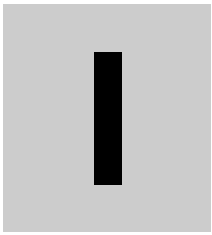

Guidelines for the Management of IT Evidence

Doc no:

telwg29/ IRF/04a

Agenda item :

Incident Response and Forensics Workshop

Submitted by:

Australia

Guidelines for the Management of IT Evidence

Contact: Ajoy Ghosh
Email: ajoy@law.uts.edu.au

APEC Telecommunications and Information Working Group
29th Meeting | 21-26 March 2004 | Hong Kong, China

Guidelines for the Management of IT Evidence

A paper for presentation at the Incident Response & Forensics Workshop APEC-Tel 29 (Hong Kong) 21st March 2004

> *The court unequivocally states that as the vast majority of documentation now exists in electronic form, electronic discovery should be considered a standard and routine practice going forward* - in re Bristol-Meyer Sqibb Securities Litigation 205 FRD 437 (D. NJ 2002)

Abstract

This paper is a presentation of the recently published Standards Australia handbook: *HB-171: Guidelines for the Management of IT Evidence*.

In adversarial legal systems, IT evidence is a tool that can be used to protect an organization by (i) litigating, including criminal prosecution; (ii) defending litigation; and (iii) justifying key decisions to regulators or stakeholders. However, the admissibility of computer records is often questionable. Computer forensics is traditionally viewed as an expensive "post-mortem" exercise that may or may not yield results. However with some planning, evidence can be discovered, preserved and presented in a cost effective manner. The handbook presents a system lifecycle methodology that maximizes the evidential weighting of electronic records.

The presentation focuses on (i) the steps in the lifecycle (ii) an overview of judicial directions involving the handbook and (iii) applying the lifecycle in other legal systems

About the Author

Ajoy has 12 years experience in the area of computer crime, IT Security and Privacy. After originally graduating as a Computer Engineer, he spent a number of years investigating computer-related crimes for law enforcement. He then joined Westpac Banking Corporation as an IT Audit Manager and then an Information Security Manager. Ajoy then performed senior consulting roles with Unisys Australia and 90East (Asia-Pacific) during which time he successfully managed delivery of key projects to headline clients.

Ajoy is the author of Standard Australia's Handbook 171: *Guidelines on the Management of IT Evidence*, advises a number of industry and government committees on information security and cyber-terrorism and is an editorial advisor to media. Ajoy lectures in cybercrime and forensics to post-graduate students at the Law Faculty, University of Technology, Sydney where he is also enrolled as a PhD candidate.

Table of Contents

Introduction

An oft-quoted statistic claims that it took radio 34 years to have 50 million listeners, television 13 years to secure 50 million viewers, and the Internet only 4 years to have 50 million users. Whether those statistics are completely accurate or not, there can be no doubt that this new technology is embraced by large portions of the populace at an increasingly rapid pace. One problem this creates is the technology becomes widespread long before society has developed a shared ethic governing its use and even longer before the legal system is adequately prepared to deal with the new technology.

Although computers, and thus digital evidence, have existed for more than 60 years, the age of computers on workers' desks, computers in the home, computers in children's bedrooms and computers in the hands of criminals is of much more recent vintage. As computers have spread into more hands, high technology crime has become far more prevalent.

Digital evidence, once the province of classic "computer crime" cases like hacking and intrusion, is now being found in cases in every crime category – from harassment to homicide, from drug dealing to securities fraud. This rapid growth in the number of criminal cases involving digital evidence has all-too-often found law enforcement and the judiciary ill prepared to deal with the new issues created by this evidence. Nothing since DNA technology has had such a large potential effect on specific types of investigations and prosecutions as computer forensic science[1]. However, the use of computer forensics to uncover the "smoking gun" is bringing it to the forefront in business[2].

What is Computer Forensics?

Introduction

"E-discovery" or electronic discovery is the part of the discovery process that focuses on finding evidence in electronic form, typically from a computer. Computer forensics is an emerging discipline dedicated to the collection of computer evidence for judicial purposes, and as such supports the e-discovery process.

The appearance of computer forensics as a discipline can be traced back to 1989 with the creation of the first "computer forensic science" course at the US Federal Law

[1] Noblett, M et al (2000) *Recovering and Examining Computer Forensic Evidence* in Forensic Science Communications Vol 2 No 4
[2] Kuchta, K (2000) *Computer Forensics Today* in Information Systems Security Elsivier, Spring 2000

Enforcement Training Centre[3] and the resultant 1991 meetings of six international law enforcement agencies to discuss computer forensic science and the need for a standardised approach to examinations[4]. Since then, many authors have contributed to practical guidelines and textbooks promoting computer forensics. The discipline is aptly described on the cover of Schinder & Tittle's book on the subject that reads:

> "*…bridges the gap between two distinct cultures; that of IT professionals responsible for building systems that prevent cybercrime, and law enforcement officials responsible for investigating and prosecuting those crimes"*.

Forensic computing encompasses four key elements[5]:

(i) The identification of digital evidence: which is the first step in the forensic process. Knowing what evidence is present, where it is stored and how it is stored is vital to determining which processes are to be employed to facilitate its recovery. In addition, the computer forensic examiner must be able to identify the type of information stored in a device and the format in which it is stored so that the appropriate technology can be used to extract it.

(ii) The preservation of digital evidence: Given the likelihood of judicial scrutiny in a court of law, it is imperative that any examination of the electronically stored data be carried out in the least intrusive manner. There are circumstances where changes to data are unavoidable, but it is important that the least amount of change occurs. In situations where change is inevitable it is essential that the nature of, and reason for, the change can be explained.

(iii) The analysis of digital evidence: the extraction, processing and interpretation of digital data—is generally regarded as the main element of forensic computing. Once extracted, digital evidence usually requires processing before people can read it..

(iv) The presentation of digital evidence: involves the actual presentation in a court of law. This includes the manner of presentation, the expertise and qualifications of the presenter and the credibility of the processes employed to produce the evidence being tendered.

As a discipline, computer forensics is in an embryonic phase that Coldwell likens to *alchemy* before it evolved into *chemistry*[6]. "As far as the criminal law is concerned, computer forensics has come a long way - but the field is still far from the position in which malicious hackers are, like ordinary criminals, caught and prosecuted often enough to provide some sought of deterrent"[7].

