3-12-2008

Validating digital evidence for legal argument

Richard Boddington
Murdoch University

Valerie Hobbs
Murdoch University

Graham Mann
Murdoch University

DOI: 10.4225/75/57b269e240cb7
6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2008.

Validating digital evidence for legal argument

Richard Boddington
Murdoch University
r.boddington@murdoch.edu.au

Valerie Hobbs
Murdoch University
v.hobbs@murdoch.edu.au

Graham Mann
Murdoch University
g.mann@murdoch.edu.au

Abstract

Digital evidence is now common in legal cases, but the understanding of the legal fraternity as to how far conventional ideas of evidence can be extended into the digital domain lags behind. Evidence determines the truth of an issue but its weight is subject to examination and verification through existing forms of legal argument. There is a need for a practical 'roadmap' that can guide the legal practitioner in identifying digital evidence relevant to support a case and in assessing its weight. A vital, but sometimes under estimated stage is that of validating the evidence before evaluating its weight. In this paper we describe a process by which the validation of relevant evidence required for legal argument can be facilitated, by an interrogative approach that ensures the chain of reasoning is sustained.

Keywords

Legal argument, digital evidence, weight of evidence, validation of evidence

INTRODUCTION

In this paper we examine the investigative and legal processes involved in preparing digital evidence for use in legal argument and suggest that evidence taken at face value may be injudicious unless its validity is established before it can be used. Validation requires confidence about inferences drawn from the evidence - can that evidence be relied upon in a legal argument? Validating digital evidence requires verification of relevant parts of the digital domain where the evidence is created, processed and transferred, including the evidence file itself, application and operating programmes and the hardware platform. While techniques of digital forensics aid in preserving and locating potential evidence from a crime scene, the extent to which this may be trusted and used as evidence in a particular legal argument still needs to be determined. We suggest that validation of digital evidence, a difficult task for the investigator, poses an even greater challenge to legal practitioners when constructing legal arguments. Legal practitioners may be unaware of the full nature and significance of digital evidence that is more technically complex compared to conventional forms of evidence.

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 the case 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, Howard, & Rodes, 1997, Schneier, 2000, Whitman, 2005, Tapper, 2004, Whitcomb, 2002). This is evident by the growth in computer-based crime that has increased reliance on digital evidence, both as partial evidence in otherwise conventional legal cases, or where the evidence exists entirely in digital form (Etter, 2001a, Thompson & Berwick, 1998, Palmer, 2001, Cohen, 2006). Digital evidence exists in complex technical environments, unfamiliar territory for most legal practitioners who have difficulty determining how far conventional ideas of evidence can be extended into the digital domain (Etter, 2001b, Losavio, Adams & Rogers, 2006, Caloyannides, 2001, Edwards, 2005).

Evidence used in legal cases proves facts that are in dispute and the weight that may be attached to the facts is examined and tested by various forms of legal argument (Anderson & Twining, 1991, Tapper, 2004). Legal argument can be a complex, convoluted process taking in a broad range of evidentiary issues; technically complex digital evidence used in constructing compelling legal arguments makes the process significantly more challenging for the legal practitioner (Caloyannides, 2001, p. 3, Tapper, 2004, pp. 30-31, Mohay, 2003, Wall & Paroff, 2004, Yasinsac, Erbacher, Marks, Pollitt & Sommer, 2003). Few legal practitioners have sufficient technical expertise to analyse digital evidence in case preparation and is difficult for them to present it in simple comprehensible terms to judges and juries; what may seem a potentially successful case based on straightforward legal argument can turn a into a needless failure (Yasinsac et al, 2003). Moreover, developing legal arguments can be frustrated if unskilled use is made of the digital evidence, with unanticipated and often detrimental outcomes. For example, when presenting a legal case based on what appears to be convincing digital evidence, the case can collapse if the defence can show that the security integrity of the network is defective and shows contamination or alteration of the digital evidence it is supposed to protect. Consequently, if the validity of the evidence can be established its weight in legal argument is enhanced; however if its validity is uncertain or invalidated then weight of the evidence is diminished or negated.

THE INVESTIGATIVE AND LEGAL DOMAINS

Figure 1 highlights the processing of digital evidence in the investigative and legal domains. The investigation domain consists of the stages taken by investigators in evidence preservation, location, selection and validation that precede the stages in the legal domain that involve legal practitioners constructing and then presenting legal arguments. This paper focuses on the validation stage, at the interface between the location and selection of evidence by the investigator and its subsequent use by the legal practitioner. We examine the challenges presented to the legal practitioner on receipt of digital evidence and describe a process by which they may assess the validity of the evidence within the context of their argument.

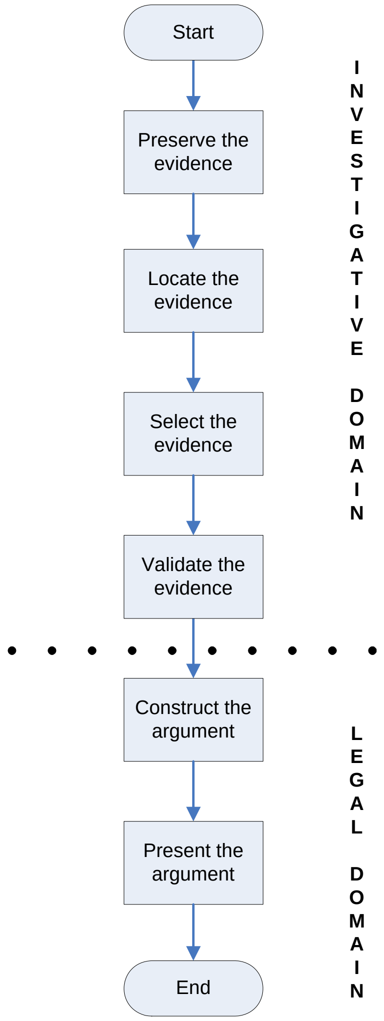


Figure 1. Evidence processing stages in the investigative and legal domains

The stages of the investigation stage shown in Figure 1 commence with the evidence preservation stage that recognises the fragility of digital evidence. Digital evidence can easily be altered, damaged, or destroyed by improper handling or improper examination and so the preservation stage attempts to stabilise and isolate the evidence scene to prevent contamination that damages its admissibility and weight (Ashcroft, 2001, Carrier & Spafford, 2003). The location stage involves locating and identifying the digital evidence for the given class of crime or violation that supports or refutes hypotheses about the incident, using various technical tools and investigative processes to accomplish this (Carrier et al, 2003). During the evidence selection stage the investigator scrutinises the evidence to determine what events occurred in the system and their significance and probative value to the case (Carrier et al, 2003).

