



Department of the
Premier and Cabinet
Office of e-Government

Forensic Plan

A technical guide to aid in the preservation of digital evidence following a computer security incident

July 2004

Preface

This *Forensic Plan* was developed by the Office of e-Government in consultation with Western Australian Government agencies, and both national and state organisations. Feedback received has been incorporated into the document. It has been written to help agencies understand how digital evidence collected as part of an incident investigation may be preserved such that it may be admissible in a court of law. As it is a technical guide to predefined procedures that are in accordance with laws and legal requirements, some of the procedures and actions outlined in this plan are, by necessity, of a technical nature and therefore should only be carried out by suitably qualified professionals. The style and language of this document is in the 'second person', and this follows the standard approach taken by other respected computer forensics-type manuals.

This *Forensic Plan* is a lower level companion document to the *Incident Response Plan*, which provides higher-level overall guidance in preparing for, detecting and responding to computer security incidents.

Both the *Forensic Plan* and the *Incident Response Plan* are available from the Office of e-Government website (<http://www.egov.dpc.wa.gov.au>) in PDF format from the Policies and Guidelines section.

If you have any comments, queries or need additional information, please contact:

The Office of e-Government,
Department of the Premier and Cabinet,
Locked Bag 10,
Cloisters Square,
PERTH WA 6850

email: egov@dpc.wa.gov.au
Phone: 9213 7100

Contact:

Sven Bluemmel
Gail Holt

Table of Contents

PREFACE	2
TABLE OF CONTENTS	3
Background	5
INTRODUCTION	6
1.1 Disclaimer	6
1.2 Introduction.....	6
1.3 Purpose and Scope	7
1.4 Police Role.....	7
1.5 Related Documents	7
Forensic Plan	8
FORENSIC PROCEDURES	9
2.1 Before You Get Started.....	9
2.2 Contemporaneous Notes	9
2.3 Actions to Take	10
2.3.1 Secure the Scene	10
2.3.1.1 Isolate the machine	10
2.3.1.2 Do not allow unauthorised personnel near a ‘suspect’ computer	10
2.3.1.3 Ascertain what the machine is doing	11
2.3.1.4 Shutdown	11
2.3.2 Search the Scene	12
2.3.2.1 Search the area carefully	12
2.3.2.2 Consider the suspect’s home drive	12
2.3.2.3 If the suspected staff member is present	13
2.3.3 Record the Scene.....	13
2.3.4 Seize the Evidence	13
2.3.5 Post Seizure.....	14
2.3.5.1 Pack the items with care	14
2.3.5.2 Transport all equipment with care	14
2.3.5.3 Do not turn on the computer or operate it at all.....	14
2.3.5.4 Do not open computer cases or attempt to remove hardware	14
2.3.6 Property / Exhibit Receipt and Management	14
2.3.6.1 Property / Exhibit Numbering Scheme	15
2.4 The Chain of Custody	15
2.5 Controlling Contamination	16
FORENSIC PRINCIPLES.....	17
3.1 Key Elements of Forensic Computing.....	17
3.1.1 Identification of digital evidence	17
3.1.2 Preservation of digital evidence.....	17
3.1.3 Analysis of digital evidence.....	17
3.1.4 Presentation of digital evidence	18

3.2	Rules of Forensic Computing	18
3.2.1	Minimise handling of the original.....	18
3.2.2	Account for any changes.....	19
3.2.3	Comply with the rules of evidence	19
3.2.4	Do not exceed your knowledge.....	20
3.3	Other Considerations	20
3.3.1	Proceed from volatile to persistent evidence	21
3.3.2	Do not run any programs on the affected system	21
3.3.3	Run unknown code in a controlled environment	21
3.3.4	Ensure that your actions are repeatable	21
3.3.5	Ensure that you collect the complete story	22
3.3.6	Be prepared to testify	22
3.4	Evidence Collection – Freezing the Scene.....	22
ACKNOWLEDGEMENTS.....		24
APPENDIX A	LOG OF EVENTS FORM	25
APPENDIX B	SEIZURE FORMS	27
APPENDIX C	CHAIN OF CUSTODY FORM	30
APPENDIX D	GUIDING PRINCIPLES DURING EVIDENCE COLLECTION	32

Background

Introduction

1.1 Disclaimer

This document is a guide to forensic procedures that may need to be taken into consideration when investigating computer security incidents that occur within Western Australian Government computer networks. It is intended to provide a general understanding of the subject matter, and to help people assess whether they need more detailed information and plans. We encourage “early” handover of any investigation to a departmental/governmental investigator or Police to maximise the evidence gathering activities and minimise the technical omissions or mistakes that a person not used to pursuing investigations may make. Users should seek their own legal advice where appropriate. Every effort is made to ensure that the material in this document is accurate and up to date. However, the Department of the Premier and Cabinet does not guarantee or warrant the accuracy, completeness or currency of the information provided.