Practitioners, uncertain of what the law requires often receive unclear direction from counsel who are equally unfamiliar with the complex technical issues and nuances that

---

[3] Anderson, M (1997) Computer Evidence Preservation Forensic International at www.forensic-intl.com
[4] Noblett, M et al (2000) *Recovering and Examining Computer Forensic Evidence* in Forensic Science Communications Vol 2 No 4
[5] McKemmish, R (1999) What is Forensic Computing? Australian Institute of Criminology Trends & Issues No. 118
[6] Coldwell, R (1994) Perceptions of computer crime Australian Institute of Criminology Conference
[7] The Economist in The Australian IT 1 May 2001

must be applied to the laws of evidence. Consequently, there has been no clear consensus on issues such as what is required to establish a sufficient foundation for computer evidence, whether a computer forensic investigator is considered a scientific expert, and how the Best Evidence rule applies to computer data.

As Professor Herschberg argues, the theory will only come through the lessons gleaned from practice[8]:

> *"Marconi successfully transmitted across the Atlantic before there was a theory of terrestrial radio-wave propagation. The Wright brothers flew by the seat of their pants, theory only came much later. I think it's fair comment that any new technology must go through the stage in which theory lags far behind practice".*

Computer forensics as a scientific discipline

There are as many as 25 distinct forensic disciplines, however computer forensic science has yet to take it's place amongst them[9]. In Australia, the National Institute of Forensic Science does not yet recognise computer forensics as a distinct discipline. However, a Court recently described an expert witness as "an experienced computer forensic investigator"[10].

Computer forensic science at its core is different from most traditional forensic disciplines[11]. Firstly, the product of forensic examination is different. Rather than producing interpretive conclusions, the computer forensic examiner produces direct information and data (i.e. computer records) that may subsequently be used to develop an opinion - most probably by someone else.

Traditional forensic science relies on the ability of the scientist to produce a report based on objective results of a scientific examination – the overall case may play a small part in the examination process. A computer forensic practitioner, to be effective, must interact closely with investigators. Failure to do so will result in critical information being ignored, or worse the derivation of misleading conclusions from the available data.

Traditional forensic analysis can be controlled in the laboratory setting and can progress, incrementally, and in concert with widely accepted forensic practices. In comparison, computer forensic science is almost entirely technology and market driven, generally

[8] In Taylor, P (1999) Hackers: Crime in the digital sublime, Routledge, London
[9] Kuchta, K (2000) *Computer Forensics Today* in Information Systems and Security Elsiever Science Spring 2000
[10] Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532 para 39
[11] Noblett, M et al (2000) *Recovering and Examining Computer Forensic Evidence* in Forensic Science Communications Vol 2 No 4

outside the laboratory setting, and the examinations present unique variations in almost every situation[12].

There is a lack of certification and standards for personnel, techniques and tools[13] which means that "the same problems and mistakes continue to re-surface and the same solutions are re-invented" [14].

The Daubert Test

Perhaps a good starting point when considering computer forensics' scientific merit is to subject the discipline to the so-called *Daubert*[15] test used by US courts to determine the validity of scientific evidence. It is a four-prong test that examines:

1. If a theory or technique can be tested - and wether it has been;
2. Whether it has been subjected to peer review and publication;
3. In respect to a particular technique, whether there is a high known or potential error rate; and
4. The theory or technique enjoys general acceptance within the relevant scientific community

Because computer forensics is in its infancy, there is not an ideal amount of testing and publishing[16]. A concerted effort is underway to test commonly utilised computer forensic tools and the manufactures of forensic software in particular have been quick to gather collections of publications favourable to their product and publicise them on their websites in an effort to satisfy the second Daubert criteria[17].

The rapid acceptance of computer forensic disciplines has not gone unnoticed by the courts for example in *re Bristol-Meyer Sqibb Securities Litigation*[18]:

> *The court unequivocally states that as the vast majority of documentation now exists in electronic form, electronic discovery should be considered a standard and routine practice going forward*

Towards a Standard

[12] Noblett, M et al (2000) *Recovering and Examining Computer Forensic Evidence* in Forensic Science Communications Vol 2 No 4
[13] NIJ (2001) Electronic Crime Needs Assessment for State and Local Law Enforcement National Institute of Justice http://www.ojp.usdoj.gov/nij/pubs-sum/186276.htm
[14] Harrison, et al (2002) Lessons learned repository for computer forensics University of Portland
[15] see *Daubert v Merrell Dow Pharmaceuticals Inc* 509 US at 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993)
[16] Patzakis, J (2003) EnCase Legal Journal Guidance Software www.encase.com p8
[17] for example a collection of published papers favourable to the EnCase hard disk imaging tool is available from the website of Guidance Software it manufacturer. See www.guidencesoftware.com/corporate/Press%20Room/2002index.shm
[18] 205 FRD 437 (D. NJ 2002)

There is little that is new in keeping evidence in electronic form - whatever the technology, the greater the attention to records design and documentation, system integrity, operational maintenance and system audit the stronger the evidence from that system will be[19]. Some commentators refer to unrealistically stringent requirements for electronic evidence:

> "*What is the purpose of the laws of evidence when we will trust our lives to computer-designed aircraft and cars, yet refuse to receive computer reports in evidence unless they have been tried through all levels of Dante's inferno? Reliability is the path that leads, hopefully, to judicially determined truth….legislators and the courts have demanded unreasonably high standards of reliability: in fact I suspect, some quasi-scientific standards of reliability are being demanded in the forensic sphere for computers, when such is not required for other 'scientific instruments', or for witnesses*." [20]

However, legal textbooks are replete with commentary on "the apparent ease with which the complexities of the Internet can be glossed over and simplified in the judicial context"[21]. The result has been a simplistic judicial consideration of electronic evidence. For example, *Macquarie Bank vs Berg*[22] relates to publication of material on two separate websites. With only screen printouts of the websites as evidence, his honour determines that:

> "*there are sufficient similarities [with the two websites]…to permit an inference that the defendant is also, if not the author, at the very least involved in and associated with its publication*".

Also, in *Australian Securities Commission vs Matthews*[23], his honour relies on the defendants own analogy of his website as "an electronic sandwich board" as the basis of subsequent findings that the defendant was operating a business illegally.

