges between legal, technical and forensic experts will abound no matter what the quality of training, or cost of tool (Livio, 2010; Ball, 2009; Jones, 2008). What is then needed is a code of conduct or practice, as this Thesis is suggesting. This provides for the case such that if two like-minded practitioners of data forensics were set off against each other in a discussion of the merits of data in an investigation, at least the validity of the results would not be brought into question. Whilst ever the credibility of the outputs of the forensic process are able to be questioned, proper technical discussions are impossible. Whether then lawyers or corporate council, or management of an entity decide to present legal, semantic or procedural challenges working on nuances of meaning or law, at least the process of data forensics will not be in question (Kelman, 2009).

"When conducting an analysis in computer forensics, the "expert" utilizes tools to examine and extract information pertaining to the crime. However, an area of contention is whether one can be considered an expert solely based on his ability to use a tool or software package, without the ability to clearly define how the tool works or reviewing the source code. The majority of the tools and software used in computer forensics is proprietary and copyrighted, thus negating the ability to access the source code" (Meyers et al, 2004, p. 5).

It is abundantly clear from this passage that the user of a tool should be able to reproduce at least the methodology that a tool is using to do an analysis or reconstruction. Further, even if the amount of data is so great that it would be impossible to perform the whole review manually, a sample should be possible to be created to support the validity of the output of the tool. Finally, it is argued that by analysing the source code, a forensics practitioner would be able to determine its true functional validity (Meyers et al, 2004). There is an intellectual challenge in this

expectation, in that the size of forensics software applications at this point in their evolution, and the number of coding experts or application programmers involved in their creation, such a review process is surely both nugatory and oversized. An expert in forensics will generally be able to determine how a tool works by its actions and outputs, and that is done on a regular basis by peers in the industry. It is for this reason that forensic tool user groups exist and how different review bodies can be confident in the outputs of analytical processes (Prince, 2007).

Meyers et al (2004) later state that when conducting an investigation an expert will use tools, this of course is obvious. We are properly presented with further suggestions that concerns should be raised if the expert cannot describe the expected functioning of that tool or a knowledge of the associated program code. This could be problematic, as the code is generally kept secret from the user of the tool in most circumstances owing to proprietary information secrecy. Again, some research would seem to have us believe that a forensic expert is going to be an expert programmer, or systems designer (Meyers et al, 2004). It would seem that to even expect each forensic analyst to be able to write application code, even less understand how someone expert in that branch of information technology has written code, is a less than realistic outline of the reality of current day forensic application usage.

4.5 Summary of tools chapter

We have seen here that the provision of and verification of supporting forensics tools is under discussion constantly. This Thesis has related examples of tools being used without proper forensics knowledge and reported proof that the outputs provided have sometimes been frankly fabricated in real terms. Derogatory terms such as *Tyke* and *Nintendo* have been variously used to describe these tendencies, as well as some very public challenges to the integrity of the industry leading tool sets. Hopefully this chapter has related these concerns to the activities that the tools are being asked to perform, and attempts to show that by working at the “bleeding edge” of computer systems data recovery, these tools can be expected to have higher failure rates than traditional robust computer applications.

5 Drivers for Action

This chapter provides deeper discussion around some of the underlying concerns and challenges in the profession today. It explores the sometimes poor performance of some forensics investigators to date. It challenges some of the dependencies upon the tool sets currently in use, and more importantly attempts to amalgamate the often contradictory advices from the various experiences in the field. A very important recurring theme in this chapter is that the profession is now being challenged from many sources and the sometimes slipshod manner in which investigations have been performed, as will be evidenced in the chapter, arguably can no longer be allowed to continue. In further drawing out arguments from previous chapters, it explores by the researchers own experience and of others, how the profession is evolving rather than being designed from scratch. It provides learning from many sources in the build towards that evolutionary process.

There are extensive references included of the ground-breaking book by author Charles A. Sennewald, "*The Process of Investigation*". First published in 1981, this is still today used as a primer for the American Society of Industrial Security Certified Protection Professional (CPP) qualification (ASIS, 2010), and provides pertinent and current support to many of the arguments in this Thesis. The insight that this text provides is invaluable as it predates most data forensics, and yet the underlying investigative themes are recurring in this emerging profession.

Once data has been gathered either from its current visible form, or as a deleted (recovered) state, it can be fed into investigative tools which vary immensely in reliability, consistency, quality and indeed price. Arthur and Ventur (2004) propose a triangulation (figure 34) between complexity, cost and functionality which inevitably leads to a biased weighting towards one of the three. Consequently, where cost minimisation is a major factor, they suggest complexity will increase and functionality decrease, leading to the potential for even less reliable output or conclusive results. Complexity can be diminished by adding more cost, functionality can be enhanced by adding more cost or increasing complexity, cost can be lowered by reducing functionality or adding complexity.

Perhaps this can be best visualised as follows:

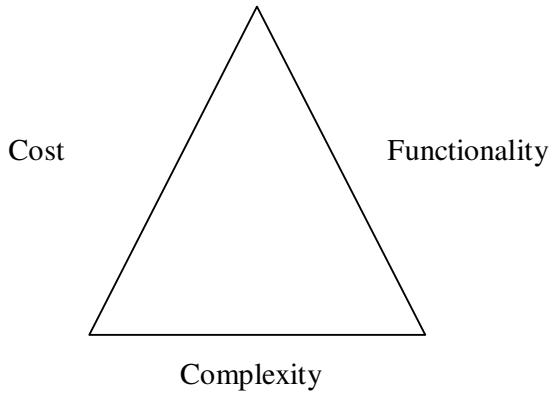

Figure 34 Cost versus Complexity versus Functionality

Conclusions and inferences drawn from the use of data forensic tools can be morally, socially and commercially damaging for the individuals or entities being investigated (Curley, 2010; Livio, 2010). This is an argument that can be applied to many professional issues. In the case of computer or data forensics, the scarcity of expertise to challenge these conclusions, as well as the propensity for data forensics experts to be automatically held in awe presents little opportunity for informed argument (Curley, 2010; Thomas and Peterson, 2008).

5.1 Distraction

"…consequently, there are many ethical dilemmas that a CFS [computer forensic specialist] must be prepared to deal with during an investigation. The most common ethical problem is managing the discovery of confidential data that is irrelevant to the case at hand" (Basset et al, 2006, p. 3).

In setting out on this path of research it was clear to the researcher, based on experience as practitioner and tutor, this relevancy problem is one of the fundamental challenges that would be at the root of answers that would need to be provided. Clearly the propensity of the untrained investigator to become distracted during review of evidence is very high given the mountain of data that is initially made available in most computer

forensic investigations. It is the experience of the researcher that the tendency to veer off course during data review is such that the outcome of an investigation can be severely jeopardised by not following a structured methodical path to the final disclosure of pertinent information. The sheer magnitude of data and history of user or program activities on any data device that has been used for any length of time is such that a clear path must be set prior to entering into any review of evidence.

"..complexity and role of forensic evidence are ever increasing" (STC, 2004, p. 2).

5.2 Trust

Thomas and Peterson (2008) make the suggestion that computer forensics, in this case the performing of such, has gone from being a fairly new technology, to something that is now frequently relied upon as a method of establishing factual information as evidence in a court of law. This Thesis would argue, that it is not in fact a technology but a skill. Whilst such sematic arguments do indeed reflect a common divergence of opinion, the overall message does support the industry experience that data forensics is seen to be domain of knowledge that only the select few are privy to. Thomas and Peterson confirm such experience by relating that because of their new found importance in "*today's criminal environment*, *[sic]"* (Thomas and Peterson, 2008, p. 2) people can often put absolute trust into computer forensic tools and processes. The underlying causes perhaps due to a belief that the evidence obtained is absolutely true, purely because it was obtained using forensic tools or methods (Curley, 2010; Carvey, 2007a; Ball, 2004). This Thesis would challenge that Thomas and Peterson (2008), in the use of the term criminal environment create an oversimplified reflection of the forensic landscape. It is arguable that not all forensic work has an outcome based on criminal drivers. In support of the requirement to understand and therefore be able to challenge the emergence of the black magic art of forensics (Ball, 2004). Thomas and Peterson do provide strong supporting opinion to this theory. It is also generally argued that that there is too much dependence on automated computer forensic tools (Ball, 2009; Jones, 2008; Carvey, 2007a). A clear statement to support these arguments;

"computer forensic analysts don't actually know just how effective these tools are" (Thomas and Peterson, 2008, p. 3).

Such claims strongly underpin what some may see as disparaging remarks in the description of inappropriate tool use as *Nintendo* Forensics (Carvey 2007a). Sennewald (1981) argues in his seminal text, that the level of experience and quality of an investigator even then was questionable. His challenges are still as valid today. Accordingly, thirty years later, in 2011 his writings are still used as a primer for the American Society of Industrial Security Certified Protection Professional (CPP) qualification (ASIS, 2010).

"Regrettably, the range or spectrum of talent, from superior to marginal or poor, is broader in the private sector. There are still a large number of unprofessional, unsophisticated and unskilled "investigators" in the security industry. And where the general public may never hear of the genuine achievements of the professionally trained and qualified private investigator, they will certainly be made aware of the illegal, immoral or sloppy work of the unprofessional practitioner" (Sennewald, 1981, p. 15).

5.3 Professionalism

Sennewald goes on to make the following observation and sets an interesting challenge.

"On balance, then, the mantle of professionalism is much more generally worn in the public sector, without question. But time and trends are shifting that balance. It would be interesting to reconsider this question in the year 2000" (Sennewald, 1981, p. 15).

Accordingly, we are now in the next millennium and the statements made are still resounding as pertinent questions and challenges being discussed. The call to challenge the professionalism of investigative practitioners is timely to explore here. If the society that the investigator delivers services into does not have absolute trust of the ability of that professional to deliver the service as described, then any decisions or inferences made as a result of the data presented will inevitably be held as potentially unsound (Curley 2010; Livio 2010; *Yorkshire Post*, 2007). Rowlinson summarises a call for better e-crime [sic] prevention and states that;

" The need for scrupulous digital forensic investigations has meant increasing number of [sic] people from both the public and private sector have now been trained in, and can undertake, digital forensics. This wider understanding and use of digital forensics has led to the need for enterprise forensic readiness as a mechanism to facilitate investigations and deter e-crime" (Rowlinson, 2007, p. 81).

Whilst, taken slightly out of context as this passage is, it could be argued that by having an ability to describe a crime, we automatically prevent it. In the broader passage Rowlinson goes on to review the power of forensic investigations as a tool to deter the actual crime itself. A suggestion that the advent of electronic crime has surged unabated because the abilities to properly investigate and prosecute it just were not there in the early days of the emergence of computer based criminal activity.

In many cases wrong inferences are drawn not purely because of the lack of experience of the investigator, but also in many cases because of the simplistic operation of the toolsets (Jones, 2008).

One description of the traits of the investigator:

"Crimes are not solved by ingenious and clever super sleuths but by hard working men and women who universally share one common denominator: perseverance…. Perseverance is the one overriding human trait or characteristic among the many deemed necessary, or at least highly desirable, for investigative work" (Sennewald 1981, p. 19).

5.4 Diligence and ethics

"computer forensics requires a well balanced combination of technical skills, legal acumen, and ethical conduct" (Bassett et al, 2006, p. 4).

The dilemma facing forensic specialists is the acknowledgment that they may have made errors in their capture or review of the data (Basset et al, 2006). The suggestion that the propensity of a forensics specialist is to continue with an investigation, even in the face of what by accidental erasure or other effect on a file system could be classed

as evidence contamination at best, or evidence tampering at worst. The view presented that forensics specialists have difficulty admitting mistakes is seemingly generally held to be true. Given that the specialist would, in the view of Basset et al rarely be challenged on such issues, the ethical debate would seem to carry significant importance in the future operation of data forensics. Without a professional conscience or ethics, and little scrutiny of actual activities, it is not difficult to extrapolate the accidental data tampering to intentional in order to support a pre-expected outcome of a case.

Whilst such sweeping suggestions cast doubts on the professionalism of many investigators, suggesting by inference that investigators routinely tamper with evidence, it should be clear that the intention is indeed to describe the simplistic activities of some forensic investigators and the none too obvious ways in which evidence *contamination* can occur. Basset et al (2006) in their obviously experienced recollections of forensic data activities, may have made their work clearer by actually using the word contamination. It is so relatively simple for an investigator to make what may seem to be unimportant mistakes in the process of forensic investigation which can have disastrous outcomes on the conclusions of that investigation (Curley, 2010; Livio, 2010).

This Thesis has already explored the possibility of evidence being contaminated by data areas used in the investigation not being properly cleaned before use, in Section 3.12, and also suggested that the careless handling of data devices during the triage process can seriously affect the quality of data available to the investigation (Livio, 2010; Ball, 2009). What has not yet been explored is the ability of tools themselves to contaminate the evidential work area.

5.5 Tool reliability and mismanagement

Forensics tools have at their heart in most cases the ability to recover data that has been marked for deletion by the user or application. In very few cases can a forensic investigator gather enough knowledge of the circumstances of the life of the data device to be absolutely sure what set of activities have been performed on that device before it was forensically captured. Just as has been previously discussed in Chapter 3, that

forensic work areas can be contaminated by prior activities, so can user devices that are captured for investigation (Meyers, 2005). Tools that perform automated recovery functions will attempt to recover any deleted files and associated data links, and in some cases these can relate to previous incarnations of files, or users. With the inexperienced investigator, files automatically recovered will all seem to pertain to the current case and as such reported and reviewed in the same light (Carvey, 2007a). Experienced investigators will always retain a pure work area for reference to ensure that only relevant file links are recovered as required, knowing that automated recovery can cause such challenges (Leyden, 2003).

Also worth considering here in some detail is a worked example of what has been coined the *Nintendo* effect (Carvey, 2007a). A tool set designed to aid the forensic analyst will attempt, in order that it is seen as being useful, to recover files and outline user activities. Using a body of knowledge that has gone before it will also attempt to interpret that data for the analyst. This body of knowledge will include reverse engineering of systems and applications by forensic analysts and software engineers in the past. Most program internal workings are held to be proprietary to the software company and thus never disclosed. Therefore, in doing this reverse engineering the tool has to make assumptions about the file system, operating system and application. As these develop and evolve, the linkages they have and the areas in which they store data can change. Whilst the expectations in the profession are that the tool should be intelligent enough to understand which version of a system or application it is dealing with, it is still incumbent on the tool user to verify the outputs of and the workings of that tool set.

As an extremely simple example, of how data could be retrieved and wrongly used to produce an inference, take what is today known, by trial and error, to be the last written date field of a database file. To illustrate, if this field description is changed by a new software version release to now actually reference the last viewed field, the tool should understand and deal with this program change correctly. Any tool that does not only confirm the actual application version, but also understand the difference and warn the reviewer of this modification can provide incorrect results or evidence claiming the

contents to be the last time the file was changed. In a case where it is important to show specific action by a user, this could be critical. Reading a field can often be done for many system maintenance reasons, but changing the contents of a field, usually requires intentional actions by the user, or by the application on behalf of the user.

Just to be clear, there is no suggestion that any software producer would intentionally cause this level of problem, but as most of the application workings for most commercial software is proprietary, and forensics software can sometimes involve educated guesswork, the situation is not unusual. Whilst necessarily simplistic so as to reduce the amount of page space, this example is not so far from occurrences that routinely happen as computer systems and applications evolve (Sheldon, 2011).

"and the very last thing forensic examiners want is for lawyers to understand the process well enough to conduct an effective cross examination" (Ball, 2004, p. 2).

This suggests that there is an implied secrecy in what is being delivered. Ball also uses the title of *tool tyke*, with a description of;

"…poorly-trained experts rely on software tools without much understanding how they work" (Ball, 2004, p. 2),

also proposing;

"…just as not every doctor is qualified as a coroner, not every systems administrator is a forensics expert" (Ball, 2004, p. 3).

These expertise arguments abound in the data forensics arena, and in many cases for good reason. As discussed in Section 1.7, there is significant availability of tools that provide instant recovery of deleted files, rebuilding of images and claimed historical analysis of web usage. This means that relatively inexperienced users of such tools can pass themselves off, or be passed off as expert forensic analysts, based on the data or reviews they provide. The outputs of those tools in a proper sense should be correlated with supporting random manual analysis of the same data sets to verify the efficacy of the tool in use. An investigator that does not have these skills will be unable to provide that secondary control and therefore his results will be seriously in question without

this. This holds true only if indeed the circumstances of the analysis are properly revealed, which unfortunately for the furtherance of the profession is not always the case (Livio, 2010; Carvey, 2007a; Ball, 2004).

"A forensic analyst will carry out several careful steps in an attempt to retrieve any potential information from a seized computer system. Much of the data that is examined is data that would not be typically viewable to the average user, such as deleted and hidden files. Most evidence is found in the files of the computer operating system itself, stored on the hard drive, storage devices or media" (Thomas and Peterson , 2008, p. 4).

The challenge therefore is to provide a proper reasoning that if the average person cannot see the data that is being presented, how do we know it is truly the data that was on the device under investigation. The *tyke* or *Nintendo* effects are most dangerous here. A proper analysis would produce a reasoned explanation of how files had been either rebuilt or recovered, along with the methodologies applied in that process. As the availability of properly professional forensic investigators grows, and therefore the ability of both sides of an argument to provide an expert testimony to support their particular argument increases, the chances that unsound conclusions from *tyke* or *Nintendo* forensics will be challenged, fortunately increases (Livio, 2010).

5.6 Reasonable doubt

"In Taylor v. Texas, the testimony by the expert showed that he used a contaminated hard drive from a prior case to make a mirror image of the appellant's drive. Furthermore, the expert formatted Taylor's drive by accident when attempting to prepare the destination drive" (Meyers et al, 2004, p. 5).

Here we have perfect examples of the two greatest "sins" of forensic capture. Both of these are simple but technically unforgivable governance errors and by being brought into a court case, and therefore remaining as public record for us to reason here show that even a claimed expert knowing that he has contaminated a case, by going forward seemingly did not expect a challenge. Earlier, the first "sin" of using contaminated working storage to perform the analysis of the captured data was introduced. The fact

that this occurred, and that it was brought out in the case, provides to us the understanding that a properly briefed, or at least forensically aware opposing council thankfully was present. Whether or not the data was indeed corrupted by the residual data from the previous activities is not actually questioned in the case. It is merely the possibility that it may have been that destroys the credibility of the so called forensic expert. As discussed in Section 1.7, a forensic tool in any guise will at least attempt to piece together data to provide as coherent a story as possible for the investigator to follow through, and any suggestion that totally unrelated data could have driven a conclusion to a different end is such that the data may as well not be there. The further (forensic) incompetence of the investigator in this case is then highlighted by the very basic precaution that he failed to take in using a write blocking device.

5.7 Write blocking

Essentially, the two activities of a data storage device are that of reading and writing. There are some housekeeping activities that move data around but in fact even these are just compound read and write operations. In the early personal computer systems, and in many cases commercial systems, in use around the nineteen seventies, data storage devices were simply magnetic tape devices that did not then contain on board index facilities. A data storage device, until it was loaded into a working state, could not be properly categorised to contain live, and potentially useful, or merely redundant data. Generally, outer containers were physically marked or labelled, but not in much greater detail than a relative volume number marking, to enable rapid retrieval from storage cabinets. A physical label would read for example, [Tape 7 Wednesday Backup, Floppy 14a System Restore] etcetera.

Reliability of systems in those early days was not that which we expect today, and system and application errors, it could be argued were more frequent than we expect in the current stage of the computing evolution. Every data storage device therefore, was supplied with the ability to physically identify it as a candidate to be used in a “read-only” state therefore only allowing read operations. The choice of whether that identifier was used and the data protected from accidental overwriting or not was finally

in the hands of the operating system, but in most cases if an operating system recognised the physical state as read only, it complied.

The first floppy disks had a hole in the mount of the sleeve to identify them as read or write enabled. The cassette tapes used by earlier mainframe and later mini-computers to distribute software and upgrades had snap off tabs at each corner to signify they should be not overwritten. The ubiquitous magnetic tape reels had what were known as “write rings” in the back face to identify their ability to be overwritten or not. Even today, the data storage devices known as “thumb drives” or “USB memory sticks” have in many versions retained a tiny sense switch to prevent their accidental overwriting. With the advent of hard drives explored in Section 3.15, the ability to physically switch to read or write mode was not so simple. The efficacy in the computer system of the hard drive was to provide storage for many differing operations and so the facility to prevent the writing of data in some areas but allow it in others, was left to the controls embedded in the computer operating system itself. One of the main advantages of the embedded hard drive in the personal computer for example was to provide what is known as “virtual memory”. That is the ability to mirror the activities of the computer memory out on disk, via a *pagefile or swapfile*; this, in essence enabled the computer operating system to seem to have much more working memory available than it in fact had. The operating system therefore had to have the ability to decide for itself when to protect a particular piece of data write activity or not. Read-only switches on hard disks generally became redundant, and the researcher has not seen a physical facility to enable/disable write on a hard disk on new devices since the late 1980s.

The forensic investigator then, in using a file system to access a data storage device, in the absence of a read/write switch cannot absolutely rely on the operating software to protect the disk. This is because the design of file system software holds the ability to both read and write. Two forensic solutions then are possible to protect the target data environment. First the file system software is modified to only allow read operations, but this would bring challenges. Primary of those challenges is that the software being used to read the data would be different to that which was used to create it, and as we discussed with Locard in Section 1.4, this could be questioned. Second, and more

reliably, the physical communication of, and with, the drive be modified outside of the data environment so that write commands can be physically blocked, but not changed so as to mirror the actual software used in the creation. It is this latter option that is the basis of any modern forensic data capture, and the reason that the term technically unforgiveable was used earlier in this chapter. These devices, known as “write blockers” (figure 35) exist solely to interrupt the write process in a file system during capture (Hamilton, 2009).

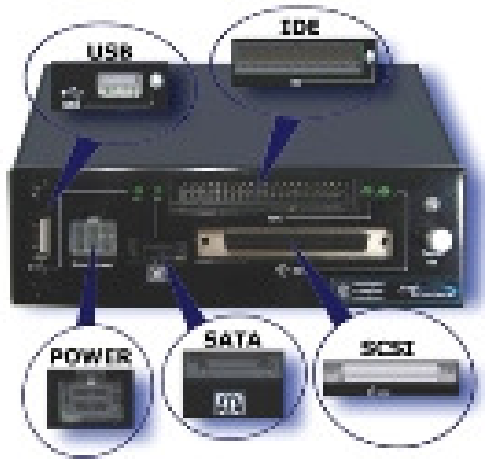

Figure 35 Write Blocker Hardware

Basic process testing prior to any data capture, which we will provide for in Section 6.6, for first responders is to test attempted writing to a disk using a write blocking device. The file system should be seen to accept the write command, properly respond to the request and then examination of the target device later should show that the write operation (usually a confirmed format or delete command) has failed to complete. If the analyst in the Meyers et al (2004) case who overwrote the primary evidence disk had used a write blocker, it would have been physically impossible to overwrite that primary evidence device. Even if that analyst had used a contaminated capture area, he could have returned and re-imaged or bit-copied the target device at a later date. The failure to use such a basic tool shows that we were indeed presented with a poignant example of *Nintendo*, *point and click* or *tyke* forensics (Jones, 2008; Carvey, 2007a; Ball, 2004).

5.8 Investigation

Palmer (2001) suggests that the primary focus for civilian and military forensic investigators is not so much a drive to prosecution, but service availability or mission continuity. The argument being that the commercial and military goals are to provide the senior management with sufficient credible and trustworthy data on which to base mission decisions. This totally supports the argument that the commercial investigator does indeed need substantially different skills than in the public prosecution and investigative services. Not all investigations in the commercial sector are designed to lead to prosecution, or are indeed a criminal investigation. Forensic investigators can be used in many cases to help understand the particular failure of a computer system, or series of events that in fact led to a non-computer related crime or failure in other areas.

Mendell (1998) suggests that computer forensics is no different to traditional forensics We are provided with the analogy that if a homicide investigator found a knife at a crime scene, he would not expect that a knife expert be brought to the scene. The knife would be carefully captured and taken back to sterile forensic laboratory conditions. Mendell provides that the responder would then be required to gather any other related evidence and note the circumstances at the scene. Such procedures, are similarly required for computer forensics investigators, and that crime scenes themselves should not be used as the investigative platform (Mendell, 1998). To provide a better reasoning for the non-technical reviewer, if a computer is found to be at the centre of a particular event or series of events that is causing either a criminal or commercial concern, it would be totally inappropriate to use that computer system itself to actually perform the forensic analysis of relevant data. The system itself could be corrupted, either deliberately or accidentally, diverting the actual integrity of an investigation, or it could contain vital information in areas of its operation that would be overwritten by its use as an investigative platform (Meyers, 2005). Mendell (1998) also further argues computer crime investigators focus too early on the technical details. Such arguing supports inputs to the triage process that a first responder training curriculum would encompass much more than purely the data capture. It also supports common arguments that the

commercial awareness of an investigator is paramount if he is to be useful in a private sector role.

Mendell's (1998) prescription for investigations starts with three simple steps, namely; gather the general facts, establish that there is a need for an investigation and preserve the evidence. Arguably we see a simple piece of advice, given in the best of reasoning that could be so wrongly interpreted. This wrongful interpretation could create havoc in an investigation. Specifically, most research shows that the establishment of need should not be in the hands of an investigator. The investigator should be there as a witness of fact to the proceedings of the investigation. If we are asking an investigator at such an early stage to provide opinion as to the potential voracity of the investigation, then we can only expect that opinion to be based upon less than coherent assumptions, rather than established fact. Good forensic practice will require an investigator to establish, in the face of a large amount of relevant data, or the inability to acquiesce the systems under review, proof that basic supporting data to underpin a continuation of capture exists (Guidance Software, 2004). This could be a rudimentary search for a particular incriminating phrase or set of credit card numbers on a hard disk, to a series of electronic mail exchanges to prove at least suspicion of connection or interchange with a particular electronic mail or computer address. This is the very least that any expert opinion of need for a continuance of investigation should be based upon. Indeed in a parallel world, that of traditional forensics, there are recent calls to challenge the reliability of forensics disciplines that deliver opinion purely on one piece of evidence such as a partial fingerprint (Spadanuta, 2010).