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 of the overall integrity of records rather than for specifically validating digital evidence (Carrier, 2005a). 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 et al, 2003).

Inordinate amounts of time and resources are required to collect and analyse digital evidence and the sheer volume of the cases and the time required to process them can have a negative effect on the capacity of investigators - and later legal practitioners - to analyse and present a complete reconstruction of the evidence (Ó Ciardhuáin, 2004). 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 analyse much relevant evidence, time constraints and 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 (unamed, 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, 2006). Carrier (2005a) points out that 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.

False evidence too can be generated upon which unreliable arguments are propounded by those unfamiliar with the true nature of the digital domain (Koehler & Thompson, 2006, Diaconis, 1989). Koehler et al (2006) caution against endeavours to locate circumstantial evidence that seem to support reasonable and compelling argument may well be unreliable because they are purely coincidental and nothing more. Moreover, investigators may miss evidence and worse still, resort to ‘cherry-picking’ when choosing or omitting evidence to gain legal advantage: the absence of evidence does not necessarily show evidence of absence - a common phenomenon of the digital domain (Koehler et al, 2006, Berk, 1983, Flusche, 2001).

There is error in every analysis method and the reliability of any particular test remains an issue for forensic investigators (Palmer, 2002, Cohen, 2006). A range of different factors can affect the validity of the evidence, including collection tools missing, failure 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 (Palmer, 2002, Cohen, 2006). Because of the complexity of the digital domain prosecution cases often fail during trial where incompetency is apparent in reconstructing the case and where validation issues are raised (Cohen, 2006). 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 (Ashley & Rissland, 1985, Perelman and Olbrechts-Tyteca, 1969). A more explicitly defined and repeatable process would be useful for the legal practitioner who may then have more confidence in the evidence derived during the validation stage.

Research to date has focussed on providing investigators with the means to preserve, locate and select digital evidence (Daum & Lucks, 2005, Lenstraand & de Weger, 2005, Schneier, 2004). For the legal practitioner, the research has attempted to enhance analysis of the weight of evidence as part of structuring legal arguments, but with limited adoption of such processes (Tillers, 2005). Computer and network security and digital forensics research provides documentation about the properties of digital evidence but it does not explain in a legal context helpful to the legal practitioner (Spenceley, 2003, Mohay, 2003). The validation of the evidence, however, is largely dependant on the skill and knowledge of investigators.

There is some ongoing legal debate calling for a replacement of conventional forensic identification science that relies on untested assumptions and intuition - including digital forensics - with sounder scientific analysis (Saks & Koehler, 2005, Tobin & Thompson, 2006, Mohay, 2003). 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 (Slade, 2004, Mohay, 2003). Compounding this deficiency is the inefficacy of conventional security processes to preserve digital evidence, for that is not their intended role (Caloyannides, 2001, Rowlingson, 2004, p. 2). Such processes are more often used as forensic tools to investigate a compromise of record integrity or as part of data recovery processes but do go some way towards identifying the evidence and reconstructing a timeline of events (Carrier, 2005a, Egan & Mather, 2004). However, a lack of recognition and acknowledgement by designers, owners and custodians of digital information as to its potential evidentiary importance means that computer system designs fall short of protecting evidence, sometimes preventing it being used as key exhibits (Rowlingson, 2004, p. 2).

Figure 2 lists broad areas of research and practice reported in the literature, highlighting the deficit in the area of validating digital evidence.

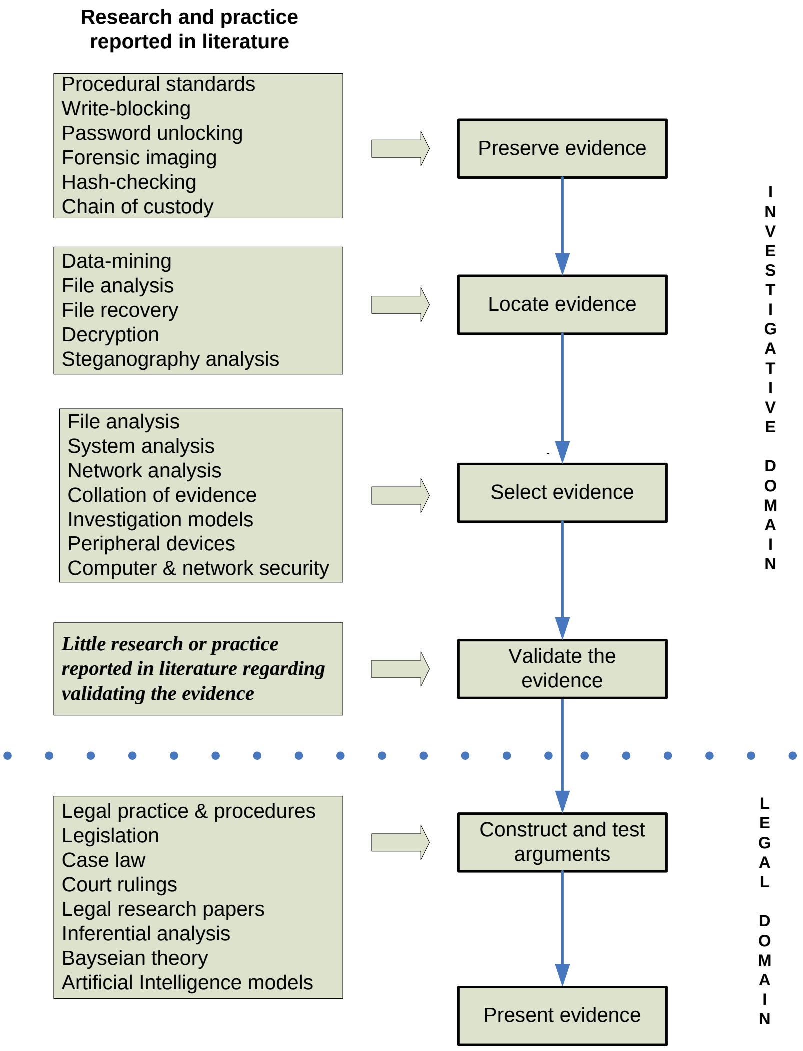


Figure 2. The gap in the research and practice reported in the literature.