This is hardly surprising given that the popular notion that "the first and most important thing [for lawyers] to know about the Internet is that it does not actually exist

In 2000, law ministers and attorney generals from small Commonwealth countries convened an expert group to develop model legislation on electronic evidence. The model law contains provisions on general admissibility, the scope of the model law, authentication, application of the best evidence rule, presumption of integrity, standards, proof by affidavit, cross examination, agreement on admissibility of electronic records and admissibility of electronic signature[24]. In 2002, the Commonwealth Secretariat

---

[19] PROA 03/08 (2003) PROV Advice to Victorian Agencies: Electronic Records as Evidence Public Records Office Victoria p3
[20] Brown, R (1996) Documentary Evidence in Australia Law Book Co p366
[21] Lim Y (2002) Cyberspace Law: Commentaries & Materials Oxford University Press p51
[22] [1999] NSWSC 526 - NSW Supreme Court
[23] [1999] FCA 164 - Federal Court of Australia
[24] LMM(02)12 (2002) Draft Model Law on Electronic Evidence Commonwealth Secretariat, London

recommended that all Commonwealth countries adopt or adapt the model legislation as a Commonwealth model.

Provision (8) of the model law states:

> *For the purpose of determining under any rule of law wether an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or preserved, having regard to the type of business or endeavour that used, recorded or preserved the electronic record and the nature and purpose of the record*.

Britain[25] and Canada[26] have already introduced standards relating to the admissibility of electronic records. Both have taken a records management approach and it was felt that Australian industry would have difficulty applying those standards[27]. The International Organisation for Computer Evidence[28] had been tasked by the G8 with developing such standards in relation to the retrieval, handling and presentation of digital evidence, however their attention had been focussed specifically on law enforcement computer forensic laboratories.

On 12th August 2003, Standards Australia HB171: **Guidelines for the Management of IT Evidence** was launched. The guidelines are part of the Australian Government's E-Security National Agenda and are Australia's starting point for satisfying the Commonwealth's recommendation. .

The guidelines had undergone a rigorous consensus procedure that is applied to all standards, be they electrical wiring standards, standards for child safety restraints or the code of practice for information security management. In this case, participants included:

- AusCERT
- Australian Federal Police
- Australasian Centre for Policing Research
- Australian Prudential Regulation Authority
- Australian Securities and Investment Commission
- Australian Taxation Office
- Action Group on E-Commerce
- Commonwealth Attorney-General's Department
- Deacons
- Defence Signals Directorate
- Standards Australia sub-committee IT/012/04 (Security Techniques)

[25] PD 0008:1999 - *Legal Admissibility and Evidential Weight of Information Stored Electronically*;
[26] CAN/CGSB-72.34 - *Electronic Records as Documentary Evidence*
[27] Minutes of a meeting of the Computer Forensic Standards working group 4-12-02
[28] see www.ioce.org

The Attorney General's Department and the Australian Federal Police have endorsed the handbook and the Australian Investment and Securities Commission described it as one of the top three e-regulatory initiatives of 2003[29].

A Lifecycle Approach

In general, corporations consider the evidentiary implications of electronic documents only when they are required for litigation and forensic practitioners have focused on collecting electronic evidence as artefacts of an investigation. However, according to Patel and O'Ciardhuain [30]: "An important issue will be the need to develop a life cycle for using the results of investigations as input to the development of security and management technologies … Forensic computing must become more proactive, rather than being only a post mortem activity as at present, so that it can help prevent crimes".

The handbook presents the *IT Evidence Management Lifecycle* that recognises the need to proactively manage the evidentiary value of electronic records and learn from litigation experience. The lifecycle also recognises that the management of electronic evidence intersects various disciplines and as yet "we do not have a generation of forensic investigators, examiners and members of the legal profession who are equally adept at conducting sound, objective thorough investigations and positioning findings in the form of sound litigation in matters involving digital evidence"[31].

What is IT Evidence?[32]

The handbook defines IT evidence as: "any information, whether subject to human intervention or otherwise, that has been extracted from a computer. IT evidence must be in a human readable form or able to be interpreted by persons who are skilled in the representation of such information with the assistance of a computer program"[33].

IT evidence is sometimes referred to as "electronic evidence" or "electronic record", a term that is used to describe the records that are stored and/or and conveyed using electronic technology as well as records that are stored and/or conveyed using magnetic technology or some other similar technology (for example a record that is stored on a CD-ROM using optical technology)[34]. Whilst the guidance in the handbook can be applied to any electronic evidence, the focus of the handbook is on computer-related evidence, including computer communications.

---

[29] Presentation by Keith Inman, Director Electronic Enforcement ASIC at the National Information Infrastructure Security Conference, 22-3 April 2003, Sydney
[30] Patel, A. & O Ciardhuain, S. (2000) *The impact of forensic computing on telecommunications* in IEEE Communications Magazine November 2000 pp64-67
[31] Talleur, T (2001) *Digital Evidence: The Moral Challenge* in International Journal of Digital Evidence www.ijde.org/archives/tom_article.html
[32] HB-171 § 1.4
[33] HB-171 § 1.4
[34] QLRC WP51 (1998) The Receipt of Evidence by Queensland Courts: Electronic Evidence Queensland Law Reform Commission p5

IT evidence can be divided into three categories[35]: (i) records that are computer-stored; (ii) computer-generated records and (iii) records that are partially computer-generated and partially computer-stored. The difference hinges upon whether a person or a computer created the substantive content(s) of the records.

Computer-stored records refer to documents that contain the writings of some person(s) and happen to be in electronic form. E-mail messages, word processing files and internet chat room messages are common examples. The key evidentiary issue is demonstrating that it is a reliable and trustworthy record of the human statement.

In contrast, computer-generated records contain the output of computer programs, untouched by human hands. Common examples are log files, telephone records, ATM transaction receipts. The key evidentiary issue is demonstrating that the computer program generating the record is functioning properly.

A third category of IT evidence can be adduced: records that are both computer-stored and computer-generated. A common example is a financial spreadsheet that contains both human statements (i.e. input to the spreadsheet program) and computer processing (i.e. mathematical calculation performed by the spreadsheet program).

Why manage IT Evidence?[36]

In many respects, IT evidence is just like any other evidence. However the following characteristics warrant special processes for its management[37]:

a) **design:** computer systems will only create and retain electronic records if specifically designed to do so;
b) **volume:** the large volume of electronic records causes difficulties with storage and prolongs the discovery of a specific electronic record;
c) **co-mingling:** electronic records relating to a specific wrongdoing are mixed with unrelated electronic records;
d) **copying:** electronic copies can be immediately and perfectly copied after which it is difficult, and in some cases impossible, to identify the original from the copy. In other cases, a purported copy may be deliberately or accidentally different from the original and hence evidentially questionable;
e) **volatility:** electronic records can be immediately and deliberately or accidentally altered and expunged; and
f) **automation:** electronic records may be automatically altered or deleted[38].

