GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Computer Forensics – We've had an incident, who do we get to investigate?

Karen Ryder

GSEC Certification: Assignment Version 1.3

Summary

Computer forensics is used to conduct investigations into computer related incidents, whether the incident is an external intrusion into your system, internal fraud, or staff breaching your security policy. The computer forensic method to be used is determined by the company's management. In deciding which method to use, whether it is in-house, law enforcement or private sector computer forensic specialists, management needs to understand what is computer forensics, the rules of computer forensics, and the implications of mishandling evidence. In Australia, there are eight different 'Evidence Act's', which govern the rules of evidence that investigators need to be aware of in order to present evidence that will be legally acceptable in any Australian court. This is particularly important for National companies where investigations can cross from one state jurisdiction to another.

A manager needs to consider these issues when deciding on which method of investigation to use. A decision regarding which method to use should not be left until an incident occurs, it should be incorporated into a company's incident response plan. There is no one size fits all solution for computer forensics investigations, your organisation may choose one or all three options depending upon the severity of the incident involved.

Introduction

"*Computer forensics is the equivalent of surveying a crime scene or performing an autopsy on a victim*" (James Borek 2001).

How many people in your organisation, who have not had law enforcement training, would have the ability to do this and present evidence that would be acceptable in a court of law? Regardless of whether the incident is an external intrusion, fraud, or internal staff misconduct, the investigation needs to be treated the same way, and the same rules of evidence apply.

So how does a manager (IT or not) decide how to investigate an incident? Does the company conduct the investigation themselves using their existing personnel, do they bring in the assistance of the Police, or do they hire the services of a professional computer forensics company? This paper's aim is to provide Australian managers with a basis to make this decision by providing an insight into computer forensics and evidence handling, and giving advantages and disadvantages for each option.

This paper is meant as a guide only; it does not provide legal advice.
Laws differ from region to region so you should always obtain your own professional legal advice where required.

What is Computer Forensics?

"*Forensic Computing is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable.*" (Rodney McKemmish 1999)

From this definition we can clearly identify four components.

Identifying

This is the process of identifying such things as what evidence is present, where and how it is stored, and which operating system is being used. From this information the investigator can identify the appropriate recovery methodologies, and the tools to be used.

Preserving

This is the process of preserving the integrity of the digital evidence, ensuring the chain of custody is not broken. The data needs to be preserved (copied) on stable media such as CD-ROM, using reproducible methodologies. All steps taken to capture the data must be documented. Any changes to the evidence must also be documented, including what the change was and the reason for the change. You may need to prove the integrity of the data in a court of law.

Analysing

This is the process of reviewing and examining the data. The advantage of copying this data onto CD-ROMs is the fact that it can be viewed without risk of accidental changes, therefore maintaining the integrity whilst examining the evidence.

Presenting

This is the process of presenting the evidence in a legally acceptable and understandable manner. If the matter is presented in court the jury, who may have little or no computer experience, must all be able to understand what is presented and how it relates to the original, otherwise all your efforts could be futile.

Rules of Computer Forensics

When conducting computer forensic examinations there are certain rules that must be applied to your investigation.

Minimal Handling of the Original

This can be regarded as the most important rule in computer forensics. Where possible make duplicate copies of the evidence and examine the duplicates. In doing this, the copy must be an exact reproduction of the original, and you must also authenticate the copy, otherwise questions can be raised over the integrity of the evidence.

Account for any change

In certain circumstances changes to the evidence may be unavoidable. For

instance, booting up or shutting down a machine can result in changes to the memory, and/or temporary files. Where changes do occur, the nature, extent and reason for the change must be documented.

Comply with the rules of evidence

The rules of evidence are the rules investigators must follow when handling and examining evidence, to ensure the evidence they collect will be accepted by a court of law.

Do not exceed your knowledge.

Do not proceed with an investigation if it is beyond your level of knowledge and skill. If you find yourself in this situation you should seek assistance from one more experienced, such as a specialist investigator, or if time permits obtain additional training to improve your knowledge and skills. It is advisable not to continue with the examination as you may damage the outcome of your case.

