Digital Business Security Development:
Management Technologies

Don Kerr, *University of the Sunshine Coast, Australia*

John G. Gammack, *Griffith University, Australia*

Kay Bryant, *Griffith University, Australia*

BUSINESS SCIENCE Reference

BUSINESS SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content: Kristin Klinger
Director of Book Publications: Julia Mosemann
Acquisitions Editor: Lindsay Johnston
Development Editor: Julia Mosemann
Publishing Assistant: Travis Gundrum; Jamie Snavely
Typesetter: Keith Glazewski; Travis Gundrum
Production Editor: Jamie Snavely
Cover Design: Lisa Tosheff
Printed at: Lightning Source

Published in the United States of America by
Business Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Digital business security development : management technologies / Don Kerr, John G. Gammack, and Kay Bryant, editors.
p. cm.
Includes bibliographical references and index. Summary: “This book provides comprehensive coverage of issues associated with maintaining business protection in digital environments, containing base level knowledge for managers who are not specialists in the field as well as advanced undergraduate and postgraduate students undertaking research and further study”-- Provided by publisher. ISBN 978-1-60566-806-2 (hardcover) -- ISBN 978-1-60566-807-9 (ebook)
1. Electronic commerce--Security measures. 2. Business enterprises--Computer networks--Security measures. 3. Computer security. I. Kerr, Don, 1952- II. Gammack, John G. III. Bryant, Kay, 1954- IV. Title.

HF5548.32.D538 2010
658.4’78--dc22

2010024585

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 2
Digital Evidence

Richard Boddington
Murdoch University, Australia

ABSTRACT

Digital evidence, now more commonly relied upon in legal cases, requires an understanding of the processes used in its identification, preservation, analysis and validation. Business managers relying on digital evidence in the corporate environment need a greater understanding of its true nature and difficulties affecting its usefulness in criminal, civil and disciplinary proceedings. This chapter describes digital evidence collection and analysis, and the implications of common challenges diminishing its admissibility. It looks at determining the evidentiary weight of digital evidence that can be perplexing and confusing because of the complexity of the technical domain. Digital evidence present on computer networks is easily replaced, altered, destroyed or concealed and requires special protection to preserve its evidentiary integrity. Consequently, business managers seeking the truth of a matter can find it a vexing experience, unless provided with a clear appraisal and interpretation of the relevant evidence. Validating evidence, that is often complex and incomplete, requires expert analysis to determine its value in legal cases to provide timely guidance to business managers and their legal advisers. While soundly configured security systems and procedures enhance data protection and recovery, they are often limited in the way they preserve digital evidence. Unprepared personnel can also contaminate evidence unless procedural guidelines and training

DOI: 10.4018/978-1-60566-806-2.ch002

are provided. The chapter looks at the benefits for prudent organisations, who may wish to include cyber forensic strategies as part of their security risk contingency, planning to minimise loss or degradation of digital evidence which, if overlooked, may have adverse legal repercussions.

INTRODUCTION: THE INVESTIGATION DOMAIN

Chapter two introduced the digital evidence domain and this chapter expands on this by providing details of how to handle digital evidence in order to preserve its integrity in court.

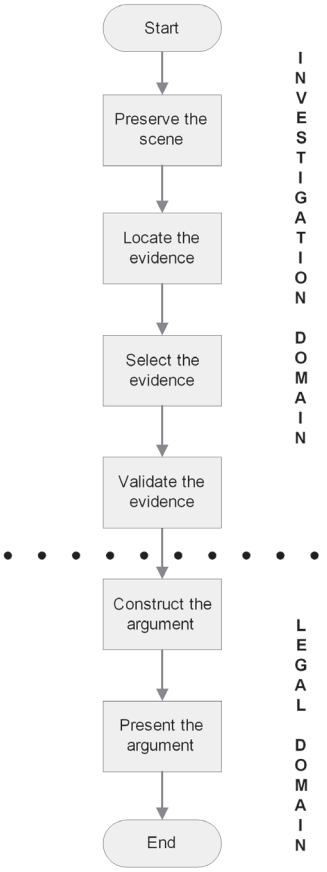
Forensic science adopts six stages in the investigation of forensic evidence that recognize, preserve the scene, classify, compare and individualize, and reconstruct the evidence (Crime Scene Investigation, 1994). Cyber forensics is still in its infancy and non-standardized processes are common in some civil and criminal investigation agencies, and standards, if they do exist, vary in different jurisdictions (Baryamureeba & Tushabe, 2006; Carrier & Spafford, 2003; Whitcomb, 2002). Courts expect computer forensic investigators and forensic auditors to have a sound understanding of computer technology for their testimony to have any credibility. This technical expertise is also important in civil actions and disciplinary proceedings, not intended to appear in court cases, to ensure that natural justice takes place (Mohay, 2003).

Several cyber forensic investigation models are in use emphasizing slightly different stages in the investigation process, and there is no universally agreed model used by investigators (Yasinsac, Erbacher, Marks, Pollitt, & Sommer, 2003). Figure 1 is a simple model highlighting the processing of digital evidence in the investigative and legal domains. The investigation domain consists of four stages taken by investigators in evidence preservation, location, selection and validation that precede the two stages in the legal domain involving legal practitioners constructing and then presenting legal arguments (Boddington, Hobbs, & Mann, 2008).

Preserving the Evidence

Preserving the evidence is the critical first stage in the investigative domain and may be overlooked by business managers, who fail to appreciate the fragility of digital evidence and take the correct steps to avoid contamination or loss of the evidence. Well-intentioned, but uninformed and improper handling and examination may fail to stabilize the evidence and may actually cause it to be altered, damaged, destroyed or contaminated (Ashcroft, 2001; Carrier, & Spafford, 2003). It is important to minimize overwriting digital evidence at the point of seizure and during the copying

Figure 1. Evidence processing stages in the investigative and legal domain. (Adapted from Boddington, Hobbs, & Mann, 2008).



process, as it must be preserved in a pristine state for the examination and analysis stages of an investigation (Carrier, 2005).

When tendering evidence during legal proceedings, proof is required about the exhibit to verify it is the same as the exhibit seized at the crime scene. For a record to be admissible in legal hearings, a history of its condition, that is, an unbroken record of its state from creation to the time of its presentation as evidence is a legal requirement (Stephenson, 2000; Tapper, 2004). This condition is commonly referred to as the chain of custody and any break in the history of the chain potentially degrades its admissibility, as well as its evidentiary value (Stephenson, 2000; Association of Chief Police Officers, 1999; Whitcomb, 2002). In the case of a computer crime, such exhibits would include a hard drive, a storage device or a forensic image of a hard drive containing digital evidence obtained from a computer or storage device.

If the chain of custody is broken, the court can deny admissibility if the break is serious or, if not, can admit the evidence and let the jury decide whether it affects the weight of the evidence during examination (Marcella & Greenfield, 2002).

The chain of custody must be maintained to show that the evidence was preserved in its original state, and was uncontaminated; otherwise, the evidence may become inadmissible if challenged by the opposing party (Casey, 2000). It is difficult, but not impossible to collect digital evidence without altering it and various processes and forensic tools are used. Otherwise, any rigorous examination of the digital evidence could pose a serious challenge to its admissibility and evidentiary weight as courts do expect assurance that the chain of custody is intact (Tapper, 2004). In submitting digital evidence, challenges must be expected from the court and opposing legal teams, who will insist on verification of key issues (Whitcomb, 2002). These include:

- Guarantees about the reliability of the history of the custody of the exhibit
- Reasonable proof that the record is in pristine condition
- Proof of who created the record
- How the record was created
- Confirmation of the record's genuineness, completeness and accuracy
- Confirmation that there been no breach of confidentiality.

In the same way as a traditional crime scene is preserved, so must the physical crime scene holding digital evidence be preserved to prevent continued access to the potential evidence that may, for example, be stored in a computer or network server (Carrier & Spafford, 2003). One of the problems confronting investigators is the well-intentioned, but often disastrous, attempts by an organization's personnel, with little investigative training, to preserve the evidence for later analysis. Such actions often lead to evidence being lost or altered, sometimes rendering it inadmissible or lessening its evidentiary worth (Rogers & Seigfried, 2004; Stambaugh, Beaupre et al., 2000).

Because of the volatile and semi-volatile nature of data stored on a computer, it is inevitable that some evidence and corroborating data will be lost or modified when attempting to access and copy digital evidence. Volatile data requires a constant power supply to remain in the computer memory and is erased when the power is interrupted or shut down, unlike non-volatile memory or persistent data (Rowlingson, 2004). Consequently, shutting down the power to a computer can cause a loss of volatile memory in registries, random access memory, caches, network topologies and so forth.

Locating digital evidence may involve seizing all the hardware and software or locating the evidence and copying the relevant data. Seizing a stand-alone computer

may inconvenience the individual suspect, but removing the entire hardware and software from an organization would be impractical and bring its operations to a standstill; therefore investigators would normally obtain a forensic image of the data (Casey, 2000, 2002).

Broadly speaking, because of the ephemeral nature of digital evidence, investigators must consider accessing the evidence through one of two processes: a live analysis and a dead analysis (and sometimes a combination of both). A live analysis occurs when the computer or network believed to hold digital evidence remains running and the investigator accesses the system to search and examine the evidence in a real-life setting (Carrier, 2005). There are disadvantages in using the live analysis approach, as it may result in data being overwritten or lost, and false information could be retrieved if some software programme has been set as a booby trap to conceal or destroy evidence (Carrier, 2005). A dead analysis occurs after the system has been shut down and trusted application tools are used to capture the evidence and may avoid the pitfalls of a booby-trapped system, but it is becoming impractical to seize anything more than actual terminals (Adelstein, 2006; Carrier).