[35] US DoJ (2002) Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, United States Department of Justice
[36] HB-171 § 1.5
[37] HB-171 § 1.6
[38] A common complaint of investigators is that key records are automatically deleted from a computer system before their probative value is realized. This is done to save storage media.

Evidence is a tool to confirm or deny the reality of a given set of purported facts and under adversarial systems of law, allows organizations to protect themselves by:

a) Taking action against those causing or facilitating damage (i.e. litigate);
b) Referring such action to the relevant authorities for prosecution; or
c) Protecting themselves from litigation.

IT evidence may be used for criminal, civil or administrative proceedings. Organizations not party to such proceeding may still have to produce electronic records or be witnesses in proceedings to which they are not a party[39]. Having electronic records in a readily accessible and reliable form will save significant time and resources for organizations required to produce such records.

Principles for Managing IT Evidence[40]

As Sommer points out, legal proof does not correlate directly with scientific proof[41]. Forensic computing specialists server two masters, technology and the law, and they must find an acceptable balance between the two[42]. Whilst the management of IT evidence is a cross-disciplinary practice, there are a number of overarching principles that can be applied to guide practitioners as they apply knowledge and experience from their own domain of expertise to solve specific problems. These are, according to the handbook:

- **Obligation to provide records**[43]
  a) Understand regulatory, administrative and best-practice obligations to produce, retain and provide records;
  b) Understand the steps that can be taken to maximize the evidentiary weighting of records and the implications of not doing so; and
  c) Understand regulatory constraints to the retention and provision of records[44].

- **Design for evidence**[45]
  Ensure that computer systems and procedures are capable of establishing the following:
    a) The authenticity and alteration of electronic records;

[39] For example an organisation may need to search through data stored by employees and customers to find MP3 music files and provided them to record industry investigators to ascertain if they were illegally downloaded (see Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532).
[40] HB-171 § 2
[41] Sommer, P (1998) Intrusion Detection Systems as Evidence Louvain-la-Neuve
[42] McKemmish, R (1999) What is Forensic Computing? Australian Institute of Criminology Trends & Issues No. 118
[43] HB-171 § 2.2.1
[44] For example, the Privacy Act (Cwth) 1988 limits the retention of personal information. It states as National Privacy Principle 4.2 that: "An organization must take reasonable steps to destroy or permanently deidentify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2".
[45] HB-171 § 2.2.2

b) The reliability of computer programs generating such records;
c) The time and date of creation or alteration;
d) The identity of the author of an electronic record; and
e) The safe custody and handling of records.

- **Evidence collection**[46]
  Collect information in a forensically sound manner. Ensure that evidence collection procedures are both:
  a) technologically robust to collect all relevant evidence; and
  b) legally robust to maximize evidentiary weighting.

- **Custody of records**[47]
  Establish procedures for the safe custody and retention of evidentiary records. Maintain a log recording all access to and handling of evidentiary records.

- **Original and copies**[48]
  Determine if you are handling the original record or a copy of the original record. Ensure that any actions performed on the original or a copy are appropriate and are appropriately documented. Original evidence should be preserved in the state in which it is first identified—it should not be altered, and in instances where alteration is unavoidable, then any changes must be properly documented.

- **Personnel**[49]
  Ensure that personnel involved in the design, production, collection, analysis and presentation of evidence have appropriate training, experience and qualifications to fulfil their role(s).

IT Evidence Management Lifecycle[50]

The handbook presents the "IT Evidence Management Lifecycle" that is illustrated in figure 10. The lifecycle articulates the proposition that computer forensics is no longer a post-mortem activity. If organisations want certainty that electronics records can be used to evidence agreements then they must learn from the past experiences of forensic experts tendering electronic evidence to design systems that maximise evidential weighting.

[46] HB-171 § 2.2.3
[47] HB-171 § 2.2.4
[48] HB-171 § 2.2.5
[49] HB-171 § 2.2.6
[50] HB-171 § 3

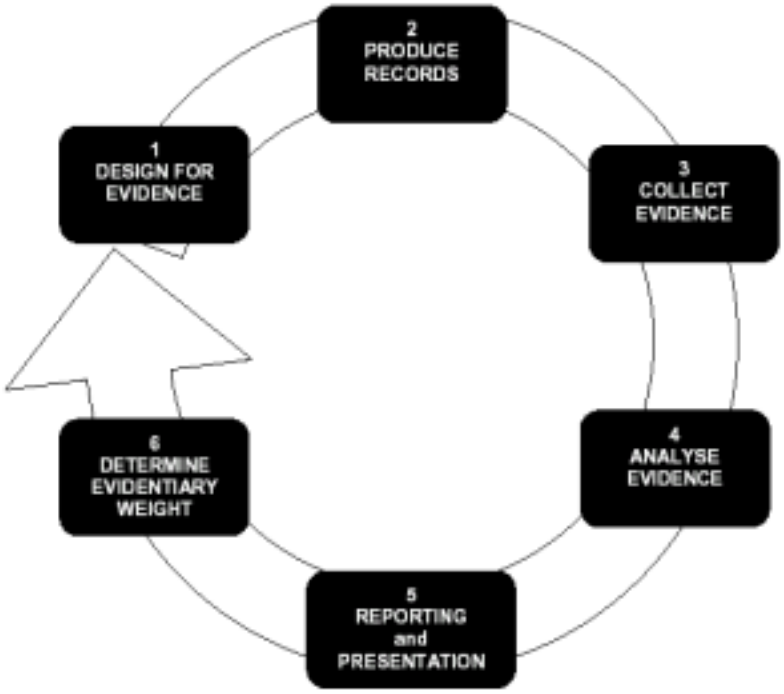

Figure 1 - IT Evidence Management Lifecycle

By segregating different stages of the lifecycle the unique but interacting roles of the different disciplines can be easily conceptualised providing for easy integration into the organisation.

Step 1. Design for evidence[51]

There are five objectives when designing a computer system to maximize the evidentiary weighting of electronic records:

a) Ensuring that evidentially significant electronic records are identified, are available and are useable;
b) Identifying the author of electronic records;
c) Establishing the time and date of creation or alteration;
d) Establishing the authenticity of electronic records; and
e) Establishing the reliability of computer programs.