5.9 Hacking or investigating

"Legitimate security researchers are at risk of being criminalised as a result of the recent amendments to the Computer Misuse Act 1990. We welcome the Minister's assurance that guidance on this point will appear later in the summer, but urge the Crown Prosecution Service to publish this guidance as soon as possible, so as to avoid undermining such research in the interim" (SCST, 2006, 2.45).

This text is introduced here to highlight the dilemma that professional forensic investigators have in many countries, as well as the challenges that less than professional *tykes* may present going forward. In reviewing the data on a computer system, as well as recovering data that has been purposely deleted, an investigator can be said often to be viewing what has been properly and intentionally removed from view. In many cases it is the designated target data, namely the personal and professional musings and activities of the person properly under investigation. In almost as many cases perhaps, people connected to that business process may also have their activities and thoughts revealed purely because of the contact they have had with that computer user or computer system (privacy.org, 1993). The laws in many countries have evolved, certainly in the last few decades, to protect us from the improper abuse of information that occurs by the inappropriate access to either our systems or data, as previously challenged in Section 1.12. These laws are properly constructed to protect the innocent. In many cases, because the speed of evolution of the information technology under question, these laws have not allowed for commercial investigation or indeed in some cases public investigation of crime and fraud. A debate continues, which would extend too far beyond the reach of this Thesis, that merely by recovering data from a target disk in a system in the UK, we may have breached the "access without consent" provisions of the Computer Misuse Act (Great Britain, 1990) and thus could be liable to prosecution (Sapphire, 2007).

5.10 Doubt and opinion

A landmark trial, in what was expected by industry experts to be simple to prove guilt, was lost because the defence argued an effective Trojan claim (Leyden, 2003). The technical director of respected security consultancy IRM, Nigel Barrett who appeared in the case as an expert witness for the prosecution, agreed with the assessment of many that the judge had set a precedent which would have to be overturned if the profession were to continue to be able to reliably argue from a provision of factual analysis of forensic data.

"This is a setback because it opens the floodgates to Trojan arguments, not just in hacking cases, but in the prosecution of paedophile cases" (Leyden, 2003, p. 1).

Barrett told *The Register*

"It's very difficult to counter the quite simple argument that someone else did it and ran away. We had hoped to show that if someone else did it they would have left footprints and that, in this case, there weren't any. It's difficult to prove something hasn't happened, the case is likely to prompt a review by police of how evidence is put before a jury in computer crime cases" (Leyden, 2003, p. 1).

In highly complex cases, this use of a jury to decide on the reasonable probability that a crime was indeed committed and the extent to which the proof has been shown is arguably solely attributable to the oratory quality of the prosecution expert witness. Quite often, the complexity of the forensic process, and the inability to prove conclusively a certain artefact existed in a certain state causes doubts to be easily introduced in the arguing process.

"Parties on both the defence and prosecution side of the case floated the opinion that complex computer crime cases might better be tried before a panel of experts, rather than a jury. However juries are frequently asked to consider complex cases involving fraud. Also since changes in the rights of a defendant to trial by jury could only by authorized by Parliament this proposal is more a debating point than a practical suggestion" (Leyden, 2003, p. 1).

The Register is a primary source of computer security opinion, and discussions continue there since this case, as to how the law should evolve to support proper function of factual forensic arguing such cases. There are parallels to be drawn in the commercial sector of such analysis. Consider where a company has subjected a particular environment to forensic analysis to provide a knowledge or circumstance of a particular event or series of events. Should it then be proper that a forceful or persuasive manager be able to redirect the findings or output based on the introduction of doubts in the guarantee of conclusions of the expert (Livio, 2010; Ball, 2004; Meyers et al, 2004). Of course one would argue this should properly not be the case, but the business world is

not generally black and white, and business is transacted based on risk and probability of success. Properly, the inputs of a forensic analyst should be taken as purely that, *input* to the overall business decision making process. A practiced forensic analyst will therefore consider the outputs, and be able and ready to provide an opinion of relevance as to the reliability of the data he has uncovered in relation to the case in hand. Should that opinion then be challenged in the light of other circumstances or artefacts, it is usually that particular risk analysis process of the business that decides the outcome of an investigation. The investigator, as a professional, will move on to the next task.

"Research into IT security in the United Kingdom is high in quality but limited in quantity. More support for research is needed—above all, from industry. The development of one or more major multi-disciplinary research centres, following the model of CITRIS, is necessary to attract private funding and bring together experts from different academic departments and industry in a more integrated, multi-disciplinary research effort. We recommend that the Research Councils take the lead in initiating discussions with Government, universities and industry with a view to the prompt establishment of an initial centre in this country" (SCST, 2006, 2.44).

5.11 The Profession

The profession of Information Security is as large as the use of information. One of the specialist disciplines is that which is under discussion here, that of data forensics. The redaction of this research and production of this Thesis intends that by adding to the body of knowledge and research that is being called for by the Select Committee and Eurim, more support will be garnered for the furtherance of the data forensics profession (SCST, 2006; Eurim, 2004). In the meantime however, it is evident that the extent of pure academic research in this area is surprisingly low. Opinion suggests that one of the reasons for this is that the profession is not one that has evolved over a long time, such as the medical or legal profession (Manunta, 1996). The data forensics profession is one which has been forced into existence by the underlying lack of basic security controls as a primary driver in the information systems revolution. This Thesis discussed the right for data forensics to be called a profession in Section 1.11. In a

simplistic fashion the evolution of the data forensic profession could be likened to the banking protective security specialisation, where the need for secure design and installation of cash safes and vaults only became apparent when the money started to be stolen.

To reinforce the need for professionally trained and qualified investigators to be more readily available to the commercial sphere, we see the clamour in light of the disclosure discussions in the USA.

5.12 Discovery and forensics models

"The US has already shown the way with two cases -Zubulake v. UBS Warburg and Coleman v. Morgan Stanley where the courts awarded damages of $29 million and $1.5 billion (yes "billion") in damages because the companies were unable to produce electronically stored data in a timely fashion and for continuously coming up with new data stores even after their counsel had certified the completeness of already disclosed ESI (electronically stored information)" (Kelman, 2009, p. 1).

Whilst this is not evidence purely of the need for an experienced investigator, it is very good evidence of the need for a proper process of discovery. As more and more data is gathered and archived by companies, their ability to retrieve it in a timely and consistent fashion is repeatedly brought into question.

Mendell (1998) offers simple, yet sound advice in determining the entry point to an investigation, suggesting that a computer crime, and importantly the investigative process around a computer crime, has three distinct stages, a beginning, a middle and an end. Whilst this may seem to be an obvious statement to make, to ensure that work and analysis efforts are properly guided, the investigator must clearly understand at which stage he is entering. Mendell also suggests that in most cases in his experience, the investigator will be brought in at the end of a computer aided crime. There is a recommendation that the use of tools to ensure timelines are correctly portrayed, and this verifies another requirement in the catalogue of training needs that have evolved from this research.

The proprietary (to the tool suppliers) methodologies of forensic data investigation lend themselves readily to the systematic process that is needed to provide for documented evidence that a thorough and coordinated data discovery process has been undertaken. It is timely therefore, to introduce formal modelling of forensics practice. Presented in the International Journal of Digital Evidence in 2002, an Abstract Digital Forensics Model was described:

"Drawing from the previous forensic protocols, there exist common steps that can be abstractly defined to produce a model that is not dependent on a particular technology or electronic crime" (Reith et al, 2002, p. 1).

The writers argued that the basis of the model was to determine the key aspects of the protocols they had outlined as well as introducing and cementing pieces of the traditional forensics deliveries. The paper used in particular the protocol for an FBI physical crime scene search. It went on to argue,

"This proposed model can be thought of as an enhancement of the [DFRW] model since it is inspired from it" (Reith et al, 2002, p. 1).

Here the writers are referring to the Digital Forensics Research Workshop, an American organisation that claims *"DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research"* (DFRW, 2001, p. 1).

The paper suggested some key components of a forensics model:

> *1. Identification – recognizing an incident from indicators and determining its type. This is not explicitly within the field of forensics, but significant because it impacts other steps* (Reith et al, 2002, p. 1).

Figure 36 Forensics Model Component 1

Clearly, the first responder has to triage a suspected scene to ensure that the correct artefacts are indeed captured. Understanding the relevance of the artefacts to any continuing investigation is critical.

2. Preparation – preparing tools, techniques, search warrants, and monitoring authorizations and management support (Reith et al, 2002, p. 1).

Figure 37 Forensics Model Component 2

The criticality of preparation was discussed already in Section 3.12 (contamination), simple activities such as ensuring the sterility of capture devices is of paramount importance.

3. Approach strategy – dynamically formulating an approach based on potential impact on bystanders and the specific technology in question. The goal of the strategy should be to maximize the collection of untainted evidence while minimizing impact to the victim (Reith et al, 2002, p. 1).

Figure 38 Forensics Model Component 3

Once again, triage is clearly critical. Whilst the paper was written before the ubiquity of cloud computing and some of the more geographically distributed databases actually started to appear, the concept of recovering data from large data entities that could not be acquiesced was already being considered. Although this references the "victim", it can just as easily be applied to a target network entity or company.

4. Preservation – isolate, secure and preserve the state of physical and digital evidence. This includes preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius (Reith et al, 2002, p. 1).

Figure 39 Forensics Model Component 4

As outlined in Section 3.5, the effects of EMP radiation or interference from static electricity to any seized devices can have enormous repercussions on a case, as well as bringing into doubt the voracity of any professional gathering of evidence. The discussions on using write protection devices and understanding the state of data during capture is important. Once again, Reith et al here assume (because their work is

produced with the public sector in mind) that the devices in question will be removed from their environment on the authority of the investigation, which is not the automatic case in commercial investigations.

> *5. Collection – record the physical scene and duplicate digital evidence using standardized and accepted procedures* (Reith et al, 2002, p. 1).

Figure 40 Forensics Model Component 5

This is the essential part of triage that a first responder absolutely must be comfortable with. Section 6.5 (first responder) will detail the exact types of procedures that should be taught and tested, but in general the discussions that have already been presented around evidence contamination and reproduction of evidence are at play in this component as outlined in Chapter 3.

> *6. Examination – in-depth systematic search of evidence relating to the suspected crime. This focuses on identifying and locating potential evidence, possibly within unconventional locations. Construct detailed documentation for analysis* (Reith et al, 2002, p. 1).

Figure 41 Forensics Model Component 6

Clearly, the first responder must be more than a technical expert, he should naturally understand how important supporting artefacts may be in an investigation, and the potential for seemingly unconnected items to bear relevance to the case. As an example, in an early investigative case which the researcher was involved in, the suspect had stolen intellectual property, and a civil search warrant had been issued in favour of the company that employed the researcher. A rudimentary key system for passwords had been employed on the seized systems which although advanced for the time was not completely secure. Upon triaging the systems it became obvious that without access to the passwords we would have had to spend so much longer on site to gather what may be relevant evidence as we were not able to interrogate the systems in question immediately. Whilst we were starting the capture process, a supporting official, there to

ensure our safety, switched on the television in the living room of the house. The official commented on the strange channel names displayed on the TV set, and there were our passwords. Arguably this, at a time when many television sets were still of the manual twist channel change type, could be described most aptly as an unconventional location, and an example of one skill that the Thesis means to outline as being important. This could better be termed the skill of curiosity.

> *7. Analysis – determine significance, reconstruct fragments of data and draw conclusions based on evidence found. It may take several iterations of examination and analysis to support a crime theory. The distinction of analysis is that it may not require high technical skills to perform and thus more people can work on this case* (Reith et al, 2002, p. 1).

Figure 42 Forensics Model Component 7

It is possible for a professional forensics investigator to be dismayed by the inference in this step that the analysis may require less technical skills than other areas (Jones, 2008; Ball, 2004). It does however support arguments that the importance that should be placed upon the quality and depth of technical knowledge required to perform proper reconstruction of recovered data is indeed, even in the profession, not properly understood.

> *8. Presentation – summarize and provide explanation of conclusions. This should be written in a layperson's terms using abstracted terminology. All abstracted terminology should reference the specific details* (Reith et al, 2002, p. 1).

Figure 43 Forensics Model Component 8

Another area dealt with in the discussions on presentation in Section 6.9, is that of how to get highly technical concepts across to the layman.

"The predominance of our current forensic analysis methodologies leave examiners woefully behind in seemingly never-ending game of catch-up with those committing computer crimes. As intrusions and other computer crimes continue to increase in

sophistication, forensic examiners need to grow beyond their current toolkits and innovate in their methods of forensic data collection and analysis. The age of "Nintendo forensics" has drawn to a close" (Carvey, 2007a, p. 4).

Attempts to provide a lay description of forensic methodologies, may actually for some people confuse forensic issues with the threats of malware. Information security generalists when discussing forensics do little to help clarify. Consider the extract below, where we suddenly find ourselves in the realm of viruses;

"The traditional forensic analysis methodology has been to unplug the system, remove and acquire a forensic image (bit-by-bit, exact copy) of the hard drive, and then analyse the acquired image using a file-based approach, within both the active file system as well as unallocated sectors. As the systems themselves become more sophisticated, the examiners tools have struggled to keep up, allowing for automated searches, as well as running anti-virus scanning applications" (Carvey, 2007a, p. 7).

It is certainly pertinent to argue that the shift in evidence gathering today in the commercial sector at least is moving from being able to physically switch off a system, to having to capture from a running system, and therefore make subjective decisions as to what to capture. This can be a requirement for partial capture from a greater size networked system than is practically possible or geographically reasonable to capture (Jones, 2008). This then is a very difficult concept to clarify to a lay person, we *sometimes* will perform certain actions but cannot be clear as to when we will or will not.

9. Returning evidence – ensuring physical and digital property is returned to proper owner as well as determining how and what criminal evidence must be removed. Again not an explicit forensic (Reith et al, 2002, p. 1).

Figure 44 Forensics Model Component 9

Whilst this Thesis has not particularly dwelled on the conceptual differences between the traditional physical forensics world and that of the data forensic analysts, here is one really important difference. The fact that a forensic analyst can have what, for all intents

and purposes, is an exact facsimile of the original data, and yet not deprive the proper keeper of access to, or the ability to further modify the original is paramount. This is potentially one of the most complex issues to deliver in understandable terms to lay practitioners of the law and commercial investigations. Crime or nefarious behaviour can continue to be committed unless the actor is deprived of the primary means by which to do so. To compare, if a murderer is not deprived of the weapon found in their possession the ability to continue to commit crime is not diminished.

5.13 Evolution

The advent of the commercial Internet and World Wide Web during the early nineteen nineties meant that it was so much easier to share exploits and more importantly ideas than had previously been possible with dialup modems etcetera,. Free, or at least at sunk cost, of an Internet link communication, meant that spreading of information was no longer something that carried a cost of a telephone call, stamp or modem connection fee. Electronic mail meant that not only did the primary recipient of a mail communication see that idea, but also any person who then was copied on a reply or forward of that mail. The originator no longer was needed to be involved in the mass dissemination of the idea.

The possibilities of exploits being abused for criminal or nefarious intent therefore became greater as their knowledge sometimes spread outside of the intended recipient audience. In the bulletin board systems of the nineteen eighties and similar shared repositories on ARPAnet curious technologists and enthusiasts would share with each other on peer invite only discussion schemes, their thoughts and current exploits (Raymond, 2000). Operating system failures would be discussed and source code glitches analysed, usually from the purely technological curiosity learning standpoint. From these discussions practitioners would evolve ways in which to identify particular failure scenarios, or look for patterns in allocation dumps (Cornwall, 1998). By looking at the data held in memory when an application (system or user) failed, it was usually possible to understand at what stage in the process the application had been, what data feeds and outputs were at play, and in most cases the particular instruction that caused

the failure. These were the early forensic analysis procedures being built. As more and more the audience for these analyses grew, so did the predictable and repeatable series of steps taken to do that analysis, or in other words, procedures. As these discussions evolved from closed clubs in university networks or members only computer societies, increasingly, to open discussion forums on the Internet, the self-regulating peer sharing controls devolved massively (Raymond, 2000).

What started to become evident was that seemingly innocuous hacking exploits, when tagged with social engineering techniques reviewed in more detail in Section 2.4.7, or other code failures, could now become predictable and dangerously systematic failures injected in application processes used to control all manner of systems. The forensic community was not as quick to open up discussions, perhaps because of the generally regarded elite nature of the profession. Maybe this is also attributable to the fact that the few practitioners available at that time were too busy dealing with this emerging activity from the expanding criminal hacking community.

"Many of the hosting organisations, such as banks, other financial institutions and healthcare organisations, are taking more strenuous measures to protect themselves (in part due to regulatory requirements, rather than their own initiative), yet they are still being successfully penetrated. As the defences around these castles are being built, the attackers are increasingly turning their sites [sic] on the target-rich environment of the relatively under-protected home users" (Carvey, 2007a, p. 5).

A central theme to this research and to the challenge presented by the emerging profession of data forensics, is that the growing dependence upon forensic tools is important to understand. The emergence of the Payment Card Industry Data Security Standard requirements (PCI-DSS, 2008) across commercial card processing entities world-wide, and the enforced forensic data analysis after any reported breach requires that so many more data forensics specialists be available. The standard (PCI-DSS, 2008) provides for management and monitoring, including certification for larger card processors and merchants. If an entity is found to have breached the standard and exposed card data, the scheme can require a complete data and network forensic investigation. This is suggested, by this research, to be the single most important factor

in the recent growth of the need for data forensic analysts world-wide. Under the scheme each company is required in certifying, either by self or an appointed assessor, (dependent on transaction numbers) that they have timely access to such an expert in case of a data breach. Controversially, a compliance assessor is required to be accredited by the PCI DSS council (PCI Standards Council, 2006), where a data forensic investigator is not, adding to the potential for *tykes, point and click* or *Nintendo* experts to grow in number. This researcher suggests that merely taking technical expertise on particular computer systems and using that to perform data forensic analysis is bound to be fraught with problems, not least those types of issues outlined so far in this Thesis. Examples of such problems are detailed earlier, such as the destruction of evidence, the contamination of data and the accidental erasure of target systems.

"In the 1990s, many computer intrusion incidents were committed by pranksters, joy-riders on the Information Superhighway, bent on causing mayhem because they could. Loading the Trojan horse application 'du jour' on a system and opening and closing the CD-Rom drive tray became more than a nuisance for many system administrators and helpdesk technicians. However, the increase in online banking, online shopping, and in short, more and more people taking their lives online has lead to an economic drive and financial goal to these intrusions" (Carvey, 2007a, p. 5).

The growth in the need for forensic practitioners is in part predicated upon the shifting patterns of the criminal fraternity. The underlying pressure therefore in working with this research subject is to ensure that the advice offered around the education, training, governance and certification of practitioners is relevant not only to the perceived need today, but also caters for the emerging challenges of the profession, as far as they can be predicted.

5.14 Hashing

"further data reduction is automated through the use of libraries of cryptographic hash tables for both 'known good' and 'known bad' files, the key word here being 'known'. Increasingly, malware authors are creating custom and even new versions of their

tools, and some have even created point-and-click interfaces that allow for the automated creation of the custom malware. On a regular basis, forensic examiners see examples of Trojans, backdoors, and worms that are not recognized by name, or even as malicious in nature, when examined by over 30 separate anti-virus scanning applications" (Carvey, 2007a, p. 7).

This clearly is again focusing on the discovery of malware. Introducing the concept of hash tables for files however is relevant at this point. The very existence of such repositories shows that there is indeed a sharing of knowledge amongst professionals. Carvey introduces for us the two primary reasons to have them, "known good" and "known bad". Simply, hashing is used predominantly in forensics to remove the "known good" files from lists of files that are run against string and number searches. The majority of image files on a personal computer as of the release on the newer Microsoft Windows [Windows-XP, Windows7, etcetera] systems will be attached to or delivered to a large amount in data terms, of known good applications [Microsoft Windows, Microsoft Office, Adobe etcetera]. The matching of the exact content of the files is important to the examiner to be able to remove a great deal of resident application image data from any searches that need to be performed. This is made possible by knowing if they match a known good signature, then they have not been tampered with since release from the manufacturer. Also introduced is the corresponding "known bad" concept, where malware or malicious files that have been previously identified have been catalogued and a cryptographic hash circulated within the data forensic community. These hashes are useful in dealing with traditional virus or malware files and they support the rapid identification of malicious files. It is relevant to note in the paragraph above that the writers of such malware are obviously well aware of the ability of forensics tools to do such rapid review and are attempting to circumvent by creating unique or random signatures and therefore defeat the efficacy of hashes against them.

5.15 Summary of concerns and challenges

This chapter summarised some of the underlying concerns and challenges in the profession today. It visited the noteworthy poor performance of some forensics investigators to date, it investigated some of the dependencies upon the tool sets currently in use, and more importantly attempts to amalgamate the often contradictory advices from the various experiences in the field. The profession is now being challenged from many sources and the sometimes slipshod manner in which investigations have been performed, as evidenced in the chapter, arguably can no longer be allowed to continue. Noteworthy is the age of many of the references, showing both that this is an aged problem, and, more importantly that it has yet to be resolved.

6 Training & Research

Throughout this Thesis there are calls to censure the *tykes* or *Nintendo* forensics investigators. There are examples of data recoveries providing non-existent files, or what experienced practitioners term basic procedural failures. This chapter will summarise an outline curriculum for investigators and analysts, along with certification challenges to allow for at least a common base of knowledge to be tested before providing forensic outputs. Necessarily much of the data is built from current tool manufacturer proprietary courses, and those courses now evolving as the need grows in the industry. The summary attempts where possible to ensure that any training remains vendor neutral to provide independence of solution.

It is logical that to hold anyone accountable to a standard, the standard should be clear and commonly held to be relevant to the considerations being applied. Data, IT or Computer forensics is a wide field, and has at its base the understanding of how information moves around computer systems and networks, how it can be stored, and the various staging points it can be held at. As with many other professions, if it is to be called one, it has branches that specialize and areas that require expertise from very specific areas of study (cryptography, printer technologies, electronics etcetera) (Manunta, 1996; Simonsen, 1996).

Taal (2007) argues that there is a lot of money spent on services in the private sector as they are seen as the experts in the field. Taal also interestingly suggests that using an Internet search engine, such as Google search is the manner by which to uncover the amount of companies supposedly expert in the field, and presents at the same time the challenge of who therefore determines the level of expertise and how is it tested. That work follows on to argue that not all investment in private sector skills is wasted, stating that there are very good companies around and claiming that some of them have fully certified consultants. Unfortunately for this research, there are no references to the certification process or bodies under review. The study concludes that sometimes it is more cost effective to engage the services of the private sector investigators than to train people up internally. We can assume therefore, that this call for training is pointed at the public sector, referring perhaps to a specific governmental institution. In rounding off it

is stated that defence lawyers are seeing the benefits of introducing forensics experts, and this by inference, increases the need for more forensic experts to be trained up. The PCI requirements for forensics analysis support this conclusion (PCI, 2009).

In 1993 Fay made inroads in formally describing the challenges that are perceived in this (or what least then was) emerging field. Fay cited that (traditional) security professionals were intimidated when they learn computers are involved in the commission of a crime, and this stemmed from their belief that they would be unable to solve any such crime as it would be beyond their ability. Fay argued that this was not true and traditional investigative skills are brought to bear in this as any other investigation, quoting statistics that even in 1993 were being used to quantify the need for computer forensics professionals. The FBI reported then (in 1993) that the average computer assisted embezzlement netted $450,000 whilst theft in person averaged $19,000. What was brought into play was the concept that in information crime, manufacturing companies were just as liable to financial fraud as the banks. A comparison with current statistics would not be relevant to the argument being presented here. Understanding that in 1993, the PC was in its infancy, computer crime would almost certainly have been committed in the main against large corporate computers, hence the astounding ratio of the numbers presented, clearly a call for action at that time. The US Computer Emergency Readiness Team (CERT) report released in 2008 made similar calls in its paper on the need for process and governance in the computer forensics field (US-CERT, 2008). By referring to computer forensics as a new field in 2008, this paper suggests that all the work of people like Fay and others was seemingly ignored at least by the US government CERT researchers producing that paper.

The first step an investigator should take is to avoid jumping to conclusions, an astute computer investigator will always question the viability of the evidence and the assumptions made around it. Important is also the ability to recognize one may be heading down a wrong path or towards as dead end is a valuable skill that investigators should attempt to develop (Mendell, 1998).

6.1 Rewards

Sennewald (1981) argued that for the public investigator, the rewards are in the sense of achievement when a criminal is taken into custody at the successful resolution of a case. For the public sector, the emphasis of the work is the successful prosecution of an offender. The frustration levels, even in 1981, were obviously rising as the number of successful prosecutions were increasingly being overturned at appeal. These reversals, based on what was described, somewhat tersely as "liberal interpretations of the law", and the "wrist slapping sentences" were even then creating a climate of dissent for the professional investigator. Sennewald concluded in his text that the satisfaction for the professional investigator should be found in the investigative process itself, not the end result, describing this as the means – not the end. The discussions around the challenges centre on various levels of frustration, based upon an earlier premise introduced in those discussions, that the primary objective of an investigator in the private sector is to protect the organizational goals, and not necessarily end in prosecution. Sennewald cites an example of closing down a counterfeiting operation where the very fact that the operation ceases, is enough of a result. In other words a psychological reward for the investigator. Another example offered is that of successfully uncovering the falsification of travel expenses during an investigation, culminating in the firing of an employee, arguing that this outcome provides job satisfaction for the investigator. O'Hara (1994) brings into play the concept of *corpus delicti*, or the proving that a crime was committed. This requirement obviously does not always exist in a private sector investigative role, but it would be a potential end goal of many investigations if the intention was to prove that the required outcome of an investigation was met. This is in many cases purely a desire to prove that something actually happened, albeit in a data sense rather than physical. There is a great deal of information available in the legal sector around tests for burden of proof. The data collated in this research suggests that a simple transposition of some of the lighter concepts from a rudimentary commercial or data law primer would suffice to be included in the training catalogue (Ball, 2009).

