

COMP6445

Start with this. Whilst it is dated and standards have evolved, the fundamental concepts remain and have been re-enforced through case law.

COURSE NOTES

Presenting IT Evidence in the Courtroom

Prepared by:
Mr Ajoy Ghosh

Preface

All that is out there is random data...waiting to be discovered, ordered and interpreted by the perceiver.

--- Deepak Chopra



As you work through this course it is useful to contextualise each of your perspectives. As an investigator, you are a perceiver, discovering, ordering and interpreting random data. As a witness, your task is to persuade a decision-maker that *your interpretation* is the right one.

As an employee or consultant, your perception will understandably and often unconsciously be biased.

As an independent expert, not only are you an investigator and witness, but you must ignore your prejudices and interpret evidence as it is.

My task is to persuade you to become a better independent expert.


ajoy.ghosh@optusnet.com.au

Table of Contents

INTRODUCTION	4
ROLE OF THE PRACTITIONER.....	4
WHAT IS COMPUTER FORENSICS?.....	6
INTRODUCTION	6
COMPUTER FORENSICS AS A SCIENTIFIC DISCIPLINE	7
THE DAUBERT TEST	9
WHY PUT THE “E” IN E-EVIDENCE?	11
INTRODUCTION	11
CHARACTERISTICS OF IT EVIDENCE	12
PRACTICAL CONSIDERATIONS	13
WHAT INFORMATION CAN BE DISCOVERED?	18
INTRODUCTION	18
HOW A HARD DISK WORKS.....	19
STANDARD RECOVERY TECHNIQUES.....	20
MY SURVEY	22
ADVANCED RECOVERY TECHNIQUES	24
BEST PRACTICE	26
INTRODUCTION	26
A LIFECYCLE APPROACH	27
WHAT IS IT EVIDENCE?.....	28
WHY MANAGE IT EVIDENCE?.....	29
PRINCIPLES FOR MANAGING IT EVIDENCE	29
IT EVIDENCE MANAGEMENT LIFECYCLE	31
SEARCHING	48
INTRODUCTION	48
SEARCH STRATEGIES	49
PRESERVATION	52
INTRODUCTION	52
PULL THE PLUG?.....	52
DIGITAL FINGERPRINTS	53
STORAGE MEDIA	54
PROVEN TOOLS	54
PRESENTING EVIDENCE	56
INTRODUCTION	56
EDUCATING THE AUDIENCE	56
WHAT NEEDS TO BE PROVED/DISPROVED?.....	56
EXPERT WITNESSES/SCIENTIFIC METHOD EVIDENCE.....	58
RECURRING ISSUES IN COMPUTER CRIME TRIALS.....	59
PRESENTING COMPLICATED/TECHNICAL ISSUES	61
EXPERT WITNESS GUIDELINES.....	62

STANDARD FORM OF REPORT.....	66
HOW TO GIVE EVIDENCE, ESPECIALLY IN CROSS-EXAMINATION.....	69
THE THREE GOLDEN RULES	69
THE FIRST GOLDEN RULE - TELL THE TRUTH	71
THE SECOND GOLDEN RULE - RESPOND TO ONLY THE QUESTION	72
THE THIRD GOLDEN RULE - KEEP YOUR ANSWERS SHORT.....	73
A FEW OTHER POINTS	73

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 electronic evidence (“e-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.

E-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 science¹. However, the use of computer forensics to uncover the “smoking gun” is bringing it to the forefront in business².

This course aims to provide practitioners, prosecutors, solicitors and barristers with the tools they need to understand how they can best utilise e-evidence. Perhaps to discover incriminating evidence, to discover exculpatory evidence or perhaps to maximise the impact of evidence provided by witnesses or to contest evidence submitted by opposing parties.

Role of the practitioner

The computer forensics practitioner might find themselves in a variety of roles as a witness. Whilst this seminar focuses on the practice of the expert witness, the discipline of e-evidence handling well serves those in other roles.

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 Elsevier, Spring 2000

Lay Witness

The role of a “lay witness” is merely to recall facts based on their own sensual experience (i.e. “I saw...”, “I heard...”) and strictly adhering to the rules of evidence. Of course, the lay witness is not expected to understand these rules of evidence and evidentiary process relies on the objection of opposing counsel.

Investigator

The role of an “investigator” is to discover facts i.e. undertake investigation. In evidence, the investigator may also merely recall fact however Courts have come to expect that the investigator has attempted to discover *as much incriminating and exculpatory evidence as reasonable*.

Expert Witness

The role of the “expert” is to answer a particular question, or questions as instructed by legal counsel. In doing so, the expert is allowed to provide an opinion based on their particular expertise.

In most Australian jurisdictions, an "expert" is loosely defined as a person who has specialised knowledge based on the person's training, study or experience³. Each Court has rules regarding the tendering of expert opinion – these are addressed later in the course notes.

Independent Expert

As well as demonstrating his or her expertise, an independent expert must demonstrate that, apart from their instructions, they have no other interest in the matter at hand.

A survey of 244 Australian judges last year by the Institute of Judicial Administration found the judges believe that the most important problem with expert evidence is that it is partisan. 27% said that expert witnesses were often biased, and 65% said they were occasionally biased. One judge commented: "Bias is almost inevitable given that the expert is paid for by one party and only called if his/her evidence helps the party's case. Experts frequently slant evidence in favour of the litigant on whose behalf evidence is given."

"I have little faith in experts' reports which are really the work of solicitors/counsel....I cannot imagine any other reality in an adversarial system"

- response of a senior judge

³ See for example s1.8 Supreme Court Rules 1970 (NSW)

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. The computer may be a single computer used by a suspect or may be one or more of many computers linked together in a network or a computer-like device.

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 Enforcement Training Centre⁴ and the resultant 1991 meetings of six international law enforcement agencies to discuss computer forensic science and the need for a standardised approach to examinations⁵. 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 elements⁶:

- 1) 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.

⁴ Anderson, M (1997) Computer Evidence Preservation Forensic International at www.forensic-intl.com

⁵ Noblett, M et al (2000) *Recovering and Examining Computer Forensic Evidence* in Forensic Science Communications Vol 2 No 4

⁶ McKemmish, R (1999) What is Forensic Computing? Australian Institute of Criminology Trends & Issues No. 118

- 2) 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.
- 3) 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..
- 4) 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*⁷. “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”⁸.

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 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 practice⁹:

“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

According to some commentators, there are as many as 25 distinct forensic disciplines and computer forensic science has yet to take its place amongst

⁷ Coldwell, R (1994) Perceptions of computer crime Australian Institute of Criminology Conference

⁸ The Economist in The Australian IT 1 May 2001

⁹ In Taylor, P (1999) Hackers: Crime in the digital sublime, Routledge, London

them¹⁰. However, in Australia, the National Institute of Forensic Science recognises some 7 “Electronic Evidence” specialities in its categorisation of forensic science disciplines¹¹. These are:

- Cybercrime
- Data analysis (computer)
- Database research
- Electronic data analysis
- Electronic data recovery
- E-mail analysis/tracing
- Image processing/enhancement

Further, a Court recently described an expert witness as “an experienced computer forensic investigator”¹².

Computer forensic science at its core is different from most traditional forensic disciplines¹³. 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 outside the laboratory setting, and the examinations present unique variations in almost every situation¹⁴.

¹⁰ Kuchta, K (2000) *Computer Forensics Today* in *Information Systems and Security* Elsevier Science Spring 2000

¹¹ See www.nifs.com.au

¹² Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532 para 39

¹³ Noble, M et al (2000) *Recovering and Examining Computer Forensic Evidence* in *Forensic Science Communications* Vol 2 No 4

¹⁴ Noble, M et al (2000) *Recovering and Examining Computer Forensic Evidence* in *Forensic Science Communications* Vol 2 No 4

There is a lack of certification and standards for personnel, techniques and tools¹⁵ which means that “the same problems and mistakes continue to re-surface and the same solutions are re-invented”¹⁶.

The Daubert Test

Perhaps a good starting point when considering computer forensics’ scientific merit is to subject the discipline to the so-called *Daubert*¹⁷ 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 whether 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

Although much has been written about computer forensics, as a discipline it is in its infancy and there is not an ideal amount of testing and publishing¹⁸ relating to specific methods, tests and results. This is hardly surprising since the vast majority of practitioners are practicing, whilst the vast majority of publishing academics remain steeped in traditional cybercrime areas of criminology, law and information security.

A concerted effort is underway to test commonly utilised computer forensic tools and the manufacturers 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 criteria¹⁹. In Australia, a concerted effort is underway to develop a validation framework for the testing and of forensic software tools.

The rapid acceptance of computer forensic disciplines has not gone unnoticed by the courts for example in *re Bristol-Meyer Squibb Securities Litigation*²⁰:

¹⁵ 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>

¹⁶ Harrison, et al (2002) *Lessons learned repository for computer forensics* University of Portland

¹⁷ see *Daubert v Merrell Dow Pharmaceuticals Inc* 509 US at 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993)

¹⁸ Patzakis, J (2003) *EnCase Legal Journal* Guidance Software www.encase.com p8

¹⁹ for example a collection of published papers favourable to the EnCase hard disk imaging tool is available from the website of Guidance Software its manufacturer. See www.guidancesoftware.com/corporate/Press%20Room/2002index.shm

²⁰ 205 FRD 437 (D. NJ 2002)

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 Australia, electronic records have become so common in litigation that the Courts have enacted special rules detailing how such records must be processed. For example, Victoria first enacted the *Guidelines for the use of Technology in Litigation in any Civil Matter*²¹ in 2002 and updated these in 2005 to recognise computer forensic best-practices.

²¹ see

<http://www.supremecourt.vic.gov.au/CA256CC60028922C/page/Courtroom+Technology?OpenDocument&1=90-Courtroom+Technology~&2=~&3=~>

Why put the “e” in e-evidence?

Introduction

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 be²². 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.”²³

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”²⁴. The result has been a simplistic judicial consideration of electronic evidence. For example, *Macquarie Bank vs Berg*²⁵ 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”.

²² PROA 03/08 (2003) PROV Advice to Victorian Agencies: Electronic Records as Evidence Public Records Office Victoria p3

²³ Brown, R (1996) Documentary Evidence in Australia Law Book Co p366

²⁴ Lim Y (2002) Cyberspace Law: Commentaries & Materials Oxford University Press p51

²⁵ [1999] NSWSC 526 - NSW Supreme Court

Also, in *Australian Securities Commission vs Matthews*²⁶, 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”²⁷. Perhaps there are three things that lawyers really ought to know:

- Not all data within an electronic document is displayed on the computer screen or in a printout;
- Because a user presses the ‘delete’ key, data is not necessarily removed from the computer;
- Electronic communication is a chain of communication, and the message may be recorded by any link in that chain.

The corollary is the very real possibility of discovering of relevant information the user didn’t realise was there or thought they had deleted.

Characteristics of IT Evidence

In many respects, IT evidence is just like any other evidence. However the following characteristics warrant special processes for its management²⁸:

- **design:** computer systems will only create and retain electronic records if specifically designed to do so;
- **volume:** the large volume of electronic records causes difficulties with storage and prolongs the discovery of a specific electronic record;
- **co-mingling:** electronic records relating to a specific wrongdoing are mixed with unrelated electronic records;
- **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;
- **volatility:** electronic records can be immediately and deliberately or accidentally altered and expunged; and
- **automation:** electronic records may be automatically altered or deleted²⁹.

²⁶ [1999] FCA 164 - Federal Court of Australia

²⁷ Edwards, L & Waede, C (1997) *Law and the Internet: Regulating Cyberspace* Hart, Oxford

²⁸ HB-171 § 1.6

²⁹ 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.

Practical Considerations

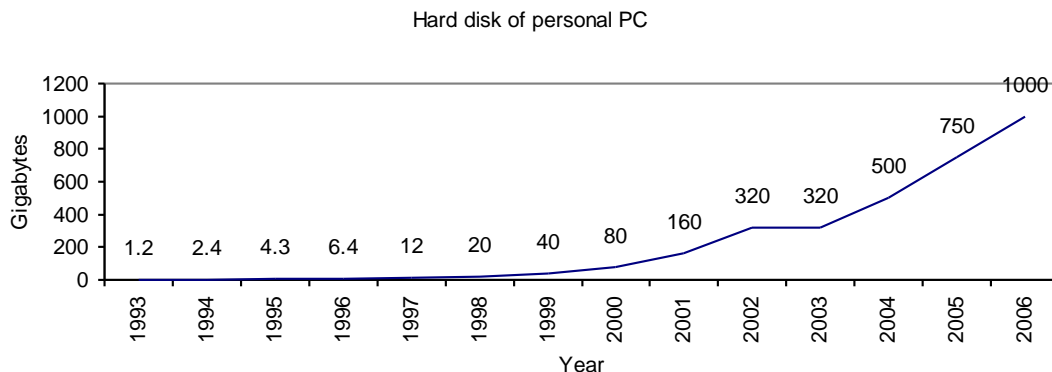
Workload

According to Interpol, law enforcement is wholly unprepared for the enormous volume of work that is being generated by the field of computer forensics³⁰. Even the best-equipped forces are unable to deal with an increasing number of reported cybercrime.