The Rules of Evidence

The rules of evidence govern how an organisation goes about proving its case in a legal proceeding.

The Australian Evidence Act's

In Australia, each state has their own 'Evidence Act', which identifies the rules of evidence that apply in those states. In addition the Commonwealth has it's own Evidence Act for proceedings before Federal and Australian Capital Territory courts.

The Evidence Acts in Australia are as follows;

> Commonwealth and ACT: Evidence Act 1995
>
> New South Wales: Evidence Act 1995
>
> Victoria: Evidence Act 1958
>
> Queensland: Evidence Act 1977
>
> Western Australia: Evidence Act 1906
>
> South Australia: Evidence Act 1929
>
> Tasmania: Evidence Act 1910
>
> Northern Territory: Evidence Act 1939 and Evidence (Business Records) Interim Arrangements Act 1984.

The Commonwealth has put forward its Evidence Act as a model for the states, in order to standardise the Act, however only NSW has adopted this model to date. There is however, an indication that some of the states are considering adoption of the Commonwealth Act.

This is important for computer forensics as often an incident occurs which involves more that one jurisdiction, and could also involve overseas jurisdictions. Currently an Australian investigator has to have a working knowledge of all eight Australian Evidence Act's and the corresponding

Crimes legislation's. A common 'local' Evidence Act would improve the functionality of investigations where only one set of domestic 'rules' is required.

Investigators also need to beware that what is acceptable, legal practice in one jurisdiction may be unacceptable in another, rendering the evidence collected inadmissible in that jurisdictions law courts.

An example where standard legislation would be beneficial is where an incident occurs in WA in a National company whose head office, and internal investigators reside in NSW. The investigators, in addition to their local NSW Act also need a to know the WA Act, and the corresponding Crimes legislations.

Similarly an incident for an Australian based international company could occur in their Tokyo or London office requiring an Australian investigator to attend the scene and conduct an investigation. This is where knowledge of international evidence handling rules is essential.

The Five Rules

The Evidence Act's are comprehensive documents, and for anyone with no legal training they can be difficult to understand. Matthew Braid, in his AusCERT paper, 'Collecting Electronic Evidence after a System Compromise' has compiled a list of five rules of evidence that need to be followed in order for evidence to be useful, and has made them easy to understand. In this paper Matthew Braid explains the rules of evidence as follows:

Admissible

This is the most basic rule – the evidence must be able to be used in court or elsewhere. Failure to comply with this rule is equivalent to not collecting the evidence in the first place, except the cost is higher.

Authentic

If you can't tie the evidence positively to the incident, you can't use it to prove anything. You must be able to show that the evidence relates to the incident in a relevant way.

Complete

It's not enough to collect evidence that just shows one perspective of the incident. Not only should you collect evidence that can help prove the attacker's actions but for completeness it is also necessary to consider and evaluate all evidence available to the investigators and retain that which may contradict or otherwise diminish the reliability of other potentially incriminating evidence held about the suspect. Similarly, it is vital to collect evidence that eliminates alternative suspects. For instance, if you can show the attacker was logged in at the time of the incident, you also need to show who else was logged in and demonstrate why you think they didn't do it. This is called Exculpatory Evidence and is an important part of proving a case.

Reliable

Your evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.

Believable

The evidence you present should be clear, easy to understand and believable by a jury. There's no point presenting a binary dump of process memory if the jury has no idea what it all means. Similarly, if you present them with a formatted version that can be readily understood by a jury, you must be able to show the relationship to the original binary, otherwise there's no way for the jury to know whether you've faked it.

Chain of custody

It is essential that any items of evidence can be traced from the crime scene to the courtroom, and everywhere in between. This known as maintaining the 'chain of custody' or 'continuity of evidence. You must have the ability to prove that a particular piece of evidence was at a particular place, at a particular time and in a particular condition. This applies to the physical hardware as well as the information being retrieved from that hardware.

If the chain of custody is broken, the forensic investigation may be fatally compromised. This is where proper management of the evidence is important.

Evidence management

This is an important aspect of any forensic investigation. Strict policies and procedures must exist to deal with the management of evidence. This is to ensure the chain of custody is not broken, and therefore the integrity of the evidence is not compromised.