As the automobile provided a swifter means by which criminals could move around and as such extend their cover of criminality, so in a similar manner the computer will

provide new avenues for them to venture into (Mendell, 1998). This gives us a direction in the training requirements that requires us to build in flexibility for the investigator to take on new skills that must complement current skills as computer crime crosses or expands into different or new areas of the information environment. An example could be the shift from skimming of credit card magstripe data as a card is read, to the interception of the Europay, Mastercard, Visa (EMV) standard data itself as the UK card issuers moved from magstripe to EMV authentication methods (EMVCO, 2009; McCue, 2008)

Supporting discussions around the training and use of toolsets:

" These tools and services have become heavily relied upon by law enforcement and with the lack of proper evaluating processes in place for tools and services individuals and companies without the appropriate qualifications, understanding or enough experience are unfortunately being relied upon as experts in the field of computer forensics" (Taal, 2007, p. 53).

Unfortunately there was no specific reference in the paper towards any research that would suggest what an appropriate qualification would be. Whilst the ideas and challenges are well presented and are very useful to discuss, the lack of references to enable us to expand the data at origin is distracting. This is a pity as the arguing was very convincing, and reflects the views of this researcher very closely.

6.2 The need

This Thesis and indeed extensive personal experience of this researcher in the sector strongly supports the call for formalised training for private sector first responders, investigators and eventually persons who we could term as evidence presenters. Forensic tool suppliers have a natural predication to offer training. This is by the very obvious fact that without training being available, the uptake of their tool could be less than others who do offer training. Companies such as the producers of Encase - Guidance Software and Forensic Tool Kit - Access Data, do offer training that is naturally heavily tool focused, and is patently biased towards using the particular

vendors tools (Access Data, 2010; Guidance, 2010). Whilst it is probably the better option than nothing, this training can be very expensive and singular in the overall skills offered. Nigel Jones in a paper at Cybercrime Forensics Education and Training conference (CFET) in September 2008, uses the descriptions *point and click* forensics and *Nintendo* forensics (Jones, 2008). The term *Nintendo* Forensics has been used extensively already, but it is useful to re-emphasise here to add weight to the challenges being levied at the professionalism of investigators overall and the availability of tools in the market as opposed to formal training of the profession.

Underlying principles of evidence capture, gathering and proper evidential procedure are followed and taught in tool based training generally. In most cases it can be argued the aim is to further the use of specific tools, rather than produce good quality output of students. Indeed it is possible that a student could attend a commercial tool based training course for a week, understand nothing and still gain the successful completion certificate. Whether this is possible with the recently emerging tool-agnostic trainings being offered by training suppliers is not clear, however the large numbers of certifications in the short periods described would suggest a significant pass ratio (Section 1.11). In the commercial training experience of this researcher, this happens because there is neither on-going evaluation, nor end of course practical examination in any of the leading training courses. It would perhaps be better then, to claim that these certificates are indeed attendance rather than proficiency certificates. Such an end of training attendance certificate can still however be very valuable. In most private sector forensics areas it is the best and perhaps the only challenge an employer may have as to the suitability of a person to perform evidential capture and examinations. Guidance software, the creators of Encase, which is the most pervasive tool set do offer an industry peer based certification Encase Certified Examiner (ENCE, 2010; Guidance, 2010). This researcher is a certified ENCE as well as previously an accredited trainer for the Guidance Software Encase Elementary and Intermediate Field Edition course set. General peer opinion received over the course of working with Encase is that without the Encase product knowledge, and use of that specific Encase tool to undergo the extensive practical examination, success and therefore ENCE certification would most likely not be probable. Discussions with peers at the CISO summits and the

London IT Security Forum suggest that the two other leading industry certifications of ACE and PCFE (Section 4.3) had similar expectations, and both offered *boot camps* intended to end in a certificated analyst on the last day of the training (MISTI, 2012). Again, it must be stressed that carrying such a certificate shows at least an intent to learn, but without formal examination and peer review does not meet the criteria we are expanding here.

We are informed that there are no mechanisms in place to assess experts or a formal process to follow when engaging with them, arguing further that people who have worked in law enforcement automatically are granted a right of passage to expert status and nothing is based on skills or capabilities (Taal, 2007). Further there are calls for a professional body to register the experts in the field and for that body to regularly check accreditation of members. We will discuss later why that concept of a register, which in fact had been implemented in the UK for the forensics profession as a whole was disbanded in 2009 (Sommer, 2011). Taal stats that Members should be:

"personally financial liable for false reporting similar to that of private investigators field" (Taal, 2007, p. 64).

Taal further arguess that the Private Security Industry Act 2001 (Great Britain, 2001) is to be used to support claims for this fiscal censure. Taal summarises very well and the text as a whole is useful to consider here as we investigate the needs of a training catalogue:

"above the most important thing… Cannot call yourself an expert if you have all the experience in the world and lack the basic understanding of computer science" (Taal, 2007, p. 64).

It is the experience of this researcher that a *basic* understanding of computer science is more likely to end in an incorrectly formulated investigation than anything else , and it is hoped that quoting Taal at this point, does not take this important text out of context, thereby diminishing the overall message of the need for a rounded experience set. The arguments laid out in this chapter qualify a need for *in-depth* expertise with extensive detailed experience of the application. Further there is a clear requirement for an

understanding of the software environment under investigation. Take for example a description of the overall module aims of the Kings College MSc. course

"The stated aim of the module is "to provide students with a solid foundation to understand the concepts involved in both computer forensics and cybercrime" (Overill, 2008, p. 2).

6.3 Required skills

Overill (2008) does emphasise the solid foundation, and is underpinned in the rounding call by Taal (2007). The required skills for the proposed entry point into the profession would probably then not be able to be met by a recent under-graduate. Perhaps leaning more towards a specialist (System, Network, Application) with underlying academic qualifications. It is suggested here that a strong requirement is some years actual practice on the type of systems under investigation. Similarly it is clear that there is a need for enough practical knowledge not only to recognise the system or application, but also enough analytical skill to formulate reasoned opinions and theories. This knowledge then is supposed to be gained through a formal course of study.

Mendell (1998) suggests that investigators, who are not necessarily natural cynics, should learn scepticism as a survival skill, also arguing that social psychology is an integral part of their work. As part of the work that they perform, looking for reasons behind malicious behaviours, the investigator learns a skill of "*reading between the lines"* (Mendell, 1998, p. 92). In discussing this behavioural analysis there are certain factors that an experienced investigator would be looking for; people who never take vacations, political extremists or financial struggles, evidenced in the data captured. It is clear that Mendell has extensive experience particularly in fraud, and the experience that this researcher had gained as a Certified Fraud Examiner (ACFE, 2010) supports this advice. Some of the particular details are useful to succinctly highlight that a crossover between the fraud examiners and forensic analysts is natural. This gives us many other potential channels to suggest further research in at a later time.

Since investigation is essentially an art there has to be room in the study of the profession to allow for the process of intuition, described as being;

"the sudden and unexpected insight that clarifies the problem where progress by logic and experiment has been end-stopped" (O'Hara, 1994, p. 23).

A suggestion that the "hunch" is well known as being an attribute of investigative work. The argument continues further putting the case for intuition in reminding us that in many cases an investigator can come to a point where;

"*plodding work and deductive reasoning*" are not working and the best one can hope for is a break using "*intuition or chance*" (O'Hara, 1994, p. 23).

A description of the learning aims of the Kings College MSc. module neatly rounds off the expectations;

"At the end of this module a student is expected to understand computer crime, together with its social and legal implications; understand the techniques for computer and network forensics; understand, and relate the above points to, the UK Computer Misuse Act and related EU legislation" (Overill, 2008, p. 2).

What is interesting and potentially different to other MSc. courses dealing in specialist areas is that this module is not delivered as a formally examined lecture or laboratory-based course (Holloway, 2010). A decision was made to provide it as a reading course ending in a dissertation and supporting oral presentation (Overill, 2008).

This Thesis will now attempt to build on the compiled arguments and bring to bear a suggested curriculum outline for forensic investigators. As previously described, the inputs for these suggested training areas are culled from a series of sources, such as current industry training offerings, training course supplier offerings as well as experiences discussed with peers as part of the research for the Thesis.

6.4 Curriculum outline

Before laying out the four areas, it is important to consider that underlying the main suggested areas is a grounding knowledge level which could simply be called “basic”.

Many course offerings involve the skills listed below, but in different configurations. For example, the PA Consulting information security training arm build their courses with the aim of a specific categorisation of investigator or skill, to enable a certificate to be granted at the end (7safe, 2012; GIAC, 2012). As a result the specific items listed below will indeed appear multiple times in their course schedules dependent on which specific certificate the attendee is looking to obtain. Where a training is offered as a specific skill, as in the case of IT Governance Ltd, we see a structured approach leading to a build-up of knowledge, rather than training to pass a specific hurdle (IT Governance, 2012). The sections below are categorised to most closely resemble such an approach. A similar vendor, QA provide a specific basic skills course, and take great care in ensuring that the prospective student understands it is a non – certified course (QA Training, 2012).QA training claim to be the *“UK’s leading learning company”* (QA Training, 2012, p.1). In the examples of tool vendors, this approach is a little different as they have structured curricula aimed at progressing towards specialised use of that particular tool. Indeed the Guidance Software website prevents you from viewing later training in the series without confirming by a click button that you would have the necessary understandings gained by the previous course (Guidance, 2012). The Infosec Institute, which interestingly offers the temptation of a 93% pass rate and two certifications to be gained from the same course, offers training using open source tools and has basic skills as one of the first study areas. It lists around thirty specific study subjects most of which appear in this section (Infosec Institute, 2012).

This section then, in laying out a suggested curriculum for forensic investigators has attempted to cull inputs from all sides, and produce a structured learning path that could be applied, and proficiency in each area tested consistently, no matter which learning tree route a professional has followed to achieve the stated knowledge level.

To be certified at a basic level in the field of computer forensics, it is suggested then, that the following skills are mandatory:

1: To be able to describe to a lay person what constitutes (or can be held to constitute) digital evidence. It is expected that the subject would be confident in discussing the various states of information (in transit, at rest, printed, electronic etc.), the differing protocols used in representing computer data (ebcidic, ascii) and the various presentation methods (binary, octal, hexadecimal etc.). The candidate for any end of level test would be expected to be understood and able to describe the differing usage of protocols and presentation methods at a rudimentary level, and be able to differentiate their various usages.

2: A basic understanding of the make-up of a modern computer system, its primary components and the inter-dependencies is also required. It is expected that the student would be able to describe the specific components of a system, such as Central Processing Unit (CPU), Input Output (IO) bus, Network Card, Video Card and so forth. The fundamental differences between an Operating System, Firmware, and Application Software is also expected to be able to be simply described.

3: Basic authentication and authorization concepts would be expected to be understood and able to be articulated. The student would be able to describe the interaction between a user and the system, and also be able to differentiate between the differing account types such as User, Programmer, System Administrator and Maintenance for example.

6.5 First Responder

The first actual peer examined certification level proposed is that of First Responder. This certainly requires an understanding of what data devices and systems may be relevant to an investigation, as well as the potential use that an examiner may make of them. Also it is critical that the responder be able to set the scene for an investigator, so performing a basic description of the environment of capture as well as any salient facts that may potentially have relevance is key.

A simple example as presented briefly earlier (section 5.2) will add understanding. During an investigation a first response investigative team entered an area of interest and found many systems that had password controls. The target was either unwilling or unable to cooperate, essentially denying all knowledge or memory of any such passwords. A potentially time consuming data capture process of all the discovered data devices was started, which based on previous experience, could in all probability only later prove that all the devices were encrypted with passwords that could not be bypassed simply using the few specialist tools available at the time. On switching on the TV, as a diversion whilst waiting for some captures to complete, one of the team was surprised by some on screen naming for the channels. The on screen channel names it was found, after trying the strings in the password challenge screens, were actually the passwords to each device. The learning being that any device that is in a target area may be relevant to the future resolution of the investigation. Any such device should not be discounted from adding to the evidence stack. Being able to do on the spot investigative analysis of the required capture is therefore also an important piece of the first responder training.

So, in summary the main task that is attributed to a first responder is to secure the complete evidence set to allow a forensic investigation to be properly applied. This involves ensuring a proper chain of evidence and a proper acquiescence if relevant of the computer system under investigation. To be able to properly accomplish these challenges the following (figure 45) is suggested to be rudimentary knowledge, and is formed from the experience in teaching and attending courses in computer forensics of the researcher.

- An understanding of types of digital evidence and how computers work
- An understanding of Computer Forensic Methodology
- Knowledge of basic make-up of the File Allocation Table (FAT), New Technology File System (NTFS) and other relevant file systems
- The ability to create a case file and how to preview/acquire media
- The ability to perform a data acquisition using a Linux boot disk
- Understanding and examination of Mac disk and file system structure (specialist)
- How to conduct basic keyword searches using various tools
- How to analyze file signatures and view files using common tools
- How to restore evidence in chosen tool sets in a forensically sound manner
- How to archive files and data created through the analysis process
- How to verify the evidence file created in various tool sets

Figure 45 First Responder Curriculum

Without extrapolating each item, the items presented in this category would provide for a rudimentary series of skills to ensure that proper evidential process can be followed and the ability to recognise the systems and data presented would enable the proper triaging of evidence for further investigation.

6.6 Evidence Preparer

The second, and probably longer and more intensive training curriculum and certification route is that of evidence preparer (figure 46). This is not, in most commercial investigative environments a task that would be the only work a person would do, but given its critically to the proper dénouement of an investigation, it is a specific skill set that should be trained, tested and importantly, certified. The training for this area would ensure that the person would be able to attest to the sterile work areas, proper evidential process for the recovery of the various data to a workable format. Required also are the skills to perform the occasional integrity checks of the toolset and data devices to ensure proper response to integrity challenges of conclusions. Again,

rudimentary skills for this specialisation, based upon experience of teaching and performing forensic investigations.

- The ability to create and use logical evidence files, versus physical files
- How to locate and recover deleted partitions and folders in disk and file systems
- How to export files, directories and entire volumes using recovery tools
- How to recover artefacts such as swap files, file slack, and spooler files using tools
- How to identify, rebuild and recover printed and faxed pages in various systems
- Hardware and software RAID technology, acquisition and examination
- Principles of encrypted data recovery, and associated challenges
- NTFS data recovery (possibly using a variety of tools)
- Linux partition recovery using specialist or open source tools

Figure 46 Evidence Preparer Curriculum

In this preparation role, the knowledge of how files and systems are related and how the different artefacts that can be found on a system are connected together. There is a need for understanding what recoveries may be possible, and how to ensure that any recovery from a deleted area is done transparently such that it can be repeated and reviewed by peers.

6.7 Investigative Analyst

The third qualification and peer certification area is probably the most intensive and repetitive area of training, that of investigator, or investigative analyst (figure 47). Entry into this training should not be attempted until a work experience level is attained to ensure that a proper grounding of the relevant computer system concepts is displayed. This requirement and experience level obviously will differ as to the specialist type of computer environment envisaged to be trained against, but in general, a minimum working experience of two years as a Microsoft Windows system administrator for example would be a prerequisite for Windows investigations training. Similarly Electronic Mail investigations would require consequent levels of experience

maintaining Electronic Mail systems. Specialisations in each area could be accumulated, and repeatable skills training such as proper evidential procedure and data integrity would not be required to be repeated. Any student completing a course would certainly be taught to use the various tools in common use, but would also be required to demonstrate a basic understanding of the basis upon which any tool draws a conclusion, such as the recovery of data from a file slack area. Experience is critical because the understanding of the outputs of many tools is aligned with an expectation that any interpretation of results by those tools, such as re-joining fragmented file structures, or recovering file headers for deleted files can be properly described outside of the tool set by the investigator. As a simple analogy, if one uses an electronic calculator to perform a calculation, it is usual to have a basic understanding of the expected magnitude of the outcome to ensure one has not put the decimal point in the wrong place during data entry.

Skills that are generally expected in this area include:

- How to conduct keyword searches and advanced searches using GREP (for some tool sets) [global search for regular expression and print -sic]
- Examination and understanding of the Microsoft Windows Registry
- Compound file types, and their uses and formats
- How to identify files using hash values and building hash libraries
- How to identify Microsoft Windows (usually XP onwards) artefacts such as link files, recycle bin, and user folders
- Detailed analysis and recovery of Microsoft Windows event log files
- Manual recovery of artefacts such as swap files, file slack, and spooler files
- Analysis of NT File System (NTFS) artefacts within Microsoft Windows
- Understanding Linux / UNIX operating and file system artefacts and their recovery
- Macintosh OS X® operating system artefacts and recovery
- Artefacts associated with peer-to-peer file-sharing applications such as BitTorrent™, LimeWire™ and BearShare

Figure 47 Investigative Analyst Curriculum

This is obviously a more specialist area and requires in depth knowledge of the systems that would be studied for forensics. It edges into areas where tools are not always available or seen to be working, such as in a partial disk recovery or corrupted data areas. It also starts to involve connectivity concepts so that a series of events that may involve data coming onto or heading off a target system can be replayed or at least properly described.

6.8 Mobile devices

Before this Thesis goes on to describe the fourth main training area, one emerging specialist area, that is worthy of separate note here is the recovery and analysis of data from mobile phones (HDForensics, 2010; MSAB, 2010). As the data on mobile devices

grows, and the features gap between personal computers and mobile devices shrinks, there is an obvious growing need to recover data from these devices, and their difference of use patterns suggests a different methodology of data capture and analysis (Legault, 2011). Without diverting the basis of this training section, that of the four major areas suggested, it is useful to highlight some of the specific additional skills that will be needed to specialise in this area, perhaps at the level of researcher above. These additional areas come from analysis of the offerings of specialist companies (HDForensics, 2010; MSAB, 2010) (figure 48).

- An understanding of mobile phone network protocols and key service providers
- Differences in the major phone types and architectures
- The ability to acquire and examine SIM cards using tools
- Understand in depth the mobile phone data storage architectures

Figure 48 Mobile Devices Curriculum

The movement from the corporate work bench or user PC to mobile media means that more and more of the target data for a private sector investigation is potentially resident on a mobile device. Also, where chains of communication are involved in understanding a particular series of events, there is a high probability that at some point a mobile device will be involved.

"…so fraud examiners have no other option but to consider evidence from them when investigating fraud in the workplace" (Legault, 2011, p. 2).

In many cases, it is expected that a specialist in the field would be injected, as the knowledge is very specific, but in the case where there is no such help, training above would provide the rudimentary skills needed to properly evidence mobile data traffic. There is also extensive discussion on the relevance of SMS messages and the value of SIM data, for which the summary overview provided in *Fraud Magazine,* is certainly recommended (Legault, 2011).

6.9 Data presenter

Finally, the reporting and presentation of evidence is the most often overlooked, and arguably the most important area that calls for training, that of data presenter (figure 49);

- Preparation of reports and evidence for presentation
- Presentation skills
- Charting skills
- Visual analysis mapping tools
- Cross-examination training
- Logical arguing

Figure 49 Data Presenter Curriculum

As this can be something that an investigator never has to do, it is not suggested that all forensic investigators follow this module, but if at any point the output of an investigation is to be presented or defended, then this module should prove useful.

Because this research is concentrated on private sector investigations, and as most such cases do not actually end up in litigation, it may seem overkill to provide intensive training in the presentation and defending of evidence. If a private sector forensic investigation evolves into criminal litigation, the whole of the excellent work that has gone before could be destroyed by a lack of preparation for or understanding of the judicial process. It is arguable that irrespective of whether a victim of a crime, or indeed a suspected perpetrator is getting; *"their day in court"* it is the ethical duty of the investigative team to process the evidence as though they were (Cavanagh, 2008, p. 1).

6.10 Public-private partnerships

To provide a brief understanding of CITRIS, that is referenced below;

"the Center [sic] for Information Technology Research in the Interest of Society (CITRIS) at Berkeley, have been instrumental in providing a bridge between policy, industry and academia" (Dillon, 2006, p. 2).

The Select Committee debated at various junctures the opportunities for public-private cooperation in training and certification (SCST, 2006);

"It is notable that while the private sector partners supporting CITRIS include major companies in the IT and telecommunications industries, companies from manufacturing, energy and other sectors also contribute. As computing becomes ever more pervasive, more and more private sector companies—for example, those providing financial services—rely on IT security, and will have an interest in sponsoring research into IT security. There is therefore an opportunity to attract a wide range of private sector partners, with diverse interests, to support a major research initiative in this area" (SCST, 2006, 2.38).

So, we can extrapolate from the Select Committee discussions that the collaborative research proposal is on the table, and yet the only partnership that the Select Committee could find as an example is that of a US university, albeit a prestigious one. Perhaps this could be the most distressing evidence that research into, in this case, the greater subject of information (or IT) security is so poorly supported by academia in the United Kingdom. The inference that could also be drawn is perhaps that without private sector funding research would not happen. This suggests a poor indictment of how research specialisations are chosen, especially where potentially, national information interests could be in jeopardy. The Select Committee report did not include any obvious desire for IT security to take a place in the national curriculum (SCST, 2006). Strangely neither was there any suggestion of a specialist government department focus being needed to drive the furtherance of the subject.

Sennewald (1981) concluded his discussions of the differences between public and private investigators in pointing out that his intention is not to dwell on the differences between the two specializations, but that with an increased understanding of where the common interests and goals lie, the possibility for communication and working together

more cooperatively is heightened. Perhaps even in 1981, Sennewald knew that without extensive private sector funding, the public and private sector would continue to depend purely upon practical field experience. More importantly we would depend upon software manufacturers tool biased trainings to drive the furtherance of the profession. Arguably the expectation was that little research would become available to actually prove a need for a deeper knowledge base, and an emerging need for expansion of the body of knowledge in the delivery of the forensics expertise.

6.11 Training and research summary

It is reasonable to conclude that further specialised training is absolutely necessary, and it will have to be modular to enable differing levels of expertise to be brought to bear at the correct point in the evidence gathering and analysis process. Having argued in this chapter the need for formalised and consistent training, we have explored an outline curriculum for investigators and analysts, along with examination challenges to allow for at least a common base of knowledge to be tested before providing forensic outputs. This Thesis also argues four main areas for training to be applied, and a confirmation of expertise be tested at each. These areas cross over some of the course subject areas offered by forensic software companies currently. This chapter then, in laying out a suggested curriculum for forensic investigators has attempted to cull inputs from all sides, and produce a structured learning path that could be applied, and proficiency in each area tested consistently, no matter which learning tree route a professional has followed to achieve the stated knowledge level. The above curriculum allows for tool neutral training to provide independence of solution

7 Certification and Oversight

This chapter expands upon the depth of training required, and explores how the professionals once trained could be peer certified and censured as necessary to retain an integrity of delivery within the profession. It explores parallel organisations that have faced and in some cases met such challenges, as well as exploring examples of good or bad practice to be taken into account when building such a framework for forensics investigators.

Having introduced the concept of ethical duty in Section 3.2, it is timely to re-examine certification and importantly oversight in somewhat more detail. This need for oversight has evolved in the research as a subsidiary requirement that is now also being expanded in this Thesis. Just as there are specialist areas that differ in the training needs, discussed in Chapter 6, there should be specific certification aligned to the areas of specialisation to avoid any challenges that the certification could be too generic.

To balance the discussions, an interesting argument against conformity;

"Spanning the realms of art and science, and dealing as we do with human frailty, computer forensics examiners are aided by instinct and gut feeling-skills which don't lend themselves to checklists" (Ball, 2004, p. 5)

The claim that gut feel automatically prevents the use of checklists is perhaps a little too rigid. An opposing view;

".. the forensic analyst needs to begin under a concrete method and finish so" (Angelopoulou, 2007, p. 5).

This need for a concrete method, as it is described here, is at the heart of one of the main recurring subjects of this research, and indeed of experience of the researcher, that of repeatability. If a method is to be used to perform a forensic examination, it should be, certainly according to Angelopoulou (2007) at least, something that can be described in a formal manner, essentially allowing the method of working to be reviewed as well as the obvious challenges to any outputs that may be made.

Even as far back as 1995 the debate for standardisation was running;

"*standards are a blessing and a curse*" also "*They should describe that which is the minimum acceptable level of performance*". The passage continues, "*standards can serve to impede progress and limit creativity*" (Pollit, 1995, p. 3).

It is interesting that this dichotomy of arguing for and against a common certification standard, within the research conducted for this Thesis, arises each time the discussion leans towards the private sector. When highly experienced forensic analysts are asked to agree that they would commit to being held to such a standard, opinion is clearly divided, or at least the peer community canvased by the researcher.

Meyers (2005) clarifies that the need for professional or formal industry recognition of a field of forensic investigation is becoming more apparent as the defence becomes more technically sophisticated. It was predicted in 2005 that the recognition of the field by the American judicial system and the underlying methodologies was not long from being formally appreciated, likening the need to that which has been understood by other forensic disciplines such as financial fraud analysis (Meyers, 2005).

In the conclusion of an earlier work;

"The inevitable fact that technology is becoming more intertwined in the daily life of the individual will lead to an increase in court cases where computer evidence is a vital component. Because the judicial system is having difficulties in mandating and interpreting standardization for computer forensics, it becomes the responsibility of the scientific community to assist in this endeavour" (Meyers et al, 2004, p. 9).

Here clearly then there is a call for the scientific or more importantly academic community to support the efforts in standardisation, research and training.

"In other fields of study, (e.g., accounting and financial fraud investigation) there are methods used to ensure that the practice is credible and reliable, and that the individuals claiming to be professionals have met a certain certification criteria" (Meyers et al, 2004, p. 10).

Without opening the profession debate again, we do see that there are similarities of need with other professions (Manunta, 1996; Simonsen, 1996). The call is clear to reuse wherever possible the experience and expertise that has been brought to bear in other professions, with the aim creating a regime of credibility and reliability of output.