In the past investigators have opted for dead analysis to capture and preserve digital evidence from fear of modifying it, yet the process of shutting down the computer modifies date and time stamps, and may permanently lock the investigator out of a password protected and encrypted hard drive (Casey, 2002). Passwords and knowledge of what was operating at the time the computer was shut down may also be lost (Casey). Evidence garnered during live analysis, however, provides evidence that would not be available from a forensic image of the system, thereby capturing a snapshot of the system that cannot be reproduced later (Adelstein, 2006). The courts have questioned the admissibility of digital evidence because of concerns of contamination during live analyses, even though it is evolving as the pragmatic means of collecting evidence from larger systems and datasets (Adelstein). However, provided any data loss is noted by the investigator, the courts may accept that the data loss does not detract from the remaining evidence presented, subject to explanation being provided by the investigator (Carrier, 2005).

Locating the Evidence

Once secured on the target computer system, the process of locating relevant evidence is undertaken. The location stage commences with an examination of the hardware devices suspected of storing the evidence and the data held on the devices. This stage includes filtering extraneous matter from that relevant to the investigation - a tedious task for trained investigators and more so for non-specialist personnel. The evidence may take the form of: electronic files; an email; user access logs; image files; traces of hacker intrusions, such as rootkit files; and records of unauthorized,

or suspect access to information (Casey, 2000). Searching through the large amount of files stored on a computer or network makes this a challenging exercise when seeking important information about the suspected crime or event of interest, so that investigators may focus on obvious areas of interest within the system. Sufficient knowledge of criminal or civil case, investigative experience, and technical expertise is required to locate relevant digital evidence. Recognizing the evidence is a major obstacle because unlike a traditional crime scene, there is no body or smoking gun and very few clues to help the investigator; often there may be no obvious telltale signs at all (Caloyannides, 2003; Stephenson, 2000). Detecting fraud, for example, has always been problematic: even acknowledging fraud exists bewilders those not previously victim to it. Auditors, who tend to concentrate on finding and analysing large discrepancies, habitually fail to see a group of smaller anomalies that collectively could indicate fraud or some other illegal or improper activity (Silverstone & Sheetz, 2007). In seeking digital evidence, it is the small anomalies, or oddities, that are just as important as the large differences.

The primary role, when seeking the truth of a matter under investigation, includes locating evidence that supports the preliminary hypothesis, but just as important is locating evidence that refutes the hypothesis, also known as exculpatory evidence (Carrier & Spafford, 2003). Locating and identifying the digital evidence for the given class of crime or violation is required to support or refute hypotheses about the incident and an investigator uses various technical tools and investigative processes to accomplish this important task. Once preserved, the data on the computer or other device is examined to locate the evidence about the incident that has prompted the investigation (Carrier & Spafford). It may be discovery of evidence on a competitor's computer network that will clarify whether intellectual property has been misused in a civil action, or it may involve seeking evidence of downloading illegal and offensive images from the Internet in a crime investigation. If, for example, illegal images or stolen documents are being sought, then files with image and document extensions will be located and examined. In the event of a security breach, where unauthorized access was gained to protected records, then the user access logs would be a logical starting point to commence an investigation (Carrier & Spafford).

Investigators use a variety of forensic toolkits to help them search large datasets and complex, computer file structures to identify files of relevance to the case. These tools help filter and data mine large datasets and identify hidden or deleted evidence in obvious and more obscure locations, but for the main part, the experience of the investigator drives the examination of potential evidence, which is predominantly a mechanical process (Gong & Chan, 2005). During examination of the available information, the investigator discards what is considered irrelevant data and selects potential evidence, which is then refined through tedious, time-consuming and

iterative processes in an attempt to recreate as much of the crime scene as possible (Gong & Chan).

It should be mentioned that not everybody wishes the evidence to be found or the crime to be investigated, and it is not uncommon for managers to conceal the misdemeanors of subordinates; sometimes to avoid bringing themselves into disrepute (Stephenson, 2000). Organizations are often inclined not to prosecute employees because of feared adverse publicity and are reluctant to seek assistance from law enforcement agencies. Many law enforcement agencies are under-resourced and have lengthy investigation waiting lists, further compounding this reluctance for organizations to seek redress through prosecution. Moreover, computer crime is sometimes considered less personal than a crime of violence or a burglary and it is not always possible to identify a victim. Investigating computer crimes involves costly, resource hungry investigations that are often protracted, seldom bringing culprits to justice, and so organizations are less inclined to resort to prosecution or litigation than in more traditional crimes, or at least in the case of smaller impact crimes.

Selecting the Evidence

The next stage in the investigation process is to select the evidence that will form part of a legal case. For those not familiar with investigations it is common to misread the readily available evidence and draw incorrect conclusions. Business managers attempting to analyze what they consider are the facts of a case would be wise to seek legal assistance in selecting and evaluating evidence on which they may wish to base a case. Selecting the evidence, sometimes referred to as the analysis stage, or event reconstruction stage, involves analysis of the located evidence to determine what events occurred in the system, their significance, and probative value to the case (Ashcroft, 2001; Carrier & Spafford, 2003). Using available evidence, including digital, physical and human evidence, a reconstruction of the crime, or events under investigation, provides a clearer understanding of what happened (Casey, 2002). Evidence that supports the initial crime hypothesis is collated along with exculpatory evidence that refutes the hypothesis for analysis (Carrier & Spafford). The outcome of this process will help refine or change hypotheses and should identify an alternative hypothesis. This is important because many jurisdictions require details of exculpatory evidence to be provided to the defending party to enable them to rebut the prosecution's case during later proceedings (Stephenson, 2000).

As in conventional crime investigations, investigators look for motive (why?), means (how?) and opportunity (when?) for suspects to commit the crime, but in cases dependant on digital evidence, it can be a vexatious process (Stephenson, 2000).

Motive

The motive of wrongdoers in cyber crime ranges from internal and external threats, such as mischief, fraud, theft and sabotage of information, extortion, threats of violence, and even business warfare.

Means

The means may vary and depend on the technical knowledge and skills of wrongdoers and their ability to access targeted systems. Reconstructing the events of the crime, by examining the computer system operating system and relevant files, can provide an insight into the means used to affect the crime or misdemeanor, but this requires considerable technical and investigative skills in more complex cases.

Opportunity

Opportunity can be difficult to verify as various issues can make it difficult or impossible to link the time of the crime to the suspect's access to the computer system (Stephenson, 2000). Poorly configured system access security, the absence of audit journals, or malicious software events, for example, can obliterate, or make event records less than reliable, and create gaps in the chain of evidence needed for the crime reconstruction process. Audit logs are often relied upon heavily to link a suspect to an event but even logs can be falsified if they are not protected adequately from mischief-makers or system errors (Stephenson, 2000).

False evidence too can be generated upon which unreliable arguments are propounded by those unfamiliar with the true nature of the digital domain (Diaconis & Mosteller, 1989; Koehler & Thompson, 2006). Koehler and Thompson advise caution when attempting to select circumstantial evidence that seems to support reasonable and compelling argument, but which may well be unreliable because it is are purely coincidental and nothing more. Moreover, investigators may miss evidence or worse still, resort to cherry-picking when choosing or omitting evidence to gain legal advantage.

Presupposing guilt or innocence of a suspect may be based on the absence of evidence. For example, a suspect may claim use of a different computer than the terminal used to commit some illegality, but the evidence to support the alibi may not be recorded in the network logs. Consequently, an absence of evidence does not necessarily show evidence of absence of some important event that did occur, but which can no longer be proven, which is a common phenomenon of the digital domain (Berk, 1983; Flusche, 2001; Koehler & Thompson, 2006).

Therefore, it should always be at the forefront of the business manager's mind that computers behave unpredictably and that they would unwise to accept any digital evidence at face value. Users can alter digital evidence intentionally or unintentionally, thereby obfuscating the chain of key events. The behavior of the computer operating system and software applications may not have been analyzed thoroughly, thereby prompting premature and unsafe conclusions. Validating the evidence, therefore, is a key stage in preparing the digital evidence for a legal case.

Validating the Evidence

During the validation stage the evidence is tested to determine its validity, namely if the assertion drawn from the digital evidence can be verified. For example, the assertion that an email message was deleted would require confirmation of the existence of the deleted file; that it was deleted at a specific time; that this information was not altered by system processes; and so forth. Whatever security measures exist on the host computer, they are not always helpful to the investigator as they are more often intended for auditing and monitoring the overall integrity of records, rather than for specifically validating digital evidence (Carrier, 2005). During the validation stage, the investigator may revisit the location and selection stages to seek verification of validity issues and to develop new lines of investigation as circumstances dictate (Carrier & Spafford, 2003).

Figure 2 shows a simple chain of evidence based on apparent or available evidence consisting of unprocessed facts from which a tentative hypothesis can be constructed. In this case, reconstruction of evidence based on human, physical, and digital evidence, suggests that the suspect accessed a computer with the intent to download illegal content from the Internet.

Figure 3 outlines a proposed validation interrogation process where exhibit F, taken from the chain of evidence example in Figure 2, requires validation (Boddington et al., 2008). A series of prompts determines if the evidence is valid. Each exhibit needs validating, and if we take Exhibit "F" for example, there is a presumption that the suspect used the peer-to-peer application Limewire to access illegal images on the Internet. Questions that should be asked include, the ability to link the suspect to the computer and the opening of the software, and that the date and times of these events can be verified. If these questions are not corroborated or are inconclusive, then this will have an adverse effect on the case. Additional evidence may be required, or other legal strategies considered, using the best evidence available.