The result is that computer-related evidence is often ignored and a fertile hunting-ground for information that might confuse the prosecution case.

Data Volume

The greatest challenge facing forensic computing today is the rapid increase in the capacity of today's storage media³¹. The advent of new storage technologies, combined with the increased demand for storage by consumers and software developers has resulted in a surge in the capacity of hard-drives. The average size of a hard disk installed in the personal computer is set to dramatically increase³²:



• Figure 1 - size of personal PC hard disk drive

It may take days or weeks to find the specific information described a judicial order because computer storage devices can contain extraordinary amounts of information³³. Investigators cannot reasonably be expected to spend more than a few hours searching for materials on-site, and in some circumstances (such as

³⁰ Interpol (2001) Criminal threats to e-Commerce, Jan 2001

³¹ McKemmish, R (1999) What is Forensic Computing? Australian Institute of Criminology Trends & Issues No. 118

³² Data provided by Dave Reinsel, the Research Manager of Hard Disk Drives of International Data Corp.

³³ DOJ (2000) Federal Guidelines for Searching and Seizing Computers US Department of Justice

executing a search at a suspect's home) even a few hours may be unreasonable. Even if the searchers know specific information about the files they seek, the data may be mislabelled, encrypted, stored in hidden directories, or embedded in "slack space" that a simple file listing will ignore.

Commingling

Commingling is not a problem unique to computer records, but equally applies to paper files. It refers to the fact that documentary evidence of a crime is stored amongst other documents that do not relate to the investigation at hand, and in fact may be protected from searchers under privilege or privacy.

The key difference between paper documents and computerised files is that 90% of files on servers are not touched for more than a year. Thus it could be asserted, they are not relevant to most cybercrimes³⁴.

When the computer involved is not a stand-alone PC but rather part of a complicated network, the collateral damage and practical headaches that can arise from seizing the entire network often counsel against a wholesale seizure. For example, if a system administrator of a computer network stores stolen proprietary information somewhere in the network, the network becomes an instrumentality of the system administrator's crime. Technically, agents could perhaps obtain a warrant to seize the entire network. However, carting off the entire network might cripple a legitimate, functioning business and disrupt the lives of hundreds of people, as well as subject the government to civil suits³⁵.

In the civil context, organisations claim that is overly onerous for them to be expected to search through thousands and perhaps millions of electronic records to find those relating to the specific matter³⁶.

Another issue of commingling is that evidence of one cybercrime may well co-exist with evidence of an entirely separate crime. If investigators seize computer equipment for the evidence it contains and later decide to search the equipment for different evidence, the new evidence discovered may not be admitted.

Digital evidence is fragile

The problem with digital evidence is that it readily damaged or destroyed, either accidentally or purposely. The destruction of information can be more complicated than may initially be acknowledged.

Inexperienced searchers are the most common reason digital evidence is destroyed³⁷. Attempting to search files on-site may risk damaging the evidence

³⁴ Farmer, D & Venema, W (2000) *Forensic Computing Analysis: An Introduction* in *Dr Dobbs Journal*, 29(9) p70-75

³⁵ See commentary on *Steve Jackson Games, Inc. v. Secret Service*, 816 F. Supp. 432, 440, 443 (W.D. Tex. 1993) in DOJ (2000) *Federal Guidelines for Searching and Seizing Computers* US Department of Justice

³⁶ See *Sony Music Entertainment (Australia) Limited v University of Tasmania* [2003] FCA 532

³⁷ Casey, E (2000) *Digital Evidence and Computer Crime* Academic Press

itself. Investigators executing a search warrant may come across a computer that employs an uncommon operating system that the on-site technical specialist does not fully understand. An inartful attempt to conduct a search may destroy evidence. Even common operating systems cause problems. For example, the Apple-Macintosh re-arranges data to the hard disk each time it is started thus a searcher that turns on the computer to search for particular files will be destroying the evidence on the hard disk.

Commonly, investigators may have reason to believe that the computer has been “booby trapped” by a savvy criminal. Technically adept users may know how to trip-wire their computers with self-destruct programs that could erase vital evidence if the system were examined by anyone else. For example, a criminal could write a very short program that would cause the computer to demand a password periodically and if the correct password is not entered within ten seconds, would trigger the automatic destruction of the computer's files.

This is a growing problem, since the so-called “knock and announce” rule usually requires searchers to announce their presence and authority prior to executing a search warrant. Technically adept suspects may “hot wire” their computers in an effort to destroy evidence. For example, technically adept computer hackers have been known to use a “hot key” i.e. computer programs that destroy evidence when a special button is pressed. If a policeman knocks at the door to announce their search, the suspect can simply press the button and activate the program to destroy the evidence.

Concealment

Cyber crimes are extremely difficult for law enforcement to trace. This is not only because hackers can cover their tracks. The logical structure of the Internet itself, with its numerous pathways through which the “packets” of data travel until they are reassembled at the destination, makes it difficult to trace hackers.

The most proficient intruders develop their own underground network of compromised systems that enable them to “leapfrog” through the net from one system to another before attempting to attack the target system. Only highly skilled and strongly motivated investigators are capable of tracking them down as well as gathering and preserving evidence in a manner that makes it possible to present it to prosecutorial authorities and be considered by the courts³⁸.

In other cases, the perpetrators use technologies of concealment. Targeted files may be mislabelled, hidden, oddly configured, written using code words to escape detection, encrypted, or otherwise impossible to find using a simple technique such as a “key word” search. Experience has shown that individuals engaged in various kinds of criminal conduct have used these techniques to obfuscate incriminating computer evidence³⁹.

Writers note that organised criminal groups are increasingly using technologies on encryption to conceal not just their criminal activities, but also the workings of

³⁸ Anderson, M (1997) Computer Evidence Preservation Forensic International at www.forensic-intl.com

³⁹ DOJ (2000) Federal Guidelines for Searching and Seizing Computers US Department of Justice

the criminal organisation. In the United States, the total number of criminal cases involving encryption is at least 500 and perhaps somewhere between 1,000 and 5,000 with an annual growth rate of 50-100%⁴⁰.

Procedural framework

Increasingly, electronic evidence necessary to prevent, investigate, or prosecute a crime may be located outside national borders. This can occur for several reasons. Criminals can use the Internet to commit or facilitate crimes remotely e.g. when Russian hackers steal money from a bank in Sydney, or when the kidnappers of a businessman's daughter deliver demands by e-mail.

Communications also can be "laundered" through third countries, such as when a criminal in Sydney uses the Internet to pass a communication through Jakarta, Singapore, and Shanghai before it reaches its intended recipient in Perth - much the way monies can be laundered through banks in different countries in order to hide their source. In addition, ISP architecture may route or store communications in the country where the provider is based, regardless of the location of its users.

Nations must modernize their procedural law as well as their substantive law. While an adequate framework of cybercrime penal law is an absolute prerequisite for effective action against cyber criminals, such action can be frustrated by antiquated procedural law which, for example, authorizes warrants only for search for and seizure of tangible evidence.

Design

Locard's Principle, upon which traditional forensic sciences are based, states that⁴¹:

Anyone or anything entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they depart.

Whilst Locard's Principle is applicable in the real world, the cyber world relies on records that must be specifically designed into a computer system. Most systems currently used for computer security are not designed with the need to track, trace and generate legally admissible evidence⁴². Even when acceptable audit trails are built, many systems regularly delete them to save hard disk space⁴³.

The emergence of forensic computing disciplines has levied new requirements on computer and telecommunications systems for the production of evidentiary

⁴⁰ Denning, D & Baugh, W (1997) Encryption And Evolving Technologies as Tools Of Organized Crime and Terrorism National Strategy Information Centre Working Group on Organized Crime

⁴¹ Casey, E (2000) Digital Evidence and Computer Crime Academic Press

⁴² Sommer, P (1998) Intrusion Detection Systems as Evidence Louvain-la-Neuve

⁴³ Farmer, D & Venema, W (2000) Forensic Computing Analysis: An Introduction in Dr Dobbs Journal, 29(9) p70-75

records. Consequently, the practice of computer forensics no longer commences from the discovery of a crime, but rather from the design of computer systems⁴⁴.

⁴⁴ Patel, A & Ciardhuain, S (2000) *The impact of forensic computing on telecommunications* in IEEE Communications Magazine, Nov 2000, p64-67

What Information can be discovered?

Introduction

It has been increasingly common for computer forensic practitioners to be referred to as “the raiders of the lost archives”⁴⁵, a reference to perhaps the most prominent task of the discovering deleted files from hard disks using the procedure of hard disk recovery. Hard disk recovery is the process of discovering data from a hard disk that had previously been deleted.

Whilst only one of many activities undertaken by computer forensic practitioners hard disk recovery has received the most prominence. Perhaps because it entails some technical wizardry - but mostly because of its utility in discovering information in high profile examples such as the Microsoft anti-trust case, the case of Wen Ho Lee the scientist turn spy, the undoing of Oracle CEO Larry Ellison’s accuser, the regulatory probes into Enron, Merrill Lynch and Credit Suisse First Boston and uncovering of evidence of terrorist activities.

Computer records are in essence electronic impulses recorded on storage media. Common media are: memory, floppy disk, hard disk, tape and cd-rom. The hard disk is probably the most common storage media since it is cheaper than memory, higher capacity than floppy disk and can be written and re-written many times unlike the cd-rom. Almost all personal computers contain at least one hard disk. The price of a hard disk is now less than 1/3¢ per megabyte⁴⁶.

To put this in perspective, a floppy disk will hold 1.44 megabytes which is the equivalent to a text document containing around 1,400,000 characters or 230,000 words. The entire Encyclopaedia Britannica, including illustrations, takes only 650 megabytes that would cost \$2.15¢.

⁴⁵ Brill, A (1998) *The secret life of computer data: How valuable evidence is ignored in litigation* in Cybercrime & Security Oceana Publication

⁴⁶ Derived from the historical price listing of hard disk drives at www.littletechshoppe.com/nlb25/winchest.html

How a Hard Disk Works

Figure 2 illustrates a typical hard disk. It is a sealed aluminium box with electronics attached to one side. The electronics control the read/write mechanism and the motor that spins the platters. The electronics also assemble the magnetic domains on the drive into bytes (reading) and turn bytes into magnetic domains (writing).



Figure 2 - a typical hard disk



Figure 3 - Hard disk without cover

Figure 3 illustrates what a hard disk looks like once the cover is removed. The shiny disc is called a platter. The **platters**, which typically spin at 3,600 or 7,200 rpm when the drive is operating. These platters are manufactured to amazing tolerances and are mirror-smooth (as you can see by the reflection).

The **arm** that holds the read/write heads is controlled by the mechanism in the upper-left corner, and is able to move the heads from the hub to the edge of the drive.

In order to increase the amount of information the drive can store, most hard disks have **multiple platters**. This drive has three platters (as shown in figure 4) and thus six read/write heads.



• Figure 4 - hard disk platters

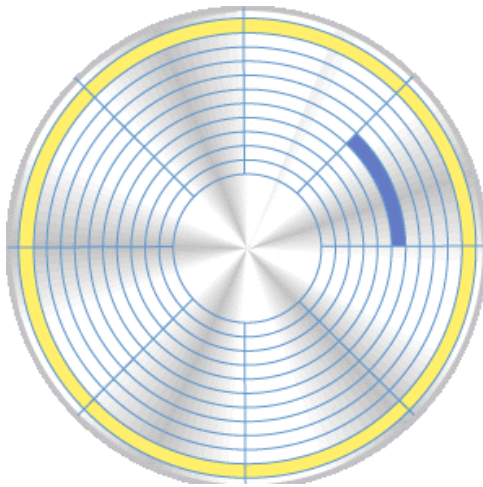


Figure 5 - hard disk tracks and clusters

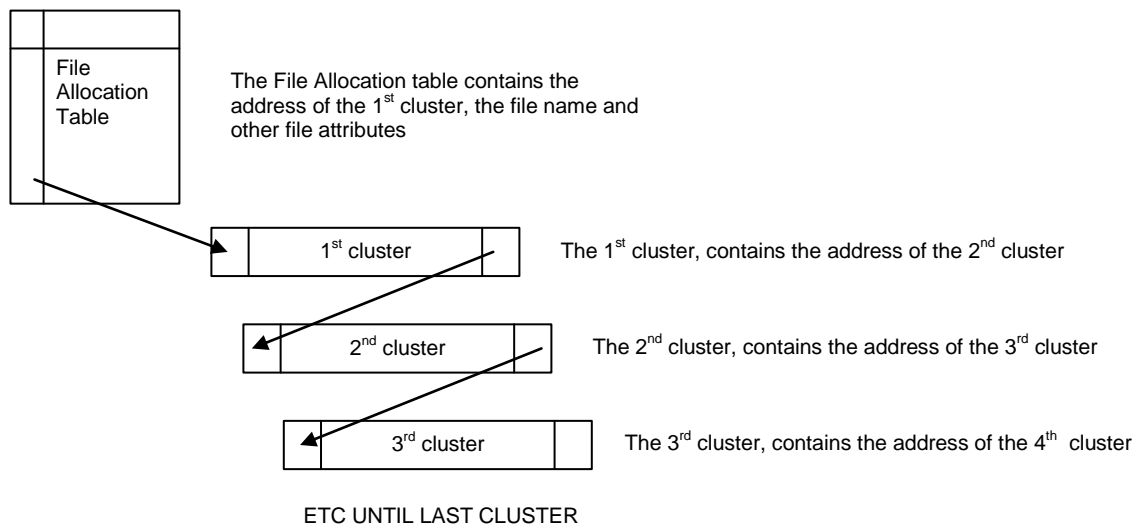
Data is stored on the surface of a platter in **sectors** and **tracks**. Tracks are concentric circles, and sectors are pie-shaped wedges on a track, as shown in figure 5.