The example of the Certified Professional Accountant (CPA), where a professional association of experts provide for a series of examination standards running against strict peer reviewed criteria is useful. A strong case is made for the fact that there are two things that bring credibility to practitioners in the field holding this certification. It can be shown, by this examination process that a holder of the credential has been certified to have a certain period of experience in the field and that his skills have been tested by formal examination (Meyers et al, 2004). Discussions that both these criteria for recognition are missing from the field of data forensics suggests that there is a need to call for a debate on the relative validity of doing something similar for the data forensics field. If agreement is then reached, the extent of the required experience and examination standards can be considered in greater detail. Given that there are already many fields using independent certification in similar areas, it has been useful to use these experiences to gauge the progress and validity of the research (ASIS, 2009; ISC^2, 2009; PCI Standards Council, 2006).

Within this section dealing with the issues of certification and oversight, a great deal of insightful arguments are most clearly formulated by the work of Meyers et al (2004). This Thesis has found general alignment with the work of Meyers et al, and indeed supporting practical experience of the researcher strongly supports the absolute need for formal recognition of the profession. Any standard to be formulated must have an understanding that it will evolve as the profession evolves, and it should allow in its governance for that to happen effortlessly. A standard that cannot change is worthless (Meyers et al, 2004). In addition to a requirement for detailed analysis of each phase of the computer (data) forensics process, and subsequent alignment of delivery procedures, it is clear a standard must remain practical. Similarly it is worth emphasising that if a standard becomes impractical to deliver against, it will wither. The area of search and seizure, obviously is an important topic the standard will have to cover. The forensic

analyst will need very different skills in the various points of the forensics process. This Thesis suggests, that the modularisation or dissecting into categories of training and certification is the most expedient manner in which to proceed. This direction is echoed in other research:

"Accordingly, the certification may need to be broken down into several qualifying examinations, since not all persons in the field will participate in all of the investigative phases (e.g., search and seizure, analysis, examination, etc.)" (Meyers et al, 2004, p. 9).

7.1 Expert witness

It is relevant to discuss further at this point the specialised area of expert witness, which although a slightly different skillset and delivery from that of a data forensic analyst, does carry many forensic capabilities and expertise challenges to warrant its inclusion here. The title of expert in any field is difficult to certify or quantify. In data forensics it is doubly so because the field has no formal training regime, no accepted independent professional qualifications, nor indeed a recognised educational progression. Many argue that an expert is recognised in the forensics profession as someone having related skills in the area under review, such as networks, operating systems or application software, as well as a number of years of experience in practicing those skills (Jones, 2008; Carvey, 2007b; Ball, 2004; Meyers et al, 2004). Preceding discussion predicts that the challenges to this means of credibility assertion will increase as the number of failed investigation and improper conclusion grows and become published. The discussions are clear in also reminding us that the introduction of a certification and educational challenge to data forensics experts may not automatically and immediately resolve the quality issues and unsound conclusions. The most obvious outcome of the education process is that that the number of such challenges should fall. Many predict that if current so called experts are all required to pass through a consistent qualification, examination and certification process, it is highly probable that the ranks of said experts will dwindle initially (Carvey, 2007b; Meyers et al, 2004). This prediction is founded on the belief that there are practitioners who would not pass peer review, an obvious assumption is that these failed experts would therefore be removed

from the peer assessed expert lists and no longer practice. An interesting review of the efforts of the UK Forensic service to establish a register of experts is offered by Sommer (2011). We see a very detailed background history of how a register of experts was achieved, and then disbanded as the forensic science body lost funding. Indeed the body itself is being disbanded in 2012 (Sommer, 2011).

An interesting side effect of having to certify even if one was previously classed as an expert, would be, that cases both in the public and private sector that have relied upon conclusion, or even opinion, based on testimony or reports from now "uncertified" experts, could be reopened or even nullified (Sheldon, 2011; Spadanuta, 2010; Meyers et al, 2004). This Thesis would also suggest that cases which have depended upon previous, now proven to be flawed or unsound tool sets should also be reviewed where the outcomes have been based solely upon the tool set in use and not any otherwise corroborating evidence. A similar challenge has been laid at the field of fingerprint forensics, after the widely publicised error that was produced by the FBI. Their fingerprint specialists had managed to correlate a partial finger print found at the scene of the 2004 Madrid train bombings with those prints taken from file of an Islamic lawyer resident in Oregon, USA (Spadanuta, 2010). Being able to resolve these issues may be somewhat difficult, given that when the data was processed and presented there was no formal or expected methodology, but it may be relevant to at least pursue cases that are presented as unsound under review by the newly certified, and therefore newly trusted, experts. Again, significant advice from the same report, quoting Dr. M. Risinger, law professor at the Sefton Hall University School of Law, USA:

"… what you used to convict people 20 years ago really wasn't as reliable as you thought it was" (Spadanuta, 2010, p. 2.).

7.2 Related acts

In any profession, a knowledge of surrounding legislation and standards is essential, and during the research project many references were found to various UK legislations. It is pertinent therefore, to assemble a summary list here to provide some view of the scope

of the work of a forensics investigator within the support of criminal and commercial prosecution:

Theft Act 1968 & 1978 (Great Britain, 1968; Great Britain, 1978a).

The Theft Act in the whole provides definitions for the removal of or depriving a person of property. It covers areas such as false accounting and provides a definition for dishonesty.

Theft (Amendment) Act 1996 (Great Britain, 1996a).

The amendment provided better definitions for obtaining services by deception, amongst others. It also provided the definitions and offence for making off without payment, which can be useful to an investigator.

Criminal Attempts Act 1981 (Great Britain, 1981).

This Act allows an investigator to support council in discovering intent of crime in the main. It provides useful support in cases where evidence of an offence is not clear in commission, but may be clear in intent.

Telecommunications Act 1984 (Great Britain, 1984).

This was the forerunner of the Communications Act 2003 which provided for prosecution of improper use of telecommunications networks and services (Great Britain, 2003). It defined the extent of the communications network, and importantly included the use and ownership of devices intended to be used dishonestly in this regard.

Public Order Act 1986 (Great Britain, 1986).

Whilst mainly providing for issues such as riot and disorder, the Act is helpful in cases where harassment or creating intentional distress is under investigation. It also provides definition for provocation and fear of violence, useful in stalking cases and such like. There are also significant sections on racial hatred.

Protection of Children Act 1978 (Great Britain, 1978b).

Whilst an extensive act, the main support for council here is that of the area of child pornography. It is very helpful in providing clear guidance on what can be considered illegal.

Obscene Publications Act 1959 & 1964 (Great Britain, 1959; Great Britain, 1964).

This Act (1959) and Amendments (1964), provide very useful definitions of what can be considered illegal in this sphere. In many cases it can be difficult for an investigator to truly understand whether the production of images or data in a forensic recovery could be considered actually performing an illegal activity. The statements of clarification around intent help greatly.

Data Protection Act 1998 (Great Britain, 1998a).

Clearly the recovery of data that identifies a living individual falls within the boundaries of this legislation. It is important therefore for the investigator to understand the legal requirements of protection and transfer of that data.

Human Rights Act 1998 (Great Britain, 1998b).

Whilst much of this Act provides for the clarification and implementation of European conventions, it is important for the investigator to understand how any tribunal or review body may be tested as to how and why data was gathered on an individual.

Defamation Act 1952 & 1996 (Great Britain, 1952; Great Britain, 1996b).

These Acts are useful in helping an investigator understand if he is dealing with libel or slander. It also allows the investigator to consider if there is the possibility of innocent dissemination, that is the passing on of information without true intent to defame. Importantly the concept of privilege, that is acting under instructions or in the public interest could be used as defence.

Freedom of Information Act 2000 (Great Britain, 2000).

This Act can be very useful to an investigator looking for corroborative data to provide support for forensically recovered information. It also can be used to challenge, in defence or against expert witnesses in the public sector where more information is expected than has been provided.

Protection from Harassment Act 1997 (Great Britain, 1997).

This legislation is particularly useful in cases where stalking is suspected. It also provides legal cover for investigators who are themselves being threatened by actors under investigation.

This list was tested for relevance against similar lists complied by Jahankhani (2007), Taal (2007) and Mitchel (2007).

To summarise, the duty of a forensic examiner is to properly preserve, analyse and present any relevant data under his control. The need for standards to control that duty as well as rigorous review requirements within the profession, have been discussed. This Thesis has examined calls for certification, or the requirements for providing proof of expertise in the understanding of the underlying architectures of the systems and applications they will be required to critique. There is clearly strong argumentation for a requirement to be able to properly describe the functioning of any forensics tools they, the practitioner will use. There are also calls to provide knowledge into the understanding of how the tools they are using are working internally. This could be argued to overextend the abilities of the majority of practitioners and could be regarded as an unnecessary skill for anyone but a forensic tool designer or tester. Preservation and analysis support procedures are similarly suggested, supported by a call for training and certification in these areas.

A call to action, which has been a valuable driver for this research;

"Although the problems of computer forensics can be correlated with the field being in its infancy, it is time to take decisive actions. Computer forensics, as a field, has experienced events that should never be repeated (e.g., lack of standards and peer review). In order for the field of computer forensics to mature, there must be a national

system for certifying individuals who claim to be professionals. The continued lack of a professional certification, investigative standards, and peer reviewed method, may ultimately result in computer forensics being relegated to a "junk science," as opposed to a recognized scientific discipline" (Meyers et al, 2004, p. 11).

What is clear from this passage is that the potential for cases to go wrong on a more regular basis is high (Livio, 2010; *Yorkshire Post*, 2007; Ball, 2009; Carvey, 2007a). Whether or not the national versus international argument in terms of certification is the aim, is not a focus of this research. In either case, what we are to conclude from all these sources is that we would see less failures of proper process or plain tool misuse if there were an appropriate governance system (Jones, 2008).

7.3 Educational need

In the call for education in the field, amongst the stronger advocates that this research has found are Oja and Davidson;

" There is mounting pressure for institutes of higher education to fill society's need for qualified IT forensics practitioners. Some of the more suitable candidates for providing such education are those departments that already have a history of teaching the subject of IT security. Many of the technical issues that are of relevance to IT forensics are already covered in the normal IT security curriculum. However, IT forensics is clearly a broad subject that should span far more than relevant technical procedures and tools" (Oja and Davidson, 2008, p. 1).

Similarly, one UK university that has been prominent in the advancement of technical computer forensics research is the University of Glamorgan. Dr Andrew Blyth, principal lecturer, Glamorgan University Information Security and Computer Crime course, and reputedly a frequent expert witness (Warren, 2007), is quoted;

" We need to have some system in place that lets us differentiate between people who are trying to deceive people, and people who are experts in this field and might not have a relevant qualification" (Warren, 2007, p. 1).

Markedly, a suggestion by Blyth that there may be so called professionals out there that are deceiving people through their activities and manage to continue because of a lack of accreditation, oversight or indeed both. A compelling argument for the reason that the take up of the forensics profession and education being greatest in the UK and America is that the majority of available training is also only available in English. Clearly and perhaps significantly, most of the available literature in IT forensics is in the English language (Oja et al, 2008). It would be worthwhile to present the challenge that we should consider the fact that the majority of system and application software that will be reviewed and therefore understood by practitioners in the Western Hemisphere is also in the English language. Therefore, a lack of deep understanding of that language no matter which language data was being stored on the computer, could have negative outcomes for any investigation, given the potential complexities and mix of the recovered data. There are also further discussions emerging, based on the need for understanding of double-byte and reverse presentation (right to left, vertical) presentation languages, but these have been omitted from this Thesis for brevity (MSDN, 2011).

7.4 Association

Button (2005) in a presentation of the Counter Fraud Professional Accreditation Board argued that there are many inter-connected facets that must be available to ensure the integrity of the rounded delivery of an association, listing various higher, post-graduate and vocational courses, a code of ethics as well as a review board for membership. The association should be considered a “professional association”. In this case the argument is neatly presented, firstly for formal training both at an academic and professional level, secondly professionalization of the field and finally the certification against a set of peer criteria. Obviously, the requirement for on-going management of an association aligned to a set of peer ratified standards is also discussed.

In reviewing other professional associations journeys towards certification, oversight and peer review, it is worth understanding the International Information Systems Security Certification Consortium (ISC^2) evolution. Initially, the ISC^2 set out on a path

of providing an international standard for information security managers in the IT profession. This certification was the Certified Information Systems Security Professional (CISSP), and the description provided by ISC^2 is as follows;

"The CISSP was the first credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. CISSP certification is not only an objective measure of excellence, but a globally recognized standard of achievement" (ISC^2, 2009, p. 1).

This researcher sat for the CISSP examination in the Hong Kong University in 2002, successfully completing the examination. This fact alone provides some situational evidence of the extent of the reach of the consortium as well as the international availability of a relevant and independent certification in the field at that time. As the computer security profession matured, the ISC^2 found that one size did not fit all in the growing information security world, and released specialised certifications relevant to particular disciplines in IT security. Some argue that this was a profit driven change and as such challenge the independent value of the new certification (Clement, 2008; Simmons et al, 2007). These discussions around the independence of the certification body give a very strong direction towards the care that needs to be taken in organising certification and governance. This Thesis outlines repeatedly the need for training to be aligned to the certification process, and is clearly emphasised;

"*The relation between ISC^2 (the non-profit side) and their training arm is dubious at best. When a certification body becomes a training entity often time that entity will lose their focus on what is the most important which is the certification itself"* (Clement, 2008, p. 1).

Another non-profit organisation, aligned to professional needs is the American Society of Industrial Security (ASIS). For many years the only offering by ASIS was the Certified Protection Professional (CPP), first awarded in 1977 (ASIS, 2010). Later the certification regime was expanded to include Professional Certified Investigator (PCI), and Physical Security Professional (PSP) in 2002. This was described as being a result

of the ASIS membership and committees having understood that specialisation in the industry was creating differing certification needs from employers (ASIS, 2009). Both organisations ASIS and ISC^2 depend upon peer nomination of entrants, and also for submission of questions for the certification exam. Both have documented ethical standards by which the entrants have to agree to abide, but in neither society has this research uncovered any expulsion for failure to abide by those ethics. Contrarily, there are some heated discussions around the lack of such expulsions (Mortman, 2009). The important signal for this research is that there must be a continual review process of the relevance of the training, examination and association governance. This if any professional association is to remain useful and credible to the professionals it serves. The example of ISC^2 and ASIS adapting their certifications, and therefore underlying educational offerings both present proof that it can be done. This may be supporting the claims that both are seen to be leading associations, at least by board certified numbers, ASIS having over 8000 and the number of CISSP and other certifications claimed by ISC^2 to be over 71,000 (ASIS, 2010; ISC^2, 2010).

"…a series of five interviews with Swedish legal experts and computer forensic professionals were conducted from late 2006 and into 2007. Among the interviewees were both the Swedish law enforcement departments; the public prosecutors office and the police, and private Swedish IT-companies. Despite differences in the legal systems, the results from the literature study and the interviews did not differ significantly. One point where the results do nevertheless differ is whether criminology should be included; it is often a part of the literature but the interviewees did not regard it as important. Somewhat unexpected was the fact that the answers between the interviewees differed depending on whether they represented the public legal system or the IT industry. One question that clearly divided these groups was whether teaching ethical issues of the subject should be included or not" (Oja et al, 2008, p. 2).

We gather from this confirmation that a formalised training curriculum is once again seen to be a critical part of any professional approach to forensics. The private sector does not seem to see a need for the teaching of criminology, which would suggest a leaning towards technical failure investigations being more normal than events of

criminal intent, but that may be attributable to the way the passage can be read. Also what may be of interest is the division of the focus groups on the question of ethics. Unfortunately the data presented clearly states there was a definite split of opinion, but it is not made clear which side, private or public sector leaned which way (Oja et al, 2008).

7.5 Oversight

Potentially, one of the most credibility affecting differences between true professional societies and industry bodies that offer certified membership, is the membership oversight. Clearly in the execution of task, an investigator does have need for clear guidelines from which to approach the examination. Investigators in corporates, in general, rely upon the premise that the company owns, or at least has a right to monitor and manage, and therefore has unfettered access to all the data on its systems (Livio, 2010; Wesche, 2002; privacy.org, 1993). Investigators have been seen to act without any moral or ethical constraint in the pursuit of information gathering against a supposed miscreant (Livio 2010; Ball 2009; Rasch, 2006). In support of the challenge against private investigators not being held to the same exacting controls as the public sector, there are claims that not all investigative actions that are legal can be automatically assumed to be ethical (Grobler and Louwrens, 2006). It is clear that commercial, or private sector investigations can often be based on a "hunch", suspicion or sometimes mere curiosity. These investigations are therefore presented in stark contrast to a police (i.e. magistrates) search warrant, which in the UK for example specifies exactly the boundaries that any investigation must remain within. Such warrants would also provide the clear foundation of the reason for search or seizure (WTWU, 2009; ACPO, 2007; Meyers et al, 2004).

"There is a need to distinguish those bodies that accredit courses, training providers and qualifications against publicly accepted criteria from those that award individuals with accredited certificates or other forms of qualification that demonstrate a level of competence and/or knowledge. Accreditation is essential if there is to be universal acceptance of the quality of training and qualifications – although there are

qualifications that are universally accepted on the basis of the reputation of the controlling body (such as ISACA). Only with formal accreditation are qualifications likely to be seen as having worth. It can also ensure that standards, once achieved, are maintained. Equally, some qualifications will require robust CPD programmes to ensure those with the qualification maintain their competence over time " (Eurim, 2004, paper 5, p. 4).

The passage by Eurim give us clear commitment from the tone of the wording that the certification of professionals in whatever form absolutely must incorporate a review process. This to ensure that any certifications granted are maintained in some way for currency to the current environment. Similarly:

"Every form of crime that goes before a court has a computer involved in it in some way, so it is imperative that we find a way to sort this out," …"We need to arrive at a body of data that experts need to know, we need a body of practice that shows what experts have done in the past, a set of formal qualifications that people should have - and the co-operation of the courts to recognise all of that" (Warren, 2007, p. 1).

The preceding excerpt highlights a suggestion that the formal challenge against the lack of standardisation and certification in the computer forensics profession was brought about by the forensics professionals themselves. It is notable that they were trying to form a specialist side arm of the register of forensics professionals which was allied purely to the practice of computer forensics (Warren, 2007).

On the subject of the differences between certification and oversight in the public and private sector, Oja et al in 2008 brought out some interesting results. We are given the conclusions of extensive research on the value of academia in the building of the training and therefore progression of the profession. One of the outputs was that learning institutions that already had IT security focus in their curricula were better placed to extend that into data forensics (Oja et al, 2008). This Thesis concurs that a system of certification in modular form, to allow specialisation to occur, supported by continuous learning or feedback processes is key. The research outcomes of this Thesis also support the requirement that any body that manages the oversight must have the

ability and commitment to censure members for transgression against the obligatory code of conduct. A recent example of such censure can be found within the Certified Fraud Examiner realm (ACFE, 2010). It is reported in the September – October edition of the society magazine that a Utah resident member had been expelled from the society, by unanimous vote of the Board of Regents. The disciplinary measure was undertaken based on a proven violation of the ethical code, in this case Article II, which deals with honesty (*Fraud Magazine*, 2011). This ability and indeed performance of censure is where this research suggests that the credibility of the process will be most validated (Clement, 2008; Warren, 2007; Eurim, 2004).

The need for adequate and effective response to the terrorist threat is shifting the intelligence led forensics landscape at an alarming rate (STC, 2004). In parallel with the work of Juhnke (2002), this Thesis similarly makes no attempt towards alarmist claims that cyber terrorism is a current major threat. There is however mounting evidence of terrorist organisations using information technology to drive their cause (Anderson, 2008; Payson, 2003). There is certainly evidence on the international front that national entities are utilising their knowledge of technology to disrupt opposing powers stability. In 2010 it was widely reported in India that the Pakistani authorities had hacked a prominent Indian parliamentary members' website, and warned it was going to turn "*Indian Cyberspace into hell*" (Kumar, 2010). This *terrorist* development will inevitably lead to a challenge as to the restrictive nature of search warrants and powers of investigators. It is to be expected we will see calls for similar powers to be granted investigators such as those granted to police authorities in specialist investigations of national importance (Great Britain, 1981).

The differences in public and private sector governance are the most critical to be dealt with if information sharing is to take place in this important emerging sector of forensics. How much data an analyst can properly reveal that is found on a disk if it was not expected to be there, and thus not included in the warrant (public) or brief (private), is key. This disclosure argument has similar basis, it is suggested, to the argument around length of detention without trial (*Guardian*, 2008). Briefly the detention without trial discussion centres on cases where the argument for freedoms are being challenged

against the need for adequate time to properly investigate complex and internationally dispersed intelligence leads. This research has further highlighted some of the variances between the diverse codes of conduct around the international policing arena which strongly supports the balancing argument against strict and formalised governance, namely that there is no one safe and agreed course of control (ACPO, 2009; FBI, 2007). It is clear that the subject is as large as the information processing world is diverse. Ball (2004) maintains that law enforcement agencies work on a "good guy / bad guy" approach and that they see computer forensics as a secret society. Ball, in providing this outline argues that this makes any discussion around the relative values of various codes of conduct difficult. This difficulty further extends the gap between the private and public sector in achieving aligned certification and oversight over what is clearly the same underlying professional role.

7.6 Verification

A critical part of the data from this research has to be the continual calls to the need for accreditation and certification in the profession. If we look at the interesting court story of Gene Morrison, a self-professed psychologist expert witness, we can clearly see at least one perfect example of how the worst can be expected without oversight. The defendant held paper degree certificates for a BSc in Forensic Science, a Masters with excellence in Forensic Investigation and a Doctorate in Criminology. These were all purchased from a website called affordabledegrees.com. Customers could even choose their own transcript grades on this site (McVeigh, 2007).

The qualifications were supposedly awarded by the Rochville University in the US - which does not exist as a traditional brick built institute of learning, merely a web presence in cyberspace (McVeigh, 2007). Morrison claimed to have learned his skills from a retired West Yorkshire detective called John Pearson and Mr X, a member of the Czech Republic Ministry of Defence he met by chance on a visit to Prague (Carvey, 2007a; Warren 2007; *Yorkshire Post*, 2007). Morrison told police officers he had begun an Open University (OU) degree in psychology (forensic). When he was cross examined he admitted merely contacting the OU for a brochure and recording some OU

television programmes from BBC2 in the 1970s. He is reported to have told the court that it looked easier than going to a real university (*Yorkshire Post*, 2007). Warren (2007) on the Morrison case summarises:

"Last month saw the downfall of Gene Morrison. A conman who masqueraded as a forensic scientist and gave evidence in more than 700 police cases, some of them involving rape and drink-driving, Morrison, 48, of Hyde, Tameside, was found guilty of 22 counts of perjury at Minshull Street Crown Court in Manchester and given a five-year jail sentence. His claims to be a forensic scientist were bogus, and the BSc and PhD qualifications he claimed were in fact bought from a university that existed only on the internet" (Warren, 2007, p. 3).

Importantly this brings out the suggestion that this may be more widespread than just a one-off occurrence. Within the same article Neil Hare-Brown, managing director of QCC, a company that carries out forensic investigations for the police;

"There are a lot of people involved in computer forensics who have no qualifications at all, I would say that between 5% and 10% of the people working in this area are incompetent and that has led to problems with investigations. We have been given [computer] discs by the police that have been examined by people who have said that there is no evidence on them and subsequently found considerable amounts of evidence" (Warren, 2007, p. 4).

Hare-Brown's comments are endorsed further in the article by Alan Phillips (Warren, 2007). Philips is the managing director of 7Safe, which according to its press release also carries out investigations for the police and certifies, to its own criteria, examiners with a course jointly run with Glamorgan University (*Yorkshire Post*, 2007). Hare-Brown is reported to have continued;

"Forensics is a fairly new profession but there are some people who have been working in the area for a long time and there are people who purport to be experts in the field who do not have qualifications" (Warren, 2007, p. 1).

Clearly then there is an expectation that there will be cases where the forensics outputs can be brought in to question. One such recent occurrence was in February 2010, in a case involving the HMRC:

"HM Revenue and Customs Barrister made very serious admissions this week in an excise duty appeal. In response to complaints made by the Barrister for the Appellant, HMRC's Barrister admitted that forensic computer evidence produced by David Lack of Pro-vent Computer Security could not be relied upon. He said that examination of the computers by a different computer expert had shown that items David Lack had claimed to be on the computers were in fact found not to be there" (Curley, 2010, p. 1).

It is worthwhile to remind at this point, this research is not intended to bring reform into the police or national intelligence services use of such tools. Neither is it the intention to fuel the debate and examination of ethical or political boundaries that are currently under discussion in that arena (Anderson, 2008; Payson, 2003; Juhnke, 2002). The lines of governance are often unclear between public and private sector, causing a common disparity of accountability between the activities of sworn officers and commercial investigators. These two bodies are in essence often performing the same tasks on connected cases under differing rule sets. The Morrison case underpins the need not purely for paper certification (section 1.11), but also for a supporting code of conduct and delivery vehicle of peer certification (Warren, 2007). This code and certification is necessary to ensure overarching ethics and morals are part of any commercial investigative delivery, if it is indeed to be trusted. Without punitive actions on transgressions, any professional body acting on the output of this research, arguably would be of little use without the controls to prevent similar conmen such as Morrison (*Yorkshire Post*, 2007) from undermining the reputation of the profession. The Chartered Management Institute (CMI) for example, as part of its by-laws, states;

*"Members should be aware that their membership may be placed in jeopardy if formal notification and evidence is received by the Institute implying a breach of any section of the Code. If any such complaint is received, it is subject to detailed investigation within the Institute's agreed disciplinary procedures" (*CMI, 2008, p. 3).

7.7 Register

As this Thesis moves forward to tabling a code of conduct or set of ethical standards, each of these important considerations start to take a place in the eventual governance model. What was not envisaged in the initial aims of this research, was a register of members, although it is probably implicit in any such certification of professionals, it was not a specified research goal.