Failure to locate all available digital evidence occurs because the location of relevant evidence is not always evident to the untrained enquirer, who may be relying solely on intuition (Cohen, 2006). While a technically astute and assiduous investigator can identify and analyze much relevant evidence, time constraints and

Figure 2. Chain of Evidence before validation of the evidence

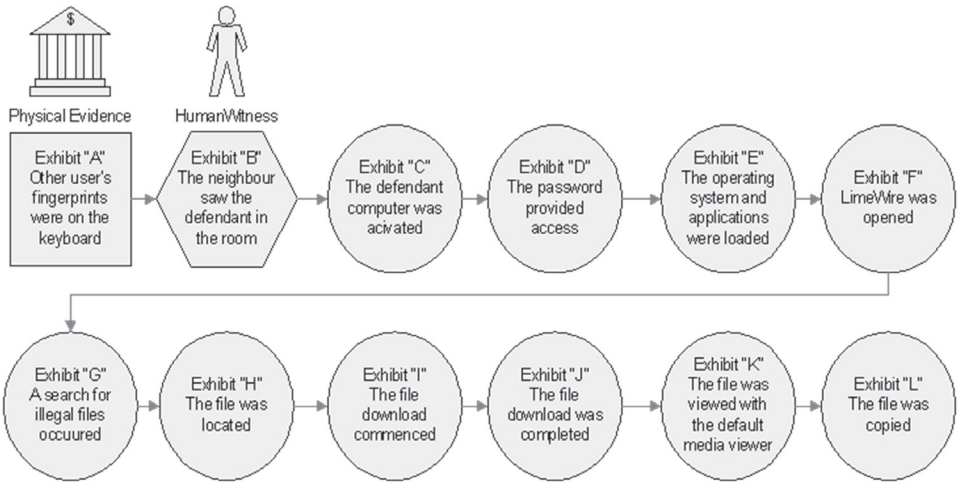
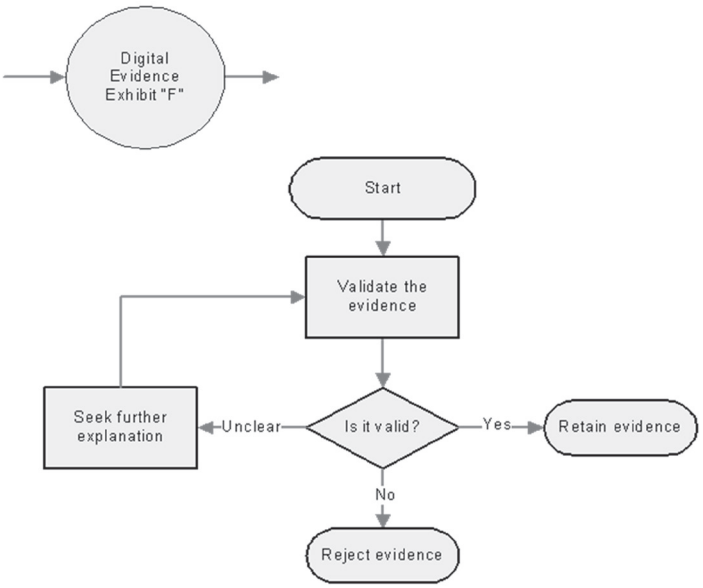


Figure 3. Chain of Evidence: Showing the validation process of digital evidence exhibit F. (Adapted from Boddington, Hobbs, & Mann, 2008).



the uniqueness of the crime scene may, nevertheless, produce incomplete identification of all that should be located, consequently denying examination and analysis of crucial facts (Australasian Centre for Policing Research, 2000). Incomplete scrutiny of the available evidence during the validation stage of the investigative process and failure to validate the evidence at that point is where the investigation can fail (Cohen). The complexity of the digital domain compounds the problem and prosecution cases often fail during trials where the incompetence of the investigation is apparent and where validation issues arise.

There is error in every analysis method and the reliability of any particular test remains an issue for forensic investigators (Cohen, 2006; Palmer, 2002). A range of different factors can affect the validity of the evidence, including collection tools missing critical evidence, failure of the prosecution or a plaintiff to report exculpatory data, evidence taken out of context and misinterpreted, misleading or false evidence, failure to identify relevant evidence, system and application processing errors, and so forth (Cohen; Palmer). When presenting a legal case based on what appears to be convincing digital evidence, the case can collapse if the defense can show that the security or integrity of the network is defective and shows contamination or alteration of the digital evidence it is supposed to protect (Akester, 2004; Mattord & Whitman, 2004; Schneier, 2000). Conversely, if the validity of the evidence can be established, its weight in legal argument is enhanced.

Caloyannides (2003) asserts that because the legal fraternity understands little about computer science, the potential for miscarriages of justice are great, adding that the cyber forensics community exploits this situation and obfuscates the environment by focusing on issues such as preserving, collecting, and presenting digital evidence. Caloyannides warns that evidence found on computer systems can be contaminated intentionally or unintentionally through a range of factors, and it may not always be possible to determine the truth of a matter; yet faulty evidence continues to be accepted by the courts without proper validation. The evidence collated and processed during the investigative stages is then presented to the legal practitioner, who must test each piece of evidence to determine its weight in the legal argument and its suitability for use to prove or disprove the case.

Presenting Digital Evidence in Legal Cases

Having located and selected digital evidence and incorporated it in legal argument in a case that results in some legal adjudication, the next hurdle a business manager must tackle is having the evidence admitted to proceedings. Before digital evidence may be admitted in court proceedings, it may be required to meet additional conditions imposed by legislation and court conventions (Caloyannides, 2001; Tapper, 2004). The first condition is acceptance by the examining body, such as a court, to

grant admission of the material tendered as evidence suitable for later examination and rebuttal by the opposing party (Tapper). Failure to have the evidence admitted precludes its use in the subsequent legal processes. The second condition subjects the evidence to rigorous, judicial examination of its evidentiary worth or weight. There is not as yet any formal accord on the admissibility and weight of digital evidence (Mohay, 2003). The following sections look at how jurisdictions treat these two conditions.

Admissibility of Evidence

Clearly, evidence that is denied admission in court proceedings becomes irrelevant to the case and detrimental to one of the contending parties (Tapper, 2004). Irrespective of whether tendered evidence is direct, circumstantial or hearsay, for it to be admissible in court proceedings, the court must be satisfied that it is authentic and unmodified. In the case of digital evidence, some forensic expertise may be required to ensure that the evidence is trustworthy (Casey, 2000).

Physical documents are tangible objects that require traditional storage and management processes to ensure, that when tendered in evidence, they comply with evidentiary requirements of the courts. Prior to the 1990s, documentary evidence was mostly on paper, with digital evidence usually taking the form of printed pages (Caloyannides, 2001). Subsequently, organizations have relied increasingly on computerized functions to manage their activities and for storing and maintaining their information records, which means the majority of documentary exhibits are digital or created from digitized information (Akester, 2004).

An organization's viability, and sometimes its continued existence, hinges on its ability to protect important information records adequately from a range of threats. The ability to preserve important digital records of potential evidentiary value is also of great importance to an organization (Baraani-Dastjerdi, Pieprzyk, & Satavi-Naini, 1996). Failure to protect digital evidence can result in it being discredited and its admissibility barred by the courts. The admissibility of documents tendered in legal proceedings is subject to legislation, case law, precedent, and the legal conventions of different jurisdictions (Caloyannides, 2001). Not surprisingly, the laws and rules governing evidence present a diversity of conditions that evidence tendered must meet before it may be admitted in court proceedings (Tapper, 2004). Evidence is often used to prove facts in issue, or facts from which facts in issue may properly be inferred; comprising the testimony of witnesses, hearsay, documents, and other physical objects. In using documents as evidence in legal processes, the contents of a document may be incorporated in the sworn evidence of a witness.

Courts have agonized over the admissibility of digital evidence, as legal anomalies may arise that hinder their presentation as evidence (Mattord & Whitman, 2004;

Schneier, 2000). Courts continue to debate the admissibility and reliability of DNA evidence used in trials, which shows some parallel issues over the admissibility and weight of digital evidence used in court proceedings (Myers, Reinstein, & Grille, 1999). These anomalies may occur because of the scientific complexities of DNA evidence, and in the case of digital evidence, complex technical issues relating to its special properties and environment, which often makes it hard for lawyers and courts to understand the nature and value of the evidence presented (Myers et al., 1999).

In 1979, the United States Department of Justice (Computer Crime, Criminal Justice Resource Manual, 1979) partitioned computer crime into three categories: computer abuse, computer crime, and computer-related crime. These definitions were blurred by the vast proliferation of computers and computer related products during the 1980s, and some technical and legal observers believed that any significant advances in computer technology should be mirrored by parallel changes in computer law (Morris, 1990).

In 1986, information technology security consultants were critical of legal practitioners, judges and legislators for failing to come to terms with technical advances in computer development that impact on the admissibility of digital evidence (Luddy Jr., 1986). This apparent failure to update legislation to enhance the admissibility of digital evidence was still not resolved when, even in 1990, a lack of universal agreement on what constitutes a computer crime, in the legal community, in the United States, was identified; such inertia being attributed in part to the rapid changes in computer technology and communications (Morris, 1990).

Some observers contend that well-defined legal definitions of computer crime are overdue and should be constructed to capture all acts which are criminal and involve computers (Morris, 1990). While acknowledging that the completeness of a definition seems problematic, some commentators believed it feasible by using technical, computer security concepts to examine a legal concept from a technical perspective that may yield insights into its strengths and weaknesses and even suggest avenues for legislative improvement (Morris). However, nothing significant has been tabled at the time of writing this chapter, in early 2009.

When admitted as evidence, difficulties remain when attempting to authenticate the authorship and antecedents of digital records - more so than in the past when paper document forgeries were common but required a high degree of technical expertise to make them convincing and avoid scrutiny (Akester, 2004). Digital forgeries are so much easier to carry out and it is not always possible to detect sufficient evidence to prove a forgery took place. Consequently, a legal precedent was set, jurisdictions were reasonably comfortable with the authenticity of paper documents, and documents presented in digital evidence form seem to have been awarded the same treatment. According to Akester, authenticity requires validation

that the record is what it purports to be, whether its author is the real author, whether it is the genuine record or a substitute, and so forth.