A typical track is shown in yellow; a typical sector is shown in blue. A sector contains a fixed number of bytes -- for example, 256 or 512. Either at the drive or the operating system level, sectors are often grouped together into **clusters**.

The process of **low-level formatting** a drive establishes the tracks and sectors on the platter. The starting and ending points of each sector are written onto the platter. This process prepares the drive to hold blocks of bytes.

High-level formatting then writes the file-storage structures, like the file-allocation table, into the sectors. This process prepares the drive to hold files.

Standard recovery techniques



• Figure 6 - File allocation and chaining of clusters

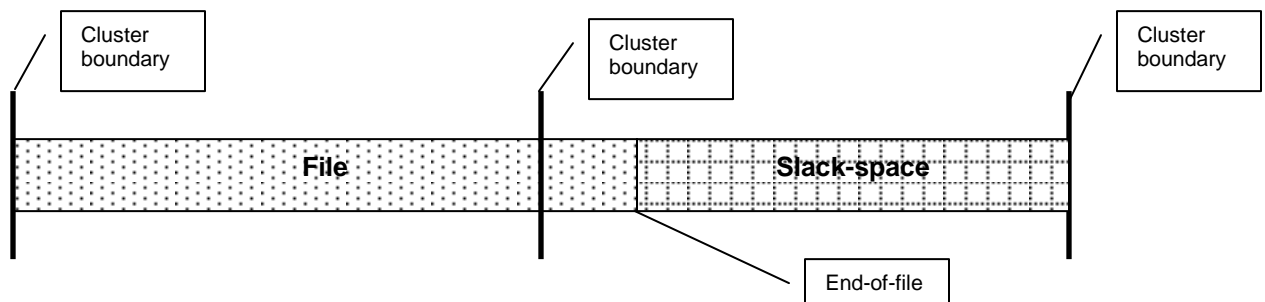
The hard disk of a computer is segmented into blocks of data called 'clusters'. A data file is made up of one or more clusters that are linked together as illustrated in figure 6. Each logical hard disk of a computer contains a 'File Allocation Table' (FAT) or similar. The FAT contains information about a file, including the address of the 1st cluster, the file's name and other metadata regarding the file. The 1st cluster contains the address of the 2nd cluster. The 2nd cluster contains the address of the 3rd cluster and so forth, until the end of the file that is marked by a special character (i.e. 'EOF').

The FAT also contains a table that indicates which clusters are used and which are not used.

When a program wants to access a file, it is assisted by the operating system, which looks for the file name in the FAT. It then uses the corresponding address to find the 1st cluster. After reading the 1st cluster, it uses the address of the 2nd cluster to find the 2nd cluster. After reading the 2nd cluster, it uses the address of the 3rd cluster to find the 3rd cluster and so forth until the end of the file.

When a file is deleted, the file's entry in the FAT is deleted (in some operating systems, such as Microsoft Windows, only the first character of the FAT entry is deleted) and the clusters are marked as 'not used'. The data stored in the clusters is not deleted until the operating system needs to write new data to that cluster (i.e. to create a new file, or change an existing file).

A hard disk is logically grouped in clusters and the start of a file is always the start of a cluster. A file will typically span more than one cluster, however the end-of-file (i.e. 'EOF') marker may not match a cluster boundary. Thus there may be some space between the end-of-file and the next cluster boundary. This is called 'slack space' and may contain data belonging to a previously deleted file.



• Figure 7 - slack space

Standard hard disk recovery processes attempt to discover files that have been deleted but not yet overwritten and reconstruct the clusters, eventually reconstructing the entire file.

Many commercial and free software tools are available to recover data. For example enCase (see www.guidancesoftware.com) is a tool favoured by many

law enforcement agencies. Recover My Files (see www.recovermyfiles.com) is Australian software that adequately performs file recovery.

Whilst standard file recovery techniques are popular and tools readily available the procedure can be somewhat lengthy. Using automated software simple analysis and recovery of a standard hard disk of 20Gb can take several hours. To perform an exhaustive search, practitioners may need to revert to manual inspection methods and that can take many days. In *Alexander v Federal Bureau of Investigation*⁴⁷ an expert testified in the high-profile investigation of President Clinton that the examination of a single hard drive would take approximately 265 hours.

Hard disk recovery is a probative test but not conclusive - if a file is recovered, its existence can be confirmed, however if the file is not recovered its prior existence cannot be denied. With experts quoting exorbitant sums for hard disk examinations - upwards of \$40,000⁴⁸ - parties subjected to discovery orders are questioning the viability of such procedures. For example in *Playboy Enterprise v Welles*⁴⁹ counsel convinced the court that recovery of e-mail files "simply was not feasible".

As with many computer forensic techniques, practitioners have focussed on practical aspects such as improving the tools of recovery, with little regard for empirical studies that measure the likelihood of success.

Garfinkel & Shelat⁵⁰ performed what they describe as an "informal survey" of hard drives demonstrating the abundance of information that can be recovered. They purchased 158 hard drives from an Internet auction. Of these, 129 still worked and they were able to recover files from all but 12. In total, they were able to recover 75Gb⁵¹ of file content.

Another informal study⁵² aimed to discover how long deleted information remains on the hard disk of a computer that is regularly used before it is overwritten. The study concluded that files deleted one year ago could still be recovered, however it was based on the examination of only three web servers that used the less popular Linux operating system.

My Survey

With little basis for a conclusion, I decided to perform my own survey.

An auction house had received a consignment of about 240 computers that had just come off an 18-month lease. The computers were from the front office of a

⁴⁷ 188 FRD (D.C. Cir 1998) §111, 112

⁴⁸ Patzakis, J (2003) *EnCase Legal Journal* Guidance Software www.encase.com p77

⁴⁹ 60 F.Supp.2d (S.D. Cal 1999) §1050-1054

⁵⁰ see <http://www.computer.org/security/garfinkel.html>

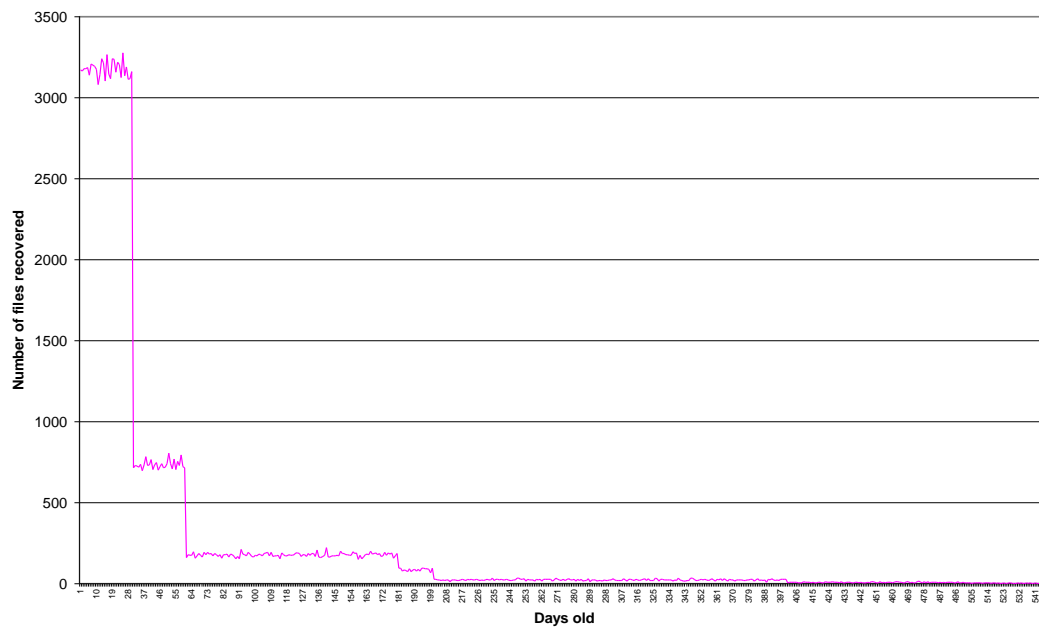
⁵¹ as a point of comparison, the entire encyclopaedia Britannica, including illustrations, fits on a single cd-rom that is 750Mb i.e. approx ¾ Gb

⁵² Venema, S (2003) Keynote address to the AusCERT Conference 2003, Gold Coast

large financial corporation so it was safe to make the assumption that they been used regularly through the lease period, although they had been formatted prior to arriving at the auction house.

All the computers used the popular Microsoft Windows 2000 operating system and most of the computers contained 20Gb hard disks although there were a number of larger ones.

Over twenty days and with the assistance of auction-house IT personnel, hard disk recovery was undertaken of each of the computers, noting the date that recovered files had been deleted⁵³. Figure 8 below illustrates the findings:



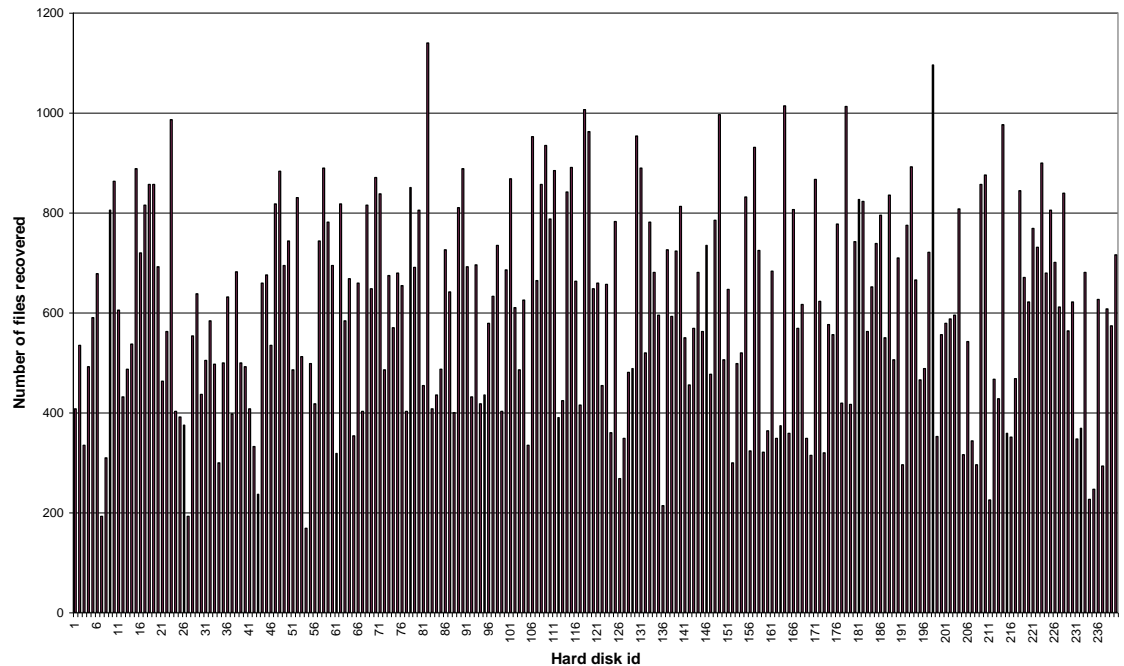
• Figure 8 - Standard hard disk recovery survey

About 145,200 files were recovered and the oldest were 549 days old (i.e. almost 1½ years). The average age of recovered files was 50 days. If the data is re-calculated for individual computers in the survey, the average is 47 days with a standard deviation of 15 days across computers. On average, it took between 5 and 6 hours to recover files from a hard disk⁵⁴.