"According to Alan Kershaw, chief executive of the Council for the Registration of Forensic Practitioners, it is early days but a start has been made. The case of Morrison very clearly demonstrates the need for a register. The problem that there has been in the past is that there has been no lead body in this area, but now we have defined the current competence and started to put people on the register. People applying to go on the list are assessed on their past casework by assessors who themselves have been assessed on their casework" (Warren, 2007, p. 4).

Kershaw further reported that the forensics council, even though it was not a private sector professional certification and governance body, had been having some success. He called the council a shining light for the forensics industry, presenting the industry a challenge to emulate, warning that there were some people unhappy with the level of exposure those challenges brought (Home Office, 2007). Kershaw used an interesting term saying that some people had responded to the challenge by "scurrying off into the darkness" (Warren, 2007, p4). The following extract also seems to agree that professional challenge is an acceptable manner by which to formulate standards of behaviour, using actual cases rather than theory alone.

"Conversely, when computer forensics evidence has been contested, it has provided the foundation for evaluating what, why, and how those issues should be considered when creating computer forensic standards and certifications for the U.S. federal and state court systems" (Meyers et al, 2004, p. 2).

The challenge therefore is how to design and drive an effective certification and governance body. Where does the greatest need stem from, and which arguments are the strongest to ensure its appropriate use and insertion into this emerging profession. The

preceding data seems to be suggesting that a history of contest against current practice and current outputs is a good starting point, perhaps using the argument that when something can be proven to have been wrongly performed, there is material argument to correct it. Meyers in a 2005 article as a part of a call for certification in the US system cites Computer Emergency Readiness Team (US-CERT) number of incidents per year growth as an argument for needing greater forensics capabilities, or at least more specialists (Meyers, 2005). Whilst the argument is strong, in providing the need for some consistent forensics review it offers little further support in attempting to have us understand why that rise would be attributable to incidents requiring forensic investigation. It could also conversely be argued that because more incidents are actually being seen, there is little need for the forensics in those cases as they are already in clear view. This is not the only logical conclusion, but without clarification, any similar argument could be attempted based purely on this data, so it has not been relied on as a differentiator for this research. It is nonetheless useful in its clarification of the obvious need at some levels for proper and consistent forensics investigations.

Warren (2007) reports that there is a strongly expressed view that the moves to create a system similar to the expert witness program of the General Medical Council are nothing short of a "shambles". Dr Andrew Blyth said;

"What we need is a professional body that registers people and checks their accreditation " (Warren, 2007, p. 1).

That registration and certification view is supported by Dr Andrew Jones, the then head of the Security Technology Research Group at British Telecom:

"At the moment I think the system for the registration of expert witnesses and the way that the courts use technological expert witnesses has to be defined" (Warren, 2007, p. 1).

Interestingly, Jones is also quoted as having related that there have been cases where the accused have themselves been the expert witnesses on the case (Warren, 2007). This situation is not one that has been explored in this research, but may become one of the discussion topics in the regulation of the professional body. At first sight there would

seem to be no issue in defending oneself if the necessary skills were present, but if the investigation turns to a criminal prosecution, then it is suggested that there may be some challenges in allowing this course of action. Jones further argues that the need to resolve this lack of registration and certification is growing, and that whilst most of the cases that have gone wrong were ones that involved expert witnesses from the medical profession, it is only a matter of time, before one involving computer forensics is uncovered.

7.8 Certification and oversight summary

In summary regarding certification and governance, this researcher supports the Eurim call to task the Skills Councils with the rationalization the "*jungle of qualifications currently confusing employers, observers and students"* (Eurim, 2004, paper 5, p. 5). In making such a demand and argument for such rationalisation, Eurim underpins the need for the work being undertaken by this researcher. More importantly the calls suggest the potential use of this research in providing some grounding for a professional governance regime in computer forensics.

Having previously explored the training required, this chapter has suggested how the professionals, once trained could be peer certified and censured as necessary to retain an integrity of delivery within the profession. By using parallel organisations that have faced and in some cases met such challenges, as well as exploring examples of good or bad practice to be taken into account when building such a framework for forensics investigators, there is now need to explore the governance around such a membership.

8 Conduct and Governance

What has remained central and obvious throughout this research is that any society that sets out upon a determined delivery path must have objectives and controls to govern that delivery. Without the ability for example, to censure or challenge members, any society quickly loses the values that it sets out to maintain. This chapter explores some of the underlying needs for that society structure and how it should be governed, populated and perhaps funded.

To summarize the arguments for a code of conduct and ethics being proposed, they would be as follows:

The ethical underpinnings of any profession are those of truth and consistency (Manunta, 1996; Simonsen, 1996; Kultgen, 1988). Each professional may have a slightly different nuance of the ethical boundaries across which they are unwilling to step. These boundaries can be founded on education, societal values or religion, but any professional in the agreement to be held to a set of values must be able to clearly articulate what those personal understandings are. That professional must also be able to demonstrate a consistent application of those principles in their working routines.

In considering how we would define truth, this research reviewed the consensus theory of truth and more importantly, the correspondence theory of truth (Kirkham, 1992; Russell, 1912). What was evident was that was the consensus theory of truth was not appropriate, given that using such a theory it would be assumed that the argument rather than the facts would have more bearing on the data. The correspondence theory suggests that for something to be regarded as true, the items under discussion must be proven to be related and in existence. For this research, the data must exist, must be reproducible and appear the same to any other observer.

This researcher believes, whilst taking into account the discussions around whether this arm of security is a profession or not that a professional code of conduct has to consider the fact that the ethical boundaries in different cultures may waiver against a defined norm (Manunta, 1996; Simonsen, 1996). So, even if the professional standards are in variance from territory to territory, perhaps they may shift based on local professional

ethics, but they should never conflict with other territories. We must also allow for the understanding that even ethics may be "situational" (Brennan and Johnson, 2004). The code of conduct for the data forensics profession absolutely must define appropriate process for reviewing and adapting as needed, the underlying guidance and rule set that the investigator must sign up to and work within.

In order that a proper accreditation scheme be made available, there should be adequate representation from the various fields of academia having an interest in the outcomes, as well as clear understanding of the varied cultural emphasis that will have to be included in the setting of procedure (Konza, 1998; Kultgen, 1988).

The consultation over private sector E-Crime skills issues, and in this case data forensics should identify those bodies relevant to the discussion and more importantly what they bring to the table. As a preliminary action the process should seek to build and populate a sample grid to illustrate the potential cross-referencing of those communities expected to develop and pay for relevant courses, materials and assessment routines (Eurim, 2004). The research suggests that the following extensive but not exhaustive list of interested parties might therefore include, as also suggested by various sources, but mainly the Digital Forensics Specialist Group (Forensic Science Regulator, 2008):

1: Public sector agencies that are currently providing roles in the area, such as skill councils, agencies such as the forensic regulator as well as the Digital Forensic Specialist Group itself.

2: Course and Qualifications developers, for example ISC^2, BCS, ASIS, Guidance Software, Access Data limited.

3: Current course providers; University of Glamorgan, University of East London, Royal Holloway College (London), Northumbria University, Open University and others.

If the interested parties above are then brought into the consultation process, what actually would this process be looking to ratify. Many experts in the field of computer

forensics have reservations about the introduction of a process of accreditation. What is argued is that the greatest issue is of the difficulty of the process itself (Jahankhani et al, 2008). There is common agreement that there should indeed be an accreditation and governance board set up, but what does not seem to be commonly agreed is who should actually lead it, and by suggestion govern. There have been variously calls for such a body to be led by universities, by government, by their peers or jointly by universities, government and businesses (Jahankhani et al, 2008).

8.1 Leadership

To be led by academia, the concern is that those who have worked in the field for many years without academic qualifications may find that in order to (continue) to be recognised as experts in the field and fully accredited they may have to achieve some formally recognised academic qualification. This would be in addition to their experience, which Jahankhani et al claim most are against. This is in fact exactly the route that this researcher is undertaking, not in this case purely for the purpose of eventual accreditation, but to hopefully become one of the bridges between the two (academic and private sector) communities. The outcomes of this research and discussions in the field suggest that accreditation will rely upon effort in both areas (study and practice). Further, educational qualifications allied with commercial or practical experience would possibly enable somewhat higher levels of accreditation than the entry level, but would not necessarily be the only way in which to achieve the same level of certification. It would be difficult for someone for example to properly analyse and perhaps challenge or support a forensics research paper if they had never written one, or similarly, discuss the file extensions on a Microsoft Windows File system if they had never seen one. Honorary certifications and grandfathering are therefore suggested not to be appropriate in such an accreditation scheme (Britannica, 2010; ISACA, 2010). It is to be understood of course that the initial membership of any scheme, i.e. the founding membership could not be certified in the first instance as no approved certified members would exist.

If the effort were to be government led, without set standards the situation will be no different from what we have at present (Jahankhani et al, 2008). Unfortunately by not providing any reference background for this conclusion it is difficult to analyse where the challenge is coming from. It is the experience of this researcher that the only area where there are indeed clear forensics standards are in the public police sector where practitioners of the forensics profession do tend to have common criteria and guidelines for execution (FBI, 2007; ACPO, 2007). It is important to clarify that this Thesis does not conclude a need for government intervention, as we have seen many cases where standards have run out of control once in the hands of government, in our UK case, of the cabinet office (Elliot, 2007). There is a strong suggestion that in the case of government intervention, it should also involve those already working in the profession to give it [Government] some direction. We are reminded that there is a certain amount of reticence to leave the issue purely to the profession, suggesting that this is where the fault lies currently, and therefore in need of change.

In concluding that the final and arguably most palatable option would be a joint partnership with government, universities and businesses, we are warned, however, that that a great deal of joint effort will be required (Jahankhani et al, 2008).

As a result of deeper study of the actual accreditation process used in other societies, an accreditation for organisations themselves, as well as the actual practitioners, may also need to be considered (ASIS, 2009; ISC^2, 2009; PCI Standards Council, 2006). Lim (2008) in arguing for a certification scheme for management consultants, suggests that purely by certifying, consultants would be recognised as being qualified, competent and credible, yet the certification scheme would not be designed to cover the technical and domain knowledge of the consultants. This certification would then seem to be geared towards a club membership, much like the Guilds critiqued by Adam Smith, rather than the *qualified and competent* claims (Kennedy, 2007). Without any examination or peer review, there can be no measure of quality or consistency of delivery. This potential failure of the scheme is an important input to the forensics accreditation argument.

Importantly, a very valuable rounding off statement, that in spirit absolutely must be captured in any proposed code output from this research:

"Membership of a chartered professional body implies that a duty of care is accepted by every one of its members in fulfilling their professional management responsibilities. The Institute's Code of Professional Conduct and Practice, which is binding on all members of the Institute, sets out the professional standards of conduct and competence, as well as the personal values, which members are expected to exemplify. It therefore encapsulates the 'essence' of a professional manager" (CMI, 2008, p. 2).

8.2 A Suggested code Of Conduct and Testing

This sectio outlines in a very basic fashion the simplistic type of code of conduct that could be used to begin dialogue within the private sector. The chapter explores a starting attempt to test joining such a scheme and the learning that can be used in building guidelines for a forensic code.

In the search for a similar problem solution, that is a profession needing to build and deliver a new certification scheme, the research came upon the newly designed British Computer Society (BCS) Chartered IT Professional (CITP) (BCS, 2009). There was a belief that following the process for this certification would give strong support and direction for the manner in which the forensics governance body could be designed. In addition, the BCS had advertised a desire to support the E-Crime initiatives of other bodies and was looking to set up a Forensics Specialist Group, for which the researcher believed to be able to both add value, as well as integrate this research into (BCS, 2008). The comprehensive registration process is designed to gather enough information about an applicant's work and career experience, as described by oneself and one's peers to enable the BCS membership board to be satisfied the entry criteria are met, again very useful considerations for similar appraisal processes. It had been some years since the researcher was in fact a member of the BCS, having let membership lapse on working abroad, so another interest was to understand how the society had modernised and adapted to the changing face of the commercial sector, and the internationalised nature of the modern computing environment. Clearly an important factor to be considered in developing any future code for IT professionals.

The application for CITP status was submitted with a full curriculum vitae and a covering letter explaining reasons for interest and current circumstances. These were that the researcher was changing employment so would submit peer references from the current, not new employment. This was a diversion from the stipulated requirements. A peer reference form was subsequently sent by the review panel to the referee submitted, and importantly for the research to learn from, with no mention to the candidate that this had happened. An important learning therefore was gained, as will later be included in the proposed governance model, in that any accreditation or certification regime should ensure communications are of the highest standard and constant.

Surprisingly, the researchers referee, rather than the accreditation administration reported progress, and only by this side communication could the actual commencement date of the review process could be ascertained. The communication from the society was erratic, and finally after some weeks the process highlighted that the experience described by the referee was now out of date and there was a break in the employment under review. The whole application was therefore halted. What were the important overall leanings for the Thesis from this exercise?

Firstly, the evaluation criteria for the peer reviews were very clear. The referee was properly supported with examples of response and levelling for the submission. Actual examples were provided in the submission notes to ensure no confusion.

Secondly, the admission process to the grade was clearly defined and the supporting application forms were properly marked up and readily available. There were solid experience requirements, properly stated goals of the review process and candidate expectations were clearly set.

Thirdly, the fees and overall admission criteria were well documented and met peer expectations of the experience levels to match such a grading.

Finally, and for this Thesis the most important learning, any scheme will be judged in some manner by the administrative excellence. In this case the rigidity of the rule set for submissions requires an exact match of the process designers' view of a submission, and seemingly any variance against that view causes an automatic refusal. The

communication of progress was slow and impersonal, and given that this was a voluntary code, one would have expected a more personal feel to the process, another important driver for any forensics accreditation process. The rule set that had been created for the administration of submissions would, by this experience seem to be inflexible and not adequately tested with exception cases, another input for the eventual data forensics accreditation process. By the actions of this process, the society has presented itself to this researcher as a society that does not seem to be flexible, responsive to change or exception. A truly important learning for the proposed forensics accreditation process is that it has to be a welcoming society, where membership brings alignment to like-minded peers in a governance model that is fair, exacting, but flexible to the varied membership circumstances. In reviewing the outputs of this research, in the drive towards submission it is especially pertinent to now add that in early 2012, the BCS approached the researcher at the exact mail address it had denied the application in 2009 and asked if the Chartered IT Professional (CITP) process was known and would there be interest in applying for certification.

In searching for other similar processes to understand if these basic failings were specific or common, the researcher embarked upon two avenues of certification with the Certified in Risk and Information Systems Control (CRISC) designation from the Information Systems Audit and Control Association (ISACA) (ISACA, 2010). Firstly, the researcher was a regular presenter at ISACA events and was well known in the International ISACA brotherhood. When the CRISC certification was released the researcher was one of the early certified members and went through the registration process without need for a certification examination by peers. What was required though was peer CRISC approval of my skills, experience and ethics to provide that *grandfathering* (Britannica, 2010). Given that any such certification developed as a follow-on to the work of this research would expect initial membership to be formed without examination, the number of candidates and level of peer control provided for the first tranche of CRISC professionals was closely followed for this research. The secondary review of the CRISC membership used the failings of the Chartered IT Professional (CITP) process as a test for improvement against the learning's already held. A direct report of the researcher was due to depart for Australia towards the end of

2010, who had expressed an interest in CRSIC certification. As the grandfathering program was coming to a close we agreed that the application could be made from Australia after migration, thus providing similar broken employment circumstances as the researcher had shown in the CITP application above. By agreeing to be the primary sponsor for the direct report, the researcher was able to monitor closely the application process. The process passed through the application, confirmation and reports from referees without hitch, and the candidate is now certified. Proof then that an organisation that understands the transient and international nature of employment can deal with migratory careers.

Finally, to be truly non-partisan, the researcher discussed with peers the most stubborn certification or membership process that had been embarked upon, in order to really understand what advice could be derived. Far outside the sphere of Forensics, or indeed computing came repeatedly the firearms certificate process. Whilst this may seem a strange area to come up, many security professionals do have military or agency backgrounds and therefore are likely to be familiar with firearms and use them at least recreationally. A candidate in the researchers office was identified as wanting to be so certified and the forms were duly downloaded and filled in (Cambridgeshire Police, 2012). All together the process was well documented, the online help for the forms process was very well done and the forms were regarded by the various peers involved in the review as appropriate and not over-burdensome. The responses initially to the application by the colleague were relatively prompt, and the referees sections were concise enough to offer character reviews in confidentiality. Overall the data capture was very good, and taken as valuable input to any membership and certification process that may follow this research. What was concerning was the follow-up or administration once the application was accepted. Approval is dependent upon two main areas, a confidence that the subject is appropriate to own a firearm, based on character statements and past records, and secure storage of any firearms. What should have been a simple process to check the correct installation of a firearms cupboard in a home became a prolonged three month confusion of administrative and personnel issues, caused by various factors, importantly with no one owner for resolution. Once again, this important learning has to remain at the forefront of the administration of any

society, code or register. The administration is what the member and users of the service actually see, and the perceived quality of the certification and value of membership will be based on that opinion.

8.3 Code

So, proposed here is a rudimentary outline code of conduct, drawing heavily on the structure of the British Institute of Management, now the Chartered Management Institute (CMI). The code of conduct supports all levels of the profession as well as deriving support for new and prospective entrants into the field (CMI, 2008). The research, in analysing the failures and successes of similar organisations has been interesting to see two main avenues of codes, be they named ethical codes, professional codes or codes of conduct. As previously discussed there are clearly two formats that seem to be prevalent. The first is the shorter succinct bullet style with appended interpretations (BCS, 2011; IISP, 2012; ASIS, 2010). The second somewhat lengthier and descriptive within the text itself (CIPR, 2012; CMI, 2011; ITI, 2012).

General peer opinion, and indeed strong opinion of forensics professionals is that most if not all will belong to at least one other IT professional body and repeating common, or worst case agreeing to perhaps conflicting codes would seem to have little added value. The code presented below therefore has attempted to simplify the items that would seem specific to the forensics profession, or those that would have a direct bearing on the credibility of an *expert* in this field. Discussion of why the item is included and how the validity could be reviewed using a larger audience is offered at each point. The Code of Conduct (CoC) is presented as a single item in appendix B.

A Code of Conduct

A Forensic Investigator will:

- Strive for factual representation and thoroughness of output at all times. Present any outputs without prejudice or personal opinion, unless opinion is requested, where I will plainly report as such.

Figure 50 CoC item 1

Discussion: It is important that the analyst present only the facts, as has been discussed, and once the facts are presented, then be prepared to offer an opinion if requested. The failures that have been highlighted in this Thesis, of incorrect, incomplete or pure fabricated data show that there is not only an educational need, but for the intended conduct of an analyst to show clear intent.

Review: The more data that is made available, whether confidentially or openly to a society intending to implement such a code would help understand the relative level of failure that is attributable to a lack of this commitment.

- Act only within their area of expertise. Where certified or accredited to that level this will accompany any report.

Figure 51 CoC item 2

Discussion: In an area such as forensics, there is clearly a need for expertise and arguably experience. This thesis has shown that failures in the process have been attributable to a lack of expertise, or the inability of a user of forensics services to understand the level of expertise of the expert provided.

Review: Clearly, the stronger the profession becomes, and the more the propensity towards certification and registration grows, the ability of the profession a s whole to “self-certify” will become evident.

- Maintain my education and experience to the best of my ability in the field.

Figure 52 CoC item 3

Discussion: As has been shown in this Thesis, the forensics profession is moving at a relatively fast pace relative to other professions. The growth in use of computers and the shifting Internet and social media landscape require that professionals are constantly re-educating to keep pace.

Review: If the process of certification, registration and membership does indeed proceed, then the educational levels of members will be better able to be tested as a group for relevance. The common experience of that membership body will provide the impetus for future education, as well as experience sharing across the sector.

- Act lawfully at all times and work within any agreed ethical boundaries for a particular investigation.

Figure 53 CoC item 4

Discussion: As mentioned many times in this Thesis, the legal challenges that analysts face are legion. Purely to have an analyst understand the various acts that may be relevant to the work in the UK alone, as we have shown is a major task. The law is not always the arbitrator of ethics, again as discussed, and what is important is that an analyst can hold up to conduct he deems ethical.

Review: To test the implantation and validity of such a clause it would be important to take a base understanding of where the operators in the field currently set their limits (law vs ethics) and see if it is possible to provide guidance to new entrants using that levelling.

- Provide wherever reasonable as much support as possible to the furtherance of others in the profession.
- Encourage any fellow practitioners not committing to such a code to consider doing so.

- Provide support for peer certification or accreditation based on common criteria.

Figure 54 CoC item 5,6,7

Discussion: The three clauses above have been left together for discussion as they relate to similar requirements of the profession, that of training and peer certification. The intent is not that this code becomes a manner in which to provide a society of self-admiration of experienced professionals. The intent of this work is to provide for clear and transparent standards of training, certification and behaviour that members and entrants can be held accountable to by the actors using their services.

Review: Clearly the success of such a scheme will be held against the potential for the profession to grow, not only in size but in reputation. Any society that provides proper training, clear growth paths and avenues for censure of members must surely mimic those that have gone before. The review of the appropriate level of this code therefore will be the stated intent of membership, once a society is found to desire to work with it and move forward, hopefully after publication of this Thesis.

This Code of Conduct has been shared with peer investigators, along with the request for feedback about national, or international memberships as well as the amount of detail that would be expected in such a code. The feedback was unanimous that the more detail that was provided the harder the code would be to translate, interpret and importantly confirm collusion with. In particular, as discussed the recent release of the updated code by CMI has caused some searching discussion amongst peers, given the expansion from earlier versions (CMI, 2011). The discussions have all centred around what the perceived added value has been given the growth in number of words used. There arguably has been little expansion of the subject areas of the code, nor any specific items that were not at least implied in the previous code, discussion therefore so far has been to have seen little added value, opinions are obviously divided. Similarly, in discussing the previous research surrounding certification and more importantly censure of forensics professionals, many were in conflict with the suggestions of Oja et al (2008) that inputs were generally split around tighter governance. Within the peer

group canvassed, this researcher found that agreement was unanimous in stating strong governance and censure would be needed.

In summary, this section set out to suggest the simplistic type of code of conduct that could be used to begin dialogue with actors in the private sector. We have explored other schemes and some of the challenges and positives found. Presented above therefore are the principles of such a code. As discussed, review amongst practicing forensics investigators around the globe provides for as simple a set of words as possible to ensure the code is simple to understand and interpret. It also has been unanimous in voice that repeating clauses from other affiliated memberships would add little value. Defining how that affiliation would proceed or be administered has not been the focus of this research.

8.4 Conclusions & Further Research

Hagan (1997) warned the researcher that care should be taken to avoid generalizing beyond the level of data that has actually been gathered.

Earlier the Thesis discussed the so called "Matthew effect" in being mindful of that path of clique worship. The areas that have been used for this research have been kept as varied as reasonably possible. Opinion and argument has been gathered from Academia, Government and importantly the wider commercial sector. Very pertinent advice, in this case an excerpt from Kerlinger (1973).

"The report should be so written that the reader himself can reach his own conclusions as to the adequacy of the research and the validity of the reported results and conclusions" (Kerlinger, 1973, p. 416).

The need for a code of conduct and a method of accreditation and censure against that code is clear. The research presented highlights the diversity of opinion around the actual delivery vehicle in the private sector. What is outstanding then is the consultation process by which the private sector can provide itself and the users of commercial

forensics services a degree of confidence in the quality and level of confidence that can be placed in a practitioner.

Saunders et al (2003) use the thoughts of Tranfield and Starkey (1998) to argue the need for research to underpin the progress of managerial practice, arguing that the process of research needs to engage with the theoretical and practical side of management practice in order that the profession can progress. The problems addressed by research should be culled from a mesh of both theory and practice, rather than a single view. This presents the hurdle of getting the correct level of rigour in the research process to balance between theoretical and practical needs. This has become a subject of much debate (Saunders et al, 2008), and that challenge has been used as a constant check and balance throughout the arguing in this Thesis.

It is the contention of this research therefore that the information security profession, and in particular the branch of data forensics is evolving to the point of needing controls outside of the organisation. This research has looked at other professions, as well as the experiences of some of the current forensics practitioners in the commercial sector as well as the private sector. As with any new profession, there have been errors, some of them very public, but also many purely internal to the organisations being served. The interface between the public and private sector, across which there is a reliance in many cases upon the integrity of data is not clear or indeed defined. Purely private sector investigations are, in many cases, being poorly served by well intentioned, but nonetheless dangerously under-trained and poorly equipped practitioners.

Data forensics is a growing profession, with a marketplace that is massively expanding not only in reaction to the proliferation of computers, but also the crimes being committed on them. Growth is being driven as well by industry standards such as PCI-DSS requiring forensic support. The problem of not defining how the qualitative measures will be agreed, nor how experts can work together or in opposition to each other will inevitably produce disagreement and erratic professional behaviours. The tool sets available and evolving skill gaps do little to challenge these quality and accountability failures. It is not surprising that we are producing "*Nintendo Forensics*" examiners, (Carvey, 2007a), or improperly named *professionals* or *experts* who have

little actual understanding of the various methodologies and procedures involved in producing the outputs.

To revisit the objectives we described at the outset of this Thesis:

- Ensure that the final output provides appropriate background to the subject of Computer Forensics;
- Analysis of related and non-related codes of conduct in similar professional evolutions;
- Review of current similar training / certifications (added during research);
- Provide that actual industry experience not just academic research is included.
- Test viability of code with peers.

We have certainly discussed in depth the background to the profession, and clarified both the proper and improper activities of actors in the field

Reviewing similar codes has helped us understand the values that such a code should instil, as well as experience of others in using those codes in practice

There has been extensive reporting of the training available in the trade and detailed discussion of how that is and perhaps should be structured and verified.

The Thesis is balanced between Industry and Academic input and review.

Finally, extensive discussion and review has been undertaken to ensure the code was both viable and useful.