The material in this document is not and should not be regarded as legal advice.

1.2 Introduction

The increased computer literacy both within Government and the general community, as well as the low cost and efficiency of the implementation of technological solutions, has increased the likelihood of technology being used to commit an unauthorised act or augment its commission. People who would not dream of stealing or maliciously damaging other people’s property in the ‘real world’ have no qualms or second thoughts in relation to the opportunities and challenges presented by technology, the Internet, and the ‘virtual world’.

Computers are used in all facets of Government work to create messages, write reports and other documents, compute financial information, transfer funds and browse the Internet. As well, Government has established a business requirement to make more extensive use of public data networks, such as the Internet. Connections to these networks carry a number of additional threats and risks over and above those already identified and for which safeguards have been provided. Government needs to understand these threats and to respond to computer security incidents with speed and skill so that incidents can be identified, contained and, in the longer term, prevented in a timely and cost-effective manner.

Government should also be in a position that enables it to prosecute any individual who damages departmental information assets or disrupts its normal business activities through connection to Government computers from any network. As part of the

Western Australian Government's initiative to establish a proactive approach to managing security incidents, the Office of e-Government WA Computer Security Incident Response Team (WA CSIRT) has been formed to provide help and advice to agencies when dealing with computer security incidents. This document has also been created as a guide to help ensure that computer evidence pertaining to such incidents may be admissible in a court of law.

1.3 Purpose and Scope

The purpose of this forensic plan is to document the mechanisms by which evidence relating to security incidents that occur on, are sourced from, or propagated through Government networks should be handled by Government staff and its contractors. The word forensic simply means 'relating to, used in, or appropriate for courts of law'. These forensic procedures define how computer data can be preserved such that it may be admissible in a court of law as evidence.

It must be stressed that these are specialised procedures, and therefore should only be carried out by suitably qualified professionals. Agencies may need to engage specialists for this purpose as the need arises. The Office of e-Government plans to set up a panel contract of companies qualified to undertake forensic examinations so that agencies may engage a suitably qualified professional through the normal government procurement processes.

This plan assumes that procedures relating to the preservation of evidence associated with 'traditional' security incidents such as fire, flood and theft are largely accounted for by current contingency mechanisms. This plan is designed to address some of the new challenges posed by the criminal exploitation of digital technologies.

1.4 Police Role

Where any investigative activity extends outside your agency, and/or when the Federal or State Police assume responsibility for further investigation, you will need to relinquish responsibility for the protection of evidence to the Federal or State Police.

1.5 Related Documents

This Forensic Plan forms part of an overall Office of e-Government WA Computer Security Incident Response Team (WACSIRT) incident response framework. This plan is a lower level companion to the WACSIRT Incident Response Plan. Also see the WACSIRT Operational Manual that documents how the WACSIRT operates, and the WACSIRT Framework that is the head document describing the objectives and scope of the WACSIRT.

Forensic Plan

Forensic Procedures

2.1 Before You Get Started

During the course of your investigation you may be required to access and copy sensitive data or obtain statements from system users in which case there will be staff management issues to consider. Before commencing your investigation, it is important to ensure you have obtained written and signed permission to proceed, and have clear instructions as to the scope of your investigation. Without clear authority to proceed, your actions may be, or be perceived to be, in breach of your agency's security policy and you may find yourself personally accountable as a result. If in doubt, talk to those that know, including obtaining the necessary legal advice. So, before you get started:

- Consult your security policy.
- If you do not have a security policy, consult with management, consult with your legal counsel, contact law enforcement agencies, and notify others within your organisation.
- Document all of the steps you take in the investigation.

2.2 Contemporaneous Notes

It is critical to maintain concise, accurate and contemporaneous written notes of everything done from the time a suspected incident is reported. Contemporaneous is defined as 'existing or occurring at the same time'. These notes may form the basis of a range of documents including:

- Witness Depositions;
- Executive Briefing Notes;
- Ministerial Briefing Notes;
- Incident Response Reports;
- Internal Investigations; and
- Criminal or Civil Briefs of Evidence.