[51] HB-171 § 3.2

1.1.1 Ensure that electronic records are identified, are available and are usable[52]

The classification and labelling of electronic records ensures that evidentially significant records are identified. Further guidance on implementing records classification controls is available in AS ISO 15489.1 - *Records management: General*[53].

Like paper records, electronic records may be required at any time after their creation and often several years after. The requirement for retaining records varies according to the purpose of the record. For example, the Corporations Act (2001)[54] requires financial records to be retained for seven years, and the Archives Act (1983)11 requires the retention of Commonwealth records. Some records, such as land titles, must be retained for 100 years.

1.1.2 Identifying the author of electronic records[55]

Although handwritten records may be penned in a distinctive handwriting style, computer-stored records consist of a long string of zeros and ones that do not necessarily identify their author[56]. This is a particular problem with electronic communications, which offer their authors an unusual degree of anonymity. For example, Internet technologies permit users to send effectively anonymous e-mails, and Internet Relay Chat channels permit users to communicate without disclosing their real names. When prosecutors seek the admission of such computer-stored records against a defendant, the defendant may challenge the authenticity of the record by challenging the identity of its author.

The problem is a practical one: generally speaking, the fact that an account or address was used does not establish conclusively the identity or location of the particular person who used it. As a result, such evidence based heavily on account or IP address logs must demonstrate a sufficient connection between the logs and the person or location.

The human author of a computer-stored record can be identified electronically. The evidentiary weighting of the recording of the author's identity will depend on the strength of the user authentication system.

In many instances a human author can also be identified from circumstantial evidence demonstrating their use of a particular computer system at the time the record was created/altered. Such evidence may be compiled from witnesses, video, building access system, telephone records or latent forensic evidence (e.g. fingerprint). Circumstantial evidence can also be used to disprove that someone was the purported author of an electronic record.

---

[52] HB-171 § 3.2.1
[53] see §9.2 - Determining how long to retain records and §9.5 - Classification .
[54] § 286 – Obligation to keep financial records.
[55] HB-171 § 3.2.2
[56] Casey, E (2000) Digital Evidence and Computer Crime Academic Press

A computer-generated[57] record is the output of a computer program untouched by human hands and thus the "author" can be considered to be a particular computer program or programs executing on a particular computer or computers. One computer program may author many records and many computer programs may author elements of a single record. Each computer and program generating elements of the electronic record must be clearly identified in the record.

When electronic records consist of both computer-stored and computer-generated components, both the author of any human entries and the computer creating any machine entries should be identified.

An e-mail is perhaps the most common example of electronic evidence that is both computer-stored and computer-generated. The body of the e-mail contains the writings of a human and it is important to identify the particular human author. The sending computer adds information (i.e. headers) as does the post-office and e-mail servers en-route to the recipient. It is important to identify the particular computer system(s) appending this information.

In some instances, it is more important to identify an organization as the record's author or modifier (i.e. corporate author). In such cases, the identity of the human or computer author should be linked to the corporate author.

1.1.3 Establishing the authenticity of electronic records[58]

Before a party may move for admission of a computer record or any other evidence, the offerer must show that it is authentic. That is, the offerer must produce evidence "sufficient to support a finding that the [computer record or other evidence] in question is what its proponent claims"[59]. The courts rightly take the view that the degree to which an item of evidence is relevant to an issue diminishes in proportion to the likelihood of its having been manufactured[60].

In relation to authenticity, the Australian Law Reform Commission[61] has noted that there is some obscurity in the common law:

> *The issue does not appear to have been discussed to any great extent in the authorities. In practice the trial judge will admit evidence of objects and other evidence on being given an assurance that evidence capable of demonstrating its connection to the issues will be led. In practice, writings are admitted into evidence on the giving of evidence-in-chief as to their authenticity - that is, the court proceeds on the basis that it assumes that the evidence will be accepted. With evidence produced by devices or systems, however, the courts appear to*

[57] Computer-generated records may be in machine-readable form (e.g. on hard disk, magnetic tape, in a memory chip) or human-readable form (i.e. a computer printout or displayed on a computer screen).
[58] HB-171 § 3.2.3
[59] DOJ (2000) Federal Guidelines for Searching and Seizing Computers US Department of Justice
[60] Gobbo, J et al (1984) Cross on Evidence Butterworths p23
[61] ALRC 26 (1985) Interim report on Evidence Australian Law Reform Commission Vol 1 para180

> *have required that the trial judge be satisfied - presumably, on the balance of probabilities - as to the accuracy of the technique and of the particular application of it.*

The standard for authenticating computer records is the same for authenticating other records[62]. The degree of authentication does not vary simply because a record happens to be in electronic form. Thus, witnesses who testify to the authenticity of computer records need not have special qualifications. The witnesses do not need to have programmed the computer themself, or even need to understand the maintenance and technical operation of the computer. Instead, the witness simply must have first-hand knowledge of the relevant facts to which she testifies[63].

In general there are two steps in establishing the authenticity of electronic records: (a) identifying the original electronic record; and (b) identifying alteration.

For documents in paper form, it has long been the accepted practice to compare a copy with the original. The problem with electronic documents, however is that it can be impossible to determine which is the original and which the copy.

If the original record is in electronic form, it must be clearly identified as the original electronic record. Any copy, or subsequent copies of a copy, must be clearly identified as copies. The original electronic records and sequence of copying may be established by timestamps attached to the electronic records or metadata.

Challenges to the authenticity of computer records often take on one of three forms. First, parties may challenge the authenticity of both computer-generated and computer-stored records by questioning whether the records were altered, manipulated, or damaged after they were created. Second, parties may question the authenticity of computer-generated records by challenging the reliability of the computer program that generated the records. Third, parties may challenge the authenticity of computer-stored records by questioning the identity of their author.

Organizations must be able to establish that a particular electronic record has not been altered. This can be achieved by:

a) Retaining the original document in non-electronic form (e.g. computer printout, microfiche, etc) for comparison;
b) Relying on computer operating system facilities and circumstantial evidence (e.g. by comparing the time the file was last changed with the time the original was created);
c) Storing the original electronic record or a validated copy on write-once media (e.g. CD-rom); or
d) Using cryptographic techniques[64] (e.g. hash or MAC).

[62] Casey, E (2000) Digital Evidence and Computer Crime Academic Press
[63] DOJ (2000) Federal Guidelines for Searching and Seizing Computers US Department of Justice
[64] Cryptography is the use of mathematical algorithms to transform text (i.e. encryption) or test the validity of text (i.e. authentication).