The research for this Thesis, does indeed qualify the urgent need for accredited impartial training for professionals, a certification and accreditation scheme for actors, as well as certified tools. The quality and choice of tools argument was not a stated research area for this Thesis, but obviously plays an important part in the overall delivery of a solution. Research across other societies that had introduced similar controls also supports an argument that there cannot be consistency, integrity and more importantly trust within the data forensics community and its customers, without a code

of conduct to allow practitioners to affirm their commitment to sound and defendable forensics practice.

A formalised training and certification scheme, a managing body and peer review process will show that the computer forensics profession will indeed meet the requirements of a profession (Manunta, 1996; Simonsen, 1996; Kultgen, 1988).

It is expected that this work has given at least an overall understanding of the challenges the industry faces, as well as some insight into how this researcher and peers are arguing that the confidence in the profession and indeed its professionalism can be heightened. As part of the proposed consultation process, the Thesis includes a peer reviewed code of conduct statement to drive further discussion, and form a basis for evolution of the profession.

8.5 Summary and recommendations for further research

As with any research, there will always be trailing questions when the Thesis is published. A major concern that recurs through this Thesis is provided as a challenge for the future, how to govern the private sector forensics profession without regulating it to the extent that the public sector has faced. A secondary challenge, stemming from the sometimes parochial or nationalistic nature of the public sector, is should such governance be national, or indeed international if it is to provide for recognition between peers in an international delivery environment.

Necessarily this Thesis has glossed over some areas that really need to be closed before any substantive changes can be made in the evolution of the profession. There exists a real need to create a certification body for the various tool sets currently in use, but more importantly those that will come into the market in the future.

The research set out to identify what practitioner training and certification requirements might be to enable a broader confidence in the commercial sector, the inputs being that the *tykes* were giving the expert practitioners a bad name. The research has proven it to be glaringly so. There is a growing need for an increasing number of data forensics practitioners to support areas such as data loss prevention, Payment Card Industry

standards and Personal Data Protection breaches. The evolution of regulation both in the public sector and within areas such as the financial services arena have extended the number of resources beyond their delivery capability. This is probably the greatest difference between the public and private sector. Drivers in the public sector are quality and governance, whereas the usual priorities in the private sector are speed of delivery and least cost of resource.

So to summarise the discussions presented in this chapter, it was stated that central throughout this research was the clear requirement that any society that sets out upon a determined course must have objectives and controls to govern that course. Without the ability for example, to censure or challenge members, any society quickly loses its values that it sets out to maintain. It is hoped that by exploring some of the underlying needs for that society structure and how it should be governed, populated and perhaps funded, there has been sufficient argument to provide for a way forwards.

The research did not set out to highlight the massive chasm between the needs of the profession and the lack in any sizeable terms of a formal forensic education response in the academic offering. If the educational institutions do not react in a more consistent and coherent manner to this growing need for properly educated and trained professionals, the code suggested and any society that evolves can itself have little effect on the problem. It is notable that the only country seemingly producing properly trained forensics professionals at an acceptable rate is China (Hayes, 2012; Si, 2011; Krekel, 2009). Oft repeated is the suggestion that the skills they are being taught and certified to, are being put to uses that we would not agree to under our suggested code of ethics, namely intelligence gathering and disruption. The call therefore is to the educational masters of this country to formulate a resolution to this massive skills training gap in our profession in the UK.

Finally, the aim of this research was to understand the need or otherwise of the forensics community in the UK for a code of conduct and perhaps a certifying body. Whilst national organisations such as the British Computer Society and the Chartered Management Institute are held up as exemplary vehicles to do so, the research has led to the suggestion that an international body such as the Information Systems $(ISC)^2$

(International Information Systems Security Certification Consortium), or ASIS (the American Society of Industrial Security) may in fact be a better means to achieve such a goal. This is because it provides for a non-profit international recognition of its certifications, currently in the information security profession, to which this Thesis has shown, data forensics is a branch.

9 References

7Safe (2012) *Education*. Available at: http://www.7safe.com/training.htm (Accessed: 26 November 2012).

Abrahams, J. (2007) *To be or not to be Certified – That is the Question.* Available at: http://www.albaglobal.com/article1397.html (Accessed: 30 November 2012).

Access Data (2010) *Forensic Toolkit.* Available at: http://www.accessdata.com/forensictoolkit.html (Accessed: 5 June 2010).

ACFE (2010) *Membership and Certification*. Available at: http://www.acfe.com/membership/membership.asp (Accessed: 6 June 2010).

AMD (2010) *Explaining Cache*. Available at: http://www.amd.com/us-en/Processors/SellAMDProducts/0,,30_177_4458_4513%5E1413%5E2128,00.html (Accessed: 20 June 2010).

American Heritage Dictionary (2000) 4th edn. New York: Houghton Mifflin.

Anderson, K. (2008) *Hacktivism and Politically Motivated Computer Crime*. Available at: http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf (Accessed: 14 February 2010).

American Society of Industrial Security (ASIS) (2009) *Certification*. Available at: http://www.asisonline.org/certification/index.xml (Accessed: 12 September 2009).

American Society of Industrial Security (ASIS) (2010) *History of the CPP® Designation.* Available at: http://www.asisonline.org/certification/cpp/about/history.xml (Accessed: 15 May 2010).

Angelopoulou, O. (2007) *ID Theft: A Computer Forensics Investigation Framework.* Proceedings of 5th Australian Digital Forensics Conference, 3rd December, 2007 at Edith Cowan University, Perth, Western Australia. Available at: www.scissec.scis.ecu.edu.au/conference_proceedings/2007/forensics/07_Angelopoulou

%20-
%20ID%20Theft%20A%20Computer%20Forensics%20Investigation%20Framework.pdf (Accessed: 2 December 2009).

Arthur, K. and Ventur, H. (2004) 'An Investigation Into Computer Forensics Tool'- *ISSA 2004 Enabling Tomorrow Conference*, Gallagher Estate, Midrand, South Africa, 30 June - 1 July 2004. Available at: http://www.icsa.cs.up.ac.za/issa/2004/Proceedings/Full/060.pdf (Accessed: 12 September 2009).

Association of Chief Police Officers (ACPO) (2007) *Good Practice Guide for Computer Based Evidence (V3).* Available at: http://www.acpo.police.uk/asp/policies/data/gpg_computer_based_evidence_v3.pdf (Accessed: 12 September 2009).

Association of Chief Police Officers (ACPO) (2009) *Good Practice Guide for Computer Based Evidence (V4).* Available at: http://www.acpo.police.uk/asp/policies/Data/ACPO%20Guidelines%20v18.pdf, (Accessed: 12 September 2009).

Ball, C. (2004) *Cross-examination of the Computer Forensics Expert*. Available at: http://www.craigball.com/expertcross.pdf (Accessed: 12 September 2009).

Ball, C. (2009) *You've Got Mail...and We've Read It*. Available at: http://www.eddupdate.com/2009/06/youve-got-mailand-weve-read-it.html (Accessed: 15 May 2010).

Barbara, J. J. (2008) *Handbook of Digital and Multimedia Forensic Evidence.* Towata, NJ:, Humana Press.

Basset, R., Bass, L. and O'Brien, P. (2006) *Computer Forensics: An Essential Ingredient for Cyber Security*. Journal of Information Science and Technology, JIST 3(1) 2006: University of North Carolina.

Becker, H. (1986) Writing for Social Scientists: How to start and finish your Thesis, book or article. Chicago: University of Chicago press.

Berners-Lee, T. (2010) *Bio*. Available at: http://www.w3.org/People/Berners-Lee/ (Accessed: 15 May 2010).

Berrong, S. (2009), *Data Remains on Discarded Drives*, Security Management, September 2009, p. 44, American Society of Industrial Society, USA.

Bhat, V., Parashar, M., Khandekar, M., Kandasamy, N.and Klasky, S., (2007) 'A Self managing Wide-Area Data Streaming Service', *Cluster Computing* - Volume 10, Number 4 / December, 2007 [Online]. Available at: http://nsfcac.rutgers.edu/TASSL/Papers/accord-mbc-grid-06.pdf (Accessed: 20 May 2010).

Boren, P. and Gates, J. (1994) *Shoars vs Epson*. Available at: http://fac-staff.seattleu.edu/mchon/web/Cases/shoars.html (Accessed: 15 May 2010).

Brand, M, Valli, C. and Woodward, A. (2010) 'Malware Forensics: Discovery of the Intent of Deception.' Originally published in the Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University: Perth Western Australia,November 30th 2010 Available at: http://ro.ecu.edu.au/adf/75 (Accessed: 26 November 2012)

Brennan, L. and Johnson, V. (2004), Social, Ethical and Policy Implications of Information Technology. Pennsylvania , USA: IGI Publishing.

Brenner, S. (2009) *Lack of Particularity in Email Search Warrant*. Available at: http://cyb3rcrim3.blogspot.com/2009/11/lack-of-particularity-in-email-search.html (Accessed: 15 May 2010).

Britannica, (2010) *Grandfather Clause*. Available at: http://www.britannica.com/EBchecked/topic/241594/grandfather-clause (Accessed: 15 May 2010).

British Computer Society (BCS) (2008), *BCS Cybercrime Forensics SG,* BCS SG, [Leaflet obtained at CFET], September 2008.

British Computer Society (BCS) (2009) *Chartered IT Professional (CITP).* Available at: http://www.bcs.org/server.php?show=nav.10972 (Accessed: 15 May 2010).

British Computer Society (BCS) (2011) *BCS Code of Conduct.* Available at: http://www.bcs.org/category/6030 (Accessed: 26 November 2011).

British Standards Institute (BSI) (2008) *BS 10008:2008 Legal admissibility and evidential weight of information stored electronically*. 08/30172972 DC

Button, M. (2005) *The CFPAB and Professionalism in Counter Fraud*, Available at: www.uki.net/php/files/icfspages.uki.net/resources/2005_markbutto.pdf (Accessed: 12 May 2009).

Byford, P. (1999) *Leo Computer Society*. Available at: http://www.leo-computers.org.uk/ (Accessed: 15 May 2010).

Cambridgeshire Police (2012) *Creating a Safer Cambridgeshire.* Available at: http://www.cambs.police.uk/firearms/forms.asp (Accessed: 26 November 2012).

Carr, N. (2008) 'How many computers does the world need? Fewer than you think', *The Guardian*, 21 February 2008 [Online]. Available at: http://www.guardian.co.uk/technology/2008/feb/21/computing.supercomputers (Accessed: 15 May 2010).

Carvey, H. (2007a) 'Why Forensic Analysis Needs To Give Up Nintendo'. *Information Security Magazine*, November 2007 [Online]. Available at: http://www.infosecurity-magazine.com/comment/071130_carvey.htm (Accessed: 12 September 2009).

Carvey, H. (2007b) '*Why "Nintendo" Forensics Is A Thing Of The Past!*'. HTCIA Asia Pacific Training Conference, University of Hong Kong, Hong Kong, December 2007. Available at: http://2007.htcia.org.hk/presentations.htm (Accessed: 12 September 2009).

Cavanagh, E. (2008) *Twombly, the federal rules of civil procedure and the courts St. John's Law Review 2008*. Available at: http://www.britannica.com/bps/additionalcontent/18/32848747/twombly-the-federal-rules-of-civil-procedure-and-the-courts (Accessed: 8 May 2010).

Chadwick, D. Gan, D. and Frangiskatos, D. (2007) *Universities – Victims or Perpetrators of Cyber Crime*. Global ESecurity – Proceedings of the international conference April 2007, London: ICGeS07.

Chartered Management Institute (CMI) (2008) *Code of Professional Conduct and Practice*. Available at: www.managers.org.uk/doc_docs/Code_of_Professional_Conduct_and_Practice.pdf (Accessed: 12 September 2009).

Chartered Management Institute (CMI) (2011) *Code of Practice for Professional Managers,* CMI, [Leaflet to Members] Northamptonshire, UK.

Chisum, W.J. and Turvey, B. (2000) 'Evidence Dynamics: Locard's Exchange Principle & Crime Reconstruction'. *Journal of Behavioural Profiling*, January 2000, 1(1), Sitka, Alaska: Academy of Behavioural Profiling.

CIPR (2012) *Code of Conduct* Available at: http://www.cipr.co.uk/content/about-us/about-cipr/code-conduct (Accessed: 26 November 2012).

CISCO, (2011), *Obtaining Software*. Available at: http://www.cisco.com/en/US/docs/security/ips/6.0/configuration/guide/cli/cliObtSW.html (Accessed: 14 October 2011).

Clement, D. (2008) *What are five things that ISC2 needs to do in order to improve the credibility of the CISSP credential?*. Available at: http://www.linkedin.com/answers/technology/information-technology/information-security/TCH_ITS_ISC/358240-23753864 (Accessed: 15 May 2010).

Clements, J. (2006) 'Getting Going: Why Your 'Lizard Brain' Makes You a Bad Investor', *Pittsburgh Post Gazette,* 25 October 2006 [Online]. Available at: http://www.post-gazette.com/pg/06298/732845-28.stm (Accessed: 15 May 2010).

Cohen F. & Associates (2009) *COFEE and the State of Digital Forensics.* Available at: http://all.net/Analyst/2009-12b.pdf (Accessed: 25 November 2012).

Comte, A. (1877) *System of Positive Policy*. London: Longmans.

Cornwall, H. (1988) *The Hackers Handbook*. London: Edbury Press.

Crispin, L. and Gregory, J. (2009) Agile Testing – A practical guide for testers and agile teams. Canada: Addison-Wesley.

Curley, V. (2010) *Very Serious Admissions by HMRC Barrister*. Available at: http://www.internationalcomputerbrokers.com/news/newsstory.aspx?story=2289 (Accessed: 15- May 2010).

Darcy, J. (2002) *Filesystem Fragmentation*. Available at: http://pl.atyp.us/wordpress/?p=241 (Accessed: 20 May 2010).

Data Clinic Limited (DCL), (2009) *Computer Investigations, Electronic Evidence - ACPO Guidelines*. Available at: http://www.dataclinic.co.uk/computer-ACPO.htm, (Accessed: 2 January 2010).

Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993). *Supreme Court*. Available at: http://www.lectlaw.com/files/exp06.htm (Accessed: 2 January 2010).

DECUS (1992) Proceedings: DECUS Europe Symposium. Available at: http://www.gbv.de/dms/tib-ub-hannover/181416336.pdf (Accessed: 26 November 2012).

Digital Forensic Research Workshop (DFRW), (2001) *DFRW*. Available at: http://www.dfrws.org/ (Accessed: 24 April 2010).

Dillon, T. (2006) Interdisciplinary collaboration , Academia, research, industry and policy relations in the development of Wireless Sensing Networks in the US . Available at: http://www.futurelab.org.uk/resources/documents/external_publications/WSN_Paper.pdf (Accessed: 8 May 2010).

Department of Defense (DoD) (2006) *National Industrial Security Program Operating Manual (NISPOM*). Available at: https://www.dss.mil/GW/ShowBinary/DSS/isp/odaa/ (Accessed: 20 May 2010).

Doyle, A. C. (1893) *The Gloria Scott*. London : George Newnes.

Dun, J. (1978) *The Ageless Chinese A History*. New York: Charles Scribner and Sons.

Easterby-Smith, M., Thorpe, R. and Lowe, A. (2002) *Management Research: An introduction* 2nd edn. London: Sage.

EC-Council (2012) *Certification.* Available at: https://cert.eccouncil.org/ (Accessed: 25 November 2012).

Elliot, F. (2007) 'Red-Tape Warning: May Contain Nonsense', *The Independent,* 7 January 2007 [Online]. Available at: http://www.independent.co.uk/news/uk/politics/redtape-warning-may-contain-nonsense-431123.html (Accessed: 15 May 2010).

EMVCO (2009) *About EMV*. Available at: http://www.emvco.com/ (Accessed: 5 June 2010).

ENCE (2010), *ENCE Application and Renewal.* Available at: http://www.guidancesoftware.com/EnCE-Application-Renewal.htm (Accessed: 5 June 2010).

Eurim (2002) *E-CRIME – A New Opportunity for Partnership.* Available at: http://www.eurim.org/briefings/BR34.htm (Accessed: 15 May 2010).

Eurim (2004) EURIM – IPPR E-Crime Study: Partnership Policing for the Information Society, Working Paper 5: Growing the Necessary Skills, Available at: www.eurim.org/briefings/ECS_WP5_web_031116 v04-10Nov03 5 (Accessed: 12 September 2009).

Evans, N. (2012) *Pay up Twits* Daily Mirror, 21 November 2012, Available at: http://www.mirror.co.uk/news/uk-news/lord-mcalpine-to-donate-payments-from-twitter-1448001 (Accessed: 27 November 2012).

Farrow, R. (2000) *Source Address Spoofing* Available at: http://technet.microsoft.com/en-us/library/cc723706.aspx, (Accessed: 26 November 2012).

Fay, J. (1993) *Encyclopaedia of Security Management*. Massachusetts: Butterworth-Heinemann.

Federal Bureau of Investigation (FBI), (2007) *Handbook of Forensic Services, U.S. Department of Justice, FBI, 2007*. Available at: http://www.fbi.gov/hq/lab/handbook/forensics.pdf (Accessed: 2 January 2010).

Feenberg, D. (2011), Can Intelligence Agencies Read Overwritten Data? Available at: http://www.nber.org/sys-admin/overwritten-data-gutmann.html (Accessed: 15 November 2012).

Forensic Science Regulator, (2008) *Manual of regulation*. Available at: http://www.homeoffice.gov.uk/police/Manual_of_Regulation_22.9.08.pdf (Accessed: 13 September 2009).

Fraud Magazine, (2011) 'Disciplinary Action', Journal of the Association of Certified Fraud Examiners, 26(5), p. 68. ACFE, USA.

Galil, Z. and Apostolico, A. (1997) *Pattern Matching Algorithms*, Oxford, Oxford University Press.

Gamer (2009), Directed by M Neveldine and Taylor B. [Film] California, USA: Lakeshore Entertainment.

Garden, S. (2010) *What is Non-Volatile Memory.* Available at: http://www.wisegeek.com/what-is-non-volatile-memory.htm (Accessed: 20 May 2010).

Gatlin, J. (1999) Bill Gates: The Path to the Future. USA: Avon.

Glamorgan, (2010) *Information Security Research Group*, Available at: http://security.research.glam.ac.uk/ (Accessed: 19 December 2010).

GIAC (2012) *Global Information Assurance Certification.* Available at: http://www.giac.org/ (Accessed: 25 November 2012).

Goodwin, (2006) 'Industry and Financial Regulations Driving the Demand For Forensic IT Specialists', *Computer Weekly* 28 February 2006 [Online]. Available at: http://www.computerweekly.com/Articles/2006/02/28/214464/industry-and-financial-regulations-driving-the-demand-for-forensic-it.htm (Accessed: 15 May 2010).

Grassrootsdesign, (2009) *Basic computer operations.* Available at: http://www.grassrootsdesign.com/intro/input.php (Accessed: 15 May 2010).

Great Britain (1297) *Magna Carta* [Online]. Available at: http://www.opsi.gov.uk/RevisedStatutes/Acts/aep/1297/caep_12970009_enm_1 (Accessed: 20 May 2010).

Great Britain (1952) *Defamation Act 1952* [Online]. Available at: http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1952/cukpga_19520066_en_1 (Accessed: 20 May 2010).

Great Britain (1959) *Obscene Publications Act 1959* [Online]. Available at: http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1128038 (Accessed: 20 May 2010).

Great Britain (1964) *Obscene Publications Act 1964* [Online]. Available at: http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1964/cukpga_19640074_en_1 (Accessed: 20 May 2010).

Great Britain (1968) *Theft Act 1968* [Online]. Available at: http://www.statutelaw.gov.uk/content.aspx?ActiveTextDocId=1204238 (Accessed: 20 May 2010).

Great Britain (1978a) *Theft Act 1978 (c.31)* [Online]. Available at: http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1978/cukpga_19780031_en_1 (Accessed: 20 May 2010).

Great Britain (1978b) *Protection of Children Act 1978* [Online]. Available at: http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1978/cukpga_19780037_en_1 (Accessed: 20 May 2010).

Great Britain (1981) *Criminal Attempts Act 1981* [Online]. Available at: http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1981/cukpga_19810047_en_1 (Accessed: 20 May 2010).

Great Britain (1984) *Telecommunications Act 1984 (c. 12)* [Online]. Available at: http://www.statutelaw.gov.uk/content.aspx?&parentActiveTextDocId=2232318&ActiveTextDocId=2232391 (Accessed: 20 May 2010).

Great Britain (1986) *Public Order Act 1986* [Online]. Available at: http://www.opsi.gov.uk/acts/acts1986/pdf/ukpga_19860064_en.pdf (Accessed: 20 May 2010).

Great Britain (1990) *Computer Misuse Act 1990* [Online]. Available at: http://www.opsi.gov.uk/acts/acts1990/ukpga_19900018_en_1.htm (Accessed: 20 May 2010).

Great Britain (1996a) *Theft (Amendment) Act 1996* [Online]. Available at: http://www.opsi.gov.uk/acts/acts1996/ukpga_19960062_en_1 (Accessed: 20 May 2010).

Great Britain (1996b) *Defamation Act 1996* [Online]. Available at: http://www.opsi.gov.uk/acts/acts1996/ukpga_19960031_en_4 (Accessed: 20 May 2010).

Great Britain (1997) *Protection from Harassment Act 1997* [Online]. Available at: http://www.opsi.gov.uk/acts/acts1997/ukpga_19970040_en_1 (Accessed: 20 May 2010).

Great Britain (1998a) *Data Protection Act 1998* [Online]. Available at: http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1 (Accessed: 20 May 2010).

Great Britain (1998b) *Human Rights Act 1998* [Online]. Available at: http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1 (Accessed: 20 May 2010).

Great Britain (2000) *Freedom Of Information Act 2000* [Online]. Available at: http://www.opsi.gov.uk/acts/acts2000/en/ukpgaen_20000036_en_1 (Accessed: 20 May 2010).

Great Britain (2001) *Private Security Industry Act 2001* [Online]. Available at: http://www.legislation.gov.uk/ukpga/2001/12/contents (Accessed: 14 November 2012).

Great Britain (2003) *Communications Act 2003* [Online]. Available at: http://www.legislation.gov.uk/ukpga/2003/21/contents (Accessed: 15 November 2012)

Grimes, P. (2009) 'Fearless New Year's Prediction: Computer Crime Gets Worse', *Infoworld Magazine*, January 2009 [Online]. Available at: http://www.infoworld.com/d/security-central/fearless-new-years-prediction-computer-crime-gets-worse-444 (Accessed: 15 May 2010).

Grobler, C. and Louwrens, P. (2006) 'Digital Forensics: A Multi Dimensional Discipline', ISSA 2006, *From Insight to Foresight* Conference 5 – 7 July 2006, Balalaika Hotel, Sandton, South Africa. Available at: icsa.cs.up.ac.za/issa/2006/Proceedings/Research/62_Paper.pdf (Accessed: 12 September 2009).

Guardian Newspaper (2008) '42-Day Detention: Home Office Rejects Major's Criticism', *The Guardian* 6 Jun 2008 [Online]. Available at:

www.guardian.co.uk/politics/2008/jun/06/terrorism.uksecurity (Accessed: 12 September 2009).

Guidance Software (2004) *Guidance Software Comments on the NIST Computer Security Incident Handling Guide*. Available at: www.encase.com/downloads/GSICommentsOnNISTIRGuidelines.pdf (Accessed: 12 September 2009).

Guidance (2010) *Encase Forensic*. Available at: http://www.guidancesoftware.com/computer-forensics-ediscovery-software-digital-evidence.htm (Accessed: 5 June 2010).

Guidance (2012) *Course Offerings.* Available at: http://www.guidancesoftware.com/computer-forensics-training-courses.htm, (Accessed: 26 November 2012).

Gutmann, P. (1996), *Secure Deletion of Data from Magnetic and Solid-State Memory.* Available at: http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/index.html (Accessed: 15 November 2012).

Hagan, F. (1997) *Research methods in criminal justice and criminology.* 4th edn. Massachusetts: Ally and Bacon.

Hamilton (2009) *Files Systems, Physical View (Disk Allocation Methods).* Available at: http://www2.cs.uregina.ca/~hamilton/courses/330/notes/allocate/allocate.html (Accessed: 20 May 2010).

Hayes, J. (2012) *Chinese Hacker Attacks On U.S. Targets And A Short History Of Chinese Hacking.* Available at: http://factsanddetails.com/china.php?itemid=1636&catid=7&subcatid=44 (Accessed: 30 November 2012).

Hayley, S. (2002*) What is Forensics.* New York: Cyber Security Institute.

HDForensics (2010) *Mobile Phone Forensics*. Available at: http://www.hdforensics.co.uk/mobile_phone_forensics.php (Accessed: 5 June 2010).

HM Revenue & Customs (2006) *Inspection of HMRC Handling of Human Intelligence Sources.* Available at: http://www.hmrc.gov.uk/about/hmic-report.pdf (Accessed: 10 July 2009)

Hof, R. (2006) 'Second Life's First Millionaire', *Bloomberg Business Week,* 26 November 2006 [Online]. Available at: http://www.businessweek.com/the_thread/techbeat/archives/2006/11/second_lifes_first_millionaire.html (Accessed: 20 May 2010).

Holloway University, (2010) *MSc in Information Security*, http://www.isg.rhul.ac.uk/msc (Accessed: 6 June 2010).

Home Office (2007) *Terms of Reference for the Forensic Science Advisory Council*. Available at: www.homeoffice.gov.uk/publications/police/790604/fsac-terms-of-reference (Accessed: 15 May 2010).

Howe, D. (1995) 'Hacker Ethic, *The Free On-line Dictionary of Computing*. Available at: http://dictionary.reference.com/browse/hacker ethic (accessed: 08 May 2010).

IBM, (2008) *IBM 301 Accounting Machine*. Available at: http://www-03.ibm.com/ibm/history/exhibits/attic2/attic2_122.html (Accessed: 15 May 2010).

IISP (2012) *The IISP Code of Ethics* Available at: http://www.iisp.org/imis15/imis15/iisp/Membership/How_to_Apply/IISP_Code_of_Ethics/iisp/Member/IISP_Code_of_Ethics.aspx (Accessed: 26 November 2012).