In the United States of America, Rule 1003 (Admissibility of Duplicates) of the Federal Rules of Evidence, indicates that a copy of a document is equally admissible as evidence as the original provided the copy is produced by a process that ensures its accuracy and genuineness (Mercuri, 2005). Many state legal codes are based on Rule 1003 and this legislation was anticipated to be the focus for lawyers to raise questions about the validity of digital evidence.

Security researchers are increasingly concerned that digital evidence held in networked computers is not protected adequately to preserve its admissibility and, ultimately, its evidentiary weight (Akester, 2004; Halleck, 1996; Schneier, 2000). As mentioned previously, digital evidence is vulnerable to a variety of threats, both intentional and unintentional, as well as technical and non-technical attacks. Technical attacks may compromise the security of a controlled system, whereas a non-technical attack may consist of natural events or insider attacks by humans (Mattord & Whitman, 2004). Cognizant of these threats to computer networks, Australian courts have expressed doubts about the reliability of digital evidence recognizing its vulnerability to a range of threats. Although not clearly defined, the courts' concern over reliability appear to focus on authenticity and integrity of digital evidence, but again provides no helpful definition and explanation of these terms in the context of a wide range of legal cases.

Concerns raised by Australian judges over Section 155 of the Evidence Act 1995 (Commonwealth of Australia) was a departure from the earlier trend towards formulating a unilateral reliability of digital evidence. This section of the legislation asserts proof of authenticity and integrity of Australian Commonwealth departmental records, or public records of a state or territory, by allowing the production of a document purporting to be such a record if signed by the relevant minister. These ministerial certificates allow the printed copies of digital records to be admitted as documentary evidence (Nezovic v Minister of Immigration and Multicultural and Indigenous Affairs, 2003). In 2003, legal challenges to the interpretation of the ministerial certificates issued under the provisions of the Migration Act 1958, resulted in two court rulings about the admissibility of digital evidence used to produce the certificates. The appeal judges ruled that while section 155 of the Act facilitated the admissibility of records that might otherwise be inadmissible, section 155 did not negate the admissibility of digital evidence. However, the judges ruled that although section 155 did provide the convenience of certifying the production of computer-generated information held by the department, if subsequently challenged, then the truth of the contents of the digital information tendered as evidence would still need to be established by the department.

The various Evidence Acts of Australia contain a number of provisions facilitating proof of digital evidence. In November 2004, the Australian Law Reform Commission (ALRC) publicly requested commentary from interested parties on the viability of the uniform Evidence Acts of Australia. Of particular interest to the ALRC was comment it sought on the impact of computer-produced evidence on court proceedings, under section 48 that permits the tendering of such documents (Review of the Evidence Act 1995, 2004). Sections 146 and 147 of the Act were intended to facilitate the admissibility of evidence produced by processes, machines and other devices. In 2005, the Commission decided that a major overhaul of the legislation was unwarranted and not desirable as there was little evidence of problems arising from the operations of sections 146 and 147 and little empirical evidence that a more rigorous test was justified (Australian Law Reform Commission, 2005a).

Australian courts will admit certificates provided by prosecutors, certifying, for instance, that a speed camera has been prepared in accordance with the appropriate legislation (Warren, 1997). The admissibility of this evidence, that the reading in the device is proof of the speed, is based on digital records; such evidence may be challenged, but defense lawyers claim that speed camera legislation is biased to the prosecution (Warren, 1997). This de facto "proof of innocence" burden (Section 5.2) contrasts markedly with most other criminal cases, where the onus is with the prosecution to prove a charge beyond reasonable doubt. Speed camera, radar device legislation reverses the onus to a defendant but this may be seen as inequitable as most defendants' ability to mount a spirited and compelling defense is restricted by high costs, including payment for technical witnesses to challenge the digital evidence (Warren, 1997).

Very few speed camera cases are challenged and most that are, rarely have a positive outcome for the defendant. However, in August 2005 the Hornsby Local Court in New South Wales dismissed a motor vehicle speeding case after the New South Wales Road Traffic Authority (RTA) failed to produce an expert witness to prove a speed camera image had not been doctored, thereby reversing the onus back on to the prosecution (Schneier, 2004). When challenged by the defense, the RTA was unable to prove the authenticity of MD5 encryption algorithms used to protect the integrity of each picture stored in the police database. The MD5 algorithm, developed in 1992, was used as a security measure to prove the pictures have not been altered after they were taken (*The Age*, 2005; Schneier, 2004). Consequently, the motorist escaped a conviction by claiming that data was vulnerable to hackers after mathematicians in China decrypted the MD5 algorithm, and the motorist's lawyer argued successfully that the algorithm was discredited technology. It is debatable that the algorithm is unreliable, as it is still in common use.

Not all evidence found may be used if it is subject to court rules of exclusion concerning evidence improperly or illegally obtained, usually relevant only to

criminal cases requiring a search warrant to locate and seize evidence. However, in corporate cases, the defendant may claim a breach of privacy in an attempt to prevent admissibility of digital evidence (Stephenson, 2000). It should be noted that although admissibility may not be an issue for digital evidence used in disciplinary proceedings, it would be prudent for an organization to ensure that the evidence has been processed, and thoroughly validated, to whether the ordeals of a potential legal suit from employees (Mohay, 2003).

Weight of Evidence

Once admitted, the evidence itself is subject to further scrutiny by the jury, or in the absence of the jury, the judge, magistrate or adjudicator, who will look at the evidentiary worth or weight of evidence of the tendered exhibits. Consequently, the legal practitioner must examine each piece of evidence to determine its weight in the legal arguments, and its suitability, whether the evidence supports or disproves the case. This analysis relies on identifying logical threads of inferences, linking one piece of evidence to another, with the strength of each inference used to determine the overall weight of a case (Silverstone & Sheetz, 2007). The persuasiveness that flows from the combined evidence presented in a legal case is used by adjudicators and juries to ascertain the guilt or innocence of the accused party or, in civil cases, the liability of a contesting party (Silverstone & Sheetz; Tillers, 2005).

A collation of evidence is tendered as part of the legal argument in an attempt to persuade the court of the probability of some truth or other matter. For example, in the case of a negligence suit, the court must be persuaded that the defendant did not exercise due care (Demougin & Fluet, 2006). In a civil case, it is important to establish a preponderance of evidence to show that something is more likely to have occurred, than otherwise (Devitt & Blackman, 1977). In the USA, the United Kingdom and Australian, for example, civil courts generally accept that the degree of certainty is above 50%. In other countries, including Germany and France, a preponderance of evidence in civil cases is often insufficient and requires a higher burden of proof; this is similar to criminal cases in Australia where proof beyond reasonable doubt is required (Demougin & Fluet, 2006).

In the past, courts may have been inclined to accept the weight of digital evidence based on expediency and intuition, or, if confused by technical issues, have dismissed cases out of hand. However, there is the likelihood of increased legal challenges that cast doubt on the weight of the evidence in the future (Ahmad, 2002; Pospesel et al, 1997; Schneier, 2000; Tapper, 2004; Whitcomb, 2002; Whitman & Mattord, 2005). This is evident by the growth in computer-based crime and greater reliance on digital evidence, both as partial evidence in otherwise conventional legal cases,

or where the evidence exists entirely in digital form (Cohen, 2006; Etter, 2001; Palmer, 2001; Thompson & Berwick, 1998).

Information held in computers may be presented to courts as a printed document; the computer having in effect served as an electronic filing cabinet that stores information in much the same ways as a traditional filing cabinet (Stephenson, 2000). Courts will admit such documents but genuineness, completeness, and accuracy may be questioned because of the properties of the electronic filing cabinet that holds the history of the document in digital form (Stephenson). It is not the printed or monitor-viewed form of the digital evidence that is of concern, but the need for some assurance that it is the genuine article; the evidence must be validated before the weight of evidence can be considered.

In the case of a Multanova vehicle speed detectors used in Australian jurisdictions, the photograph of the speeding vehicle's number plates suggests that a vehicle registered to the owner was exceeding the speed limit at a confirmed location, date, and time. Unless there is other evidence to link the owner to the vehicle, such as a photograph of the driver, there is no proof the owner was driving the vehicle at the time of the offence; additional evidence is required to link the owner to the vehicle at the relevant time. Constructing legal argument is the next stage in progressing a case through the legal system.

Constructing Legal Argument

Legal argument relies on evidence that proves or disproves a case; based on the available evidence, the defendant is guilty or innocent of a crime. Legal practitioners use logical chains of inferences, linking one piece of evidence to another with the strength of each inference used to determine the weight of a case. The persuasiveness that flows from the combined evidence presented in a legal case is used to enable adjudicators and juries establish proof of guilt or innocence of the accused party (Silverstone & Sheetz, 2007). Legal arguments are based on logical probabilities that collectively prove the case and are constructed from the simplest logic possible. They may be mapped, for example, by a timeline of reconstructed events, or through inferential analysis processes. The weight of the evidence depends on the various relationships between key evidence, as well as the reliability of the supporting evidence (Silverstone & Sheetz).

It is unusual for legal cases to rely solely on circumstantial evidence, including digital evidence. Direct evidence, such as witness testimony, may be required to corroborate or, from the defense perspective, refute the digital evidence that asserts that the defendant accessed the computer at the time of an offence. Locating this supplementary evidence, often intuition-based, helps develop argument and strengthen the overall weight of available evidence. The example shown previ-

ously in Figure 2 of a simple chain of evidence was based on apparent or available evidence consisting of unprocessed facts from which tentative legal argument can be constructed. This amount of preliminary evidence is readily comprehensible to legal practitioners but is most likely incomplete, as digital evidence is complex and events are related to and dependant on a range of systems and application programs.