Of particular note, is that a large number of files were recovered from every PC examined (see figure 9).

⁵³ based on the 'last modified' timestamp that is updated on each file modification, including erasure.

⁵⁴ When comparing this to estimates given for forensic analysis, note that the time quoted here is only for hard disk recovery and does not include creation of the hard disk image nor subsequent analysis. In my own experience it takes between 4-5 hours to image a 20Gb hard disk using forensically sound procedures.



• Figure 9 - number of recovered files per PC

One could hypothesize that staff deleting files prior to returning their computer skews the survey. Delivery records revealed that computers were collected from branch offices across the country in the month preceding my examination and it is reasonable to speculate that staff deleting files prior to giving up their computer accounted for the large number of files recovered within the first 30-day period. If these files are ignored the average then becomes 97 days.

Advanced recovery techniques

Software such as the freely downloaded PGP Freespace Wipe or a vast number of other wiping software is increasingly being used to frustrate investigators relying on standard hard disk recovery techniques.

For example, law enforcement agents have reported such software being used by paedophiles such as Robert Keating who ran a 184-member club distributing Internet child pornography from his home in Mackay⁵⁵. Keating not only used the software himself but also provided it to others in the club. The software was also found on one of the two laptops used by Yousef Ramsay, the World Trade Centre bomber, but fortunately for investigators they were able to recover information from the other.

⁵⁵ Anon (2002) Internet child porn king jailed for four years The Age 30-8-02
<http://www.theage.com.au/articles/2002/08/30/1030508121294.html>

Advanced hard disk recovery techniques permit the recovery of data even after the same portion of the hard disk has been overwritten.

Figure 10 is an image of the platter of a hard disk that has been enhanced by an electron microscope using a technique called Magnetic Force Microscopy (MFM)⁵⁶.

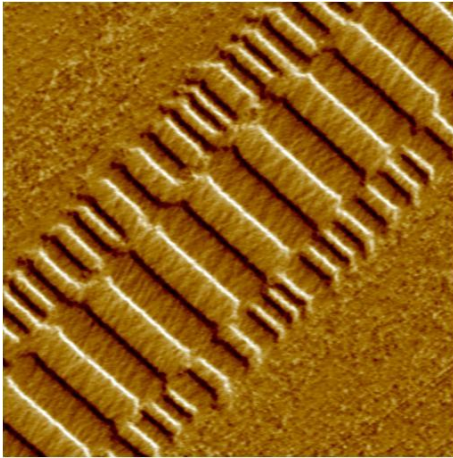


Figure 10 - Microscopic examination of hard disk platter

A single track is prominent in the centre of the illustration. This is the image of the electrical impulses recorded on the hard disk and constitutes the currently written file. As the platter spins, the impulses are recorded onto the platter by a tiny motor-controlled head, forming concentric tracks on the media.

In this illustration, the current data consists of "010101010101010101" that visualize as alternate ridges and valleys⁵⁷.

On either side of the prominent track, is other data. Like any instrument the motors controlling the head have a small margin of error. When the head again comes to the track to rewrite data, it is not always in exactly the same position. Thus on the outside of the prominent track, we can see the coding of previously written data. In this particular illustration, we can see the previous 3 tracks of data.

Advanced recovery techniques require specialised equipment and take many hours to analyse even the smallest hard drives. An estimate for performing this kind of recovery on a 20Gb hard drive is in the order of \$250,000, so is not reasonable for most litigation.

⁵⁶ Also see http://www.veeco.com/nanotechnology/nano_view.asp?CatID=3&page=2&recs=20&CP=#

⁵⁷ as an example. It may be "101010101010101010" depending on the polarity of the microscope.

Introduction

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 signature⁵⁸. In 2002, the Commonwealth Secretariat 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 whether 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.

Britain⁵⁹ and Canada⁶⁰ 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 standards⁶¹. The International Organisation for Computer Evidence⁶² 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:

⁵⁸ LMM(02)12 (2002) Draft Model Law on Electronic Evidence Commonwealth Secretariat, London

⁵⁹ PD 0008:1999 - *Legal Admissibility and Evidential Weight of Information Stored Electronically*,

⁶⁰ CAN/CGSB-72.34 - *Electronic Records as Documentary Evidence*

⁶¹ Minutes of a meeting of the Computer Forensic Standards working group 4-12-02

⁶² see www.ioce.org

- 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)

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 2003⁶³.

Standards Australia handbooks provide guidelines for implementation - they provide instruction but not justification and what now follows is a brief commentary on its contents.

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'Ciardhuain⁶⁴: "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

⁶³ Presentation by Keith Inman, Director Electronic Enforcement ASIC at the National Information Infrastructure Security Conference, 22-3 April 2003, Sydney

⁶⁴ Patel, A. & O Ciardhuain, S. (2000) *The impact of forensic computing on telecommunications* in IEEE Communications Magazine November 2000 pp64-67

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”⁶⁵.

What is IT Evidence?⁶⁶

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”⁶⁷.

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 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)⁶⁸. 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.

IT evidence can be divided into three categories⁶⁹: (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

⁶⁵ Tailleir, T (2001) *Digital Evidence: The Moral Challenge* in *International Journal of Digital Evidence* www.ijde.org/archives/tom_article.html

⁶⁶ HB-171 § 1.4

⁶⁷ HB-171 § 1.4

⁶⁸ QLRC WP51 (1998) *The Receipt of Evidence by Queensland Courts: Electronic Evidence* Queensland Law Reform Commission p5

⁶⁹ US DoJ (2002) *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, United States Department of Justice

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?⁷⁰

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 party⁷¹. 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 Evidence⁷²

As Sommer points out, legal proof does not correlate directly with scientific proof⁷³. Forensic computing specialists serve two masters, technology and the law, and they must find an acceptable balance between the two⁷⁴. 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 records⁷⁵
 - 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

⁷⁰ HB-171 § 1.5

⁷¹ 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).

⁷² HB-171 § 2

⁷³ Sommer, P (1998) Intrusion Detection Systems as Evidence Louvain-la-Neuve

⁷⁴ McKemmish, R (1999) What is Forensic Computing? Australian Institute of Criminology Trends & Issues No.

118

⁷⁵ HB-171 § 2.2.1

- c) Understand regulatory constraints to the retention and provision of records⁷⁶.

- Design for evidence⁷⁷

Ensure that computer systems and procedures are capable of establishing the following:

- a) The authenticity and alteration of electronic records;
- 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 collection⁷⁸

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 records⁷⁹

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 copies⁸⁰

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.

- Personnel⁸¹

⁷⁶ 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".

⁷⁷ HB-171 § 2.2.2

⁷⁸ HB-171 § 2.2.3

⁷⁹ HB-171 § 2.2.4

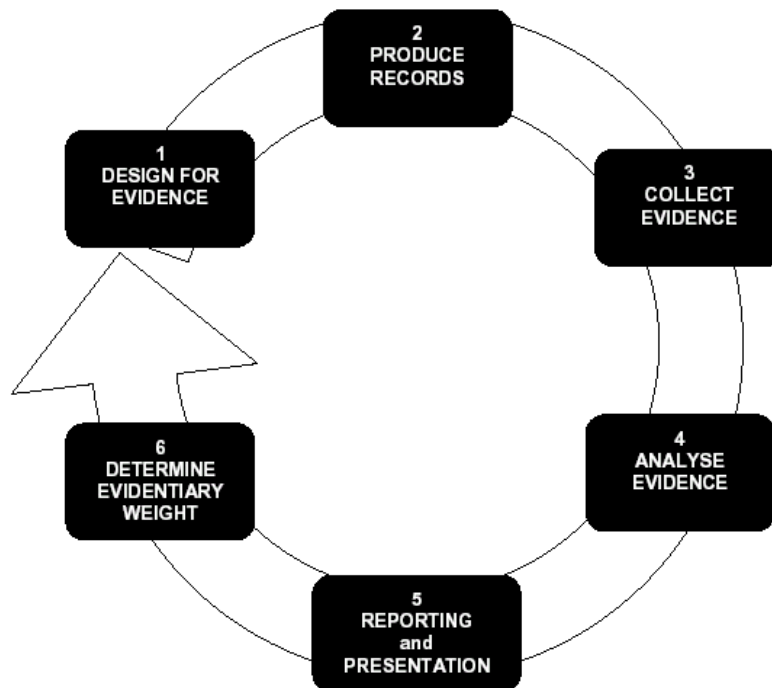
⁸⁰ HB-171 § 2.2.5

⁸¹ HB-171 § 2.2.6

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 Lifecycle⁸²

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.



• Figure 11 - 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.

⁸² HB-171 § 3

Step 1. Design for evidence⁸³

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.

Ensure that electronic records are identified, are available and are usable⁸⁴

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*⁸⁵.

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)⁸⁶ 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.

Identifying the author of electronic records⁸⁷

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 author⁸⁸. 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

⁸³ HB-171 § 3.2

⁸⁴ HB-171 § 3.2.1

⁸⁵ see §9.2 - Determining how long to retain records and §9.5 - Classification .

⁸⁶ § 286 – Obligation to keep financial records.

⁸⁷ HB-171 § 3.2.2

⁸⁸ Casey, E (2000) Digital Evidence and Computer Crime Academic Press

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/alterd. 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.

A computer-generated⁸⁹ 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.

Establishing the authenticity of electronic records⁹⁰

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"⁹¹.

"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

⁸⁹ 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).

⁹⁰ HB-171 § 3.2.3

⁹¹ DOJ (2000) Federal Guidelines for Searching and Seizing Computers US Department of Justice

manufactured⁹². This is a long-standing principle supported the often quoted words of Eyre: "The presumption...is, that no man would declare anything against himself, unless it were true, but that every man, if he was in difficulty, or in the view to any difficulty, would make declarations for himself"⁹³.

In relation to authenticity, the Australian Law Reform Commission⁹⁴ 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 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 (Casey, 2000). 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 themselves, 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. For example, an FBI agent who was present when the defendant's computer was seized can authenticate seized files or a telephone company billing supervisor can authenticate phone company records or the head of bank's consumer loan department can authenticate computerized loan data⁹⁵.

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.

⁹² Gobbo, J et al (1984) Cross on Evidence Butterworths p23

⁹³ Gobbo, J et al (1984) Cross on Evidence Butterworths p23

⁹⁴ ALRC 26 (1985) Interim report on Evidence Australian Law Reform Commission Vol 1 para180

⁹⁵ DOJ (2000) Federal Guidelines for Searching and Seizing Computers US Department of Justice

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.

Computer records can be altered easily, and opposing parties often allege that computer records lack authenticity because they have been tampered with or changed after they were created. For example, in *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997), detectives retrieved files that implicate the defendant from the computer of a drug dealer named Frost. Detectives required the assistance of Frost to help retrieve the files and allowed him to do so. The defence argued that with a few quick keystrokes, Frost could have inserted or changed data in the file to implicate their client.

The courts have responded with considerable scepticism to such unsupported claims that computer records have been altered. Absent specific evidence that tampering occurred, the mere possibility of tampering does not affect the authenticity of a computer record. In the case described, the trial judge ruled that computer records were admissible because the allegation of tampering was “almost wild-eyed speculation without evidence to support such a scenario”⁹⁶. In the absence of specific evidence of tampering, allegations that computer records have been altered go to their weight, not their admissibility.

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 techniques⁹⁷ (e.g. hash or MAC).

In many situations, records will be admitted with significant evidentiary weighting even though minor changes have occurred, so long as those changes are

⁹⁶ Also see *United States v. Glasser*, 773 F.2d 1553, 1559 (11th Cir. 1985)

"The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible."

⁹⁷ Cryptography is the use of mathematical algorithms to transform text (i.e. encryption) or test the validity of text (i.e. authentication).

“immaterial”⁹⁸ and arise in the normal course of communication, storage or display.

Establishing the time and date a particular computer electronic record was created or altered⁹⁹

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 3339¹⁰⁰ 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.

Establishing the reliability of computer programs¹⁰¹

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"¹⁰².

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 than not in working order¹⁰³. The basis of this view was laid down in a case having little to do with computers¹⁰⁴. In the *Statute of Liberty*¹⁰⁵ a collision occurred between two vessels on the Thames estuary. The estuary was monitored by radar and a film of the radar was admitted into evidence on the premise that where machines have replaced human beings it makes little sense to insist upon the rules devised to cater for human beings, as Simon P says “the law is bound these days to take cognisance of the fact that mechanical means replace human effort”¹⁰⁶.

This presumption is stated in the *Evidence Act 1915 (Cwth)* as:

⁹⁸ See Electronic Transactions Act 1999 (Cwth) §11 (3).