Research and practice in the new field of cyber forensics is late in offering practical pedagogical models, leaving investigators to rely solely on their investigative skills and technical knowledge (Yasinsac at al, 2003). For the legal practitioner without firsthand technical skills, some form of practical ‘roadmap’ is needed that can prompt him or her to identify all pertinent digital evidence relevant to a case and help assess the weight of the evidence more effectively. Research attempts to help legal practitioners through such processes as computer-assisted analysis of legal arguments based on evidence reconstruction, and theories including probability theory and inferential analysis (Silverstone & Sheetz, 2007, Huygen, 2002). To date, however, attempts to present the inference processes in diagrammatic form has tended to confuse the legal practitioner rather than promoting a better understanding of the dynamics of digital evidence (Tillers, 2005).

In criminal cases the prosecution, usually a law enforcement agency, has the advantage of government investigators with experience and resources; resources not always available or affordable to the defence: the defence team relies on an outline of the prosecution's case and forensic evidence images so that it can prepare a defence (Mercuri, 2005). Even with some technical help, the defence team may have little understanding of the properties of digital evidence and may not have clear understanding of the relationship between key digital evidence and potential corroborating evidence that could be used to its advantage in developing legal counter-arguments. In civil cases, there may be a more equitable allocation of technical expertise; nonetheless, the legal practitioners would still need additional help with the complexity of digital evidence. An experienced investigator would be unwise to 'second guess' the legal practitioner but may have difficulty explaining the significance and relationship of the various pieces of evidence. The legal practitioner may take the evidence at face value but suffer its eventual overturn by a more technically astute legal opponent. It is during this validation stage that we believe the legal practitioner needs some prompting to minimise this risk.

In this paper, we are concerned specifically with the validation of the evidence, rather than the subsequent process of interpretation. We describe a process of methodical interrogation of the digital evidence that establishes whether it is valid and therefore suitable for use in legal arguments. The process we propose also offers relevant prompts guiding the legal practitioner to supplementary evidence that may corroborate, negate or offer alternative hypotheses about the validity of the evidence.

THE NATURE OF EVIDENCE AND LEGAL ARGUMENT

Evidence used in legal cases may consist of witness testimony, hearsay, documents and things, and proves facts that are in dispute through directly proving the ultimate fact without relying on other evidence to prove any intervening, penultimate steps (Anderson & Twining, 1991, Tapper, 2004). Evidence is also used to prove the plausibility of facts from which facts that are being disputed, may be understood - most notably, circumstantial evidence (Tapper, 2004). Digital evidence shares many common features with conventional forms of evidence yet it is its technical properties that tend to confound the legal practitioner.

The nature of digital evidence

Although electronic evidence is defined as information of investigative value relating to a broad range of devices and data formats (Ashcroft, 2001), a formal legal definition of digital evidence is elusive, but is generally accepted to be information held in digital form that has some probative value (Carrier et al, 2005b, Pollitt, 2001). Digital evidence typical sought in legal cases includes system logs, audit logs, application logs, network management logs, network traffic capture, and file system data (Sommer, 1998).

Digital evidence is often considered superior to conventional paper evidence being easier to locate and process, and also contains useful data containing details of key dates, times and a history of the file, and, because of its persistency in recording key data, can provide evidence that a defendant may prefer not to exist (Caloyannides, 2001, Janes, 2000). Digital evidence tends to provide metadata about itself prior to the fact, more so than paper-based evidence, and this can provide valuable information relating to a crime such as linking a defendant to an offence and showing evidence of intent, ability and opportunity leading up to the commission of the crime (Janes, 2000, Flusche, 2001).

Several authors contend that digital evidence is not fundamentally different from conventional forms of evidence but is problematic because of its volatility, the complexity of the digital domain, large datasets, and rapid changes to technology that require current technical understanding that is certainly beyond the capability of most legal practitioners (Sommer, 2000, Mercuri, 2005).

Other authors point out that there seems little difference between digital evidence and physical evidence as both forms are required to establish the commission of an offence and link the crime and the victim, or provide a link between the offence and the perpetrator (Carrier et al, 2003, Saferstein, 2000). Similarly, in the digital domain there is much merit in using conventional, crime scene investigation techniques; again showing a degree of fundamental similarity between the domains. Carrier et al (2003) provide helpful definitions to put this in better perspective by suggesting that the computer, computer hardware and peripherals are physical evidence, while the data in memory held in these devices is digital evidence.

Circumstantial evidence, which includes digital evidence, is used to construct inferences that indirectly prove the ultimate fact in a legal case (Anderson, 1991) but before it may be admitted or given any credence in legal cases, it must meet additional legal conditions and conform to courtroom conventions (Caloyannides, 2001, p. 3, Tapper, 2004, pp. 30-31). Circumstantial evidence is probabilistic in nature, often challenging and confounding observers attempting to determine the truth of an issue because the examination processes used are poorly defined (Fiske & Taylor, 1991, Nisbett, Krantz, Jepson & Kunda, 1983, Nisbett & Ross., 1980). Digital evidence is analogous to the more conventional forms of circumstantial evidence, most notably documentary evidence, and both forms are subject to the same degree of legal scrutiny afforded to direct evidence tendered by a human witness (Caloyannides, 2001, p. 3, Tapper, 2004, pp. 30-31).

Inherent differences between digital and conventional evidence exist as digital evidence is more easily altered than conventional forms and such manipulation is sometimes not evident or even possible to detect (Caloyannides, 2001). Digital evidence is mutable – it may be altered far more easily than physical records – and consequently is more susceptible to unauthorised manipulation, making it problematic to validate its admissibility and weight (Schneier, 2000, Mattord & Whitman, 2004, Akester, 2004).

Inaccuracies in attribution of authorship and the content of digital evidence occur frequently and affect legal argument as to the completeness, correctness, validity and faithfulness to an original source, thereby raising doubts as to the worth of the evidence (Akester, 2004, p. 436). More disturbing is that even in the absence of any obvious irregularity of the software platforms examination of any material of evidentiary value does not in itself attest to the accuracy or integrity of the evidence (Spenceley, 2003, pp. 130-131). The more pessimistic argue that it cannot be assumed that there is a low risk of inaccuracy in computer output due to application failures (Spenceley, 2003, pp. 130-131).