While experienced investigators may identify the less than obvious leads, or seek expert advice where their technical expertise fails, explaining the complexity of the digital evidence located to the legal practitioner may be difficult (Yasinsac et al., 2003). If the investigator is diligent, has sufficient technical and investigative expertise and skills, and is dedicated to seeking all relevant evidence, then the legal practitioner would be well served. Nevertheless, and it should not be understated, the legal practitioner must be able to determine whether enough evidence has been located and whether the validity of the digital evidence has been satisfactorily described and determined. The interface between the investigator, or auditor, and the legal practitioner is where organizations should ensure they obtain full information about the case in question, to ensure they have a sound understanding about the accuracy, nature, and relevance of the digital evidences.

Difficulties Using Digital Evidence in Legal Cases

Large, complex data sets and computer systems and networks can make evidence interpretation problematic and time-consuming. Sometimes there are too many potential suspects to investigate leading to protracted investigations (Mohay, 2003). Unlike traditional offences that are relatively easy to reconstruct, where evidence is tangible and with a narrower range of suspects, digital-based crime, especially if it involves networked computers and the Internet, has the problem of a larger number of potential suspects to investigate (Mohay). There is the common difficulty of determining whether a crime has actually occurred, for example in network computer crime, the nature of the event is often less obvious and immediate and victims may be unaware of a crime until well after it has taken place. Most notable attacks of this category are identity thefts (Hoar, 2001; Mohay). Moreover, there is often too much potential evidence to process, and when located, the evidence may easily be contaminated and ruin other digital evidence (Mohay). The increased storage size of computer hard drives and servers allows datasets to be stored that contain many terabytes of data, thereby making it difficult for investigators to determine how much of the dataset is evidence before commencing examination.

Another problem is the relative ease with which digital evidence can be contaminated when compared to evidence taken from a traditional crime scene that uses a series of separate analysis and preservation techniques (Mohay, 2003). The handling of digital evidence retrieved from a crime scene requires great care and

expertise to avoid contamination, as the digital files are susceptible to corruption during the copying process. It is not uncommon that forensic copying techniques may inadvertently contaminate or destroy the evidence. Furthermore, contamination of some evidence may ruin all the other evidence used in a case. Unlike physical evidence, which may be a single component without which the case may still succeed, digital evidence is highly interconnected and its loss at any point in the chain of evidence may destroy the entire case.

Digital evidence may be modified without leaving any obvious trace of the commission of a crime or misdemeanor and although its previous existence is suspected, it is irretrievable; to reiterate, absence of evidence does not necessarily show evidence of absence of a relevant occurrence (Koehler, 2006). Considerable effort and expertise by an investigator would be required to seek corroboration to show that evidence existed but was later obliterated (Stephenson, 2000). For example, an illegal image may have been deleted and attempts made to erase links that show it existed; however, closer examination of the computer may not recover the deleted file name or its contents but may locate some metadata that shows proof of the file's existence (Carrier, 2005). Such occurrences are not unusual, and if overlooked by an investigator, it is unlikely that the business manager would understand their significance.

Other legal loopholes in the technical domain exist. Consider a hacker trespassing into a computer network for some illegal or improper reason, or perhaps out of idle curiosity. Some jurisdictions may require compelling evidence to prove some illegal action by an attacker that violated the data held on a proprietary network of an organization (Stephenson, 2000). Furthermore, it has been argued that if a network was within or adjacent to the public domain (Internet) and that even if unauthorized access was denied, the hacker should be warned that contrived access would be in breach of the proprietary rights of the organization, otherwise any legal reprisal against the hacker would be ineffectual.

These are just a few common problems, but there may well be others yet to emerge as lawyers gain a better insight into the network systems that host digital evidence. An experienced investigator, for example, may produce compelling digital evidence, only to lose the case because the integrity of the network security is questionable. Even if the network security does have a high level of integrity, the jury may not understand the expert opinion supporting this contention and reject the evidence out of hand.

It seems that the primary evidence, for example, a threatening email sent by a suspect, and corroborating evidence, such as computer logs linking the email to the suspect, can be undermined if the network security is unable to provide accurate records that cannot be validated. Similarly, it is improbable that a jury would have much confidence in evidence at a homicide trial, if claims that the murder weapon

exactly matched the stab wound in the corpse were undermined by the effects of mutilation of the wound by maggots or wild animals. The environment was not conducive to preserving the crime scene in the natural world anymore than on a computer network. So for digital evidence to be of any use it must have validity and that can only be guaranteed if the environment is well protected.

How well does Computer Security Protect Digital Evidence?

This section looks at computer security and its ability to protect digital evidence. Digital evidence is fungible and when held on a storage device, such as a hard drive, or as a forensic image copied on to a storage disc, it can be easily replaced, altered, and destroyed; hence, the need for robust protection (Stephenson, 2000). During legal proceedings, examination of a record by opposing parties wishing to challenge its authenticity frequently occur (Tapper, 2004). Similarly, if the chain of custody is broken, or its robustness placed in doubt the opposing party may argue that the evidence has been contaminated or falsified and prevent its admission in legal proceedings. The chain of custody is important, and so is the need to validate the evidence itself and this begs the question as to the efficacy of conventional security measures protecting the operational and functional integrity of digital records (Caloyannides, 2003). Spenceley (2003) advocates that systems should provide a verifiable history of a record from its dates of creation to the date it is required as evidence in legal processes, thereby assisting the courts to determine the authenticity of digital evidence. An organization that owns a record may be less fastidious in accepting and accommodating gaps in the record's history but the same expediency is unlikely to occur during legal processes; greater scrutiny of records is necessary during legal proceedings (Tapper, 2004).

Inaccuracies in attribution of authorship and the content of digital evidence, for example, are common occurrences affecting legal argument as to the completeness, correctness, authenticity, and faithfulness to an original source; thereby, raising doubts as to the worth of the evidence (Akester, 2004; Mocas, 2004). More disturbing is that even in the absence of any obvious irregularity of the software platforms housing the evidence, examination of any material of evidentiary value does not in itself attest to the accuracy or integrity of the evidence (Spenceley, 2003). The more pessimistic argue that it is imprudent to assume that there is a low risk of inaccuracy in computer output due to application failures. However, this raises the question as to whether the courts are fully aware of the problems these issues can create as courts in various jurisdictions do not seem to be overly concerned about such serious deficiencies in system security (Spenceley).

Computer security includes such diverse counter-measures as cryptography, controlling authorized computer access, managing computer accounts and user privileges,

copy protection, malicious code protection, database security, and protection for network connections against such threats as, password keystroke loggers, malware, and hackers (Schneier, 2000). Security analysts question how an organization can maintain a large database and communication networks where many users have different access privileges, and yet maintain sufficient operational functionality and security protection, thereby raising the specter of the reliability of the environment holding digital records that may later be used in evidence.

Some organizations have adopted a piecemeal approach to information security management, commonly assessing strategic risks at the time new technology is initiated, but subsequently do not always monitor their information systems to ensure they are configured securely (Jordan & Silcock, 2005). Even organizations, that have well configured and maintained systems, seldom prepare for events that require the use of potential digital evidence at some later time (Ghosh, 2004). Those responsible for information security within organizations may give scant regard to protecting and preserving digital evidence, yet a greater awareness and understanding of the importance of digital evidence is imperative.

However, if there has been such an abject failure of technical solutions to solve technical problems affecting computer database security, other non-technical countermeasures and intervention strategies, such as physical access controls and barriers, audits, biometric devices, and monitoring or surveillance, do not seem to have enjoyed more than partial success (Schneier, 2000). Notwithstanding the implementation of these and other security processes, there are additional factors that may impact negatively on their efficacy (Leiwo, 1999; Schneier, 1996). These include:

- A lack of mechanisms for evaluating security
- A gap between management and enforcement of information security
- Conflicts with top-down system design principles
- Lack of support for information security in non-traditional organizations
- Lack of consensus of definitions of concepts involved
- Scientific difficulties in information systems security research.

The United Kingdom's Computer Misuse Act of 1990 attempted to check the threats posed to network security by unauthorized activities (Coleman & Sapte, 2003). It created three specific offences of:

- Unauthorized access to computer material;
- Unauthorized access with intent to commit or facilitate commission of further offences; and
- Unauthorized modification of computer material.

However, the legislation was criticized by industry as having little deterrent value and, furthermore, the United Kingdom's Home Office figures revealed only thirty-three prosecutions for offences under the Computer Misuse Act in 1999 and 2000 (Coleman & Sapte, 2003). It would seem that the legislation was not a successful deterrent, with few successful prosecutions and lenient sentences handed out during the period. Coleman & Sapte quote the United Kingdom Home Office as explaining that while the number of successful prosecutions is low because of the difficulties of meeting the requirement to prove intent on the offender's part, another explanation is an apparent inadequacy in training the police and judiciary to understand and deal with cyber crime.

Networked computer and information security consist of procedures and processes designed to protect the reliability of an organization's information records from intentional and accidental threats. Such measures are intended to preserve the validity of records for operational and functional purposes of organizations rather than any planned concerns over digital evidence retrieval and preservation (Bettino, Jojodia, & Samarati, 1993; Castano, Fugini, Martella, & Samarat, 1995). By implementing various security measures, it is possible to prevent or minimize the corruption and degradation of the records from a range of threats. However, whatever security measures are used, they are more often used to assist in the auditing and monitoring of the overall integrity of records, rather than directly evaluating the evidentiary integrity of digital information (Carrier, 2005).