⁹⁹ HB-171 § 3.2.4

¹⁰⁰ Date and time on the internet: Timestamps

¹⁰¹ HB-171 § 3.2.5

¹⁰² See US Federal Rules of Evidence 901

¹⁰³ Gobbo, J et al (1984) *Cross on Evidence* Butterworths p44

¹⁰⁴ Hoey, A (1999) *Analysis of the Police and Criminal Evidence Act s69 – Computer Generated Evidence in Cybercrime & Security* Oceana Publications

¹⁰⁵ *Statute of Liberty* [1968] All ER 195

¹⁰⁶ in Hoey, A (1999) *Analysis of the Police and Criminal Evidence Act s69 – Computer Generated Evidence in Cybercrime & Security* Oceana Publications

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.

(2) 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)¹⁰⁷. In *Murphy & Anor v Lew & Ors*¹⁰⁸ Smith J of the Supreme Court of Victoria observed that in relation to 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 they 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

¹⁰⁷ QLRC WP51 (1998) *The Receipt of Evidence by Queensland Courts: Electronic Evidence* Queensland Law Reform Commission p53

¹⁰⁸ Unreported Sup Ct, Vic, No 12377 of 1991, 12 September 1997

- 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. ISO/IEC 21827 describes a CMM for systems security engineering and includes audit trails and log files. ISO/IEC 21827 specifies means to assess the maturity level of each of the ISMS management processes using the capability levels summarised in figure 12.

Capability Level	Description
Level 1 – Performed Informally	"Performed Informally," focuses on whether an organization or project performs a process that incorporates the base practices. This level can be characterized by the statement, "you have to do it before you can manage it."
Level 2 – Planned and Tracked	"Planned and Tracked," focuses on project-level definition, planning, and performance issues. This level can be characterized by the statement, "understand what's happening on the project before defining organization-wide processes."
Level 3 – Well Defined	"Well Defined," focuses on disciplined tailoring from defined processes at the organization level. This level can be characterized by the statement, "use the best of what you've learned from your projects to create organization-wide processes."
Level 4 – Quantitatively Controlled	"Quantitatively Controlled," focuses on measurements being tied to the business goals of the organization. Although it is essential to begin collecting and using basic project measures early, measurement and use of data is not expected organization wide until the higher levels have been achieved. This level can be characterized by the statements, "you can't measure it until you know what 'it' is" and "managing with measurement is only meaningful when you're measuring the right things."
Level 5 – Continuously Improving	"Continuously Improving," gains leverage from all the management practice improvements seen in the earlier levels, then emphasizes the cultural shifts that will sustain the gains made. This level can be characterized by the statement, "a culture of continuous improvement requires a foundation of sound management practice, defined processes, and measurable goals."

• Figure 12 - The capability levels of ISO/IEC 21827

Organizations that purchase software can refer to the formal assessment criteria of the provider to demonstrate the reliability of acquired software.

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 requests¹⁰⁹. 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 admissibility¹¹⁰.

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 document¹¹¹. 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 Records¹¹²

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.

Correct operation¹¹³

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.

¹⁰⁹ See *United States v. Dioguardi*, 428 F.2d 1033, 1038 (C.A.N.Y. 1970)

¹¹⁰ DOJ (2000) *Federal Guidelines for Searching and Seizing Computers* US Department of Justice

¹¹¹ McKemmish, R (1999) *What is Forensic Computing?* Australian Institute of Criminology Trends & Issues No.

118

¹¹² HB-171 § 3.3

¹¹³ HB-171 § 3.3.1

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*¹¹⁴ 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 Evidence¹¹⁵

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.

Standards for Evidence Collection¹¹⁶

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*¹¹⁷ provides a cautionary perspective:

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

¹¹⁴ see § 8.4 - Housekeeping

¹¹⁵ HB-171 § 3.4

¹¹⁶ HB-171 § 3.4.1

¹¹⁷ 167 FRD 90 (D. Colorado) at 90 and 112

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”.

Contemporaneous Notes¹¹⁸

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.

Relevance¹¹⁹

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.

For example, a suspect claimed that he was in his workplace working on a computer at the time Police alleged he was at a murder scene. The suspect claimed that his employer’s computer login records would demonstrate this. The systems administrator was asked by police to examine computer login records on a certain day. The systems administrator was unaware of the reason for the request and provided login records for the central computer system that did not include the suspect’s login. Had the system administrator known the reason for the request, she would have produced records for a little-used computer system that in fact demonstrated that the suspect was using a computer in the workplace at the time in question.

The indiscriminate copying of all data residing on a computer system may breach evidentiary rules that only permit the seizure of relevant evidence¹²⁰. 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.¹²¹

¹¹⁸ HB-171 § 3.4.2

¹¹⁹ HB-171 § 3.4.3

¹²⁰ see Bartlett V. Weir & Anors (1994) 72 A Crim R 511

¹²¹ 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.

Chain of Custody¹²²

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.

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 document¹²³;
- 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.

Non-readable electronic records¹²⁴

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*¹²⁵: “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.

¹²² HB-171 § 3.4.4

¹²³ 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).

¹²⁴ HB-171 § 3.4.5

¹²⁵ 1 F.3d 1274 (D.C. Cir 1993)

Limitations¹²⁶

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 privilege¹²⁷, 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:

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 evidence¹²⁸

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.

¹²⁶ HB-171 § 3.4.7

¹²⁷ See §3.10 of the Evidence Act (1995).

¹²⁸ HB-171 § 3.5

Use evidence copy¹²⁹

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.

Personnel qualifications¹³⁰

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 experience¹³¹. Experts must comply with procedures of the relevant Court. For example, the Federal Court and higher Courts require that experts adopt the ‘expert witness code of conduct’.

79 Exception: opinions based on specialised knowledge

If a person has specialised knowledge based on the person’s training, study or experience, the opinion rule does not apply to evidence of an opinion of that person that is wholly or substantially based on that knowledge.

Completeness of evidence¹³²

IT evidence is circumstantial. Persons conducting analysis of IT evidence must be provided with an explanation of: (a) The circumstances in which the electronic

¹²⁹ HB-171 § 3.5.1

¹³⁰ HB-171 § 3.5.2

¹³¹ See for example Federal Court rules order 34A rule 2 and NSW Supreme Court rules, interpretation.

¹³² HB-171 § 3.5.3

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. For example, a suspect claimed that he was in his workplace working on a computer at the time Police alleged he was at a murder scene. The suspect claimed that his employer's computer login records would demonstrate this. The systems administrator was asked by police to examine computer login records on a certain day. The systems administrator was unaware of the reason for the request and provided login records for the central computer system that did not include the suspect's login. Had the system administrator known the reason for the request, she would have produced records for a little-used computer system that in fact demonstrated that the suspect was using a computer in the workplace at the time in question.

Step 5. Reporting & presentation¹³³

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*¹³⁴, 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. Section 117 of the *Evidence Act 1915* states:

Certificates of expert evidence

(1) Evidence of a person's opinion may be adduced by tendering a certificate (expert certificate) signed by the person that:

- (a) states the person's name and address; and
- (b) states that the person has specialised knowledge based on his or her training, study or experience, as specified in the certificate; and
- (c) sets out an opinion that the person holds and that is expressed to be wholly or substantially based on that knowledge.

¹³³ HB-171 § 3.6

¹³⁴ [2002] FCA 906

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 complied¹³⁵.

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. For example in *United States v. Whitaker*¹³⁶, the defendant objected to admission of computer records obtained from a seized computer, on the basis that they were not properly authenticated because the government's witness, a federal agent, did not testify as to how the records were made. Under cross-examination, the agent admitted that he was not a computer expert, but rather an investigator. The agent's testimony that he was present when defendant's computer was seized and when the records were retrieved from the computer was sufficient to establish their authenticity.

Lay witnesses may also testify to the regular business use of a computer system and the resulting records. In *People vs Lugashi*¹³⁷, a bank employee produced printouts relating to transactions performed using one of its accounts. The defence incorrectly assumed that only a computer expert "who could personally perform the programming, inspect and maintain the software and hardware, and compare competing products, could supply the required testimony". Instead, the court determined that "a person who generally understands the systems operation and possesses sufficient knowledge and skill to properly use the system and explain the resultant data, even if unable to perform every task from initial design and programming to final printout, is a *qualified witness* for the purpose of establishing a foundation for the computer evidence". An important aspect in this case is that the Bank was a disinterested party, merely being the holder of the computer records.

Step 6. Determine evidentiary weighting¹³⁸

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.

When producing, collecting or analysing electronic evidence, its purpose and final arbiter may not be clear. "Given the likelihood of judicial scrutiny"¹³⁹, 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

¹³⁵ See Commonwealth Development Bank & Anor v Cassegrain [2002] NSWSC 980 and Makita (Australia) Pty Ltd v Sprowles [2001] NSWCA 305

¹³⁶ 127 F.3d 595 (U.S. App. 1997)

¹³⁷ (1999) 205 Cal.App.3d at 636

¹³⁸ HB-171 § 3.7

¹³⁹ McKemmish, R (1999) What is Forensic Computing? Australian Institute of Criminology Trends & Issues No.

own inquires”¹⁴⁰. 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 whether 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 acceptance¹⁴¹. In the US, this has become known as the *Daubert*¹⁴² 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”¹⁴³ 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.

¹⁴⁰ QLRC WP51 (1998) The Receipt of Evidence by Queensland Courts: Electronic Evidence Queensland Law Reform Commission p6

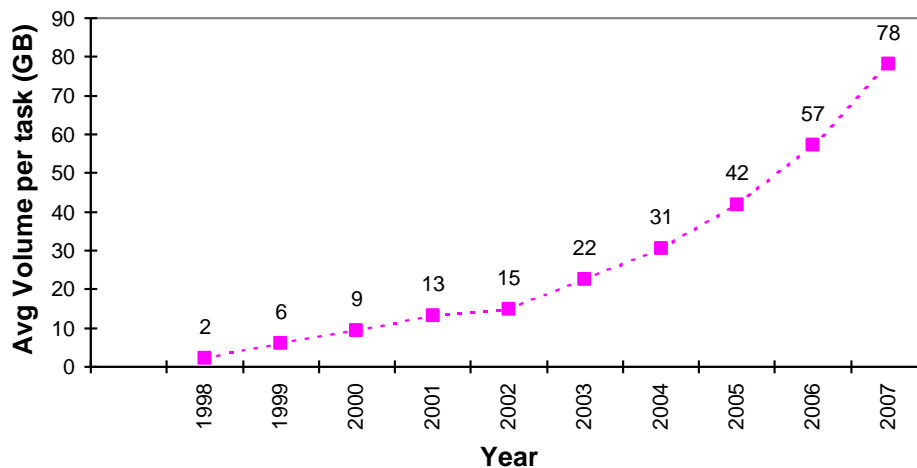
¹⁴¹ Dermen, J (1998) *Virtual Reality Evidence* in Cybercrime & Security Oceana Publications p11

¹⁴² see *Daubert v Merrell Dow Pharmaceuticals Inc* 509 US at 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993)

¹⁴³ ALRC 26 (1985) Interim report on Evidence Australian Law Reform Commission Vol 1 para180

Introduction

One of the problems of e-discovery is searching huge volumes of information for relevant records. Figure 13 illustrates the average size of hard disks searched by police computer forensic examiners and expected in the near future. This data reflects the usage of common desktop and laptop computer systems by criminals and victims.



• Figure 13 - volume of data submitted for analysis¹⁴⁴

In a civil context, the situation is somewhat different. Whilst most desktop computers contain hard disk in the order of 20-100Gb, commercial network servers and storage area networks are much larger. The systems for banks, telecommunications carriers and ISP's are frighteningly large. For example, a mid-size ISP would commonly have at least one 2-terabyte storage system which is 500,000 times that of most desktops and the large banks each have several 20-terabyte storage silos.

As with other types of discovery, the success of e-discovery depends on the searcher's ability to recognise relevant records commingled with other records.

¹⁴⁴ derived from data in Wheeler, P (2003) Submission by Victoria Police to the Parliamentary Joint Committee on the Australian Crime Commission Victoria Police

Search Strategies

Keyword searches

Searching for a keyword, or a text string, is perhaps the simplest form of searching. Keyword searching is only effective if the relevant records are stored on the hard disk in text format - most word processors, many spreadsheets, many databases and most e-mail are stored, at least partially, in text format. Keyword searches will reveal nothing about sound or image files.

Keyword searches are most commonly used by Police to establish if a computer contains any evidence, prior to seizing it under search warrant.

There are many free and commercial tools that can be used to conduct keyword searches. GREP is perhaps the most popular and it allows the searcher to use various wildcards in the keyword. A common mistake is to use tools available on the target computer to perform the search. A Windows computer has a "Search" or "Find" tool, however performing the search changes critical metadata such as the time the file was last accessed.

Keyword searches are often used to search the entire hard disk, a practice that may be appropriate for small desktop computers but will take too long for larger drives. For example the search of the entire 2 Terabyte storage system of a small ISP took about 32 hours.