Representing 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 (Silverstone et al, 2007). 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 et al, 2007). Further discussion of legal argument and its forms is beyond the scope of this paper.

Legal arguments are based on logical probabilities that collectively prove the case and are constructed from the simplest logic possible and may be mapped, for example by a timeline of reconstructed events, or through inferential analysis processes (Silverstone et al, 2007). The use of such processes displayed in graphic form makes the evidence collected more readily comprehensible with relevant evidence arranged as coherent discreet lines leading to the ultimate probandum.

It is unusual for legal cases to rely solely on circumstantial evidence; direct evidence such as witness testimony may corroborate, refute or obfuscate whether the defendant accessed the computer, etc. Therefore, an inferential analysis should include wherever possible evidence of direct evidence, physical evidence such as a fingerprint linking the defendant to the computer as well as the digital evidence. Locating this supplementary evidence, often intuition-based, helps develop argument and strengthen the overall weigh of available evidence. The weight of the evidence depends on the various relationships between penultimate probanda and the reliability of each probanda (Silverstone et al, 2007).

Figure 3 shows a simple chain of evidence based on apparent or available evidence consisting of unprocessed facts from which tentative legal argument can be constructed.

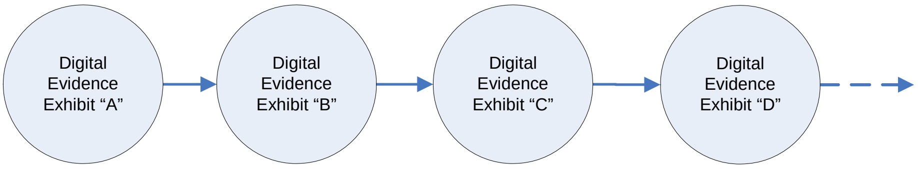

Digital Evidence Exhibit “A”
Digital Evidence Exhibit “B”
Digital Evidence Exhibit “C”
Digital Evidence Exhibit “D”

Figure 3. Chain of Evidence: Before validation of the evidence

This amount of preliminary evidence is readily comprehensible to legal practitioners but is most likely incomplete. 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. 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 will be well served. But the legal practitioner must be able to determine whether enough evidence has been located and whether the validity of the digital of evidence has been satisfactorily described and determined.

A PROCESS FOR VALIDATION OF DIGITAL EVIDENCE

The interrogation process

Figure 4 outlines the basic validation interrogation process where exhibit B, taken from the chain of evidence example in Figure 3 requires validation.

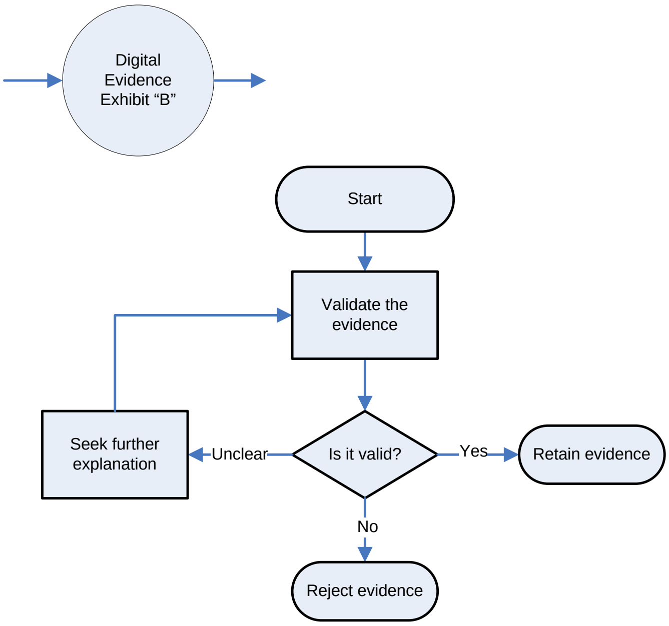


Figure 4. Chain of Evidence: Showing the validation process of digital evidence exhibit “B”.

A series of prompts determines if the evidence is valid. Each prompt requires a response of ‘yes’ (the evidence can be considered valid), ‘no’ (the evidence is invalid) or ‘unclear’, (suggesting that further explanation should be considered). The “yes” and “no” outcomes are considered definitive, the “yes” indicating that the evidence can be retained and a “no” indicating that the evidence should be rejected. An “unclear” result is inconclusive and requires a further explanation to provide clarification to establish if the evidence is valid. Where further explanation continues to be inconclusive, a decision to terminate the process is required and at that point, the expertise of the legal practitioner will be required to retain or to reject the evidence based on the available validation evidence.

Each piece of digital evidence considered for inclusion in legal argument is judged on the weight of inference of at least one assertion used, for example, whether the existence of the deleted email file does infer the view that there was an attempt to conceal evidence. In other words, an assertion claims deliberate deletion of the email file with intent to remove all trace of the evidence. As evidence-based assertions are contestable, it is critical to establish their validity.

Figure 5 shows a graphic decomposition of assertions provided by a digital evidence exhibit and the systematic process required to determine its validity. Each assertion is evaluated to determine whether it is confirmed or negated by other available evidence. Each circle in Figure 5 represents an assertion underpinning the evidence, for instance "the defendant accessed a file on a computer". The primary assertion 1 requires confirmation or negation, provided by the secondary assertions 2 and 3. For example "the deleted email file existed" requires validation. The file metadata may or may not confirm the assertion and the assertion the metadata provides may itself need further confirmation by other assertions and so forth until the interrogation is considered sufficiently strong to support the primary assertion.