In many situations, records will be admitted with significant evidentiary weighting even though minor changes have occurred, so long as those changes are "immaterial"[65] and arise in the normal course of communication, storage or display.

1.1.4 Establishing the time and date a particular computer electronic record was created or altered[66]

Organizations must be able to establish the time and date that a particular electronic record was created or altered. To achieve this, a timestamp can be attached to the electronic record upon creation. RFC 3339[67] specifies a format for timestamps that may be used or a new timestamp appended to the record with the date and time of alteration.

Organizations should document the time system being used, any reference time source, the time zone and if/how daylight saving has been implemented.

1.1.5 Establishing the reliability of computer programs[68]

The authenticity of computer-generated records sometimes implicates the reliability of the computer programs that create the records. For example, a computer-generated record might not be authentic if the program that creates the record contains serious programming errors. If the program's output is inaccurate, the record may not be "what its proponent claims"[69].

A presumption that serves the purpose of saving time and expense in calling evidence is that mechanical instruments were in order when they were used. In the absence of evidence to the contrary, the courts will presume instruments were in order at the material time, but they must be of the kind as to which it is common knowledge that they are more often then not in working order[70]. The basis of this view was laid down in a case having little to do with computers[71]. This presumption is stated in the *Evidence Act 1915 (Cwth)* as:

> ***146 Evidence produced by processes, machines and other devices***
>
> *(1) This section applies to a document or thing:*
>
> *(a) that is produced wholly or partly by a device or process; and*
>
> *(b) that is tendered by a party who asserts that, in producing the document or thing, the device or process has produced a particular outcome.*

---

[65] See Electronic Transactions Act 1999 (Cwth) §11 (3).
[66] HB-171 § 3.2.4
[67] Date and time on the internet: Timestamps
[68] HB-171 § 3.2.5
[69] See US Federal Rules of Evidence 901
[70] Gobbo, J et al (1984) Cross on Evidence Butterworths p44
[71] Hoey, A (1999) *Analysis of the Police and Criminal Evidence Act s69 – Computer Generated Evidence* in Cybercrime & Security Oceana Publications

(1) If it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily produces that outcome, it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document or thing on the occasion in question, the device or process produced that outcome.

Example: It would not be necessary to call evidence to prove that a photocopier normally produced complete copies of documents and that it was working properly when it was used to photocopy a particular document.

Without more, computer records generally cannot be assumed to be *prima facie* reliable as books of account (including computerised books of account)[72]. In *Murphy & Anor v Lew & Ors*[73] Smith J of the Supreme Court of Victoria observed that in relation to the the *Evidence Act 1958 (Vic)*:

> *The apparently more rigorous requirements of s55B rather point to a concern that computer-produced documents needed special treatment because thay may not carry with them prima facie guarantees of reliability, such as are found with books of account, of the kind referred to in s58A.*

The objective of establishing the reliability of a computer program that produces computer-stored records is to demonstrate that the text (or graphic, voice, etc) is an accurate recording of the human author's statement. The objective of establishing the reliability of a computer program that produces computer-generated records is to demonstrate that the computer program was operating correctly.

In both cases, the organization must demonstrate that:

a) the computer program was designed correctly i.e. the output is: (i) consistent with design; (ii) predictable; and (iii) repeatable; and
b) the computer program was operating correctly when the electronic record was created, copied or altered.

Organizations that produce their own software can demonstrate that a computer program was designed correctly by adhering to methodologies such as ISO/IEC TR 15504 *Information technology—Software Process Assessment* or by accreditation to the appropriate level of the Capability Maturity Model (CMM). A Capability Maturity Model is a way of measuring how well developed management processes are. Organizations that purchase software can refer to the formal assessment criteria of the provider to demonstrate the reliability of acquired software.

[72] QLRC WP51 (1998) The Receipt of Evidence by Queensland Courts: Electronic Evidence Queensland Law Reform Commission p53
[73] Unreported Sup Ct, Vic, No 12377 of 1991, 12 September 1997

The reliability of a computer program can be established by expert analysis of the source code.

In many instances, if an organization can demonstrate that it relies upon the records produced as a basis for decision-making, it is sufficient to assert that a regularly used computer program is performing the task that it was designed for. This generally applies for popular computer programs (e.g. word processor, spreadsheet, e-mail, etc).

In most cases, the reliability of a computer program can be established by showing that users of the program actually do rely on it on a regular basis, such as in the ordinary course of business. When the computer program is not used on a regular basis and the prosecution cannot establish reliability based on reliance in the ordinary course of business, the prosecution may need to disclose "what operations the computer had been instructed to perform [as well as] the precise instruction that had been given" if the opposing party requests[74]. Notably, once a minimum standard of trustworthiness has been established, questions as to the accuracy of computer records "resulting from . . . the operation of the computer program" affect only the weight of the evidence, not its admissibility[75].

However, even when a program is operating correctly, the defence may introduce issues of context. This can best be demonstrated by the situation where the forensic examiner utilises a third party software package to display and reproduce the data contained within a computerised document[76]. As an example, consider a spreadsheet containing extensive financial data. If a third party product is used to reproduce the spreadsheet in its entirety, and that third party product does not accurately and concisely represent the location of each item of data, the entire meaning of the document may be changed. This in turn can have a significant impact should the document be tendered in evidence. Not only does it cast doubt over the processes employed during the forensic examination, but also over the skill and expertise of the examiner producing the document in evidence.

Step 2. Produce Records[77]

In terms of an organization's ICT systems, this is the operational phase of the life cycle. The objective in this stage is to be able to establish:

a) that a particular computer program produced an electronic record;
b) for computer-stored records, the human author;
c) the time of creation; and
d) that the computer program is operating correctly at the time the electronic record is created or altered.

---

[74] See United States v. Dioguardi, 428 F.2d 1033, 1038 (C.A.N.Y. 1970)
[75] DOJ (2000) Federal Guidelines for Searching and Seizing Computers US Department of Justice
[76] McKemmish, R (1999) What is Forensic Computing? Australian Institute of Criminology Trends & Issues No. 118
[77] HB-171 § 3.3

1.1.6 Correct operation[78]

Organizations should be able to demonstrate that a computer program was operating correctly during the time a particular electronic record was created or altered. This requirement is twofold, with organizations having to demonstrate: (a) that the computer program was operating; and (b) the reliability of a computer program.