File signatures

There are thousands of file types, many of which have been standardised by the International Standards Organisation (ISO). Files types are typically associated with a specific file extension. For example if a file is named EXAMPLE.GIF, the file extension is ".GIF" and could be expected to contain a particular image format.

File extensions however are discretionary and a user may choose to replace a default file extension with something else. For example an employee may replace the ".GIF" extensions with ".DOC" so that the resulting file EXAMPLE.DOC appears to be a document. File extensions are also shared by many similar applications.

File types are also associated with particular signatures - i.e. the beginning portion of the file - that are unique for the file type. By examining a file signature, the searcher can determine the file type. For example, a Microsoft Word document will always begin with:

```
D0,CF,11,E0,A1,B1,1A,E1  
00,00,00,00,00,00,00,00  
00,00,00,00,00,00,00,00  
3E,00,03,00,FE,EF,09,00
```

• Figure 14 - Microsoft Word document file signature

The file signature identifies the type of file, but does not reveal anything else about the data contained in that file.

Signature analysis can be used to locate files of a particular type that can be viewed by the searcher. It can also be used to locate files for which the extensions have been purposefully changed.

A fruitful strategy is to use signature analysis to locate particular file types that contain text e.g. documents, spreadsheets and e-mail. These can then be searched using a keyword search.

Hash library

A “hash value” is a sort of digital fingerprint that can be created for any file and for all practical purposes is unique. A hash library is a collection of hash values for known files and can be used by a search program to identify files that are known to be of little interest, such as operating system files and common application programs. It can also be used to identify known files of interest, such as a particular pornographic image.

A computer program automatically searches the entirety of the hard disk. For every file it finds, it calculates a hash value and compares it to the library creating a list of files that are important or that can be excluded or that need to be manually searched.

For searching purposes, hash libraries are only useful for previously encountered files but for unknown files are an efficient mechanism for narrowing the search. For example, on an office desktop hash libraries typically reduce the search to less than 10% of the data on the hard disk. When searching for particular attachments to an e-mail utilising a hash library typically automates the search altogether.

Compression

Compression refers to various techniques used to ‘squash’ data files to minimise the space they occupy on a hard disk. The result of compression is a file that can be interpreted by a compression program but is not recognisable text. Consequently a keyword search strategy will not discover a compressed file.

Unfortunately for e-discovery purposes, compression techniques are increasingly commonplace. Sometimes compression may be achieved using a computer program such as PKZip, resulting in the familiar .ZIP file extension. Many such programs exist. Sometimes compression may be included within the computer's operating system with a common example being Microsoft's compressed folder.

The key distinction between compression and encryption is that a compressed file may be reconstructed by anyone with the appropriate computer program.

There are two avenues for dealing with compression. Firstly, a file signature or hash library search can be used to identify compressed files or folders that can be decrypted using the appropriate compression program. Secondly, the searcher may pre-prepare a hash library that includes compressed versions of the relevant files.

When compression is included as an operating system feature, it may be appropriate to search for files on the 'live' system.

Encryption

Encryption refers to various techniques used to "scramble" data files so that they only become legible to authorised parties. There are many encryption techniques and many ways to defeat them, discussions of which are beyond the scope of this seminar.

Encrypted files will not be discovered using a keyword or hash library search. The best that a searcher can hope is to identify encrypted files using a file signature search.

Whilst good encryption technologies are almost impossible to decipher, many common encryption programs contain weaknesses that allow experts to decipher data with reasonable effort. Sometimes experts might try to find or guess the password.

An alternate strategy is to discover a legible (or clear) version of the encrypted file. Often a document will be authored 'in the clear' and only encrypted upon completion. In such cases a useful copy of the file may be discovered as a deleted file on the hard disk.

Introduction

Preservation of computer files is perhaps the simplest concept to describe but is perhaps the least followed of forensic principles.

The practical will demonstrate the ease at which a searcher can preserve a hard disk by making a copy that can be validated as an exact copy of the original.

Pull the plug?

If a computer is already on when a searcher discovers it, the first decision is whether to stop the computer or to perform the search on the computer. Each case must be assessed carefully, but the searcher must consider:

- If keeping the computer could damage data. For example if the computer is connected to a network, a person may access that computer via the network. Alternatively a special program may be installed to delete data.
- If stopping the computer could damage data.
- If stopping the computer could prevent future access. For example if a password is required or encryption has been used.


If the decision is made to stop the computer, the searcher must decide on the appropriate way to do this. Some operating systems change the data on the hard disk as part of a system shutdown. Other operating systems may not restart properly if they are not properly shutdown. The following table provides a quick guide for common operating systems:

Operating System	Strategy
DOS	Pull the plug
Windows 3.1	Pull the plug
Windows 95 & 98	Pull the plug
Windows NT & 2000 (desktop)	Pull the plug
Windows NT & 2000 server	Gracefully shutdown
Linux	Gracefully shutdown
Unix	Gracefully shutdown
Novell	Gracefully shutdown
Macintosh	Pull the plug

Digital fingerprints

Section 3.2.3.2 of the Guidelines for the Management of IT Evidence describe techniques for identifying alterations to evidence. One such techniques is to use a cryptographic mechanism such as a “hash” or “MAC”¹⁴⁵. A hash or MAC is essentially a digital fingerprint that uniquely identifies digital data such as a computer file.

The following table illustrates how a hash or MAC can be used to confirm that a copy of a hard disk or computer file is an exact copy of the original:

TIME 	Original	Copy	Compressed or encrypted copy
	Create or received the <i>original</i>		
	Apply hash or MAC algorithm to <i>original</i> . Output is MAC1	Create the <i>copy</i>	Compress or encrypt the original/copy (i.e. create the <i>compressed copy</i>)
		Apply hash or MAC algorithm to <i>copy</i> . Output is MAC2	Uncompress compressed copy to create copy
		If MAC2=MAC1 then copy is identical to original	Apply hash or MAC algorithm to <i>copy</i> . Output is MAC3
	Apply hash or MAC algorithm to <i>original</i> . Output is MAC4		If MAC3=MAC1 then copy is identical to original
	If MAC4≠MAC1 then record has been altered.		

The studies used to justify the admissibility of human fingerprint evidence suggest that:

¹⁴⁵ Message Authentication Code

- The Galton study suggests that the chances of any two human beings having the same fingerprint is one in 6,400,000,000;
- The Osterburg study suggests that the chances of any two human beings having the same fingerprint is one in 100,000,000,000,000,000 or 100 billion billion;

An MD5 is a standard hash algorithm. The chance of any two files having the same MD5 hash is 2^{128} that is approximately 340,282,366,920,938,000,000,000,000,000,000,000,000,000 or 340 billion billion. Another common algorithm is the SHA-1 with even better odds.

Storage Media

The original hard disk must be duplicated onto stable media. Typical choices are cd-rom, magnetic tape or another hard disk.

For smaller hard disks or single files a cd-rom is a good choice since, in the CD-R format, data can only be written so there is little scope for allegations of tampering. The problem is that each cd-rom only hold 750Mb of data so the copy will require many cd-roms.

For large hard disks, magnetic tape is a popular choice. The main drawback is that it is slow to copy and the tape itself cannot be used for analysis - the analyst must copy files from the tape onto his or her computer before use.

Using another hard disk overcomes the problems of cd-roms and magnetic tapes. However the resultant copy is as fragile as the original so care must be taken to ensure it does not change.

Proven Tools

The National Institute of Justice's Computer Forensic Tool Testing project certifies three commonly used hard disk imaging tools with testing performed by the US National Institute of Standards and Technology¹⁴⁶. At the time of writing, the following tools have been tested:

- SafeBack version 2.18
- EnCase version 3.20
- dd GNU fileutils version 4.0.36 (included with Red Hat Linux); and
- BSD dd

¹⁴⁶ www.ojp.usdoj.gov/nij/sciencetech/cft.htm

These tools have been certified against stringent criteria and practitioners use other tools at their peril.

Presenting Evidence

Introduction

In *Kabushiki Kaisha Sony Computer Entertainment v Stevens*¹⁴⁷, 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”.

A trial involving digital evidence differs in two fundamental respects from most other trials. Firstly, legal issues concerning the admissibility of digital evidence will nearly always arise. Secondly, a trial involving digital evidence may involve complex or unfamiliar terms, issues and concepts. Careful planning of how a case will be presented and how digital evidence will be used are essential to the successful outcome of a trial.

Educating the audience

If a case is complex, educate the audience – other solicitors, barristers, judges and the jury – at every stage of the litigation process.

While it is important to bring the audience up to a minimum level of competency or understanding, do not make them experts: that is what experts are for. The general rule of prosecution is keep it simple and that holds especially true in the presentation of a case that is complex by nature. Let the defence make things complex. Consider which issues will be handled during case-in-chief and which to save for cross examination or rebuttal.

What needs to be proved/disproved?

Every case requires careful examination of the elements of the charges to ensure that convincing evidence will be presented as to each and every element. Digital evidence cases often require a determination by the prosecutor of what can and should be eliminated as reasonable explanations for the digital evidence. The key questions are:

- Is it necessary to disprove all alternative explanations?
- Can all reasonable alternative explanations be disproved?

¹⁴⁷ [2002] FCA 906

Technical Anomalies

The nature of computer 'incidents' means that in some instances there will be no complete or clearly adequate explanation for a particular anomaly in the evidence or the time and money costs of explaining each anomaly will be prohibitive.

As computers and operating systems have become more complex, most network administrators and computer maintenance personnel limit their problem solving to the most frequently recurring problems. If a problem goes away upon rebooting and does not recur, it is a problem is not solved, even if there is no explanation for the problem.

Computer experts accept the existence of unexplained 'bugs' or 'glitches' without doubting the validity of information stored or processed by computers. Often there will be a conflict between the practical limits on what you want to or can prove or disprove and a defence attorney's use of alternative explanations to create reasonable doubt.

Disproving Alternatives

What a prosecutor has to disprove depends on what issue is involved and the strength of the rest of the case. When a crucial element is knowledge (e.g. in a possession of child pornography case), the prosecutor must be prepared to disprove defence claims that the pornography was stored on the defendant's computer without his knowledge.

The prosecutor does not need to disprove unreasonable alternatives (e.g., the pictures appeared on the defendant's computer out of the ether). When the hash values are different between the original evidence and the forensic copy, but there is an overwhelming amount of evidence on the computer (e.g., thousands of child porn pictures) the discrepancy in the hash values can be described and argued as irrelevant to the real issues in the case.

Timing is Everything

When to rebut a defence is important. For example, if the defendant's knowledge of the contents of her/his computer will be crucial, it is sometimes wise to let the defendant raise the issue and allow the evidence (either through cross examination or rebuttal) rebut this claim, rather than asserting the disproof in the case-in-chief. A jury will often attach more importance to issues raised in the state's case, and hold the prosecutor to a higher standard than when the defence has raised the issue and the prosecutor is merely attacking the defence argument.

Expert Witnesses/Scientific Method Evidence

Deciding Whether a Technical Expert Witness is Needed

A major decision in cases that involve complex technology and extensive forensic examination of the digital evidence is whether to use an 'expert witness' (i.e., one qualified by special training, knowledge, or experience, to give an opinion). A witness can testify to extremely complex matters without having to qualify as an expert witness or be asked to give an expert opinion about a particular matter at issue in the case.

For example, in many cases involving digital evidence, either the investigator at the scene or an expert forensic examiner could testify as to how digital evidence was located. While the forensic examination process may involve a scientific method and the examiner may well have used experts skills and techniques, the only relevant issue at trial is whether the evidence in question was on the suspect's computer, not how it was located. Either it is or is not on the computer. For that question, the examiner is a fact witness.

Using Technical Fact Witnesses and Expert Opinion Witnesses Effectively

There may be situations in digital evidence cases when expert opinion testimony is needed. When working with expert witnesses in digital evidence cases, pay special attention to the following:

- Identifying a community of qualified experts
- Explaining the issues in the case and the legal constraints for examining the available evidence
- Planning to Deal with a Daubert gatekeeping challenge
- Preparing the expert witness for trial
 - Learning to tell technical stories
 - Making direct examination simple and interesting
 - Developing visual aides that teach complex concepts
 - Avoiding bias in demeanour and testimony
 - Preparing the witness for defence experts and theories
 - Helping experts draft their own reports
 - Preparing for cross-examination
- Practice, practice, practice

Recurring Issues In Computer Crime Trials

While each digital evidence case will be different, there are some common issues that arise both with regard to the basic elements of the crimes charged and with regard to the nature of computers and computer networks. These include:

Identity

Although the digital evidence may show that a crime was committed from the defendant's computer, the prosecution may need to directly connect the defendant to the computer. The defendant can be tied personally to information found on the computer in a variety of ways, including:

- Confession or admission
- Circumstantially (the defendant was the only resident at the computer location, the defendant is the registered user of the hardware or software)
- Substantive information on the computer uniquely within the defendant's knowledge
- Content analysis. The existence of unique similarities between the grammar, spelling, or other characteristics of the evidence and other writing known to have been authored by the defendant.