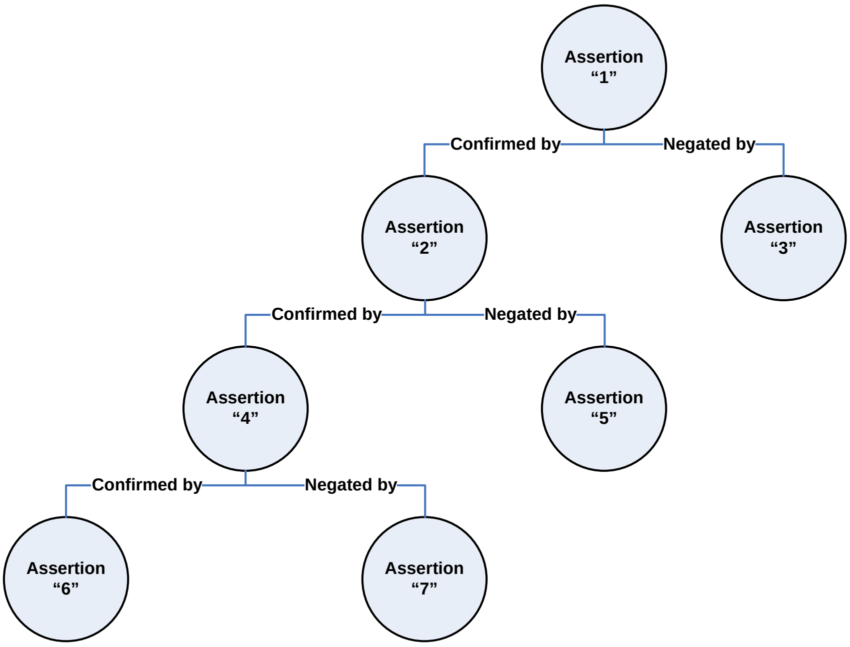


Figure 5. Decomposition of the evidence through validation process

Figure 6 shows an example of a chain of evidence where the evidence has been validated.

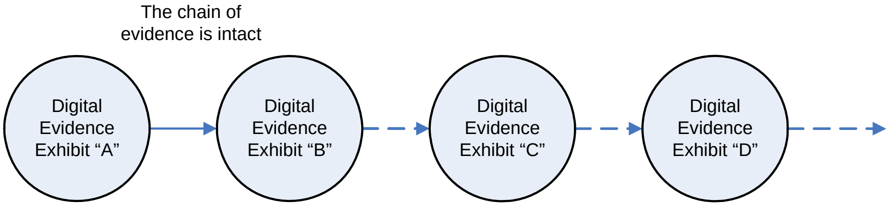

The chain of evidence is intact
Digital Evidence Exhibit "A"
Digital Evidence Exhibit "B"
Digital Evidence Exhibit "C"
Digital Evidence Exhibit "D"

Figure 6. Chain of evidence: After validation of digital evidence exhibit "B" is achieved.

Conversely, the primary assertion may be negated from the outset or at a later point, breaking the chain of evidence as shown in Figure 7.

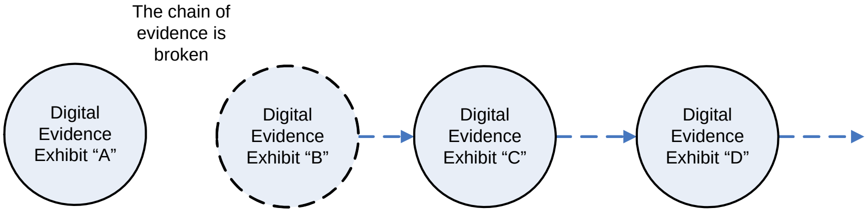
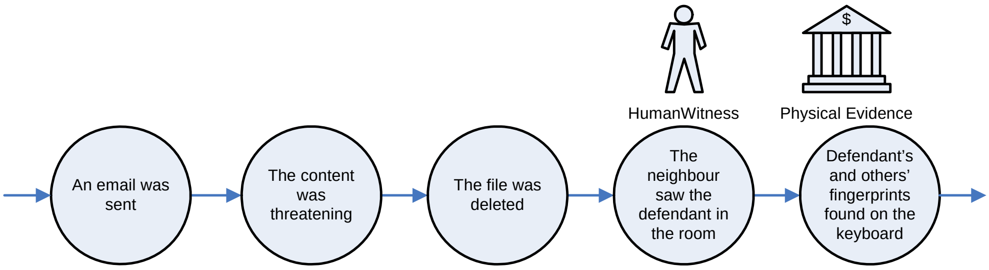

The chain of evidence is broken
Digital Evidence Exhibit "A"
Digital Evidence Exhibit "B"
Digital Evidence Exhibit "C"
Digital Evidence Exhibit "D"

Figure 7. Chain of evidence: After validation of digital evidence exhibit "B" is negated.

Example

We present a hypothetical case to demonstrate the validation process. Consider a case involving a defendant accessing a computer and sending a threatening email to another party, then deleting the email in an attempt to conceal the evidence on the computer. A neighbour witnessed the defendant inside the room at the time of the suspected offence, and police recovered the defendant's and other persons' fingerprints from the computer keyboard, as shown in Figure 8.



HumanWitness
Physical Evidence
$
An email was sent
The content was threatening
The file was deleted
The neighbour saw the defendant in the room
Defendant's and others' fingerprints found on the keyboard

Figure 8. Hypothetical case showing digital, human and physical evidence

If we look at one piece of the evidence, that the file was deleted, it would be prudent to find out the processes involved and whether it was possible to link the date and time of the deletion to the defendant's known presence in the room. In our hypothetical example, we seek explanations about key properties of the file evidence. We need to find out the nature of the pertinent evidence, in this case the email application properties and from that, attempt to validate the date and time of the file deletion, and then view the outcomes of that examination.

If we decompose the hypothetical case, it shows that the validation of the evidence can be a lengthy and complex process. In Figure 9 we examine the deleted file and drill down through each sub-set of evidence that provides assertions attesting to the validity of the evidence at the higher level. We expect to reach a conclusion that is acceptable in the legal practitioner's opinion as validation of the primary assertion corroborated by supporting evidence.