Data audits do not prevent attacks (although they may have some deterrent effect on would be attackers and are useful in analyzing attacks after the event) but they do play an important role in collecting digital evidence (Schneier, 2000). Database auditing, for example, is based on conventional standards and regulations for the documentation of an organization's financial transactions (Afyouni, 2006). In terms of information management, as in the case of a database audit, the auditor looks specifically at the information in the database and recognizes that security measures in place are inseparable from the auditing activity (Afyouni). If these security measures are weak, or the audit process inappropriate because of large datasets or both exist, then presumably it becomes unsafe to assume that all potential digital evidence in a database is valid.

This raises concerns for business managers about accepting digital evidence at face value, and whether there should be a rigorous examination of the evidence irrespective of the cost, resources, and time involved. The next section looks at these issues.

Proof of Innocence

In Australia, the Office of the Director of Public Prosecutions of New South Wales in a submission to the Australian Law Reform Commission (ALRC) was dismissive of a call for a higher threshold for admissibility of digital evidence for reasons summarized below. This was despite some scientific solutions put before the ALRC (Director of Public Prosecutions (NSW), 2005b). The submission stated that:

- A more rigorous testing is unjustified because of the absence of solid evidence to support the need for the provision and no cases are evident of wrongful conviction from computer-generated error;
- Litigation in Australia depends on an adversarial system and the burden of proof that rests on the prosecuting party, or plaintiff, ensures proper testing of evidence of this sort;
- It would impose a higher threshold than for other machine produced evidence;
- Data manipulation occurs with any machine-generated information, such as photos, tapes, and videos;
- The party challenging the accuracy of the evidence would have to be given the opportunity to inspect the relevant computer and perform their own tests, which is a costly and time-consuming exercise.

The New South Wales Director of Public Prosecution's stance could be seen by some observers as expedient and denying parties wishing to challenge the accuracy of the evidence to find some legislative remedy. The Australian Government Attorney-General's Department's response to the ALRC (Attorney-General's Department, 2005) was equally dismissive of the need for higher standards of admissibility of digital evidence, asserting that in criminal cases, the prosecution were hamstrung over the type of documentary material available in prosecuting cases. The department argued that it was not in the interest of justice to require a court to reject what appeared to be logical and reliable evidence, that may be corroborated by other material because preconditions of admissibility were not satisfied (Attorney-General's Department, 2005). However, such rulings may be potentially unjust to defendants, even if the potential numbers of cases where the evidence is challenged are numerically small.

Accepting digital evidence at face value may be imprudent, with adverse consequences for those most affected by its inappropriate use in trials. Consider the case of Aaron Caffrey, who in 2003 was acquitted of an offence under the United Kingdom's Computer Misuse Act 1990 offence of causing unauthorized modification of computer material by sending a flood of data from his computer that shut down the computer server operating the Port of Houston, in Texas, United States of America (George, 2004). Caffrey claimed that unknown hackers gained control

of his computer and launched programs to hack into the Port of Houston computer to incriminate him. The prosecution's technical expert could find no evidence of a Trojan virus on Caffrey's computer. Caffrey claimed it was impossible to test every file on the computer, suggesting that a Trojan virus could have deleted itself leaving no trace – a claim strongly contested by the prosecution (George). This was one of a few cases where a Trojan virus defense was accepted by the court without any proof of the virus being found on the computer, although it is unlikely to set any legal precedent (George).

The prosecution of Julie Amero, a former Connecticut substitute schoolteacher, whose classroom computer displayed pornographic advertisements to her students, was dismissed in 2007 after legal experts and security professionals assisted her by providing a forensics report exonerating her after the prosecution failed to investigate all of the evidence (Lemos, 2008). Amero's support group, who criticized prosecutors for failing to exercise care before charging suspects with possession of child pornography, claimed that laws were poorly framed, and investigators and crazed fellow citizens were too quick to claim that mere possession of unlawful images establishes guilt (Lemos). Another child pornography case was thrown out of court in Massachusetts in 2008 involving a sacked government servant, Michael Fiola, who was able to hire a forensic investigator to show that a virus on his work computer terminal was responsible for downloading the illegal images (Lemos).

Conversely, parties appearing before the court have attempted to create fraudulent information and have benefited from the inability of forensic analysis to identify associated digital evidence to strengthen the claim against them. In a civil suit between Kucala Enterprises and Auto Wax Company, over a patent infringement and counter suit, it was claimed that Kucala had installed the software programme Evidence Eliminator for the purpose of destroying evidence (Meyers & Rogers, 2004). Although computer forensic analysis demonstrated that the software was installed, it could not provide evidence about the extent to which the programme was used. While Kucala paid court costs, the suit against the company was dismissed because of a lack of evidence (Meyers & Rogers).

It should be recalled that previous strength of DNA evidence was challenged in the OJ Simpson case when his defense team had unlimited access to funds, scientific and legal expertise, and photographic and video footage of the actual crime scene investigation, normally denied a defense team (Edwards, 2005). Consequently, Simpson was acquitted of the homicide charge, and although his guilt remains a matter of much public debate, errors in handling the DNA exhibits in the laboratory was unprofessional and contamination of the evidence was proven (Edwards, 2005). Could the same not occur with digital evidence in the investigator's laboratory?

Why a Sound Understanding of Digital Evidence is Essential

Current laws may be considered incapable of dealing with many of the current information and communication technologies as there are gaps, or deficiencies, in process procedures that require amendment, or the introduction of new laws (Berwick & Thompson, 1998). Spenceley (2003) looked at the gaps in the legal procedures vis-à-vis networked computers, asserting that computer software application failures may produce outputs that appear correct, but which incorporate some information that is inaccurate. These cases of latent inaccuracy pose serious challenges to legal fact finding, and while not deliberate, such inaccuracy has the potential to invite malicious exploitation.

Spenceley (2003) warned against preferential evidentiary treatment by the courts and legislators of computer output, which he believes is not always justified, and calls for a more rational foundation for asserting that a source of information will enable the courts to identify the reliability of the evidence presented. He suggested that the argument, that evidentiary treatment of digital evidence should be undertaken according to different standards, is imprecise in what it seeks and is concerned that such an argument does not define the boundaries beyond which different standards should not be applied. Spenceley feared that the complexity of digital evidence may encourage the legislators and courts to be injudiciously expedient with determining the reliability of the evidence, in respect of which various dispensations of proof might be superficially attractive.

To mitigate the unreliability of networked computers, Spenceley (2003) advocated a redundant mechanism approach rather than increasing the functional capacity of the computer system. The redundant mechanism uses a separate computer with identical input and processing to that of the processing computer, to compare both outcomes and to detect an otherwise unnoticeable change in outcomes. Section 59B of the South Australian Evidence Act of 1929 recognized the value of a redundant mechanism to validate the reliability of a computer system, but the Australian Law Reform Commission viewed the legislation with some reservation, believing it failed to provide a sufficiently reliable measurement of testing the reliability of evidence ALRC Discussion Paper 69, 2005.

Judges and juries attempt to determine the probability of the guilt (or liability in civil cases) or the innocence of the person or parties appearing before them and are partially influenced by the behavior and conduct of defendants, or contesting parties (Rubinfeld & Sappington, 1987). A greater effort in preparing a robust legal argument, and a more comprehensive collation of evidence, will influence judges and juries in estimating the probability of innocence (Rubinfeld & Sappington). The court is required to choose the standard of proof of innocence, and if the party does not meet the standard, then the court awards the appropriate penalty. Further-

more, courts are expected to minimize the social consequences of convicting the innocent and acquitting the guilty, all within the spirit of fairness, equity, and of course, deterrence.

There is some ongoing legal debate calling for a replacement of conventional forensic identification science that relies on untested assumptions and intuition, including cyber forensics, with sounder scientific analysis (Mohay, 2003; Saks & Koehler, 2005; Tobin & Thompson, 2006). Most writings on the examination and analysis of digital evidence focus on the preservation of evidence and the chain of evidence, with scant mention of the properties of the evidence itself, which may reflect the comparatively recent emergence of digital evidence and cyber forensics (Mohay; Slade, 2004). Irrespective of different legal views and understanding of digital evidence, some scientific research would no doubt be of value to business managers, as well as to the courts, lawyers, and investigators, especially if some standard definitions were established. For example, defining what is required to validate digital evidence in a broad range of legal settings. The terms accuracy, certainty, authenticity, integrity, in terms of the chain of custody, are mentioned in some literature but are not comprehensively defined in any standards (Mocas, 2004).

What of digital evidence itself? For example, the primary evidence may be a threatening email sent by a suspect or other digital evidence, such as a user access entry logs, links the suspect to the computer at the critical time. However, this evidence does not exist in isolation as there is associative information that may corroborate or refute the primary evidence (Mocas, 2004). The access logs do not prove the suspect was using the computer at a specific time any more than fingerprint or DNA conclusively links the suspect to the computer keyboard at a particular time; other corroboration is required to confirm or refute the assertion.

Casey (2007) warns against focusing too much on digital evidence being altered per se, as this obfuscates the worth of the evidence in the event that even if there had been some alteration, it does not necessarily negate the reliability or authenticity of the evidence. Casey stresses the importance of a sound forensic approach in analyzing digital evidence against using unrealistic standards that further confuse and obfuscate the truth of the evidence. However, the absence of standards and robust guidelines is unhelpful to investigators and legal practitioners and by association, the management of organizations.

Implications for Business Managers

This section looks at the implications of digital evidence for business managers. Fundamentally, poor perception of cyber crime and the impact of illegal actions themselves on a business are most likely to be problems, rather than apathy on the part of business managers, who take their responsibility for protecting information

assets as seriously as their other responsibilities. Protective security of vital assets is obviously important but this needs to be considered in broader terms than is commonly considered as best-practice. For example, a major change in thinking by organizations is needed to see if security can be enhanced in advance of a crime, rather than treated as an after-thought in routine security strategies or as an ineffective, reactive remedy after a disaster (Williams, 2002). Certainly, complementary to computer and information security, cyber forensic planning should form a key part of an organization's risk management strategy.