Evidence management includes such things as;

- Being able to determine which evidence came from which piece of hardware,

- Where that piece of hardware was retrieved from,

- Documenting all persons handling the evidence,

- Ensuring secure storage of the evidence with limited accessibility,

- Documenting all processes used to extract the information,

- Ensuring that those processes used are reproducible, and would produce the same result.

If the evidence handling procedures followed are found to be flawed then the evidence will most likely be disqualified from the proceedings

Quality Control

Quality control is required to maintain standards in the forensic community. It is important to ensure that only qualified personnel are conducting the analysis and to maintain a certain standard within the forensics profession.

Quality control ensures such things as

- Qualified personnel are conducting the analysis
- The work performed is of a quality recognised by the expert community, and acceptable as evidence
- Evidence handling management procedures are adhered to
- Retention of electronic information is within privacy limitations
- The possibility for repeat tests to be carried out, if necessary by experts hired by the other side
- Check-lists are followed and checked to support each methodology

Security Policy is essential

In June 2001 both 'Houses' of the NSW Parliament passed the Crimes Amendment (Computer Offences) Bill 2001. This Bill was to amend the NSW Crimes Act 1900 and the Criminal Procedure Act 1986 with respect to computer offences.

The changes to this legislation "*places an increased liability on the computer owner to engage in best practice principles regarding security and computer usage policie*s" (Detective Sergeant Philip Kaufmann, leader of the NSW Police Computer Crime Investigation Unit.)

Accordingly even the most comprehensive evidence may be useless if it is proven that security policies and practices in an organisation are inadequate.

The Australian Standard **AS/NZS 7799.2:2000** (Information Security Management - Specification for Information Security Management Systems) specifies the requirements for establishing, implementing and documenting information security management systems. In addition the Australian Standard **AS/NZS ISO/IEC 17799:2001 (**Information Technology - Code of Practice for Information Security Management) provides recommendations for best practice in support of **AS/NZS 7799.2:2000.** These standards can be purchased from Standards Australia.

These standards may be used as a foundation for developing your organisational security policies and procedures.

Even if you don't use these standards as a guide to developing your organisation's security policies, you must ensure that your policies are complete, be able to show that your employee's are aware of them, and must also be able to show that they are being enforced. You may find a court will rule in favour of an employee in a wrongful dismissal hearing if it is proven that your Security policies are not enforced.

Skills required to conduct forensic computer investigations

To conduct a forensic computer investigation, the investigator requires certain skills, some of which we have already discussed. The following list provides an overview of the skills a manager should look for when deciding which option to use for an investigation.

- Programming or computer-related experience

- Broad understanding of commonly used operating systems and applications

- Strong analytical skills

- Patience to invest days in taking computers apart in search of evidence

- Strong computer science fundamentals

- Broad understanding of security vulnerabilities

- Strong system administrative skills

- Excellent verbal and written communication skills

- Knowledge of the latest intruder tools

- Knowledge of and experience with the latest forensic tools

- Knowledge of cryptography and stegonography

- Strong understanding of the rules of evidence and evidence handling

- The ability to be an expert witness in a court of law

Training

There are many training courses to learn the art of computer forensics, however Australians generally have to travel to the USA or England to attend.

 "*We don't have the facilities to provide the kind of training they have in the US. A lot of training isn't available in Australia. I've sent NSW Police to Canada for specialist training, and we bring software developers from the US to do training courses here.*" (Detective Sergeant Philip Kaufmann, leader of the NSW Police Computer Crime Investigation Unit.)

The issues raised by Mr Kaufmann highlight the requirement for local training, both for law enforcement and the private sector. The trend throughout the world seems to indicate a sharp increase in the number of private sector participants in these training courses, which were traditionally dominated by law enforcement officers.

There seems however, to be improvements in recent times for local training courses. The following companies also offer training courses in Australia, and some in New Zealand

- **eSec Limited and Foundstone Education** - conduct 4 day training courses on Incident Response and Computer Forensics,

- **Guidance Software -** offers six, four day courses: EnCase Introduction to Computer Forensics, EnCase Intermediate Analysis and Reporting, EnCase Internet and E-Mail Examinations, EnCase EScript Programming, EnCase Prosecutor Training, and EnCase Advanced Training. Each has a curriculum designed to address the various skill levels of the students. Not all of

these courses are available in Australia.