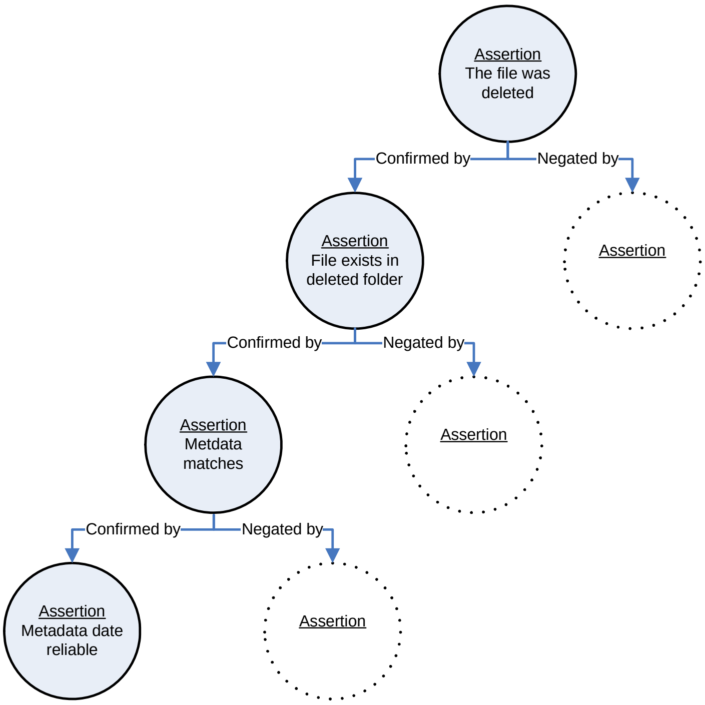


Figure 9. Hypothetical case decomposition showing the validation of assertions

Figure 10 shows an alternative path in which the decomposition established that the evidence was invalid through the absence of corroborating evidence at the fourth secondary assertion.

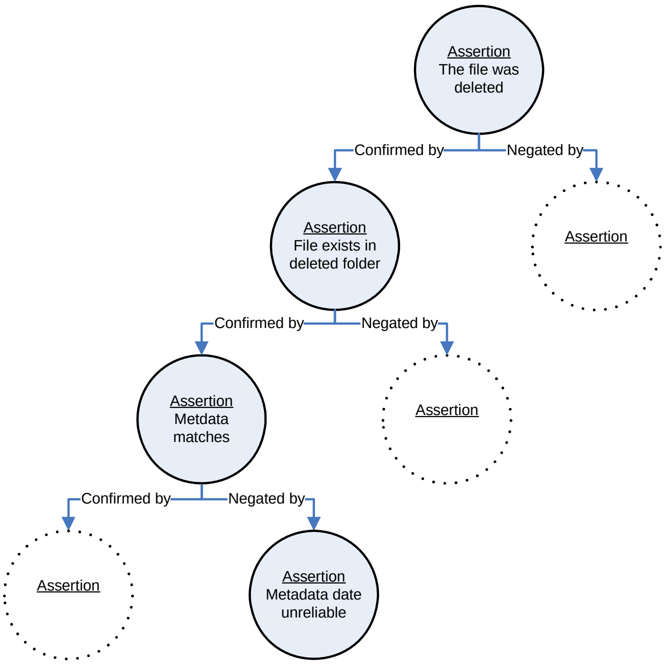


Figure10. Hypothetical case decomposition showing the invalidation of assertions

Figure 11 shows an alternative scenario where an anomaly existed about the validity of email file metadata matching the time of the suspected deletion. This required further explanation confirming modification of the metadata by virus scanning activity.

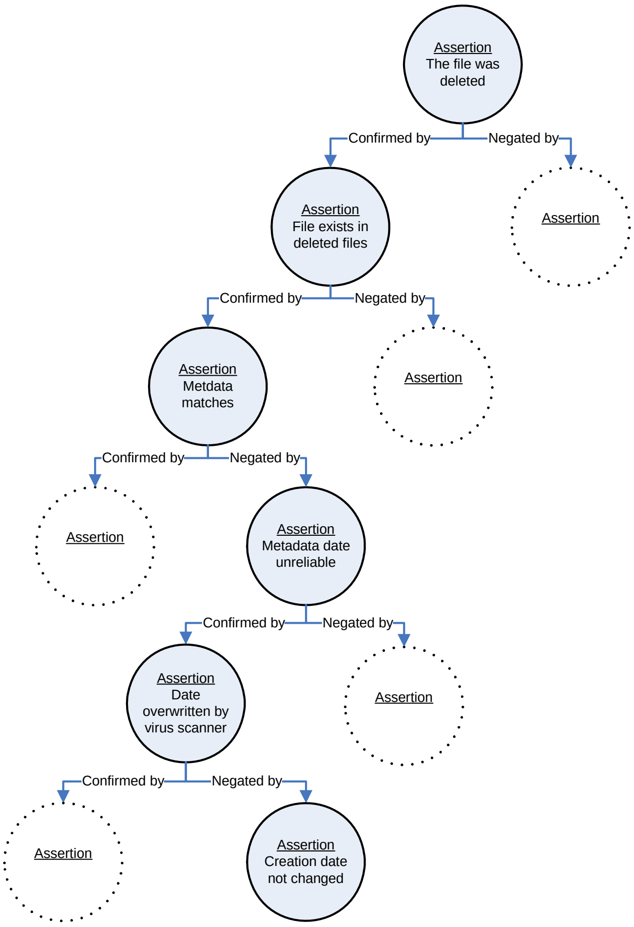


Figure 11. Hypothetical case decomposition showing the validation of assertions by drilling down through negative assertions

Further explanation showed that the virus scanning activity did not alter the actual date and time of deletion of the email file and thus validity is sustained. This scenario emphasises the importance of searching for evidence that negates an assertion as well as seeking confirmation.

Although potentially many questions about the evidence exist in our hypothetical and relatively simple example, the number of questions may increase exponentially in complex cases. The process of decomposing the original hypothetical evidence uncovered additional evidence clarifying the truth of the original bland assertion about the file deletion. While this was a positive outcome, one path of validation did identify a negative assertion but this was later nullified by other evidence, thus demonstrating the complexity of the digital domain.

Using the decomposition of the simulated result in Figure 11 the chain of evidence gained more pieces of validated evidence to replace the simple assertion that a deleted file existed. The decomposition ended with the assertion confirming the validity of the creation date of the deleted file and for the sake of brevity, we have not decomposed the process further. So, accepting the new evidence, the chain of evidence may be modified with validated evidence that is also more complete as shown in Figure 12.

The validation process described has identified a possible weakness in the evidence regarding a critical time, the date and time of the file deletion. It is an important part of the legal argument to be able to state categorically the exact time of deletion, but future counter-argument can be dispelled because it can be shown that only partial modification occurred which does not weaken the assertion about the deletion time. The process has validated the evidence providing clarification that allows the legal practitioner to gain a far greater understanding of the strengths and weaknesses of the evidence available.