It is useful to keep a chronological "Log of Events" or "Running Sheet" that includes date, time and place of creation of other documents. If such a "log" ties to all activities then it shows meticulous record keeping and a chain of events, and may prove to be an invaluable item able to be tendered in evidence. Document everything. Your procedures may be questioned later, so it is important that you document everything that you do. Timestamps, digital signatures and signed statements are all important – don't leave anything out. If any legal action arises out of the incident under investigation, lengthy delays in the legal system are common. You are unlikely to fully recall all the relevant details of a particular incident after some time has passed, and will need to rely on your notes. Also, you may be called upon to account for an action that

you have taken. It is important that you fully document the circumstances under which certain actions/decisions were made. A frequently quoted and useful rule of thumb is:

If it is worthwhile making a mental note of something, it is worthwhile making a written note.

2.3 Actions to Take

You should notify the Office of e-Government WA Computer Security Incident Response Team (WACSIRT) of this incident by sending them a completed IT Security Incident Reporting Form. All incidents should be notified to WACSIRT, even if they are not investigated/escalated, so that the incident can be collected for statistical purposes. Refer to your *Incident Response Plan* for incident notification procedures and forms.

If you need direct assistance with search/seizure operations please submit a request to WACSIRT as soon as possible. Depending upon the severity of the incident, the WA Police Computer Crime Investigation Unit (CCI) may also be called upon to directly assist in search/seizure/examination operations. However all requests for such assistance should be directed to WACSIRT in the first instance, and they will then liaise with the CCI if this is deemed necessary.

Document everything that you do.

2.3.1 Secure the Scene

2.3.1.1 Isolate the machine

Disconnect all network and modem cables. A person with access to the machine across a network or via a modem could easily and quickly destroy evidence. Note any mounted/connected drives prior to disconnection.

2.3.1.2 Do not allow unauthorised personnel near a 'suspect' computer

Experience shows that when an incident occurs, personnel, even with the best of intentions, often compromise potential evidence on a suspected computer by unintentionally changing or even destroying what was there. Incidents have also been reported where suspects have convinced officers they were going to show them the evidence, only to encrypt or destroy it the moment they had access. It is important to ensure that only authorised staff members are given access to the area in which the computer is kept.

If a senior member of staff over whom you have no authority insists on being given access to a 'suspect' computer, inform them that you are required to make notes in relation to their access and invite them to sign your notes upon completion. This will assist the forensic specialists when conducting an investigation at some later stage.

In making these notes, make sure that they are concise and accurate and are taken at the time outlining:

- The senior staff member's name;
- The date and time of this person's request;
- The reason this person insisted on access;
- Actions taken by this person including systems accessed, activities undertaken in that system, and any codes used; and
- The date and time this person left the area.

If the senior staff member declines to sign these observations, make a notation to that effect and if possible or appropriate ask for a reason for non-signing and include that in the information.

2.3.1.3 Ascertain what the machine is doing

If the computer is off, leave it off. If the computer is on, record what it is doing. Record what operating system(s) is (are) running, what applications are running, any documents that may be open in a word processor, and what system processes are running. If any documents are open in word processing software, dump these to floppy disks, as they may be lost in a subsequent system shutdown. (Remember to use new floppy disks, and to correctly label them – see section 3.4 Evidence Collection – Freezing the Scene.) Check any URLs being accessed if an Internet browser is open, and Newsgroups being accessed if a News browser is open. If possible, photograph or video the screen display first encountered.

2.3.1.4 Shutdown

You need to decide whether or not to shutdown the machine. If the computer is up and running and you do not need to transport it for forensic examination, you may decide not to shut it down. If you decide that it needs to be shutdown, before doing so ask yourself the following:

- Is shutting it down going to prevent access to password protected data that may be accessible (for example encrypted volumes or hard disk drives);
- Is the user name and password of a network computer known;
- Is shutting it down going to cause considerable disruption to the business (for example a critical file server);
- Is the computer in the process of carrying out a critical legitimate function (for example a large automated batch process for invoices);
- Is shutting it down going to alert other potential staff members or suspects to the discovery of the incident;
- Have the shutdown/boot up scripts been trojaned to wipe/disguise evidence.

As well, before you shut down you may need to capture and record system information that may be lost in the shutdown, or not captured during the execution of your backup procedure. This includes:

- All current network connections;
- All current system processes;
- Active users currently logged on;
- All open files (files may be deleted if a process exits when the network is disconnected);
- Any other volatile data that may be lost (see 3.3.1 Proceed from volatile to persistent evidence).