Knowledge

In some cases it may be necessary to show the defendant's knowledge of the digital evidence on the computer. For example, one common defence in possession of child pornography cases is the claim that the defendant was not aware the images were on his computer. Such a claim can often be disproved by:

- The number of such images found
- The directory structure. Were the pictures placed in directories that were logically related to the pictures (e.g., C:\Pictures\young\girls\sex.)?
- File names. Are the files names unique and do they accurately describe the contents of the files (e.g., 8yrold.jpg.baby.jpg)?
- Other indications on the computer of the defendant's interest in child pornography, such as newsgroup subscriptions, history of Internet activity, etc.

Chronology of Events

Time and date stamps on files can be powerful evidence tying the defendant to the computer and the computer to the crime. The evidence may show that time and date stamps have limitations:

- The accuracy of a computer's time and date stamps is directly dependent upon the accuracy of the computer's internal clock.
- Time and date stamps are tied to a particular time zone.
- Time and date stamps can be easily manipulated.

The accuracy or inaccuracy of a time/date stamp can be shown in a variety of ways, including:

- Consistent offsets: Are the files consistently off by a specific amount of time or date (i.e., always one hour off or two days off.)? If so, there is a persuasive argument that the file times and dates can be adjusted by that offset and reflect accurate times/dates.
- Internal file accuracy: Is the time/date on a file consistent with the contents of a file? For example, is the date stamp on a file consisting of a letter consistent with the date in the introductory portions of the letter?
- E-mail header dates compared to time - date stamps assigned by the system: On e-mail systems where e-mail is saved as individual files (or where e-mail has been copied to a file) is the time and date information contained in the header of the e-mail consistent with the time and date stamp the system assigned the file?
- Compare known times and dates to system assigned times and dates: Were files downloaded from the victim at a known date and time? Do the files appear on the suspect's computer with time and date stamps consistent with that date and time?
- Networked computer: Many networks are configured to automatically update a client's internal clock when the client is logged on. Is the computer in question a network computer? Are the clocks on computers on that network auto updated?
- Patterns of file creation times and dates:
 - Is there a cluster of files created at the same date/time? The relative date/time (i.e., all created at the same time) may be more important than the absolute date/time of creation.
 - Experiment: Use the suspect's hardware (but not the original drive) to create and alter files. Observe the discrepancies, if any, and compare to the evidence files.

Presenting complicated/technical issues

There are some methods of presenting complicated evidence, whether in digital evidence cases or other complex cases, which work well. These include:

- Using very simple analogies can explain general concepts (e.g., sending email is like sending a postcard. It goes from the mail box to the local post office through other post offices to the recipient's local post office and then to their mail box.). Keep in mind, however, that all analogies can have legal consequences.
- Define technical words in terms the jury can understand
- Use pictures, drawings or graphs to demonstrate complex systems or concepts.
- Build the knowledge of the jury through the opening statement and through each successive layer of the testimony of the witnesses. Introduce them to simple concepts, explain those concepts in detail, and then move to more complex issues, which rely on understanding the initial concepts.
- Where possible, relate the technology in the case to the technology the jurors indicated in voir dire they were familiar with or used.

Federal Court of Australia



Practice Direction : Guidelines for Expert Witnesses in Proceedings in the Federal Court of Australia

This Practice Direction replaces the Practice Direction on Guidelines for Expert Witnesses in Proceedings in the Federal Court of Australia issued on 4 September 2003.

Practitioners should give a copy of the following guidelines to any witness they propose to retain for the purpose of preparing a report or giving evidence in a proceeding as to an opinion held by the witness that is wholly or substantially based on the specialised knowledge of the witness (see - Part 3.3 - Opinion of the [Evidence Act 1995 \(Cth\)](#)).

M.E.J. BLACK
Chief Justice
19 March 2004

Explanatory Memorandum

The guidelines are not intended to address all aspects of an expert witness's duties, but are intended to facilitate the admission of opinion evidence ([footnote #1](#)), and to assist experts to understand in general terms what the Court expects of an expert witness giving opinion evidence. Additionally, it is hoped that the guidelines will assist individual expert witnesses to avoid the criticism that is sometimes made (whether rightly or wrongly) that expert witnesses lack objectivity, or have coloured their evidence in favour of the party calling them.

Ways by which an expert witness giving opinion evidence may avoid criticism of partiality include ensuring that the report, or other

¹⁴⁸ Federal Court of Australia practice guideline see http://www.fedcourt.gov.au/how/prac_direction.html

statement of evidence:

- (a) is clearly expressed and not argumentative in tone;
- (b) is centrally concerned to express an opinion, upon a clearly defined question or questions, based on the expert's specialised knowledge;
- (c) identifies with precision the factual premises upon which the opinion is based;
- (d) explains the process of reasoning by which the expert reached the opinion expressed in the report;
- (e) is confined to the area or areas of the expert's specialised knowledge; and
- (f) identifies any pre-existing relationship between the author of the report, or his or her firm, company etc, and a party to the litigation (eg a treating medical practitioner, or a firm's accountant).

An expert is not disqualified from giving evidence by reason only of the fact of a pre-existing relationship with the party that proffers the expert as a witness, but the nature of the pre-existing relationship should be disclosed. Where an expert has such a relationship with the party the expert may need to pay particular attention to the identification of the factual premises upon which the expert's opinion is based. The expert should make it clear whether, and to what extent, the opinion is based on the personal knowledge of the expert (the factual basis for which might be required to be established by admissible evidence of the expert or another witness) derived from the ongoing relationship rather than on factual premises or assumptions provided to the expert by way of instructions.

All experts need to be aware that if they participate to a significant degree in the process of formulating and preparing the case of a party, they may find it difficult to maintain objectivity.

An expert witness does not compromise objectivity by defending, forcefully if necessary, an opinion based on the expert's specialised knowledge which is genuinely held but may do so if the expert is, for example, unwilling to give consideration to alternative factual premises or is unwilling, where appropriate, to acknowledge recognised differences of opinion or approach between experts in the relevant discipline.

The guidelines are, as their title indicates, no more than guidelines. Attempts to apply them literally in every case may prove unhelpful. In some areas of specialised knowledge and in some circumstances (eg some aspects of economic "evidence" in competition law cases) their literal interpretation may prove unworkable. The Court expects

legal practitioners and experts to work together to ensure that the guidelines are implemented in a practically sensible way which ensures that they achieve their intended purpose.

Guidelines

1. General Duty to the Court ([footnote #2](#))

- 1.1 An expert witness has an overriding duty to assist the Court on matters relevant to the expert's area of expertise.
- 1.2 An expert witness is not an advocate for a party.
- 1.3 An expert witness's paramount duty is to the Court and not to the person retaining the expert.

2. The Form of the Expert Evidence ([footnote #3](#))

- 2.1 An expert's written report must give details of the expert's qualifications, and of the literature or other material used in making the report.
- 2.2 All assumptions of fact made by the expert should be clearly and fully stated.
- 2.3 The report should identify who carried out any tests or experiments upon which the expert relied in compiling the report, and state the qualifications of the person who carried out any such test or experiment.
- 2.4 Where several opinions are provided in the report, the expert should summarise them.
- 2.5 The expert should give reasons for each opinion.
- 2.6 At the end of the report the expert should declare that "[the expert] has made all the inquiries which [the expert] believes are desirable and appropriate and that no matters of significance which [the expert] regards as relevant have, to [the expert's] knowledge, been withheld from the Court."
- 2.7 There should be included in or attached to the report (i) a statement of the questions or issues that the expert was asked to address; (ii) the factual premises upon which the report proceeds; and (iii) the documents and other materials which the expert has been instructed to consider.
- 2.8 If, after exchange of reports or at any other stage, an expert witness changes a material opinion, having read another expert's report or for any other reason, the change should be communicated in a timely manner (through legal representatives) to each party to whom the expert witness's report has been provided and, when appropriate, to the Court ([footnote #4](#)).
- 2.9 If an expert's opinion is not fully researched because the expert considers that insufficient data are available, or for any other

reason, this must be stated with an indication that the opinion is no more than a provisional one. Where an expert witness who has prepared a report believes that it may be incomplete or inaccurate without some qualification, that qualification must be stated in the report ([footnote #4](#)).

2.10 The expert should make it clear when a particular question or issue falls outside the relevant field of expertise.

2.11 Where an expert's report refers to photographs, plans, calculations, analyses, measurements, survey reports or other extrinsic matter, these must be provided to the opposite party at the same time as the exchange of reports ([footnote #5](#)).

3. Experts' Conference

3.1 If experts retained by the parties meet at the direction of the Court, it would be improper conduct for an expert to be given or to accept instructions not to reach agreement. If, at a meeting directed by the Court, the experts cannot reach agreement about matters of expert opinion, they should specify their reasons for being unable to do so.

footnote #1

As to the distinction between expert opinion evidence and expert assistance see *Evans Deakin Pty Ltd v Sebel Furniture Ltd* [2003] FCA 171 per Allsop J at [676].

footnote #2

See rule 35.3 Civil Procedure Rules (UK); see also Lord Woolf "Medics, Lawyers and the Courts" [1997] 16 C.J.Q. 302 at 313.

footnote #3

See rule 35.10 Civil Procedure Rules (UK) and Practice Direction 35 – Experts and Assessors (UK); *HG v the Queen* (1999) 197 CLR 414 per Gleeson CJ at [39]-[43]; *Ocean Marine Mutual Insurance Association (Europe) OV v Jetopay Pty Ltd* [2000] FCA 1463 (FC) at [17]-[23]

footnote #4

The "Ikarian Reefer" [1993] 20 FSR 563 at 565

footnote #5

The "Ikarian Reefer" [1993] 20 FSR 563 at 565-566. See also Ormrod "Scientific Evidence in Court" [1968] Crim LR 240.

Standard form of report

Note: This is provided as an example only

Introductory

1. I am Ajoy Ghosh of 34 Ryries Parade, Cremorne 2090 in the state of New South Wales.

Since the report is written in the first-person, identify “I”. Depending on the jurisdiction, you might be required to provide a home address.

Professional Experience

2. I am a UniSearch consultant and have completed their Expert Witness training course.
3. The Faculty of Law at the University of Technology, Sydney also employs me as a lecturer for postgraduate and international courses. There, I am also a candidate for PhD and my thesis is entitled “Crime in Cyberspace: an interdisciplinary study of law, technology and practice”.
4. I am the author of Standards Australia HB171: Guidelines for the Management of IT Evidence, a handbook commissioned jointly by the Attorney General’s Department and the Australian Federal Police and launched on 12 August 2003. I am the co-author of Standards Australia HB231: Guidelines for Information Security Risk Assessment a handbook first published in 2000.
5. I have over 12 years experience in information technology, specializing in computer crime and forensics, information technology security, audit and reliability. My resume is included as the attachment marked “A” that details my professional and academic qualifications.

Qualify yourself as an expert. Briefly state qualifications, affiliations and experience – use your standard resume for the details. Expect the other solicitor to check your resume and expect to explain any changes to previous publications.

Scope & Engagement

6. Deacons provided a letter of instruction dated 9 August 2004 (“**the letter of instruction**”) in which they instruct me to:
 - (i) Investigate the alleged PABX fraud at Sharp’s Blacktown premises;
 - (ii) Identify the reason or reasons for the alleged fraud, including which entity or entities is responsible for it and which entity or entities are not in any way responsible for it; and
 - (iii) Prepare a report of the findings, which identifies clearly the extent of the fraud, the reasons for it and the entities responsible for it.

You should always be “instructed” by a solicitor’s firm, not a particular solicitor – although in some jurisdictions the requirement varies. Recall your instructions exactly as they appear on the letter of instruction. You might attach the letter of instruction.

7. Gadens Lawyers has provided me with additional material with the letter of instruction that is listed in the “Index of Documents” attached to the letter of instruction.
8. Sharp Corporation of Australia have provided me with three CD-roms marked:
 - (i) “PABX DATA”;
 - (ii) “LOG FILES & MD5 CHECKSUM”; and
 - (iii) “ACCESS DATABASE + MORE LOG FILES”.
9. My opinion is based on the above-mentioned material, enquiries detailed in this report and my own knowledge/experience.

State any material upon which you rely in arriving at your opinion particularly any material provided by instructing solicitors.


10. I have read Schedule K of the Rules of the New South Wales Supreme Court (“*Expert Witness Code of Conduct*”) and agree to be bound by its terms.