Infosec Institute (2102) *Computer Forensics Training.* Available at: http://www.infosecinstitute.com/courses/computer_forensics_training.html (Accessed: 26 November 2012).

Innamorato, D. , Krulewicz D. (2010) 'New Jersey High Court Limits Employer's Right To Review Employee Emails', *Employment Watch*, April 2004 [Online]. Available at: http://www.employmentlawwatch.com/2010/04/articles/employment-us/new-jersey-

high-court-limits-employers-right-to-review-employee-emails/ (Accessed: 15 May 2010).

International Intelligence Limited (IIL), (2009) *Investigation Case Study 2*. Available at: http://www.international-intelligence.co.uk/case-studies/ (Accessed: 10 January 2010).

ISAF (2010) *Convergence of Security Risks*. Available at: http://www.theisaf.org/documents/Security_Risk_Convergence.pdf (Accessed: 27April 2010).

ISACA, (2010), *CRISC Application Process*, Available at: www.isaca.org/Certification/CRISC-Certified-in.../CRISC-Brochure.pdf (Accessed: 5 December 2010).

ISC^2 (2009) *CISSP for Professionals*. Available at: http://www.isc2.org/uploadedFiles/Credentials_and_Certifcation/CISSP/CISSP_for%20 Professionals.pdf (Accessed: 15 May 2010).

ISC^2 (2010) *(ISC)2® Wins SC Magazine Award For Best Professional Certification Program*. Available at: http://www.isc2.org/PressReleaseDetails.aspx?id=6132 (Accessed: 15 May 2010).

IT Governance (2012) *Computer Digital Forensics Training Course*. Available at: http://www.itgovernance.co.uk/products/2519 (Accessed26 November 2012).

ITI (2012) *ITI Code of Professional Conduct for Individual Members*. Available at: http://www.iti.org.uk/attachments/article/154/Code%20of%20Conduct%20-%20individual.pdf (Accessed: 26 November 2012).

Jahankhani, H. (2007) *Global ESecurity – Proceedings of the international conference - Foreword*, ICGeS07, 3rd International Conference on Global E-Security, University of East London, London, April 2007.

Jahankhani H, Taal, A. and Mitchell I, (2008) *The importance of funding and training to manage and investigate computer crime ,* 3rd Annual International Conference on

Cybercrime Forensics Education and Training - CFET 2008, 1-2 September 2008, Canterbury, UK, [CD-ROM], Canterbury Christ Church University.

Jankowicz, A. (2000) *Business Research Projects*. 3rd edn. London: Thompson learning.

Jones, N. (2008) *IT Forensics – 22 years on*, 3rd Annual International Conference on Cybercrime Forensics Education and Training - CFET 2008, Canterbury Christ Church University, 1-2 September 2008, Canterbury, UK,[CD-ROM], Canterbury Christ Church University.

Juhnke, D. (2002) *Cyber Terrorism or Cyber Crime*?. Available at: http://www.forensics.com/pdf/Cyber.pdf (Accessed: 24 August 2009).

Kelman, A. (2009) 'Digital Disclosure in the UK from this autumn', *Finextra,* 24 June 2009 [Online]. Available at: http://www.finextra.com/community/fullblog.aspx?id=2982 (Accessed: 28 June 2009).

Kennedy, G. (2007) *Adam Smith's lost legacy*. Available at: http://adamsmithslostlegacy.blogspot.com/2007/11/did-elizabethan-guilds-promote-general.html (Accessed: 15 May 2010).

Kerlinger, F. (1973) *Foundations of Behavioural Research*. 2nd edn. New York: Holt Reinhardt and Winston.

Kirk, P. (1953) Crime investigation: physical evidence and the police laboratory. New York: Interscience Publishers Inc.

Kirkham, R. (1992) *Theories of Truth: A Critical Introduction*, Cambridge, MIT Press.

Kleiman, D. [ed] (2006), *Winternals Defragmentation, Recovery, And Administration Field Guide*, Rockland MA, Syngress, isbn: 1-597490-79-2

Knorr, E. (2009) 'What Cloud Computing Really Means', *Infoworld,* July 2011 [Online] . Available at: http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031?page=0,2 (Accessed: 25 July 2011).

Konza D. (1998) *Ethical Issues in Qualitative Research: What Would You Do*? Available at: http://www.aare.edu.au/98pap/kon98027.htm (Accessed: 5 May 2010).

Krekel, B. (2009) *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* The US-China Economic and Security Review Commission: Northrop Grunman, McLean, USA.

Kruse, W. and Heiser, J. (2004) *Computer Forensics Incident Response Essentials*. New York: Addison Wesley.

Kultgen, J. (1988) *Ethics and Professionalism*, USA: University of Pennsylvania Press.

Kumar, S. (2010), 'Liquor baron Mallaya latest victim of Indo-Pak cyber war', *DNA India*, 18 August 2010, p. 18.

Leyden, J. (2003) 'Caffrey Acquittal A Setback For Cybercrime Prosecutions', *The Register,* 17 October 2003 [Online]. Available at: http://www.theregister.co.uk/2003/10/17/caffrey_acquittal_a_setback (Accessed: 5 June 2009).

Legault, J. (2011), "Mobile Phone Forensics, the New Frontier", *Fraud Magazine*, Journal of the Association of Certified Fraud Examiners, 26(4), p. 6.

Lister, L. (2004) *Privacy & Workplace Investigations.* Available at: www.utm.utoronto.ca/difa/PDF/xxxResearch_Projects/Privacy%20&%20Workplace%20Investigations.pdf (Accessed: 12 September 2009).

Lim, D (2008) *New Certification Scheme for Management Consultants in Singapore*. Available at: http://imcusa.site-ym.com/resource/collection/ED794C9B-35AF-48F8-9A96-7A9389F8A40B/Meridian_ICMCI_Q1_2008.pdf (Accessed: 15 May 2010).

Linden Research, (2010) *Second Life FAQ*. Available at: http://secondlife.com/whatis/faq.php (Accessed: 20 May 2010).

Livio, (2010) *NJ Court Upholds Privacy of Personal Emails at Work*. Available at: http://www.nj.com/news/index.ssf/2010/03/nj_supreme_court_sets_new_ruli.html (Accessed: 15 May 2010).

Manunta, G. (1996) 'The Case Against: Security Management Is Not A Profession', *International Journal of Risk, Security and Crime Prevention*, Vol 1(3), pp. 233-240.

Marcella, A. and Menendez, D, (2008) Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. New York: Auerbach.

The Matrix (1999), Directed by Larry and Andy Wachowski, Village Roadshow Pictures, USA.

Matthew 13: 11-12, King James Edition of the Bible.

McCue, A. (2008) *Criminals Hack Chip And PIN Terminals*. Available at: http://www.silicon.com/management/cio-insights/2008/08/14/criminals-hack-chip-and-pin-terminals-39271413/ (Accessed: 5 June 2010).

McVeigh, K. (2007) 'The £250,000 'Psychologist' Who Fooled The Courts For 27 Years', *The Guardian*, Thursday 22 February 2007 [Online]. Available at: http://www.guardian.co.uk/uk/2007/feb/22/ukcrime.uknews4 (Accessed: 12 September 2009).

Mellor, C. (2009) 'Disk Platter Sizes Vary With Drive Speeds', *The Register,* 7 May 2009 [Online]. Available at: http://www.theregister.co.uk/2009/05/07/platter_size/ (Accessed: 20 May 2010).

Mendell, R. (1998) *Investigating Computer Crime*. Springfield, USA: Thomas.

Meyers, M. (2005) *Computer Forensics: Towards Creating a Certification Framework*. Centre for Education and Research in Information Assurance and Security, Illinois: Purdue University.

Meyers, M. and Rogers, M. (2004) 'Computer Forensics: The Need For Standardization and Certification'. *International Journal of Digital Evidence*, Fall 2004, V3(2). New York: Utica.

Microsoft, (2010) *Learning*. Available at: www.microsoft.com/learning (Accessed: 20 May 2010).

MISTI (2012) *CISO Summit Series*. Available at: www.mistieurope.com/ciso (Accessed: 24 November 2012).

Mitnick, K. (2003) *The Art of Deception*. New York: Wiley and Sons.

Moore, G. (1965) *Cramming More Components Onto Integrated Circuits*. Available at: ftp://download.intel.com/museum/Moores_Law/Articles_Press_Releases/Gordon_Moore_1965_Article.pdf (Accessed: 2 January 2010).

Mortman, D. (2007) 'Perspectives: Smoke And Mirrors Certifications', *Techtarget Magazine,* July 2007 [Online]. Available at: http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1264772,00.html (Accessed: 15 May 2010).

Mortman, D. (2009) 'How Serious Is (ISC)2 About Its Code Of Ethics?', *Techtarget Magazine,* September 2009 [Online]. Available at: http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1457012,00.html (Accessed: 15 May 2010).

MSAB (2010) *Micro Systemation*. Available at: http://www.msab.com/home/page.php (Accessed: 5 June 2010).

MSDN (2011) *Issues Specific To The Double-Byte Character Set (DBCS).* Available at: http://msdn.microsoft.com/en-us/library/aa242129(v=vs.60).aspx (Accessed: 13 October 2011).

Nanoscan Ltd. (2006) *High Resolution Magnetic Force Microscope hr-MFM.* Available at: http://www.nanoscan.ch/pdf/MFM.pdf (Accessed: 15 November 2012).

Netfocus (2012) *Netfocus UK 2012.* Available at: http://netfocus.baptie.com/themes/hawaii/events/ViewEvent.aspx?evId=e62b464e-be5c-4add-b2f9-7f41ee958744&view=sessions (Accessed: 24 November 212).

Newman, N. (1998) *Source Code Secrecy and Microsoft's Copyright Monopoly*. Available at: http://www.netaction.org/monitor/mon34.html#secrets (Accessed: 5 June 2010).

O'Hara, C. (1994) *Fundamentals of Criminal Investigation*. 6th edn. Illinois: Thomas.

Oja, R. and Davidson, A. (2008) *A Swedish IT Forensics Course - Expert Opinions*. CFET 2008, proceedings of 2nd International Conference on Cybercrime Forensics Education & Training, Canterbury University, Canterbury, UK, [CD-ROM], Canterbury Christ Church University.

Oracle (2010) *Oracle University*. Available at: www.Oracle.com/university (Accessed: 20 May 2010).

OSDP (2012a) *Operating System Documentation Project, - Mac System Software*. Available at: http://www.operating-system.org/betriebssystem/_english/bs-macos.htm (Accessed: 25 November 2012).

OSDP (2012a) *Operating System Documentation Project, - Windows Family*. http://www.operating-system.org/betriebssystem/_english/bs-windows.htm (Accessed: 25 November 2012).

Overill, R. (2008) *Development of a Masters module in Computer Forensics and Cybercrime*, CFET 2008, proceedings of 2nd International Conference on Cybercrime Forensics Education & Training, Canterbury University, Canterbury, UK, [CD-ROM], Canterbury Christ Church University.

Palmer, G. (2001) *A Road map for Digital Forensics Research*. Available at: http://www.dfrws.org/2001/dfrws-rm-final.pdf (Accessed: 5 July 2009).

Parry, R. (2008) 'Jilted Japanese Woman Questioned By Police After 'Murdering' Her Virtual Husband', *The Times*, 23 October 2008 [Online]. Available at:

http://www.timesonline.co.uk/tol/news/world/asia/article5008156.ece (Accessed: 20 May 2010).

Payson (2003) *Examining the cyber capabilities of terrorist Islamic groups* Available at: http://www.paysontechnology.com/terrorist_cyber_capabilities/terrorist_cyber_capabilities.html (Accessed: 15 May 2010).

PCI-DSS, (2008) *Payment Card Industry Data Security Standard (DSS) v 1.2*. Available at: https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html (Accessed: 24 April 2010).

PCI Standards Council, (2006) *Become a Qualified Security Assessor (QSA)*. Available at: https://www.pcisecuritystandards.org/qsa_asv/become_qsa.shtml (Accessed: 15 May 2010).

PCMAG (1996) *Solid State memory*. Available at: http://www.pcmag.com/encyclopedia_term/0,2542,t=solid+state+memory&i=51728,00.asp (Accessed: 20 May 2010).

Perlustro, (2010) *IlookPi*. Available at: http://www.perlustro.com/ (Accessed: 6 June 2010).

Plato, (c350bc.) *The Republic*. Available at: http://www.filepedia.org/the-republic (Accessed: 15 May 2010).

Pollit, M. (1995) *Principles, Practices and Procedures: An Approach to Standards in Computer Forensics*, 2nd International Conference on Computer Evidence, Baltimore, Maryland, April 10-15 1995. Available at: www.digitalevidencepro.com/Resources/Principles.pdf (Accessed: 12 September 2009).

Prince, B. (2000) *Guidance Software's New Computer Forensic Software to Debut at Annual IACIS Conference; EnCase V2*. Available at: http://www.allbusiness.com/crime-law-enforcement-corrections/law-forensics/6415226-1.html (Accessed: 5 June 2010).

Prince, B. (2007) *Debate Breaks Out Over Breakable Forensics Software Charges; In a report set for Black Hat, iSEC outlines problems in software packages, while Guidance disputes the findings.*. Available at: http://www.allbusiness.com/crime-law-enforcement-corrections/law-forensics/13446106-1.html (Accessed: 5 June 2010).

Privacy.org (1993) *Fact Sheet 7: Workplace Privacy and Employee Monitoring*. Available at: http://www.privacyrights.org/fs/fs7-work.htm (Accessed: 15 May 2010).

QA Training (2102) *Introduction to Computer Forensics.* Available at: http://www.qa.com/training-courses/technical-it-training/ia-and-cyber-security/ia-and-cyber-security/non-certificate-technical-skills/introduction-to-computer-forensics/ (Accessed: 26 November 2012).

Rasch, M. (2006) 'Employee privacy versus employer policy, US court rulings cast doubt on privacy policy', *The Register,* 3 November 2006 [Online]. Available at: http://www.theregister.co.uk/2006/11/03/workplace_digital_privacy/ (Accessed: 15 May 2010).

Raymond E. S. (2000) *A Brief History of Hackerdom.* Available at: http://www.catb.org/esr/writings/homesteading/hacker-history/ar01s02.html (Accessed: 26 November 2012).

Reith, M. Carr, C. and Gunsch, G. (2002) 'An Examination of Digital Forensic Models'. *International Journal of Digital Evidence*, Fall 2002 V1(3). Available at: www.ijde.org (Accessed: 21 March 2010).

Rifkin, G. and Harrer, G. (1988) The Ultimate Entrepreneur: The Story of Ken Olsen and Digital Equipment Corporation. Boston: Contemporary books.

Rosenberg, B. (2007) *A Push to Standards for Net Forensics*. Available at: http://www.pcworld.com/article/133327/a_push_to_standards_for_net_forensics.html (Accessed: 12 December 2009).

Rowlinson. R. (2007) *Towards a Strategy for E-Crime Prevention*. Global ESecurity – Proceedings of the international conference, London: April 2007 ICGeS07 pp. 77-81.

Russell, B. (1912) The Problems of Philosophy. Oxford: Oxford University Press.

Sapphire (2007) *Computer Forensics*. Available at: http://www.sapphire.net/downloads/ForensicsWhitePaper.pdf (Accessed: 20 June 2010).

Saunders, M., Lewis, P. and Thornhill, A. (2003) *Research Methods for Business Students*. 3rd edn. London: Prentice Hall.

Science and Technology Committee (2004) *Forensic Science on Trial*, Science and Technology Committee, Session 2004–05, Seventh Report [Online]. Available at: http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/9610.htm (Accessed: 20 June 2010).

Select Committee on Science and Technology (SCST) (2006) *Fifth Report* [Online]. Available at: http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16505.htm#a2 (Accessed: 1 July 2009).

Sennewald, C. (1981) *The Process of Investigation*. Newton: Butterworth-Heineman.

Sheldon, A. (2011) *All the Gear and No Idea: Scalable, Fast incident Response Using NOOBS*, [presentation] Netfocus, Bournemouth, UK, 5 October 2011.

Si, C. (2011) *The Threat of China's Patriotic Hacker Army.* Available at: http://www.theepochtimes.com/n2/opinion/the-threat-of-chinas-patriotic-hacker-army-60695.html (Accessed 30 November 2012).

Simmons, J., Harley, A. and Wright C. (2007) *Security Basics mailing list –archives - CISSP Question*. Available at: http://seclists.org/basics/2007/May/323 (Accessed: 15 May 2010).

Simonsen, E. (1996) 'The Case for: Security Management is a Profession', *International Journal Of Risk, Security And Crime Prevention*, Vol 1(3). pp. 229-232.

Sommer P. (2011) *Certification, registration and assessment of digital forensic experts: The UK experience.* Available at: eprints.lse.ac.uk/37662/ (Accessed: 26 November 2012).

Sommer, P. (2012) *The Importance of the Forensic Readiness Program.* [presentation] IT Security Forum, Merchants Hall, London, 31 October 2012.

Spadanuta, L. (2010), "Judging the Evidence", Security Management, August 2010, American Society for Industrial Security, USA.

Spitzner, L. (2003) *Definitions and Value of Honeypots* Available at: http://www.tracking-hackers.com/papers/honeypots.html (Accessed: 26 November 2012)

Stanage, N. (2007) 'From Second Life To Second-Degree Murder', *The Guardian,* 16 January 2007 [Online]. Available at: http://www.guardian.co.uk/commentisfree/2007/jan/16/fromsecondlifetoseconddegr (Accessed: 20 May 2010).

Standler, R. (1999) *Computer crime.* Available at: http://www.rbs2.com/ccrime.htm (Accessed: 15 February 2010).

Stanley, P. (1991) *Proceedings of the IFIP TC11 Seventh Conference on Information Security*, editors Lindsay, D. Price. W, The Netherlands: Elsevier.

Taal, A. (2007), *Report Examining The Weaknesses In The Fight Against Cyber-Crime From Within.* Global ESecurity – Proceedings of the international conference, London: April 2007 ICGeS07 pp. 62-81.

Thomas, P. and Peterson C. (2008) *An Investigation Into The Vulnerabilities Of Computer Forensic Processes As Shown Through An Anti Forensics Tool.* CFET 2008, proceedings of 2nd International Conference on Cybercrime Forensics Education & Training, Canterbury University, Canterbury, UK, [CD-ROM], Canterbury Christ Church University.

Thompson, J. (2010) *How to Create your Own Free Computer Forensics Kit on a USB Drive.* Available at: http://www.techradar.com/news/computing/how-to-create-your-own-free-computer-forensics-kit-on-a-usb-drive-680396#articleContent (Accessed: 25 November 2012).

Tranfield, D. and Starkey, K. (1998) 'The Nature, Social Organization And Promotion Of Management Research: Towards Policy'. *British Journal of Management*, Bedford: Cranfield University Press, Chapter 9, pp. 341-53.

University of East London (UEL) (2010) *Entry Requirements*. Available at: www.uel.ac.uk/programmes (Accessed: 20 May 2010).

United States Court of Appeals (USCA) (2006) OSRecovery, Inc. v. ONE GROUPE INTERNATIONAL, INC., Court of Appeals, 2nd Circuit 2006. Available at: http://scholar.google.co.uk/scholar_case?case=3535127684482874501&hl=en&as_sdt=0,5&sciodt=0,5 (Accessed: 30 November 2012).

US-CERT (2008) *Computer Forensics.* Available at: http://www.us-cert.gov/reading_room/forensics.pdf (Accessed: 17 July 2011).

Veeravalli, V. (1987), *Detection of Digital Information from Erased Magnetic Discs* Available at: www.ifp.illinois.edu/~vvv/veeravalli_ms_thesis.pdf, (Accessed: 15 November 2012)

War Games (1983), Directed by J. Badham [Film]. Los Angeles: Metro Goldwyn Mayer (MGM).

Warren, P. (2007) 'The Evidence Mounts On the Need For Expert Witnesses', *The Guardian,* 8 March 2007 [Online]. Available at: http://www.guardian.co.uk/technology/2007/mar/08/epublic.guardianweeklytechnologysection, (Accessed: 1 July 2009).

Washington Post (2005) 'British Intelligence Warned of Iraq War', *The Washington Post,* 13 May 2005 [Online]. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2005/05/12/AR2005051201857.html, (Accessed: 15 October 2011).

Wells, J. T. (2000), *Ponzi vs. the Postal Inspection Service.* Available at: https://postalinspectors.uspis.gov/radDocs/consumer/Ponzi_vs_USPIS.html (Accessed: 6 November 2011).

Wesche, T. (2002) *Reading Your Every Keystroke: Protecting Employee E-mail Privacy*. Available at: http://192.138.214.75/highlights/stuorgs/jhtl/docs/pdf/TWESCHEV1N1N.pdf (Accessed: 15 May 2010).

Whitcomb, M.C. (2007) 'The Evolution of Digital Evidence in Forensic Science Laboratories' *The Police Chief*, vol 74-11. International Association of Chiefs of Police. Alexandria, USA.

WTWU (2009) 'UK Computer Forensics Expert Jim Bates Wins High Court Appeal Against a Police Search Warrant' *Spyblog.* Available at: http://p10.hostingprod.com/@spyblog.org.uk/blog/2009/05/uk-computer-forensics-expert-jim-bates-wins-high-court-appeal-against-a-police-s.html (Accessed: 15 May 2010).

Yorkshire Post (2007), '700 Court Cases Thrown Into Doubt By Fraudster', *The Yorkshire Post,* 22 February 2007 [Online]. Available at: http://www.yorkshirepost.co.uk/news/700-court-cases-thrown-into.2066400.jp (Accessed: 15 May 2010).

Appendix A

A code of Conduct for Forensic Investigators

by

James Ronald Gay MSc. CFE CISSP CPP MCMI

Professional Doctorate in Information Security

University of East London, School of Computing,
Information Technology and Engineering

2009

Supervised by Dr. David Preston BSc., MSc., Ph. D.

Peterborough, England

Paper Presented to:

IT Security Conference for the Next Generation

November 21-22, 2009

University of East London, London, UK

Submission for Category: Law and Security

Abstract:

The amount of electronic data that is held about individuals and their actions is staggering. Much of the data believed to have been deleted by that subject is recoverable. Forensics tools to enable the recovery are legion, and importantly, vary in consistency and reliability of result.

Visible or recovered, it can be fed into investigative tools which also vary immensely in reliability, consistency, quality and indeed price.

Conclusions and inferences drawn from the use of these tools can be morally, socially and commercially damaging for the individuals or entities being investigated.

A common ethical problem is managing the discovery of confidential data that is irrelevant to the case at hand. Often wrong inferences are drawn not purely because of the lack of experience of the investigator, but also because of the simplistic operation of the toolsets.

Whilst strong guidelines exist in the public sector for the proper handling, analysis and reporting of computer evidence, very little guidance exists in the private sector.

My research outlined in my presentation, will provide examples of challenges in extrapolation, operator understanding and tool use, argue a proposal for a code of conduct to ensure correct and repeatable process is followed, along with a suggested outline for the creation of the supervision of conformity to that code in the private sector.

Background

The advent of computers into the everyday world has brought with it many benefits. There is hardly a profession that has not gained either efficiency or precision from the use of computers. Early predictions as to the value of computers to the masses and the incursion of the ubiquitous personal computer into our homes are laughable as we look in retrospect. The founder of the greatest computer empire so far is reputed to have stated that "I think there is a world market for maybe five computers". The then second largest manufacturer of computers, Digital Equipment Corporation Chairman and CEO, Ken Olsen in 1977 stood up and announced "There is no reason anyone would want a computer in their home".

Knowing now what we do, that the majority of homes in the industrialized world not only has access to a computer, but is also almost certainly connected to the Internet, it is easy to see that these predictions were so badly formed. What is clear, however, is the growth of the use of computers has brought with it some unwanted side effects. It is a sad fact that almost every scientific advance brings with it both a positive and a negative side. Take the splitting of the atom, that absolute wonder of science brought us unlimited free power, but also brought us weapons of mass destruction that had been unimaginable before their harnessing of its power. Look at the combustion engine, a marvelous solution to the needs of transportation, but also a medium for transport of even better weapons. Finally, and I could draw upon legion examples, look at the wonders of flight, so efficacious in moving people and goods around the world, but also a new way to rain death upon populations.

To return to the subject of my studies, the computer, and more importantly it’s use and abuse. As the power of computers grew, from the earliest tabulators, arguably produced by IBM in 1924 - the Type IV, that for the first time could actually subtract values as well as add, to the intermediate LEO (Lyons Electronic Office) which is also arguably the first real multi-processing commercial system, to today’s cloud computing, where

the amount of processing power and storage is potentially unlimited, the benefits to the good and the bad were equally visible.

To understand the potential of a computer to offer itself to both good and bad, it is probably useful to understand the basic make-up of what we all take for granted. A computer is a collection of electronic parts that work together to store and process information in a predictable and repeatable fashion. The nerve centre of the operation is the central processing unit or CPU which provides calculations on information presented. It does this by manner of a series of decision gates, at its most rudimentary. The information or input and output is channelled to and from the CPU down a series of pathways known as IO busses. These busses can (in the simplest terms) direct the information to either storage medium, visual display, or network connection. The decisions as to where to send the information, and indeed what to do with it when presented at the various decision points is controlled by operating system software. This software is common across all similar hardware setups and is usually maintained by either a systems specialist in a larger enterprise, or by a system “user” in the case of most personal computers. The ability of the maintainer to modify the actual workings of this software is usually very limited. Given a computer, with an operating system, for the machine to do useful work, it is necessary to use an “application”. An application can be something like an office suite, which provides for word processing, spread sheets, presentations and the like. An application can also be more specific and singular in purpose, such as an Internet banking system, or a payroll calculation engine. These applications are more likely to be bespoke to the task, and therefore more specialized in their maintenance and usage. All of the activities above, because of the nature of computers, can be expected to make some changes to input, and therefore produce output. It is this output that is the basis of value of the machine, and the focus of most nefarious activity in the realm of computing.