If you determine that shutting down the computer is safe and expeditious, based on the operating system, shut down the computers as follows:

- | | |
|----------------------------|---------------|
| • DOS..... | Pull the plug |
| • Windows 3.1..... | Pull the plug |
| • Windows 95..... | Pull the plug |
| • Windows 98..... | Pull the plug |
| • Windows NT..... | Pull the plug |
| • Windows NT Server..... | Shut down |
| • Windows 2000..... | Pull the plug |
| • Windows 2000 Server..... | Shut down |
| • Linux..... | Shut down |
| • Unix..... | Shut down |
| • Macintosh..... | Pull the plug |

2.3.2 Search the Scene

2.3.2.1 Search the area carefully

Diskettes, CD-ROMs, zip disks and other removable media can be stored or hidden just about anywhere. If conducting a search for these items is necessary in the initial stages, make careful notes of the area searched, what was found, and by whom. If possible, photograph or video record the items in situ before they are removed and labelled. Trace all network cables, and look for written down passwords, particularly under desk or chair.

2.3.2.2 Consider the suspect's home drive

The suspect's home drive may be on a networked server. You may need to consider system backup media if it is believed that the suspect has removed evidence from the server.

2.3.2.3 If the suspected staff member is present

Make careful notes of anything said to you and if possible, have another person present. Ask the staff member for passwords and other relevant details during the initial interview with them. Once again, make careful notes of any conversations and make sure that there is another person present to corroborate what was said. This is critical in the subsequent investigation for reasons outlined in Section 2.2 Contemporaneous Notes

2.3.3 Record the Scene

- Photograph and/or video record the suspect machines in situ including all cabling. Photos and videos should show the date and time even if it has to be written on something and displayed in the frame;
- Make a sketch of the area / room in which the suspect machine is, noting where the machine and other furniture is, where personnel were standing upon your arrival, and any other identifying items that may assist specialists in any subsequent investigations;
- Label all hardware, cables and the holes from which they were removed before disconnecting, in a manner that makes it easy to identify the original location of the items. This may assist in the reconstruction of the system to its original configuration later, or simply to assist others with understanding its configuration;
- Similarly, collect and label all removable storage media, bag and tag all floppy disks, CDROMs etc, and note the location in which they were found;
- Label all computers, hardware and cables using the numbering scheme detailed in Section 2.2.6.1 – Property / Exhibit Numbering Scheme.

2.3.4 Seize the Evidence

Ensure that all components and peripherals related to the computer being seized are also taken. There may be only one opportunity to gather all the available evidence for further investigation or action. Leaving behind computer equipment or software may make further investigation difficult, or allow evidence to be destroyed. When removing equipment and / or components:

- If you are seizing laptop computers, PDAs or other memory retention devices, ensure you also seize the associated power supply. Ask for passwords;
- Collect all necessary computer storage media such as USB drives, hard disk drives, floppy disks, CD-ROMs, backup tapes and any unusual or suspected software such as encryption programs;
- Collect all relevant manuals or other documentation related to the computer hardware, software or peripheral equipment. These may be required by forensic specialists later;
- Keep magnetic media, such as floppy disks, separate from other items seized, and away from magnetic and radio sources;

- When seizing items, only group items together if they are found together. Do not mix many similar items (for example floppy disks) found in different locations with the intention of sorting them out later. Many computer related items such as floppy disks look the same and it may be impossible to differentiate between items found at different locations later on. (For example producing these items in court proceedings.)

Record all components and peripherals seized on Seizure Detail forms – see Appendix B. A signed copy of each completed Seizure Detail form should be left with the appropriate person at the site, and the original forms transported with the seized equipment.

2.3.5 Post Seizure

2.3.5.1 Pack the items with care

Computer equipment is fragile and easily damaged even where transporting it for short distances.

2.3.5.2 Transport all equipment with care

All computer equipment should be treated carefully so as to ensure that no damage is caused during transit. Given the equipment's sensitive nature, knocks, bumps, vibration or moisture could render the data inaccessible. Never transport equipment near radio transmitters or other magnetic field generation devices as data loss may result.

2.3.5.3 Do not turn on the computer or operate it at all

Information that is stored on the machine may be destroyed permanently. Additionally, the nature of most operating systems is such that merely turning them on changes original evidence, for example swap files / page files change, thereby compromising the integrity of any evidence located on the machine.