- **Guidance Software –** offers the **EnCase Certified Examiner** (EnCE) program. Certification is available to anyone who meets the minimum requirements for the program. Information can be found at http://www.guidancesoftware.com/html/ence.htm.

There are also many recognised international qualifications available, but again the majority of these are conducted in the USA. Organisations such as International Association of Computer Investigative Specialists (IACIS), New Technologies Inc (NTI) and the National White Collar Crime Centre (NWCCC) are recognised training providers who offer these qualifications. There are others, and beware, some of these organisations only provide training for law enforcement officers.

The Options

Basically, a manager has three options for Computer Forensics investigations, conduct the investigation in-house, call on law enforcement (local Police), or hire the assistance of the private sector forensic specialist.

In-house Investigation

Conducting investigations in-house using your existing IT personnel may be the least expensive method however; depending on the incident, may be the least effective method.

Your IT staff, particularly your IT security staff, are the ones who know your system best, therefore when it comes to obtaining information from internal logs and audit trails they are probably the most appropriate personnel to handle the investigations involving internal logs.

However, when it comes to more complex investigations, in order to conduct them in-house, your IT personnel will need to have the skills and the knowledge of the forensic specialist, thorough knowledge of the rules of evidence and detailed procedures need to be established. If the procedures are found to be flawed the evidence collected may be deemed inadmissible in court.

Even in terms of a staff misconduct incident where the employee is dismissed. If the employee lodges a dispute with the 'Unfair Dismissal Board' your evidence could still undergo the scrutiny of the court system, even though not initiated by your organisation. Also your investigator could be called upon as an expert witness

Your company could develop an in-house specialist forensic team, hire specialist staff, provide regular training and up to date resources, however, when there is not an incident to investigate, you still have to pay to maintain these staff and their awareness of current trends and tools.

Advantages	Disadvantages
Least expensive option	Time intensive
Quick response time	Requires multi-skilled investigators

Does not require outside intervention for potentially 'brand' damaging incidents	Does not ensure evidence integrity
Potential to develop in-house forensic teams	Requires technical diversity
Security staff know your system	Requires constant awareness of hacker tools and methods
	Requires constant awareness of current forensic tools
	Requires constant awareness to changes in relevant legislation
	Funds not always available in companies budgets to allow for the required training and resources to maintain the required expertise.

The Police

May not always be resourced to conduct your investigation and you may be required to provide some evidence first. Also many companies are reluctant to report incidents to law enforcement when a public investigation of the incident may result in loss of 'brand' that far outweighs the cost of the incident.

However, the Australian police are well equipped to conduct thorough computer forensic investigations, with most state police services and the Australian Federal Police having specialist electronic crimes units.

Advantages	Disadvantages
Preserve the chain of custody	Time intensive
Ensures evidence integrity	Resources not always available – could cause slow response time
Specialised crimes units in operation in most states	Requires constant awareness of hacker tools and methods
Specialist units provide technical diversity	Requires technical diversity that may not be available through your local law enforcement office
Provides multi-skilled investigators	Requires constant awareness of current forensic tools
Produce evidence in court that is professional and easy to understand	Requires constant awareness to changes in relevant legislation
Provides recognised international qualifications	Potential loss of 'brand' if certain incidents reach the public arena

Availability of software utilities developed for law enforcement only.	May require some evidence prior to launching an investigation
Electronic crimes units in most states	Restricted to their jurisdiction

The Private Sector Forensic Specialist

With the increased number of ex-police joining the private sector they know the rules of evidence, and they have the expertise, and the resources to provide you with service when you need it, where you need it.

Although the professional's do not advertise their pricing schedule, the cost of some forensic computer investigations can run into the hundreds of thousands of dollars, but these would be uncommonly large investigations.

I was recently told of a forensic investigation where costs were in excess of $25,000 AUD (approx $50,000 USD) for some forensic imaging and manipulation of the imaged data, and the company involved did not intend to prosecute the case.