As well as providing a background to computing, it is also worthwhile to provide a brief overview of the discipline of forensic science. Since man first walked the earth, he has

used the skills of analysis and reasoning allied to curiosity and experience to better understand the happenings in the world around him. We see representations of early cave men using animal tracks and droppings to understand if an animal was nearby and likely to attack for food. We are told of evidential deduction both fictitious and factual that lead to criminals being apprehended in the days long before formal police forces. We see all around us people using facts and experiences to piece together a picture of what has happened in a particular situation. The science of criminal forensics has long been a specialization in the police force. Forensic science now even has its own regulator in the UK, to ensure the conclusions that are drawn by its practitioners are as sound as possible. There are many methodologies in use to provide the science, but the one most pertinent here is the “Daubert test” (Daubert 1993). Daubert states that any theory used to provide an opinion in forensics must; be generally in use in the forensic community, that it has been peer reviewed and tested, and where specific, the predicted reliability and error rate is reported. There is also an important theory of crime scenes that will become evident as to its importance as we progress. The Locard principle, which argues that any person entering a crime scene will take something with them, as well as leaving something behind, and every contact leaves a trace. “Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value" (Locard in Chisum & Turvey 2000).

Forensics, the American Heritage Dictionary (2000) describes as, “the use of science and technology to investigate and establish facts in criminal and civil courts of law”. Hayley (2002) describes computer forensics as “… the analysis of information

contained within and created with computer systems and computing devices, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved. “ Taal (2007 p62) outlines some useful theories into the evolution: “Computer Forensics is a field that developed from the introduction of new technology which is readily accessible, affordable and heavily depended upon both in the home and businesses [sic].

Back in the days when the World Wide Web was in it’s infancy, and its creator was still working at CERN in Geneva, there were discussions being had around the need for training investigators properly. Stanley (1991 p427) calls for “ an educationally sound concept of incremental training in computer crime investigation, together with a suitable syllabus which has application on a national and international basis.” He argues that the international nature of computing even then made the application of national boundaries a farce in the investigation of computer crime. He then also sensibly calls for discussion what exactly makes up a computer crime, and calls for a proper and commonly accepted definition of computer crime. It is worth remembering that his is many years prior to most countries enacting computer crime legislation. Fay (1993 p154) also calls for a better definition of computer crime. He suggests that the lack of such a definition adds to the difficulty of prosecuting it. He suggests a start point would be “a computer is used in an act, or an act is committed against a computer to steal money, services, property or information for invasion of privacy, extortion and even committing a terrorist act.”. He also wisely suggests that when an investigation is being progressed, it helps to know who the criminals are.

The Crime Scene

In traditional terms, a crime scene is usually able to be physically segregated and cordoned off until the investigating office is happy that enough evidence has been gathered, or that there is no further use in segregating the area. We imagine things like

shootings, suicides, armed robberies and bombings as crime scenes, all well defined areas and bounded by assumed relevance to the criminal event. The crime scene that a computer forensic investigator is faced with is rarely so well defined. Usually an unexpected event will cause either a suspicion or claim that data may be available on a computer system to prove or disprove the particular event, or series of events. A first responder in a computer forensic investigation is generally the computer user or system operator of that system. To provide a parallel, it is not dissimilar to the victim of a violent crime being asked to cordon off their understanding of the crime scene in case evidence of the crime be available. This is the first area that I question in my research, if proper evidential procedures are expected to be followed, and indeed they must if proper investigative procedure can be depended upon, then evidential first responders absolutely must have proper and relevant training. This training would encompass the proper seizure of computer systems, relevant media gathering and evidential triage. I will discuss each of these concepts in turn.

Seizure: Any device that is used to capture data evidence must be certified as free from contamination. Just as in traditional crime forensics the scene of crime responder would use gloves and sterile receptacles to gather evidence so should any data devices or containers used in computer forensics also be sterile. In some cases, where electro-magnetic interference is a concern, such as in areas of high voltage or microwaves, then EMF shielded carriers may need to be used. Properly trained and aware first responders would be fully au fait with the need in such cases.

Traditionally, when media was delivered from the factory, it was contained in anti-static bags, to ensure that any on-board electronics could not be contaminated by static or other electronic discharges, it is good practice to maintain this method of transport for ny media that could be affected by static or other discharge.

Media: In most forensic captures, there will be the potential to make either a search based extraction, for example from a large server farm, or in the case of a single or small system full disk capture. The media used should be certified (and there are legion

discussions as to what this would entail) clear and malware free. Whilst the research has not concentrated upon targeted malware, as this is a different subject area, it would be worthwhile looking at methodologies for future use to certify media as being as free of contamination as is reasonable to expect.

Triage: As we will see in the training and certification section, the aim of the first responder is to categorise evidential capture in the most effective manner. This can be in the form of urgency for example where data is likely to change or be overwritten, or in some cases where the devices are in a state of decay. It also should classify any reasoning for using search techniques to selectively extract relevant data in the cases described above.

The Evidence

All data gathered during an investigation has value of some kind. It is the duty of the investigator to provide reasonably argued conclusions as to the relevance of the data being presented. As I have outlined, data moves around the computer systems in different forms at different times, but usually will be at in a reproducible and recordable format when it is on a data storage medium of some type. Dependant upon the type of device, this may be a one time copy that the investigator is presented with, such as in the case of a volatile media such as solid state (memory) or even a snapshot stored to disk as in the case of network traffic. It is important to the investigative process that wherever possible, the original or primary copy not e used for any analysis, but a copy is used. This has two benefits, if the investigation has to be restarted, to follow a different path, then the slate can be wiped, but also in cases where there is a defense, the defense investigation has exactly the same data to work from as the challenger. Evidential process is central to the challenges that my research is presenting. What constitutes due process has to be properly defined and agreed by interested parties before any evidence collection or triage is performed. It is generally accepted that any

data device prepared for investigative capture should be in the most reasonable state of acquiescence possible. Traditionally this has meant for disks or hard drives that the system in question was either idle, or indeed switched off. Systems that have power applied cannot be ever assumed to be truly acquiesced as error management routines as well as system cocks still continue to function either by means of batteries on board the machine, or by trickle power such as in a standby state that most televisions nowadays have. Public sector guidelines, as for example the ACPO guide or FBI guide [ref] have, in the past, instructed first responders to immediately kill all external power supplies and or disconnect hard drives from the system board to ensure no contamination be possible. As systems have moved to more intelligent disks, and indeed memory chip only devices that lose their contents when powered off, guidelines are having to be revisited. Overall, the advice now must be reformulated to provide triage at first entry, rather than all-off as in the past. Of course, triage takes time, and we all have seen the movie clips of hackers zapping disks in microwaves and degaussing pads being run up and down the front of systems (ref war games). This also brings in the second challenge that my research is presenting, the validity of evidence presented based on physical proof or testimony. In the perfect world, any evidence presented to a deciding authority, remember we are talking about guidance for the private sector here, would be safely stored in EMP protected containers, copied in a bit stream copy that can be replicated as many times as needed without recourse to the original, and Files or data entities presented would be in their readable state. The reality is that most systems in the current information era are “always-on”, in that the ability to shut them down, or indeed postpone their operation is very limited, so a first responder has to make an executive decision wither before the evidence is seen, or at first sight as to what data could be gathered to support the case under investigation. Having decided this, the training I will refer to in the training section will help that person in becoming singular minded in gathering what data is needed for that task, any ancillary data that may be relevant, and most importantly the circumstances of the capture. If you accept that many systems just cannot be acquiesced, perhaps because they reside in a different town, or in many cases,

continent, then the data gathering has to be very carefully bound with supporting data that can be used to frame that capture. To provide an analogy, the first responder, may, in the case of newer technologies, never be able to produce what is colloquially known as the smoking gun (reference), or indeed a body to prove the crime, but there may be enough circumstantial data in evidence to show a reasonable case that the crime was committed. It is this understanding that is critical for any further discussion on evidence, the problem of placing a person or a computer in a certain series of event with reasonable certainty. Again, to provide an analogy, with no witnesses to a car hit and run crime, the only evidence that will be available is that there is a body (the victim) , fragments caused by the collision, that will point to either a particular type of car, or if the car is found, a specific car, and a reasonable series of circumstantial arguments about the habits of the owner or regular driver of that car. Other circumstantial evidence can then be researched to narrow down the likelihood of improper conclusion. If evidential procedure, and triage moves further towards snapshots of live data which cannot be reasonably reproduced, then any investigation that depends upon the skills of the data gatherer to properly capture and store relevant facts is deeply reliant upon the qualities not only of that gatherer, but the training and expertise he brings to bear at that crucial point.

The Laboratory

Evidential contamination is the single most worrisome trend in computer forensics. Because of the simplistic nature of the various tool sets and the lack of certification or accreditation of their use, any private sector investigator providing evidence to any degree must be challenged as to the sterility of the evidence work bench. Data devices as described before, can be re used multiple times to provide work areas for the investigation. Data that has previously resided on these devices can “bleed” into an investigation, and as such contaminate the evidence. It is goods evidential procedure to reset the data media contents to a predicted pattern (usually 1-0-1-0) to ensure this cannot happen. Good practice requires a peer confirm the clean before evidence is loaded for review.

Prior to using any tools, the expected outcome of a series of calibration tests should be applied to the tool set. This is usually a search on a known environment as well as an extract and recovery of known state data points. This provides a last check that the tools about to be used are still repeatable in effect. Any outputs of tools that cannot be verified by a secondary check should never be relied upon as sole means of evidence. Tool operators that do not have an understanding of, for example, the file system that the tool set is rebuilding or extracting from should not be allowed to provide evidence that has not been verified by properly experienced peers.

I introduced in the evidence section the concept of selective data gathering for first responders, that is the capture of data, that according to their or collective experience, would be relevant and useful to the investigator. It is critical that the investigator understand that process, and also that there is sufficient handover of intent between the gather and investigator, to ensure that methodology of thinking be understood. The disparity of data devices available to the investigator in the field to capture from and to mean that a proper thought process has to be applied both to the evidential trails. i.e. being able to show that the integrity evidence has not been compromised since capture, and also that reliability of device and credibility of capture are not brought into

question. Many researchers have quoted the “Nintendo” forensics methods, where analysis of forensic data is done with a common off the shelf toolset (COTS) and conclusions and inferences are drawn buy the output of the tool that are outside of the knowledge boundaries of the investigator. Whilst I do agree that an investigator should not rely solely on a tool to draw inferences or conclusions, I do challenge the naysayers to provide a better solution. Whatever underlying systems and mechanisms are used to provide support to the investigative process, the forensics community will always be on the edge of innovation, doing things with systems and data that were never in the initial specification. Take recovering deleted files for example in the Microsoft Windows environment, a simple file delete by a user merely shifts the file pointer to the wastebasket, something that we all have praised at least once in our journey with the delete key. To properly delete a file you need to use the shift delete function, which destroys the pointer from connection to a directory. Because file operations are expensive in terms of efficiency in computer operations, the actual data is just left where it is, not cleaned, this is the simplest clinical description of file operations on windows and leaves more questions than answers, but this paper is not about windows files systems, so sorry, go to Wikipedia if you need more. The fact that the data is still, at that point in an undisturbed state, we can also expect many artefacts that accompany the file to be also similarly undisturbed, so a nirvana for recovery. Again, to drag back into the annals of computing history, disks were small, so data areas would be overwritten relatively quickly, and as such programmers did not worry about swathes of data being left around to recover. As disks grew larger, the expectation of data being overwritten quickly dropped, and as the windows system is designed to grab the largest piece of unallocated disk space, smaller files, notionally the ones we look for as evidence, had very low probabilities that they would be overwritten. There is a side field of forensics that includes residual magnetic patterns of data enabling recovery in some cases after data areas have been overwritten up to five or more times, but this is very specialised and a distraction for this paper, nonetheless important in the knowledge bank of anyone attempting a recovery though. As systems followed Moores law [ref]

and multiplied in size, the rotational speeds of disks did not keep up and the disks became sever limitations of speed. Creatively, system programmers decided that to enable fast writing to disks, instead of continually asking for small chunks of data areas to fill, they would ask for one large area and just stream data down into it. Various algorithms were designed to optimise this against wasted space, which an investigator has to understand, but importantly, this created another nirvana of recovery known as file slack, where the data are was reserved by a program, data was written into that area until the program had finished then the file was closed. If the program hadn't filled the file, data from the previous use of that disk area was then captured in time until a program deleted that file and the cycle was restarted. Whilst this is a simplistic explanation, similar effects can be found in volatile memory, it is an important outline of the knowledge an evidence analyst or investigator needs to display when he is challenged to describe why a telephone number found in a seemingly non-connected file directory structure for example could in fact be contributory proof of a particular event, when in all probability all the tool set would state is that it found the number in slack, linked to a previous incarnation of a file that may have been in a relevant area to the investigation.

Presentation

Whatever the skill level of a forensic investigator, analyst or researcher, it is highly probable that their effort will have to be presented either to a peer community or a panel of deciding actors. The strength of their conclusions and the proper analysis and reasoning of their outputs will be a critical factor in the value of their work and indeed the positive conclusion of their intended goals. Most, but not all investigations are begun because there is a suspicion or evidence of a nefarious event that is having, or has had negative effects on the current state. Most investigations require many hours of painstaking analysis of data, long question sessions with peers around alternative

theories, and most importantly challenges both in the defensive sense as well as the credibility of methods used to provide a conclusion to some body or other. It is unfortunate then that there is not a common methodology or even a suggested format for presenting investigative outputs. That there is no industry standard to describe the investigative process in use, or indeed the methodologies used. My research has found that many supposedly watertight conclusions of relatively simple evidential analysis has been dismissed because of improper presentation of facts, less then professional drawing of conclusions, or simple misunderstanding of the investigative process. There is, in most areas of post graduate study, for example, a course requirement to undergo research and presentation or report writing modules before a student can be admitted, or indeed begin study. Why then, in an area that is so important to, in many cases, the lives of people it touches, absolutely no formal education for the presentation of forensic evidence in the private sector. The presentation skills module, will of course be best presented as an optional module, being given its own certification as not every investigator will either be comfortable or be required to present evidence. This area is the one piece of research that has strikingly different aims to that of the forensic regulator's work. For the public sector investigator, the presentation of findings is rarely one of persuasion, it is almost always a pure presentation of facts, which will be interpreted, in most cases by another expert, sometimes defence, but often prosecution. The private sector investigator is usually in a position where they are expected to produce a factual recount of the activities performed, and then provide an "expert" opinion as to the relevance of items found. The training for this then is by necessity diverse. Formal presentation of detailed facts and the ability to answer questions based purely on the facts and not embellish with any opinion is a difficult skill to teach, and my research suggests one that is not generally available in the sector. This then is an area that will require detailed analysis before I am able to confidently state that the methodologies and skills chosen to drive the training will have the desired outcomes. Secondly, being able to offer an analytical step though artefacts in an investigation, draws upon not only skills, but also underlying knowledge of the system in review. My

research shows that this is one area that, whilst critical to the proper execution of an investigative review the measurement and teaching of these skills can be best handled elsewhere for example through Microsoft system training, Oracle database administration training, ISC(2) security training etcetera.

Training

My research and indeed personal experience in the sector strongly supports my calls for formalised training for private sector first responders, investigators and eventually as introduced already, presenters. Companies that that have a natural desire to offer training such as Encase and FTK , do offer training that is tool based, but it is very focused on the particular vendors tools, and whilst it is probably the better option than nothing, can be very expensive and single minded. Underlying principles of evidence capture, gathering and proper evidential procedure are followed and taught, but in most cases the aim is to sell tools, not produce good quality output of students Indeed it is argued that a student could attend a commercial tool based training for a week, listen to nothing and still gain the completion certificate, which in most areas is the best challenge an employer may have as to the suitability of a person to perform evidential capture and examinations. Guidance software, the creators of Encase, which is the most pervasive tool set, do offer industry based certification (ENCE) but, being certified, I have to agree with the dissenters that without the Encase knowledge, and using that tool, certification would not be possible.

So, training is necessary, and it has to be modular to enable differing levels of expertise to be brought to bear at the correct point in the evidence process. My research concludes that there at least four main areas for training to be applied, and a confirmation of expertise be tested at each end of level.

The first, as we have discussed above, is that of first responder. This obviously requires an understanding of what data devices and systems may be relevant to an investigation, as well as the potential use that an examiner may make of them. Also as we have seen, it is critical that the responder be able to set the scene for an investigator, so snapshotting the environment of capture as well as any salient facts that may have relevance is key. A simple example, during an investigation a “grab squad” entered an area of interest and found many systems that had password locks. The user was either unwilling or unable to cooperate, so a long drawn out data capture process off all the data was started, in all

probability only to find that all the devices were encrypted with passwords. On switching on the TV, the channel names were actually the passwords to each device, the moral being that any device that is in a “grab area” may be relevant to the future resolution of the investigation. Being able to do on the spot analysis of the required capture is therefore also an important piece of the first responder training.

The second, and probably longer and more intensive training is that of evidence preparer. This is not, in most environments a task that would be the only work a person would do, but given its critically to the proper dénouement of an investigation, it is a specific skill set that should be trained and tested (and as we see later – certified). The training for this area would ensure that the person would be able to attest to the sterile work areas, proper evidential process for the recovery of the various data to a workable format, as well as the occasional integrity checks of the toolset as well as data devices to ensure proper response to integrity challenges of conclusions.

The third area is probably the most intensive and repetitive are of training, that of investigator, or investigative analyst. Entry into this training should not be allowed until a work experience level is attained to ensure that a proper grounding of computer system concepts is displayed. This obviously will differ as to the type of environment envisaged to be trained, but a minimum of two years experience as a windows system administrator for example would be a prerequisite for windows investigations training. Similarly email investigations would require similar levels of experience maintaining email systems. Specialisations in each area could be accumulated, and repeatable skills such as proper evidential procedure and data integrity would not be required to be repeated. Any student completing a course would certainly be taught to use the various tools in common use, but would be required to demonstrate a basic understanding of the basis upon which any tool draws a conclusion, such as the slack discussions above.

Finally, the reporting and presentation of evidence is the most often overlooked, and probably the most important area that calls for training. Because we are discussing private sector investigations here, and most cases do not actually end up in litigation, it

may seem overkill to provide training in the presentation and defending of evidence, but if a private sector case turns into litigation, the whole of the excellent work that has gone before could be destroyed by a lack of understanding of the judicial process. It is also my argument that whether or not a victim of a crime, or indeed a perpetrator is getting “their day in court”, it is the moral duty of the investigative team to process the evidence as though they were.

Certification and Oversight

Having introduced the Moral duty clause, it is timely to introduce certification and oversight as a requirement that is also being drawn out from my research. Just as there are areas that differ in the training needs, there should be separate certification in that area. Very quickly ISc2 (ref) realised that one size did not fit all in the information security world, and released specialised certifications relevant to particular disciplines in security, although some still argue that this was a profit based change, which is strange for a supposedly non-profit organisation. Similarly. ASIS after many years of only having the CPP designation, expanded their regime to PCI,PSP in turn, professional Certified investigator and Physical Security Professional (ASIS 2009), having understood that specialisation in the industry was creating differing certification needs from employers. Both organisations depend upon peer submission of entrants, and also of the examination questions for the certification exam. Both have ethical standards by which the entrants have to agree to abide, but in neither example has my research uncovered any expulsion for failure to abide by those ethics. My research suggests this is potentially the most credibility affecting difference between true professional societies and industry bodies that offer certified membership, the membership oversight. It is important that in the execution of task, and investigator does have clear guidelines from which to approach the examination. Investigators in corporates, in general, rely upon the premise that "the company owns all the data on its systems". Once this belief is held, investigators have been seen to act without any moral or ethical boundary in the pursuit of information gathering against a supposed miscreant. Grobler & Louwrens (2006) poignantly argue that not all investigative actions that are legal can be automatically assumed to be ethical. Commercial investigations often based on a "hunch", suspicion or sometimes plain curiosity, are arguably in direct contrast to a police (magistrates) search warrant, in the UK for example, which specifies exactly the boundaries that any investigation must remain within.

On the subject of the differences between certification and oversight in the public and private sector, some research done by Oja and Davidson in 2008 (Oja, Davidson 2008) brought out some interesting results. Their research drew the conclusion the that subject of inclusion of ethics into a forensics curriculum was opposite dependant on whether the interviewee sat in the public of private sector. Their further research on the value of academia in the building of the training and therefore progression of the profession was that learning institutions that already had IT security focus in their curricula were better placed to extend that into data forensics. My research therefore concludes that a system of certification in modular form, to allow specialisation to occur, supported by continuous learning or feedback processes is key. It also supports my claim that any body that manages the oversight must have the ability to censure members for transgression against the obligatory ode of conduct. This one requirement is where my research suggests that the credibility of the process will be most underpinned.

One critical part of my research output is the accreditation, if we look at the amazing court story of Gene Morrison, a self professed psychologist expert witness, we can clearly see at least one perfect example of how the worst can be expected without oversight. The defendant held paper degree certificates for a BSc in Forensic Science, a Masters with excellence in Forensic Investigation and a Doctorate in Criminology - all purchased from a website called affordabledegrees.com. Customers could even choose their own grades.

The qualifications were awarded by the Rochville University in the US - which does not exist, except in cyberspace.

He claimed to have learned his skills from a retired West Yorkshire detective called John Pearson and a mysterious Mr X, a member of the Czech Republic ministry of defense he met by chance on a visit to Prague.

Morrison told officers he had begun an Open University degree in forensic or social psychology. But in court he admitted really only phoning the OU for a brochure and tape recording OU TV programmes from BBC2 in the 1970s. It looked easier than going to a real university, he told the court.

So, if I were to summarize the code of conduct and ethics being proposed, it would be as follows:

The ethical underpinnings of any profession are those of truth and consistency. Each professional may have a slightly different nuance of the ethical boundaries across which they are unwilling to step. These boundaries can be founded on education, societal values or religion, but any professional in the signing against a set of values must be able to clearly articulate what those understandings are. That professional must also be able to demonstrate a consistent application of those principles in their working routines.

A code of conduct has to take into account the fact that the ethical boundaries in different cultures may waiver against a norm, but they should never conflict. The code of conduct for the profession absolutely must define proper process for reviewing and adapting as needed the proper guidance and rule set that the investigator must sign up to and work to.

In order that a proper accreditation scheme be made available, there should be adequate representation from the various fields of academia having an interest in the outcomes, as well as formal deference to the varied cultural emphasis that has to be included in the setting of procedure. In my research output I propose a detailed set of such procedures in line with some other codes of conduct from other internationally recognised professions.

The Conclusion

It is the contention of my research that the information security profession, and in particular the branch of data forensics is evolving to the point of needing controls outside of the organisation. My research as I have outlined above has looked at other professions, and the experiences of the current forensics practitioners in the field. As with any new craft, there have been errors, some of them public, but many internal to the organisations being served. The interface between the public and private sector, across which there is a reliance in many cases upon the integrity of data is not clear or indeed defined. Pure private sector investigations are, in many cases, being poorly served by well intentioned, but nonetheless dangerously under-trained and poorly equipped practitioners. In an evolving profession, with a marketplace that is growing exponentially owing to the proliferation of computers, as well as standards requiring forensic support, but not defining how the qualitative measures will be defined, it is obvious that the entrepreneurial system will produce respondents to the challenge. The tool sets available and evolving do little to challenge these evolutions, producing "Nintendo Forensics" (Carvey 2007) examiners, i.e. people who have little understanding or the machinations involved in producing the outputs..

I submit that my arguments, supported in greater depth by my full research paper do indeed qualify the need for training for professionals, a certification and accreditation scheme for actors, as well as indeed tools, which was not a primary goal of my research. My research across other societies that had introduced similar controls also supports my claim that there cannot be consistency, integrity and more importantly trust within the data forensics community and its customers, without a code of conduct to allow practitioners to affirm their commitment to sound and defendable forensics practice.

Obviously the amount of time here to present my research in detail is limited, but I hope that this brief overview has given you at least an overall understanding of the challenges the industry faces, as well as some insight into how I and my peers are arguing that the confidence in the profession and indeed its professionalism can be heightened. I invite

you to provide comment on my draft thesis which I will be happy to share under controlled conditions prior to my academic supporters final release agreement.

References

ASIS, 2009, http://www.asisonline.org/certification/index.xml

Carvey, H., (2007), Why "Nintendo" forensics is a thing of the past!", http://2007.htcia.org.hk/presentations.htm

Chisum, W.J., & Turvey, B. "Evidence Dynamics: Locard's Exchange Principle & Crime Reconstruction," Journal of Behavioral Profiling, January, 2000, Vol. 1, No. 1

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

Fay, J, (1993), "Encyclopedia of Security Management, Butterworth-Heinemann, Massachusetts

Grobler, CP, Louwrens P, (2006), Digital Forensics: A Multi Dimensional Discipline, icsa.cs.up.ac.za/issa/2006/Proceedings/Research/62_Paper.pdf

Guardian Newspapers, http://www.guardian.co.uk/uk/2007/feb/22/ukcrime.uknews4 (Accessed: 11 October 2009).

Hayley, S, (2002), What is Forensics, Cyber Security Institute

Stanley, P, (1991) in "Proceedings of the IFIP TC11 Seventh Conference on Information Security", eds Lindsay D, Price W, Elsevier The Netherlands

Taal, A. (2007), Report examining the weaknesses in the Fight against Cyber-Crime from Within – In ICGeS07, Global ESecurity – Proceedings of the international conference, London April 2007 p62-81

Appendix B

Code of Conduct

A Forensic Investigator will:

- Strive for factual representation and thoroughness of output at all times. Present any outputs without prejudice or personal opinion, unless opinion is requested, where I will plainly report as such.
- Act only within their area of expertise. Where certified or accredited to that level this will accompany any report.
- Maintain my education and experience to the best of my ability in the field.
- Act lawfully at all times and work within any agreed ethical boundaries for a particular investigation.
- Provide wherever reasonable as much support as possible to the furtherance of others in the profession.
- Encourage any fellow practitioners not committing to such a code to consider doing so.
- Provide support for peer certification or accreditation based on common criteria.