2.3.5.4 Do not open computer cases or attempt to remove hardware

Contact the WACSIRT for guidance and advice if you think that this is necessary.

2.3.6 Property / Exhibit Receipt and Management

If the seized computing equipment is to be handled by WACSIRT, the Property / Exhibit Receipt and Management procedures detailed in the WACSIRT Operations Manual will apply. If the seized equipment is to be handled directly by the WA Police Computer Crime Investigation Unit then their property receipt and management procedures will apply.

2.3.6.1 Property / Exhibit Numbering Scheme

All work undertaken by the WACSIRT of a computer forensic nature is subject to a standardised numbering scheme, which is based around an incident number. Each computer dealt with is allocated a unique number based on the incident number.

Incidents are numbered #yyyy-*nn* where *yyyy* is the year and *nn* (or *nnn!*) is a sequential number starting from 1 for the first incident of the year. So incident #2002-13 is incident number 13 that occurred in 2002.

If incident #2002-13 results in the seizure of 3 computers, they will be allocated numbers 2002-13A, 2002-13B and 2002-13C.

Each storage device within a computer is also allocated a unique identifying number. For example, if computer 2002-13A contains two hard disks they will be allocated numbers 2002-13A1 and 2002-13A2.

Peripheral storage devices, such as floppy disks, are allocated numbers in lots. For example, fifty floppy disks found on a desk and seized as part of the job may be given number 2002-13D, and twenty CD-ROMs found under the desk and also seized may be given number 2002-13E.

2.4 The Chain of Custody

A complete account must be kept of what has happened to each piece of evidence collected that may be tendered in court. The goal of carefully maintaining this chain of custody is not only to protect the integrity of your evidence, but also to make it difficult for a defence lawyer to successfully argue that the evidence was tampered with while it was in your custody. The chain of custody procedure is a simple yet effective process of documenting the complete journey of your evidence during the life of the case.

When the evidence is collected, you should create a register that details all evidentiary items. This register should then be used to record any movement or action taken on any item. The details for each piece of evidence recorded in the register should show:

- Who collected it;
- How and where it was collected;
- Who took possession of it;
- How was it stored and protected;
- Who accessed it, for what purpose, and the date and time of such access;
- Who removed it, for what purpose, and the date and time of removal and return;
- Details of any forensic procedures that were carried out.

A chain of custody form doesn't have to be complex; a simple spreadsheet with the appropriate cells to collect the relevant information will do, as long as it is completely filled out. A sample chain of custody form is shown in Appendix C.

2.5 Controlling Contamination

The fewer people who have access to your evidence the better. Defence lawyers love to argue that everyone who had access to the evidence could have altered it. They don't have to prove that the evidence was in fact altered for this tactic to work. They only have to show that the evidence was not adequately safeguarded and hope that the seed of doubt is sown that someone could have planted or altered the evidence.

Any evidence you collect must be stored in a secured area or container that is accessible by as few people as possible, and only on a need-to-know basis. Identify an evidence custodian who is responsible for the security of and access to the storage container so that you can prove who has access to it. If there is a key lock, each key should be stamped *do not* duplicate. Make sure, by policy and practice, that each person with access understands they are required to control access to these items. Any and every person with access to the evidence may have to testify if the incident results in a court trial.

Whenever copies of electronic data are made, the original data, not the copy, should then be sealed for evidence. Number, date, and sign notes and printouts. Seal disks with original, unaltered, complete logs in an envelope or other container; then number, date, and sign the container. Original handwritten notes should be copied, and the original notes sealed as part of the chain of custody. Electronic data should be captured as soon as possible, and the process of making copies of the evidence should be witnessed.

The following rules should apply:

- Access to labelled evidence shall be restricted to members of the incident response team and State and Federal Police only, and such access shall be for activities directly related to aspects of the ongoing investigation or prosecution;
- Any officer given access to labelled evidence shall record details of the access in writing in the register established for the purpose (see 2.4 The Chain of Custody);
- The receiving party must issue a receipt for any labelled evidence handed over to a specialist forensic investigator or State or Federal Police.

Forensic Principles

The application of computer technology to the investigation of computer based crime has given rise to a new field of specialisation – forensic computing – which is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable. This section explains the key elements and rules of forensic computing.

3.1 Key Elements of Forensic Computing

3.1.1 Identification of digital evidence

This 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. Personal computers are not the sole focus of forensic computing – it can extend to any electronic device that is capable of storing information, such as mobile phones, digital diaries and smart cards. 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 to that the appropriate technology can be used to extract it.