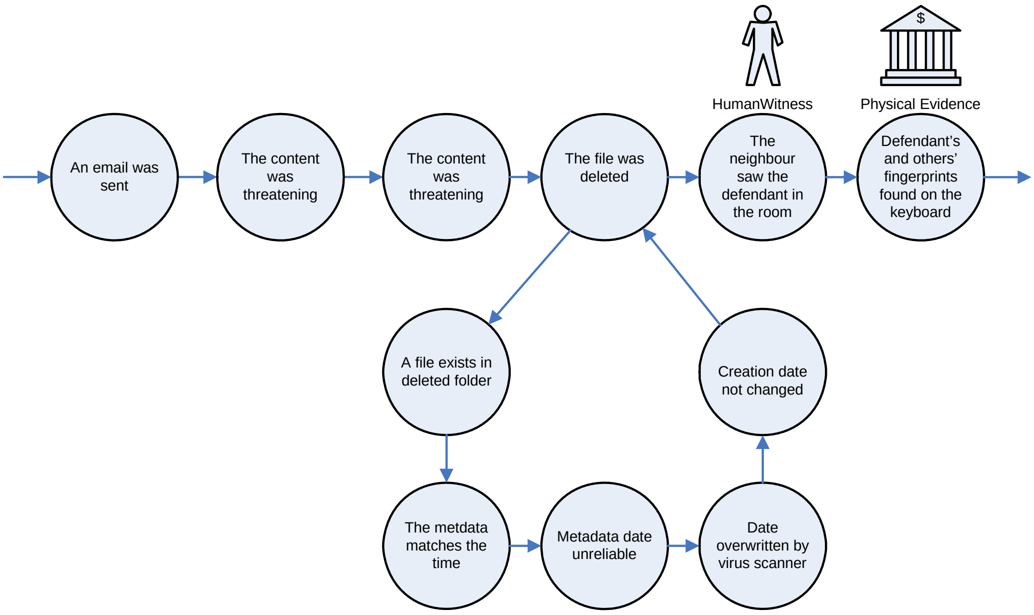

HumanWitness
Physical Evidence
$
An email was sent
The content was threatening
The content was threatening
The file was deleted
The neighbour saw the defendant in the room
Defendant's and others' fingerprints found on the keyboard
A file exists in deleted folder
Creation date not changed
The metdata matches the time
Metadata date unreliable
Date overwritten by virus scanner

Figure 12. Hypothetical case: modified chain of evidence after validation

The search for validation shown in the hypothetical example assumes that the enquirer has both investigative and technical skills but the legal practitioner may be unable to know what questions to ask to test the validity of the evidence. In the next section we describe how we may assist the legal practitioner in seeking relevant information by providing prompts at each step of the process.

An interrogation checklist

To assist the legal practitioner, it is useful as part of the validation interrogation process to provide prompts that firstly provide explanation about the properties of digital evidence, and secondly alert the legal practitioner when further validation of the digital evidence is prudent. Providing an interrogation checklist of digital evidence properties that offers a suite of prompts would enable the legal practitioner to make more discerning judgement on the weight of evidence knowing that is has been validated or invalidated, or needs more research to a point of reasonable termination of endeavour.

An interrogation checklist, which supplements the validation interrogation process, supplies prompts to direct enquiry to seek facts confirming or negating the validity of the evidence. The enquirer has two options, to seek confirmation of validity or to seek negation. These two options offer separate search patterns for the legal practitioner who may seek validation of incriminating evidence, or wishes to develop an alternative hypothesis as part of a counter-argument. We suggest that this system has the advantage of being more inclusive because it would cover a broader range of potential evidence overlooked in the selection and validation stages of the investigation process shown in Figure 1.

Table 1 provides a small example of the proposed checklist based on the hypothetical case. A set of categories - “subject”, “assertion”, several “prompts” and “known issues” – guides the legal practitioner to identify and locate corroboratory evidence to validate each piece of evidence. Using the example of the hypothetical case, the email is the subject of the validation process and the occurrence of file deletion, the assertion. The first prompt provides the enquirer with a list of file locations to commence a search. The second prompt suggests what tool should be used, such as the email application, and the third prompt provides a range of information that should be sought with the tools suggested and at the location suggested. The fourth prompt suggests conditions that could assist in validating the assertion.

Subject	**Assertion**	**Prompt** **Where to search?**	**Prompt** **How to search?**	**Prompt** **What to seek?**	**Prompt** **How do we know if : Yes / No / Unclear?**	**Known issues**
Email	[Email was] Copied	Application	Search tool	Metadata	Date/time match	Metadata can be falsified
					No date/time match	
					Date/time missing	
	[Email was] Deleted	**Email trash**	**Application**	**Metadata**	**Date/time match**	**Retention affected by storage limitations**
					No date/time match	
					Date/time missing	
		Recycle bin	**Windows Explorer** **or** **Forensic tool**	**File contents**	**Intact**	**File can be overwritten**
					Not evident	
					Part missing	
					Intact	**File can be unrecoverable**
					Not evident	
					Part missing	
				File header	**Intact**	**File can be overwritten**
					Not evident	
					Part missing	
					Intact	**File can be unrecoverable**
					Not evident	
					Part missing	
		Drafts	**- ditto -**	**- ditto -**	**- ditto -**	**- ditto -**

Table 1. Checklist entries showing prompts to assist in validating an email file deletion

In this sample, the assertion can be checked against the metadata of the email file to compare the data and time available with the known time of the offence. This prompt provides “Date/time match”, “No date/time match”, and “Date/time missing”. The final column “Known issues”, provides supplementary information about previously identified validation issues.

Subject	**Assertion**	**Prompt** **Where to search?**	**Prompt** **How to search?**	**Prompt** **What to seek?**	**Prompt** **How do we know if : Yes / No / Unclear?**	**Known issues**
Deleted email metadata	**Falsified**	**Inside the file properties table**	**Application**	**Authorship details**	**Present**	**Not possible to detect manual alteration of the properties using the parent application**
					Not present	
					Cannot resolve if present	
		The hard drive	**Forensic tool**	**File attribute modification application**	**Traces of the application**	
					No traces of the application	
					Unclear if traces of the application	
		Inside the application		**Other copies of the file**	**Metadata match**	
					Metadata mismatch	
					Metadata irregular	

Table 2. Checklist entries relevant to the metadata of an email file.