While the relevance of computer forensics to information security is gaining recognition in IT circles, due to its technical nature, it is often misunderstood and undervalued by organizations (Quinn, 2005; Volonino, 2003). According to Quinn and Rowlingson (2004), an enhanced understanding by business managers of some of the common difficulties in preserving, locating, selecting, and validating digital evidence, can help organizations significantly enhance the worth of digital evidence in legal cases and employee disciplinary hearings. Moreover, recognition and tightening of poorly configured computer and network security reduces the likelihood that the value of digital evidence will be diminished, thereby minimizing potentially undesirable consequences (Quinn).

There does appear to be some awareness by more prudent organizations that they will benefit from some forensic strategies included in their security risk contingency planning. Well-conceived strategies recognize the potential value of digital evidence to an organization and ensure that it is gathered and secured at the time of a crime or when a security breach occurs. Such foresight must benefit an organization by better preserving potential evidence, whilst minimizing the costs of future investigations and the likelihood of more favorable outcomes for an organization (Rowlingson, 2004). Questions also arise over whether straightforward means exist to validate how effectively built-in security processes preserve evidence. It would be advantageous to be able to tender digital evidence with reliable knowledge of how well the measures in place do, in fact, preserve its admissibility and evidentiary weight. But how well do organizations understand the effectiveness of their own security measures for that purpose?

As Ghosh (2004) points out, cyber forensic specialists serve the law and technology, and while management of digital evidence is a cross-disciplinary practice, there are some common principles that can help business managers deal with digital evidence. Firstly, there is an obligation to provide records that:

- Understand regulatory, administrative and best-practice obligations to produce, retain, and provide records
- Understand the steps that can be taken to maximize the evidentiary weighting of records and the implications of not doing so

- Understand regulatory constraints to the retention and provision of records.

Secondly, Ghosh suggests that computer systems, procedures and documentation must be capable of establishing:

- The authenticity and alteration of electronic records
- The reliability of computer programs generating such records
- The time and date of creation or alteration
- The identity of the author of an electronic record
- The safe custody and handling of records.

Great difficulties confront organizations that are unprepared for the eventuality that their information holdings and computer networks may be accessed by external authorities to retrieve digital evidence. Rowlingson (2004) attempts to address this in a ten-step forensics readiness programme, which are:

- Define the scenarios that require digital evidence
- Identify available sources and different types of potential evidence
- Determine the evidence requirement
- Establish a capability for securely gathering legally admissible evidence to meet the requirement
- Establish a policy for secure storage and handling of potential evidence
- Ensure monitoring is targeted to detect and deter major incidents
- Specify circumstances when escalation to a full formal investigation should be launched
- Train staff in incident awareness
- Document an evidence-based case describing the incident and its impact.
- Ensure legal review to facilitate action in response to the incident.

Organisations should also consider the need for forensic readiness within the contemporary security culture and budgetary climate (Rowlingson, 2004). Using existing risk assessment standards, such as ISO17799, can form a base for implementing a forensic contingency strategy but do not cover many areas of cyber forensics where digital evidence may be required. Even when responding to discovery in civil litigation cases in something ostensibly straightforward as a litigant's request for an internal email can be a time consuming and costly exercise (Volonino, 2003). Searching for an email may be a relatively simple and quick process, or it may require exhaustive searches through large datasets that may need culling of confidential and non-relevant material (Sleek, 2000). In the Monica Lewinsky case, the

cost of undertaking a search of relevant email files cost in excess of US$17 million (Streza, 2003).

Organisations might also consider employing the services of a Computer Incident Response Team (CIRT) in the event of an incident that requires a professional investigation and response under pre-established practice and standards (Stephenson, 2000). A CIRT investigates computer security incidents, manages evidence collection, interviews witnesses, and stabilises the business operations, by providing some forensic contingency planning for an effective response when needed (Stephenson). However, not all organisations can afford the services of in-house or external teams of computer forensic investigators. Many of the business managers and IT personnel are unlikely to possess sufficient understanding, let alone experience of dealing with digital evidence. A few tertiary institutions offer cyber forensic courses but there is no consensus on curriculum requirements that meet industry expectations (Kruse & Heiser, 2002). University IT departments generally turn out graduates able to deal with incident response against activities, rather than skills suitable for forensic investigation, and not necessarily rounded IT security professionals with forensic understanding and useful skills. Perhaps computer application and systems designers, in tandem with academic researchers, could consider widening their research and incorporating some processes, such as suggested by Spenceley (2003) that would enhance the identification and preservation of digital evidence, so that validation is a less tortuous task.

CONCLUSION

This chapter has characterized digital evidence, outlined the investigative and legal processes used to prepare it for a legal case, and has described how digital evidence fits into the legal domain. The challenges to business managers in dealing with digital evidence are many, but these can be overcome. Difficulties confront business managers and non-specialists. They are often the unwitting custodians of digital information, with limited understanding of computer security and cyber forensic methods. They may be unaware that illegal or improper use of their information has taken place. Organizations need to be cognizant of the complexity and difficulty in locating and using digital evidence, and be well prepared that measures are in place to protect the validity and preservation of the evidence. Such unpreparedness makes it difficult to determine what needs preserving for later use, and how that can be achieved without contaminating and diminishing its admissibility and evidentiary weight.

In addition, businesses relying on the legal fraternity need to recognize that most courts and lawyers still have a limited understanding of these issues. This lack of

understanding can be further compounded by courts, legislators, and governments that make bad legal decisions. Such outcomes perhaps erode natural justice with the attendant negative implications for organizations mounting or defending legal battles. Explaining to the courts the technical complexities of digital evidence used in a legal case, might very well result in bad decisions for an organization. Reliance on a costly technical team may be a burden to many organizations, and even if such expertise is available, the outcome of a case is far from assured. Tightly-configured security of computer networks is more likely to satisfy the courts that the storage of digital evidence is of a high standard and enhance the likelihood of evidence being admissible and retaining its weight. The process of validating the security configuration of systems, and the digital evidence itself, is a further highly desirable enhancement, worthy of endorsement by professional and cyber forensic investigators. An understanding of the nature and complexity of digital evidence will enable business managers to develop contingencies to meet these aims, or at least minimize any potentially adverse consequences.

ACKNOWLEDGMENT

I would like to acknowledge and extend my sincere gratitude to my colleagues Dr. Val Hobbs and Dr. Graham Mann who have supported me and guided me in preparing this chapter, and empowered me to undertake other challenging ventures in the field of digital evidence validation.

REFERENCES

Adelstein, F. (2006). Live forensics: Diagnosing your system without killing it first. *Communications of the ACM*, *49*(2), 63–66. doi:10.1145/1113034.1113070

Afyouni, H. A. (2006). *Database security and auditing: protecting data integrity and accessibility*. Boston: Thomson Learning Inc.

Ahmad, A. (2002). The forensic chain of evidence model: Improving the process of evidence collection in incident handling procedures. *The 6th Pacific Asia Conference on Information Systems*.

Akester, P. (2004). Internet law: authenticity of works: authorship and authenticity in cyberspace. *Computer Law & Security Report*, *20*(6), 436–444. doi:10.1016/S0267-3649(04)00088-3

Ashcroft, J. (2001). *Electronic crime scene investigation: A guide for first responders*. Washington: U.S. Department of Justice.

Australian Law Reform Commission. (2005). *ALRC Discussion Paper 69*. Canberra: Australian Law Reform Commission.

Baraani-Dastjerdi, A., Pieprzyk, J., & Satavi-Naini, R. (1996). *Security in databases: a survey study*. Wollongong: Unpublished Survey, University of Wollongong.

Baryamureeba, V., & Tushabe, F. (2006). The Enhanced Digital Investigation Process Model. *Asian Journal of Information Technology*, *5*(7), 790–794.

Berk, R. A. (1983). An introduction to sample selection bias in sociological data. *American Sociological Review*, *48*, 386–398. doi:10.2307/2095230

Bertino, W., Jojodia, S., & Samarati, P. (1993). Access controls in object-oriented database systems: some approaches and issues . In Bhargava, N. A. A. B. (Ed.), *Advanced Database Concepts and Research Issues* (*Vol. 759*). Springer-Verlag.

Berwick, D. R., & Thompson, D. E. (1998). *Minimum provisions for the investigation of computer based offences (No. 1320-5579)*. Payneham, South Australia: National Police Research Unit.

Boddington, R. G., Hobbs, V. J., & Mann, G. (2008). *Validating digital evidence for legal argument.* Paper presented at the SECAU Security Conferences: The 6th Australian Digital Forensics Conference, 1st - 3rd December 2008, Perth, WA.

Caloyannides, M. A. (2001). *Computer forensics and privacy*. Norwood, Minnesota: Artech House.

Caloyannides, M. A. (2003). Digital evidence and reasonable doubt. *IEEE Security and Privacy*, *1*(6), 89–91. doi:10.1109/MSECP.2003.1266366

Carrier, B. (2005). *File system forensic analysis*. Upper Saddle River, New Jersey: Addison-Wesley.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*.

Casey, E. (2000). *Digital evidence and computer crime: Forensic science, computers and the Internet*. London: Academic Press.

Casey, E. (Ed.). (2002). *Handbook of computer crime investigation: forensic tools and technology*. London: Elsevier Academic Press.

Casey, E. (2007). What does "forensically sound" really mean? *Digital Investigation*, *4*(2), 49–50. doi:10.1016/j.diin.2007.05.001

Castano, S., Fugini, M., Martella, G., & Samarati, P. (1995). *Database Security: Addison-Wesley*. ACM Press.