For computer programs that produce computer-generated records, organizations must ensure that records of operational faults are maintained (for example see AS/NZS ISO/IEC 17799:2001 - *Code of practice for information security management*[79] and ISO/IEC 15288 - *Systems engineering: systems lifecycle and process*).

For many business records, the mere production of the electronic record may be sufficient demonstration of correct operation, unless evidence is produced otherwise. Circumstantial evidence may also be used to demonstrate that a computer program is operating correctly. For example, a statement by a person asserting that he/she was using a particular computer program at a particular time and that he/she observed certain things, could be strong evidence of the operation of a computer program that produces computer-stored records.

Step 3. Collect Evidence[80]

The objective of this stage of the lifecycle is to locate all relevant information and preserve original electronic records so that nothing in the original evidence is altered.

1.1.7 Standards for Evidence Collection[81]

The standard of evidence collection is one factor determining the evidentiary weight of electronic records. Whilst some organizations will seek to maximize evidence collection capability, not all electronic records will require the highest standard of collection. The standard used to collect a particular electronic record will depend on an assessment of its evidentiary value.

Evidence collected using “forensically sound” procedures has the best chance of being admissible. However these can be expensive and time-consuming so forensic specialists have not collected the vast majority of records that Courts have admitted into evidence. The judiciary have significant discretion regarding the admission of records and their evidentiary weighting and can and do admit records collected by frontline IT and business personnel.

Gates Rubber Company v Bando Chemical Industries Ltd[82] provides a cautionary perspective:

---

[78] HB-171 § 3.3.1
[79] see § 8.4 - Housekeeping
[80] HB-171 § 3.4
[81] HB-171 § 3.4.1
[82] 167 FRD 90 (D. Colorado) at 90 and 112

The plaintiffs were sanctioned for failing to create a mirror image of the defendant's hard drive before their examination. Instead, they ran a program on the original hard drive, which "obliterated at random seven to eight percent of the information which would otherwise have been available". The court therefore ruled that sanctions were inappropriate because the plaintiff "had a duty to utilize the method which would yield the most complete and accurate results" and "should have done an image backup of the hard drive which would have collected every piece of information on the hard drive".

1.1.8 Contemporaneous Notes[83]

Individuals involved in evidence collection must be able to recall for a Court, often years later, any actions performed on original electronic records or evidentiary copies.

Individuals must make contemporaneous notes of any actions performed on original electronic records or evidentiary copies, specifically recording the time and date. Individuals may make contemporaneous notes of any decision-making process, including information available, persons consulted, authorities sought and reasons for the decision. Contemporaneous notes must record facts (i.e. actions performed and observations) and not opinions.

1.1.9 Relevance[84]

Individuals involved in the collection of evidence must be acquainted with the matter under investigation well enough to determine if particular bits of evidence are relevant.

The indiscriminate copying of all data residing on a computer system may breach evidentiary rules that only permit the seizure of relevant evidence[85]. An example of this is when the entire computer hard drive is "imaged" despite the fact that the only relevant information consists of specific files.[86]

1.1.10 Chain of Custody[87]

Organizations must be able to identify who has access to a particular electronic record at any given time from collection, to creation of the evidence copy to presentation as evidence. The evidentiary weighting of electronic records will be substantially reduced if the chain of custody cannot be adequately established or is discredited.
A deficiency in the chain of custody is a favourite avenue for lawyers to discredit corporeal evidence and this is fast become so for electronic evidence.

---

[83] HB-171 § 3.4.2
[84] HB-171 § 3.4.3
[85] see Bartlett V. Weir & Anors (1994) 72 A Crim R 511
[86] In Australia, amendments to definition of *data*, *data held in a computer* and *data storage device* in the Crimes Act 1914 (Cwth) now mean that searching Police with a warrant can copy or remove an entire hard disk.
[87] HB-171 § 3.4.4

When the evidentiary significance of an electronic record is realized, an organization should create an evidence copy of the record and demonstrate the chain of custody of that copy. The evidence copy may be created by:

a) Reproducing the electronic record as a printed document[88];
b) Copying the electronic record to offline media (e.g. floppy disk, CD-rom, backup tape); or
c) Using system access controls to restrict access.

When an electronic record is copied, organizations must be able to demonstrate that it has not been altered.

1.1.11 Non-readable electronic records[89]

Many evidentially useful electronic records are non-readable, that is they do not consist of characters that can be printed or displayed - such non-readable records are only readable by special programs. For example, the slack space of a disk drive may contain deleted files or an encrypted file may contain key electronic records.

Another example that contains non-readable records is the common e-mail. When printed the paper version does not include key information contained in the electronic version - as stated in *Armstrong v The Executive Office of the President*[90]*:*

> *"hardcopy" paper printout of an electronic document would "not necessarily include all the information held in the computer memory as part of the electronic document…essential transmittal relevant to a fuller understanding of the context and import of an electronic communication simply vanish".*

Non-readable electronic records may be critical during the "analyse evidence" stage of the lifecycle. When collecting electronic records, care must be taken to discover and not to alter non-readable electronic records.

1.1.12 Limitations[91]

Evidence collectors must also ensure that they adhere to rules governing the access to or disclosure of certain information. In some circumstances, electronic records will be subject to privilege[92], for example, communications with a legal advisor, self-incrimination or a religious confession. Violation of the rules will reduce the evidentiary weighting of electronic records and may result in electronic records being inadmissible. Further, organizations or individuals may incur pecuniary penalties.

Another common limitation is contained in the *Telecommunications (Interception) Act (Cwth) 1979* that defines "communication" as:

---

[88] This will result in the loss of any non-printable but still relevant information (e.g. electronic timestamp, previous changes to the text of a document that is retained, but not visible, in a word processing file).
[89] HB-171 § 3.4.5
[90] 1 F.3d 1274 (D.C. Cir 1993)
[91] HB-171 § 3.4.7
[92] See §3.10 of the Evidence Act (1995).

communication *includes conversation and a message, and any part of a conversation or message, whether:*

(a) in the form of:

(i) speech, music or other sounds;

(ii) data;

(iii) text;

(iv) visual images, whether or not animated; or

(v) signals; or

(b) in any other form or in any combination of forms.

Evidence collectors must carefully consider if any of the data they are collecting constitutes unlawful interception.

Step 4. Analyse evidence[93]

The objective of this stage of the lifecycle is to:

a) Assemble from IT evidentiary records material facts;
b) Deduce from IT evidentiary records opinions relating to those facts; and
c) Determine what other IT evidence is lacking that will assist the enquiry.