The information supplied through Table 1 may still be an inconclusive result but will provide additional prompts to direct further searches in a different part of the checklist to locate more information to assist the validation process. This is shown in Table 2 where a series of further prompts point to possible scenarios that may relate to the deleted email file. The validation prompt offers an extra suite of prompts such as “metadata mismatch” or “traces” and so forth.

Although it is outside the scope of this paper to develop fully the checklist we plan further research to test its feasibility and usefulness to the legal practitioner and possibly investigators in validating digital evidence. Formulating a database of digital evidence properties that can link back to the evidence in a given context would be especially useful in enhancing understanding of the evidence validation in a wide range of cases.

CONCLUSION

We have presented a practical process that can assist legal practitioners in validating digital evidence through a process of guided questioning. We suggested that the process can be supported by a checklist of appropriate prompts, and presented a hypothetical example of how the questioning and checklist of prompts might be used in practice. We suggest that such a process could be of great value to legal practitioners as it makes explicit a vital stage in the investigation of digital evidence that can easily be overlooked or underestimated. Further research is planned to progress the checklist further, with the aim of developing a generic model based on an ontology of the digital evidence field. Research will also focus on developing an appropriate representation for the process, so that it is usable as a practical tool for legal practitioners in validating digital evidence.

REFERENCES

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**,** 436-444.

Anderson, T., & Twining, W (1991) *Analysis of evidence: How to do things with facts based on Wigmore's Science of Judicial Proof,* Evanston, IL, Northwestern University Press.

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

Ashley, K., & Rissland, E. (1985) Toward modelling legal argument. University of Massachusetts.

Berk, R. A. (1983) An introduction to sample selection bias in sociological data. *American Sociological Review,* 48**,** 386 - 398.

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

Carrier, B. (2005a) *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.*

Carrier, B. D., & Spaford, Eugene. H. (2005b) Automated digital evidence target definition using outlier analysis and existing evidence. *Digital Forensic Research Workshop.* New Orleans.

Cohen, F. (2006) Challenges to digital forensic evidence. New Haven, Fred Cohen & Associates.

Daum, M., & Lucks, Stefan. (2005) Attacking hash functions by poisoned messages: The Story of Alice and her boss. Bochum, CITS Research Group, Ruhr-Universität Bochum.

Diaconis, P., & Mosteller, F. (1989) Methods for studying coincidences. *Journal of the American Statistical Association,* 84**,** 853 - 861.

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

Egan, M., & Mather, Tim (2004) *The executive guide to information security: Threats challenges and solutions,* Indianapolis, Addison-Wesley:Symantec Press.

Etter, B. (2001a) Computer crime. *4th National Outlook Symposium on Crime in Australia - New Crimes or New Responses.* Canberra, Australian Institute of Criminology.

Etter, B. (2001b) The forensic challenges of e-crime. *Australasian Centre for Policing Research,* 3**,** 1-8.

Fiske, S. T., & Taylor, S. E (1991) *Social cognition* New York, McGraw-Hill.

Flusche, K. J. (2001) Computer forensic case study: Espionage, Part 1 Just finding the file is not enough! *Information Security Journal,* 10**,** 1 - 10.

Huygen, P. E. M. (2002) Use of Bayesian Belief Networks in legal reasoning. *17th BILETA Annual Conference.*

Janes, S. (2000) The role of technology in computer forensic investigations. *Information Security Technical Report,* 5**,** 43 - 50.

Koehler, J. J., & Thompson, William. 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.

Lenstraand, A., & De Weger, Benne. (2005) On the possibility of constructing meaningful hash collisions for public keys. *Australasian Conference on Information Security and Privacy 2005.* Brisbane, Lucent Technologies, Bell Laboratories, and Technische Universiteit Eindhoven.

Losavio, M., Adams. J., & Rogers, M. (2006) Gap Analysis: Judicial experience and perception of electronic evidence. *Journal of Digital Forensic Practice,* 1**,** 13 - 17.

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**,** 17 - 21

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

Nisbett, R. E., & Ross, L. (1980) *Human inference: Strategies and shortcomings of social judgment,* Englewood Cliffs, NJ, Prentice Hall.

Nisbett, R. E., Krantz, D. H., Jepson, C., & Kunda, Z (1983) The use of statistical heuristics in everyday inductive reasoning. *Psychological Review,* 90**,** 339-363.

Ó Ciardhuain, S. (2004) An extended model of cybercrime investigations. *International Journal of Digital Evidence,* 3.

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

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

P**e,** C., & Olbrechts-Tyteca, L. (1969) *The new rhetoric: A treatise on argumentation,* Notre Dame, Indiana, University of Notre Dame Press.

Pollitt, M. M. (2001) Report on digital evidence. *13th INTERPOL Forensic Science Symposium* Lyon, France, INTERPOL.

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

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

Safterein, R. (2000) *Criminalistics: An introduction to forensic science,* Pearson.

Saks, M. J., & Koehler Jonathan. J (2005) The coming paradigm shift in forensic identification science. *Science,* 309**,** 892 - 895.

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

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

Silverstone, H., & Sheetz, Michael (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.

Sommer, P. (1998) Intrusion detection systems as evidence: Recent advances in intrusion detection. London School of Economics & Political Science.

Sommer, P. (2000) Digital footprints: Accessing computer evidence. *Criminal Law Review***,** 61 - 78

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

Tapper, C. (2004) *Cross & Tapper on evidence,* London, LexisNexis Butterworths.

Thompson, D. E., & Berwick, Desmond. 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. *Gerechtigkeitswissenschaft: Kolloquium aus Anlass des 70: Geburtstages von Lothar Philipps.* Berlin.

Tobin, W. A., & THOMPSON, WILLIAM. C (2006) Evaluating and challenging forensic identification evidence. *Champion Magazine.*

Unamed (2000) The virtual horizon: meeting the law enforcement challenges: developing an Australasian law enforcement strategy for dealing with electronic crime: scoping paper. *Police Commissioners' Conference - Electronic Crime Working Party 2000.* Adelaide., Australasian Centre for Policing Research.

Wall C., & Paroff, Jason. (2004) Cracking the computer forensics mystery. *UtahBar Journal,* 17.

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

Whitman, M. E., AND Mattord, H. J. (2005) *Principles of information security,* Boston, Massachusetts, Thomson Learning.

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003) Computer forensics education. *IEEE Security & Privacy,* 1**,** 15 - 23.

COPYRIGHT