Cohen, F. (2006). Challenges to digital forensic evidence. Retrieved June 22, 2006, from http://all.net/Talks/CyberCrimeSummit06.pdf

Coleman, C., & Sapte, D. W. (2003). Cyberspace security: securing cyberspace: new laws and developing strategies. *Computer Law & Security Report*, *19*(2), 131–136. doi:10.1016/S0267-3649(03)00208-5

Computer Crime. (1979). *Criminal Justice Resource Manual*. United States: United States Department of Justice.

Demougin, D., & Fluet, C. (2006). Preponderance of evidence. *European Economic Review*, *50*(4), 963–976. doi:10.1016/j.euroecorev.2004.11.002

Devitt, E. J., & Blackman, C. B. (1977). *Federal Jury practice and instructions* (3rd ed.). St. Paul, Minnesota: West Publishing.

Diaconis, P., & Mosteller, F. (1989). Methods for studying coincidences. *Journal of the American Statistical Association*, *84*, 853–861. doi:10.2307/2290058

Edwards, K. (2005). Ten things about DNA contamination that lawyers should know. *Criminal Law Journal*, *29*(2), 71–93.

Etter, B. (2001, 21-22 June). *Computer crime.* Paper presented at the 4th National Outlook Symposium on Crime in Australia - New Crimes or New Responses, Canberra.

Flusche, K. J. (2001). Computer forensic case study: Espionage, Part 1 Just finding the file is not enough! *Information Security Journal*, *10*(1), 1–10. doi:10.1201/1086/43313.10.1.20010304/31394.6

George, E. (2004). Trojan virus defence: Regina v Aaron Caffrey, Southwark Crown Court. *Digital Investigation*, *1*(2), 89. doi:10.1016/j.diin.2004.04.005

Ghosh, A. (2004). *Guidelines for the management of IT evidence*. Paper presented at the APEC Telecommunications and Information Working Group 29th Meeting. Retrieved 5 October 2009 from http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

Gong, R., & Chan, K. Y. (2005). Case-relevance information investigation: Binding computer intelligence to the current computer forensic framework. *International Journal of Digital Evidence*, *4*(1), 1–13.

Halleck, J. (1996). Administrator ethical dilemma. Retrieved 23 June 2005, from http://www.cc.utah.edu/%7Enahaj/ethics/administrator.html

Hoar, S. B. (2001). *Identity theft: The crime of the New Millennium* (Vol. 49).

Jordan, E., & Silcock, L. (2005). *Beating IT risks*. Chichester: John Wiley & Sons Ltd.

Koehler, J. J., & Thompson, W. C. (2006). *Mock jurors' reactions to selective presentation of evidence from multiple-opportunity searches*. American Psychology-Law Society: Division 41 of the American Psychological Association.

Kruse, W. H. J. (2002). *Computer forensics: Incident response essentials*. Indianapolis: Addison-Wesley.

Leiwo, J. (1999). *Observations on information security crisis*. Bangkok: King Mongkut's Institute of Technology.

Lemos, R. (2008). Lax security leads to child-porn charges [Electronic Version]. *Security Focus*. Retrieved 22 November 2008 from http://www.securityfocus.com/brief/756.

Luddy, W. J. Jr, & Wolk, S. R. (1986). *Legal aspects of computer use. Prentice Hall*. Prentice Hall.

Marcella, A. J., & Greenfield, R. S. (Eds.). (2002). *Cyber forensics: A field manual for collecting, examining and preserving evidence of computer crimes*. Boca Raton, Florida: CRC Press Ltd.doi:10.1201/9781420000115

Mattord, H. J., & Whitman, M. E. (2004). *Management of information security*. Boston: Thomson learning.

Mercuri, R. (2005). Challenges in forensic computing. *Communications of the ACM*, *48*(12), 17–21. doi:10.1145/1101779.1101796

Meyers, M., & Rogers, M. (2004). Computer forensics: The need for standardization and certificate. *International Journal of Digital Evidence*, *3*(2).

Mocas, S. (2004). Building theoretical underpinnings for digital forensics research. *Digital Investigation*, *1*(1), 61–68. doi:10.1016/j.diin.2003.12.004

Mohay, G. M. (2003). *Computer and intrusion forensics*. Boston: Artech House Inc.

Morris, G. (1990). *Computer security and the law*.

Myers, R. D., Reinstein, R. S., & Griller, G. M. (1999). Complex scientific evidence and the jury. *Judicature Genes and Justice: The Growing Impact of the New Genetics on the Courts, 83*(3).

Nezovic v Minister of Immigration and Multicultural and Indigenous Affairs (2003).

Palmer, G. L. (2001). *A road map for digital forensic research.* Paper presented at the First Digital Forensic Research Workshop (DFRWS), Air Force Research Laboratory, Rome Research Site.

Palmer, G. L. (2002). Forensic analysis in the digital world. *International Journal of Digital Evidence*, *1*(1).

Pospesel, H., & Rodes (jnr), Robert. E. (1997). *Premises and conclusions: Symbolic logic for legal analysis*. New Jersey: Prentice-Hall, Inc.

Quinn, S. (2005). Examining the state of preparedness of information technology management in New Zealand for events that may require forensic analysis. *Digital Investigation*, *2*(4), 276–280. doi:10.1016/j.diin.2005.10.005

Review of the Evidence Act 1995. (2004). Australian Law Reform Commission. Issues Paper 28. Retrieved 5 October 2009 from http://www.austlii.edu.au/au/other/alrc/publications/issues/28/

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Computers & Security*, *23*(1), 12–16. doi:10.1016/j.cose.2004.01.003

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, *2*(3).

Rubinfeld, D. L., & Sappington, D. E. M. (1987). Efficient awards and standards of proof in judicial proceedings. *The Rand Journal of Economics*, *18*(2), 308–315. doi:10.2307/2555555

Saks, M. J., & Koehler, J. J. (2005). The coming paradigm shift in forensic identification science. *Science*, *309*(5736), 892–895. doi:10.1126/science.1111565

Schneier, B. (1996). *Applied cryptography: protocols, algorithms, and source code in C* (2nd ed.). New York: John Wiley Sons, Inc.

Schneier, B. (2000). *Secrets and lies: digital security in a networked world*. New York: Wiley Computer Publishing.

Schneier, B. (2004, August 19, 2004). Opinion: Cryptanalysis of MD5 and SHA: Time for a new standard: Crypto researchers report weaknesses in common hash functions. *Computerworld*.

Silverstone, H., & Sheetz, M. (2007). *Forensic accounting and fraud investigation for non-experts*. New Jersey: John Wiley & Sons, Inc.

Slade, R. (2004). *Software forensics: Collecting evidence from the scene of a digital crime*. New York: McGraw Hill.

Sleek, S. (2000). Good e-recordkeeping saves you money, protects you from liability. *Digital Discovery and e-Evidence, 1*(1), 4-5.

Spenceley, C. (2003). *Evidentiary treatment of computer-produced material: a reliability based evaluation*. Sydney: University of Sydney.

Stambaugh, H., Beaupre, D., Icove, D. J., Baker, R., Cassaday, W., & Williams, W. P. (2000). *State and local law enforcement needs to combat electronic crime*. Retrieved 22 November 2008 from http://www.ncjrs.gov/txtfiles1/nij/183451.txt

Stephenson, P. (2000). *Investigating computer-related crime*. Boca Raton, Florida: CRC Press.

Streza, R. (2003). Discovery unplugged: Should internal e-mails be privileged confidential communications? *Defense Counsel Journal*, *70*(1), 36–41.

Tapper, C. (2004). *Cross & Tapper on evidence* (10th ed.). London: LexisNexis Butterworths.

TheAge. (2005). NSW speed cameras in doubt. August 10.

Thompson, D. E., & Berwick, D. R. (1998). *Minimum provisions for the investigation of computer based offences*. Payneham, South Australia: National Police Research Unit.

Tillers, P. (2005). Picturing factual inference in legal settings. In *Gerechtigkeitswissenschaft: Kolloquium aus Anlass des 70: Geburtstages von Lothar Philipps*. Berlin.

Tobin, W. A., & Thompson, W. C. (2006). Evaluating and challenging forensic identification evidence. *Champion Magazine* (July, p.12).

Unamed. (1994). (H. C. Lee Ed.). *Crime scene investigation*. Taoyuan: Central Police University Press.

Unamed. (1999). *Association of Chief Police Officers: Good practice guide for computer based evidence*. Retrieved 5 October 2009. from. http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

Unamed. (2000). *The virtual horizon: meeting the law enforcement challenges: developing an Australasian law enforcement strategy for dealing with electronic crime: scoping paper*. Paper presented at the Police Commissioners' Conference - Electronic Crime Working Party 2000, Adelaide. Retrieved 5 October 2009 from http://www.acpr.gov.au/publications2.asp?Report_ID=102

Unamed. (2005b). Australian Law Reform Commission: Review of the Evidence Act 1995. Submission E 17. Retrieved 5 October 2009 from http://www.austlii.edu.au/au/other/alrc/publications/reports/102/

Volonino, L. (2003). Electronic evidence and computer records. *Communications of the Association for Information Systems*, *12*, 457–468.

Warren, L. (1997). *Radio National Transcripts: Santa, smog, and speed! The Law Report*. Australia: Australian Broadcasting Corporation.

Whitcomb, C. M. (2002). An historical perspective of digital evidence: A forensic scientist's view. *International Journal of Digital Evidence*, *1*(1).

Whitman, M. E., & Mattord, H. J. (2005). *Principles of information security* (2nd ed.). Boston, Massachusetts: Thomson Learning.

Williams, P. (2002). *Organized crime and cyber-crime: Implications for business*. Retrieved 9 February 2009, from http://www.cert.org/archive/pdf/cybercrime-business.pdf

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer forensics education. *IEEE Security & Privacy*, *1*(4), 15–23. doi:10.1109/MSECP.2003.1219052