Advantages	Disadvantages
Preserve the chain of custody	Time intensive
Ensures evidence integrity	Most expensive option
Quick response time	Requires constant awareness of hacker tools and methods
Resources available	Potential loss of 'brand' if certain incidents reach the public arena
Provides technical diversity	Requires constant awareness of current forensic tools
Provides multi-skilled investigators	Requires constant awareness to changes in relevant legislation
Produce evidence in court that is professional and easy to understand	
Provides recognised international qualifications	
Skilled staff often have law enforcement background	

There are many organisations in Australia, which offer forensic computing services, such as PriceWaterhouseCoopers, Ernst and Young, Arthur Andersen, Delloite Touche Tomatsu, and KPMG,

It's your choice

Ultimately, the decision for which computer forensic method to use will rest

with management.

There is no one size fits all solution for computer forensics investigations, nor does an organisation have to commit itself to one or the other option. You may find your organisation uses all three options depending upon the severity of the incident involved.

Finally, deciding which method to use should not be left until an incident occurs. Your investigation method should be documented as part of your incident response plan, therefore when an incident occurs, your organisation is prepared and ready to go.

References

Borek, James – Leave the cyber sleuthing to the experts, 15 July 2001 http://www2.idg.com.au/infoage1.nsf/all/957738B0F8F8313BCA256A6C001 BB7A4?OpenDocument last visited 14 March 2002

Braid, Matthew - Collecting Electronic Evidence After a System Compromise, AusCERT, 2001: http://www.auscert.org.au/Information/Auscert_info/Papers/Collecting_Eviden ce_After_A_System_Compromise.html last visited 20 March 2002

Chappell, Michael – Computer Forensics and litigation Support, Computer Forensics Consultants Ltd: http://www.sinch.com.au/articles/2000/computer_forensics.htm last visited 5 March 2002

Chen, Anne - Digital detectives track hacks, eWEEK 26 April 2001: http://www.zdnet.com.au/newstech/security/story/0,2000024985,20217893,0 0.htm last visited 18 March 2002

Ho, Christina – Criminal pursuit – March 2002: http://www.smh.com.au/icon/0103/21/news3.html last visited 21 March 2002

Horton, Fabian – What clients should know! Computer Forensic Management:http://www.sinch.com.au/articles/2000/Fhorton1.htm last visited 5 March 2002

Incident Response and Computer Forensics – eSec Limited and Foundstone Education: http://www.esec.com.au/training/forensics.html last visited 5 March 2002

Issues Paper: Evidence and the Internet, September 2000 – Action Group into the Law Enforcement Implications of Electronic Commerce. ". http://www.austrac.gov.au/publications/agec/ last visited 5 March 2002. Paper downloaded from http://www.austrac.gov.au/publications/agec/evidence_and_the_internet.pdf

Kaufmann, Phillip Detective Sergeant, Commercial Crime Agency NSW Police Service - ICAC Symposium May 2001 - Proposed Legislation, NSW Crimes Act – Part 6 Computer Offences, AND Forensic Computing, 22 May 2001

Law, Gillian – Corporates sign up for computer forensic training, 1 March 2002:http://www.thestandard.com.au/idg2.nsf/All/D64DD96E6E5C5088CA25

6B6E00758141?OpenDocument last visited 5 March 2002

McKemmish, Rodney. What is Forensic Computing? June 1999 Australian Institute of Criminology trends and issues No. 118: http://www.aic.gov.au/publications/tandi/ti118.pdf last visited 5 March 2002

NSW Crimes Amendment (Computer Offences) Bill 2001 http://www.parliament.nsw.gov.au/prod/parlment/nswbills.nsf/61dac74c1735 1ae7ca25688e00780dff/_Section1 last visited 5 March 2002

NSW Evidence Act 1995 http://www.austlii.edu.au/au/legis/nsw/consol_act/ea199580/ last visited 17 March 2002

Virtual Horizon, The: Meeting the Law Enforcement Challenges, Australasian Centre for Policing Research, Scoping Paper, Report Series No. 134.1