1.1.13 Use evidence copy[94]

Analysis must be performed using an evidence copy. An exception is when the original electronic record is used to determine (a) if copies are duplicates of the original; or (b) if the original has been altered.

1.1.14 Personnel qualifications[95]

Persons conducting analysis of electronic evidence should be suitably qualified for the role they are performing. Organizations should determine if analysis requires an ordinary witness or an expert witness. Ordinary witnesses must confine their analysis to matters of fact, whilst experts may deduce matters of opinion from the IT evidence.

An ordinary witness is sufficient for the vast majority of admitted electronic records. For example, to establish regular business use of a computer system the witness need not be familiar with the operation of the computer program. They only need to know that a particular computer system is ordinarily used by the business, that it was used at the time the electronic record was created or altered and that the electronic record produced was relied upon to make a business decision.

An expert witness must be able to demonstrate the appropriate qualifications and experience to substantiate their claim as an "expert". In Australia, "expert" means a person who has specialized knowledge based on the person's training, study or experience[96]. Experts must comply with procedures of the relevant Court. For example,

[93] HB-171 § 3.5
[94] HB-171 § 3.5.1
[95] HB-171 § 3.5.2
[96] See for example Federal Court rules order 34A rule 2 and NSW Supreme Court rules, interpretation.

the Federal Court and higher Courts require that experts adopt the 'expert witness code of conduct'.

1.1.15 Completeness of evidence[97]

IT evidence is circumstantial. Persons conducting analysis of IT evidence must be provided with an explanation of: (a) The circumstances in which the electronic records were created; and (b) The computer system(s) creating the electronic records. Without a thorough understanding of the background, material electronic records may be neglected or their significance diminished.

Step 5. Reporting & presentation[98]

The objective of this stage of the lifecycle is to persuade decision-makers (e.g. management, lawyer, judge, etc) of the validity of the facts and opinion deduced from the evidence.

In *Kabushiki Kaisha Sony Computer Entertainment v Stevens*[99], the judge said: "the court should not be left in a position where it has to guess as to the operation of technical processes and how these processes satisfy the statutory language". For most IT evidence, the original electronic record consists of electronic impulses stored on media. It must be converted into human readable format prior to presentation, either by computer printout or by using a computer program.

Experts are required to comply with the procedures of the court, such as providing a certificate. Expert witnesses may also be required to comply with applicable expert witness codes of conduct and Courts routinely exclude reports written by experts that have not complied[100].

Electronic evidence does not necessarily have to be presented by an expert. Lay witnesses can give testimony regarding things that they perceived such as what they typed into a computer, what they saw on the screen and what they saw being printed. Lay witnesses may also testify to the regular business use of a computer system and the resulting records.

Step 6. Determine evidentiary weighting[101]

Assessment of the evidentiary weighting of electronic records occurs during all stages of the lifecycle. A final assessment is performed by an independent fact-finder who may be a magistrate or judge; a member of a tribunal or an arbitrator; or senior organizational management.

---

[97] HB-171 § 3.5.3
[98] HB-171 § 3.6
[99] [2002] FCA 906
[100] See Commonwealth Development Bank & Anor v Cassegrain [2002] NSWSC 980 and Makita (Australia) Pty Ltd v Sprowles [2001] NSWCA 305
[101] HB-171 § 3.7

When producing, collecting or analysing electronic evidence, its purpose and final arbiter may not be clear. "Given the likelihood of judicial scrutiny"[102], each assessment should consider the judicial standpoint i.e. (a) Is the document admissible?; and if so (b) what weighting should it carry?

"Courts of law are not so free to gather information as other decision-makers. Generally they depend on the parties to inform them and may not conduct their own inquires"[103]. The party tendering the electronic records must convince the court of its admissibility and the contending party may challenge it.

In addition to the ordinary tests for relevance and the balancing of probative value with the likelihood that evidence will be misleading, confusing or prejudicial, some courts apply an additional test for evidence that is considered novel scientific evidence. This test considered wether the evidence has gained general acceptance in the scientific field in which it belongs and excludes novel scientific evidence if it has not gained such acceptance[104]. In the US, this has become known as the *Daubert*[105] test, and its application to computer forensic evidence has been previously discussed.

In Australia, the vast majority of computer records are tendered as business records, thus according to the Australian Law Reform Commission "the issue does not appear to have been discussed to any great extent in the authorities" [106] however the processes and procedures described in the earlier parts of the Guidelines for the Management of IT Evidence now provide a benchmark which judges can use when considering the admissibility of computer-based evidence.

Judicial Adoption

At the time of writing, the handbook has been tendered in civil proceedings in the NSW District and Supreme Courts, the Victorian County Court and the Federal Court - I have personally been involved in at least 8 matters. In each instance the handbook was accepted as the Australian benchmark for assessing the admissibility of computer generated evidence or the practices of computer forensic specialists. Unfortunately, the litigants have settled the matter prior to hearing so the proceedings are not published.

The handbook has been introduced in evidence for a variety of criminal matters in the higher Courts that are scheduled to be heard in the coming months and on the 11th of March 2004, the handbook is about to be publicly challenged in criminal Contempt of Court proceedings and I am hoping to be able to update you at the conference.

---

[102] McKemmish, R (1999) What is Forensic Computing? Australian Institute of Criminology Trends & Issues No. 118
[103] QLRC WP51 (1998) The Receipt of Evidence by Queensland Courts: Electronic Evidence Queensland Law Reform Commission p6
[104] Demen, J (1998) *Virtual Reality Evidence* in Cybercrime & Security Oceana Publications p11
[105] see *Daubert v Merrell Dow Pharmaceuticals Inc* 509 US at 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993)
[106] ALRC 26 (1985) Interim report on Evidence Australian Law Reform Commission Vol 1 para180

Next Steps

The Guidelines for the Management of IT Evidence have received wide-ranging interest from agencies of developed economies such as Australia, New Zealand, Canada and Germany to those modernising their legal systems such as the People's Republic of China and Indonesia to developing nations such as Vietnam and Fiji. They have been included in University curricula, law enforcement training courses and as a reference for computer forensic certifications.

The handbook was published on 12th August 2003. It is Australia's starting point for a computer forensic standard and in August 2004 will be reviewed and updated in readiness for escalating its status from handbook to Australian Standard.

I urge you to read the handbook and participate in the review process by sending any comments to ajoy@law.uts.edu.au.