Acknowledge the relevant *expert witness guidelines* or *code of conduct* prior to detailing your investigations and conclusion(s). If in doubt, use the highest Court in that jurisdiction e.g. in NSW use the Supreme Court.

Declaration

100. I declare that I have made all enquires that I believe are desirable and appropriate and that no matters of significance which I regard as relevant have, to my knowledge, been withheld from the Court.

Some jurisdictions require the above declaration. State any limitations of your enquires (e.g. time) and any further investigation that qualifies your opinion.

Signed: 

Date: 25th January 2005

Ajoy Ghosh

Sign and date you report.

How to give evidence, especially in cross- examination¹⁴⁹

For most people, giving evidence (and especially being cross-examined) is a strange and unnerving experience. This document is designed to help you through the process. If you have any questions at all about the case or your evidence or what will happen in court, never hesitate to ask the solicitor and/or barrister for the party which has “called you” (asked you to give evidence).

THE THREE GOLDEN RULES

You will read below a number of suggestions about how to give your evidence. However, you probably won't remember them all in the witness box. Don't worry about that. All you really need to remember are the Three Golden Rules. To do so you can use this memory aid: SHO.R.T.

Your answers must be: SHOrt

Responsive

Truthful

Just to confuse things, the order of importance of the Three Golden Rules is the reverse — your answers must be truthful, responsive and short — but TRSHO is not so easy to remember! After some preliminaries, each of these rules is considered below.

HOW TO PREPARE TO GIVE EVIDENCE

Above all else, you must know the contents of your affidavit (or witness statement) and its exhibits and annexures as well as you possibly can. Read and re-read them carefully. While no one expects you to be “word perfect” you should be aware that the cross-examiner will probably try to make a point out of even minor variations between your affidavit and what you say in court.

Learn the Three Golden Rules and familiarise yourself with the rest of these guidelines.

¹⁴⁹ Adapted from notes by Francious Knuc, Barrister

Do not hesitate to raise any questions or concerns you have with the solicitor and/or barrister for the party which has called you. In particular, if you find an error in your affidavit, something you no longer agree with or if you have remembered more about something, please raise it immediately with the solicitor and/or barrister. There is no problem about changing or adding to your evidence if your recollection alters or if you become aware that you have made a mistake.

WHAT HAPPENS WHEN YOU GO TO COURT

This will usually be the order of events when you go to court:

- i. Unless you have been told otherwise, you will have to sit outside the court. In addition to your affidavit or witness statement, bring something to read or work on. It is difficult to know exactly when you will be needed, so you may be kept waiting for some time. Every effort will be made to waste as little of your time as possible.
- ii. The court officer will call your name outside the court and will direct you to the witness box. You should bow to the judge both when you enter and leave the court. (Everyone also stands and bows to the judge whenever the judge enters and leaves the court.) Unless you are giving expert evidence, the only thing you should take into the witness box is a copy of your affidavit. Place it face down in front of you. You can leave your briefcase etc with the solicitor for the party which has called you.
- iii. The court officer will ask you to swear an oath on the Bible or to make an affirmation to tell the truth. To tell the truth is your only obligation in the witness box. Whether you swear on the Bible or make an affirmation is entirely up to you. The court will not consider your evidence any more or less believable depending on which option you choose. You remain standing and face the judge when swearing or affirming. You may then sit or stand in the witness box as you wish in order to give your evidence. You can ask for a glass of water if there isn't one already in front of you.
- iv. The barrister for the party which called you will then ask you your name, residential address and occupation. He or she will then ask you to confirm that you have made an affidavit(s) dated such and such in the proceedings.
- v. One of two things may then happen. The barrister may ask you some questions about the case. He or she will usually have discussed those questions with you beforehand. They will be designed to clarify or add to what appears in your affidavit. This is called "examination-in-chief". If the barrister does not have any such questions, the opposing barrister will begin to cross-examine you.
- vi. During the course of your cross-examination the barrister for the party which called you may make "objections" to the questions you are being asked. These are requests to the judge for a ruling as to whether the question is a proper one for you to be asked. What you should do when an objection is made is dealt with below in relation to the second of the Three Golden Rules.

- vii. After you have been cross-examined, the barrister for the party which called you may ask you a few questions arising from the answers you have given in cross-examination. This is called “re-examination”. It is not always done and, when it is, it is usually quite short. Whether it is done or not is not a reflection on you or how well you have given your evidence.
- viii. When your evidence has concluded you will usually be “excused” (told your attendance is no longer required). You will be free to go, although if you wish you will be welcome to stay in the court and watch the rest of the proceedings as a member of the public. It is theoretically possible that you may be “recalled” (asked to come back to court to give further evidence). The solicitor and/or barrister for the party which called you will usually raise this possibility with you. Being recalled is not a reflection on you or your evidence. It generally means an issue has unexpectedly arisen during the course of the trial and one side or the other considers that you may be able to give evidence relevant to that issue.

WHAT IS CROSS-EXAMINATION?

Cross-examination is a method of testing your evidence in an effort to assist the court in determining the truth: what “really” happened. The opposing barrister has two basic tasks to perform:

First, to show that, for whatever reason, the evidence you have given for the party which called you is in some way inaccurate or unreliable and therefore should not be used by the court in reaching its decision. Sometimes this may involve a challenge to your “credit”. Even if this does not go so far as saying you are lying (although it can), it will usually involve a suggestion that for some reason your evidence is skewed in favour of the party which has called you.

Second, to ask you to agree to facts which the opposing barrister will ultimately say are helpful to his or client. These are called “admissions” and are said to have particular weight when they are made by a witness called in an opposing interest.

The major difference between examination-in-chief and re-examination, on the one hand, and cross-examination, on the other hand, is the type question you can be asked. In the former, questions which suggest their answer (leading questions) cannot be asked. In cross-examination, leading questions are not only allowed, but they are the usual form of question. For example, in examination-in-chief or re-examination you can only be asked “what colour was the car?”. In cross-examination the question will be “it was a red car, wasn’t it?”.

THE FIRST GOLDEN RULE - TELL THE TRUTH

- This is your only obligation in the witness box.
- Do not worry about the effect of your answer on the case of the party which has called you. That is for the lawyers to worry about.

- Your answer should be based on your best recollection, not reconstruction or speculation. We use the word “would” a great deal in ordinary conversation: avoid it completely in giving evidence. In answer to “did you do X?” your response must never be “I would have” but rather “I did/didn’t recall”. The one exception is if you have an invariable practice, e.g. “Did you clean your teeth last Friday?”, “I don’t actually remember doing so, but I clean my teeth every day so I would have done.”
- If you have no actual recollection but there is a document (your affidavit or something else) from which you could refresh your memory, say so and ask the court for permission to look at it.
- Don’t be afraid or embarrassed to say that you don’t remember something or don’t know the answer to a question. No one expects you to have perfect recall. Never guess or speculate or make something up just for the sake of giving an answer. You will almost always be found out.
- If you realise while in the witness box that you have made a mistake in the answer you have just given or in any previous answer, say so and give a corrected answer.

THE SECOND GOLDEN RULE - RESPOND TO ONLY THE QUESTION

- In order to do this, you must first understand the question. Listen to the question very carefully and think about it for as long as you need to. If you don’t understand the question, say so and ask for the question to be repeated or rephrased. There is no problem with doing this.
- Taking time to think about the question also gives the barrister for the party which called you an opportunity to object to the question by saying “I object!”. If you hear that, do not answer the question or, if you have started to answer, stop immediately. Do not complete your answer. Remain silent until the judge tells you that you should answer the question. If you have forgotten the question because of the time taken to deal with the objection, say so. The question can then be read back to you.
- Answer only the question asked and nothing more. Do not volunteer information. For example, if the question is “what did you have for breakfast today?” the answer is “tea and toast”. Do not tell the cross-examiner about everything that happened to you from the time your alarm went off until you sat down to breakfast.
- Do not try to second guess the cross-examiner by trying to anticipate where you think he or she wants to get to with the questions or by giving the answer you think the cross-examiner wants as opposed to answering the actual question.

THE THIRD GOLDEN RULE - KEEP YOUR ANSWERS SHORT

- Your answers should be as short as possible, consistent with your primary obligation to tell the truth.
- If a question can be completely and honestly answered, for example, “yes” or “no”, then that is the answer you should give. If the answer requires some explanation, then that explanation should be short and to the point. There is a good reason for this. To use a graphic metaphor: the cross-examiner feeds off every word you say like a great white shark feeds off every chunk of meat thrown to it. The less you say, the less the cross-examiner has to go on or to get excited about. Also, the less you say, the less there will be to be clarified or explained in re-examination: “the less said, the more easily mended”.
- Do not try to fill in any silence between your answer and the next question by elaborating on your previous answer unless you genuinely believe that answer was incomplete or inaccurate.
- Some barristers use dramatic pauses and silent stares in an effort to get a witness to add to an answer they have just made. If you believe your answer was complete, do not give in to this, even if you feel the silence is embarrassing. You can break that silence by saying something like “That’s my answer”.

A FEW OTHER POINTS

- When giving evidence, speak clearly at a reasonable volume and a little more slowly than you would normally. The acoustics in a courtroom are not always good and your answers are being transcribed either by a stenographer in the court or from tapes. The stenographers/transcribers are fast, but not superhuman! The need for transcription also means that you should always say “yes” or “no” and not just nod or shake your head in answer to a question.
- When answering questions from any of the barristers or the judge, always address your answer to the judge. The judge is addressed as “your honour”. If you don’t know the cross-examiner’s name and you want to address him or her by title, use “sir” or “ma’am”.
- While you should take your affidavit into the witness box, keep it face down and do not refer to it unless you are asked to or unless you are unable to answer without doing so.
- If you are shown a document and referred to a particular part of it, you should look carefully at the whole of the document before you answer unless you are told by someone not to do so.
- The cross-examiner is not limited to asking you questions about what is in your affidavit. Do not be surprised if you are asked about things which seem to you to be irrelevant to the case or your evidence. Relevance is for the

lawyers to argue about. Just answer the questions in accordance with the Three Golden Rules.

- Do not argue or get angry with the cross-examiner. He or she is not attacking you personally. The cross-examiner has a job to do (and could just as easily have been arguing the case for the party which called you if he or she had not been retained by their opponents). Remain calm and polite at all times and think of the Three Golden Rules. This is particularly necessary if the cross-examiner accuses you of lying about something or aggressively puts an alternative version of events to you that does not accord with your evidence. In fact, the cross-examiner has a legal obligation to put the alternative to you. For example, if you say the accident happened on a wet road and the cross-examiner's client says the road was dry, the cross-examiner generally must suggest to you that you are mistaken and that the road was dry.
- Sometimes, particularly if you are an expert witness, the cross-examiner will ask you to make certain assumptions and then ask you questions based on those assumptions. Do not argue with the cross-examiner about the assumptions or comment on them (unless asked to do so), even if you think they are unrealistic or absurd. Just make sure you fully understand the assumptions and answer any questions in accordance with the Three Golden Rules on the basis of the assumptions you have been asked to make.
- Avoid getting into a machine gun pattern with the cross-examiner where you answer as soon as he or she has asked the question and the cross-examiner immediately asks another question. Some cross-examiners use this technique to try to confuse or trip up a witness. Always take as long as you need to think about the question and your answer, even in the face of a sarcastic comment from the cross-examiner like "you don't need to think about that, do you?".
- The cross-examiner may try to force you to confine your answer to "yes" or "no". Don't do so unless that is a totally accurate answer. If the cross-examiner is insistent, your answer should be "The answer is yes/no, but I would need to qualify that". If the cross-examiner doesn't ask you what the qualification is, you will be asked in re-examination. This is a way of telling the barrister for the party which called you that there is more that you feel you need to say that the cross-examiner is not letting you say. If you are cut-off by the judge or the cross-examiner if you attempt to give the qualification, don't worry about it. It is for the lawyers to decide whether your qualification is relevant to the legal issues in the case.
- Another helpful variation on the "qualified" answer is in relation to questions like "he said X?" or "Y happened, didn't it". A sufficient answer may be "yes" or "no", but a better answer will be "No, he said something else" or "No, something else happened" or "Yes, but he said more than that" or "Yes, but something else happened as well". If the cross-examiner doesn't ask you what the something else was, you will probably be asked in re-examination.

- Questions asked by the judge should be treated exactly in the same way as questions asked by the cross-examiner. There is no special “magic” just because the judge has asked the question.
- While being cross-examined (including during tea adjournments, overnight etc) do not discuss your evidence or the case with anyone including lawyers, family, other witnesses or colleagues.
- In the unlikely event that anyone approaches you at any time in relation to your evidence (e.g. asking you about it, seeking to induce you to change it) you should report that approach to the solicitors for the party which has called you. There is, however, nothing wrong with the legal representatives for the other side contacting you to see if you will talk to them about your evidence, but you are under no obligation to speak to them if you do not want to do so.