3.1.2 Preservation of digital evidence

This is a critical element in the forensic process. 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. (Also see 3.2.2 Account for any changes.) Alteration to data that is of evidentiary value must be accounted for and justified. This applies not only to changes made to the data itself, but also includes physical changes that are made to the particular electronic device to facilitate access to the data.

3.1.3 Analysis of digital evidence

The extraction, processing and interpretation of digital data are generally regarded as the main elements of forensic computing. Once extracted, digital evidence usually requires processing before people can read it. For example, when the contents of a hard disk drive are imaged, the data contained within the image still requires processing so that it is extracted in a humanly meaningful manner. The processing of the extracted product may occur as a separate step, or it may be integrated with extraction.

3.1.4 Presentation of digital evidence

This involves the actual presentation in a court of law. It 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.

The feature of forensic computing that sets it apart from any other area of information technology is the requirement that the final result must be derived from a process that is legally acceptable. Consequently, the application of technology in the investigation of technological crimes must be carried out with due regard to the requirements of law. Failure to do so can result in the digital evidence being ruled inadmissible, or, at the very least, being regarded as tainted.

3.2 Rules of Forensic Computing

Given that the final product of the forensic process is subject to judicial scrutiny, it is important that the rules governing it be followed. Essentially, the four rules of forensic computing are:

3.2.1 Minimise handling of the original

The application of computer forensic processes during the examination of original data should not occur unless absolutely essential, and then shall be kept to an absolute minimum. This can be regarded as the single most important rule in forensic computing. Any examination of original evidence should be conducted in such a way as to minimise the likelihood of alteration. Where possible, this is achieved by duplicating the original and examining the duplicate data. (Also see 3.4 Evidence Collection – Freezing the Scene.)

The duplication of evidence has a number of advantages. Firstly, it ensures that the original is not subject to alteration in the event of an incorrect or inappropriate process being applied. Secondly, it allows the examiner to apply various techniques in cases where the best approach is not clear. If, during such trials, the data is altered or destroyed it simply becomes a matter of working on a fresh copy. Thirdly, it permits multiple forensic specialists to work on the data, or parts of the data, at one time. This is especially important if specialist skills (for example, cryptanalysis) are required for various parts of the analysis. Finally, it ensures that the original is in the best state possible for presentation in a court of law.

Whilst there are advantages to duplicating evidence, there are also disadvantages. Firstly, the duplication of evidence must be performed in such a manner, and with such tools, as to ensure that the duplicate is a perfect reproduction of the original. Failure to properly authenticate the duplicate will result in questions being raised over its integrity. This in turn may provoke questions over the accuracy and reliability of both the

examination process and the results achieved. Secondly, by duplicating the original, we are adding an additional step into the forensic process. Additional resources are required to accommodate the duplicated data, and extra time is required to facilitate the duplication process. Furthermore, the methodology employed must be expanded to include the duplication process. Finally, the restoration of duplicated data in a way that re-creates the original environment can be difficult. In some instances, in order to recreate the original environment, specific items of hardware etc may be required. This again adds further complexity and time to the forensic process.

3.2.2 Account for any changes

Changes to evidentiary material should not occur. However in situations where it is inevitable, the examiner has a responsibility to correctly identify the nature, extent and reason for the changes and document these - a process directly dependent on the examiner's skills and knowledge. During any examination it may be necessary for either the original or duplicate to be altered. This applies both at a physical and logical level. In such cases it is essential that the examiner fully understands the nature of the change, and is the initiator of that change. Additionally, the examiner must be able to correctly identify the extent of any change and give a detailed explanation of why it was necessary. Essentially this applies to any evidentiary material that is derived from a forensic process in which change has occurred.

During the forensic examination this point may seem insignificant, but it becomes a critical issue when the examiner is presenting their findings during judicial proceedings. Whilst the evidence may be sound, questions regarding the examiner's skills and knowledge can affect their credibility as well as the reliability of the process employed. Given sufficient doubt, the results of the forensic process can, in the worst case, be ruled inadmissible.

Whilst the need to alter data occurs infrequently, there are instances where the examiner is required to initiate change in order to facilitate the forensic examination process. For example, where access to data is restricted by means of some form of access control, the examiner may be forced to change either a logical flag (i.e. access bit) or an entire string of binary data to gain access. In such instances the examiner may be required to offer expert testimony that the meaning of the data accessed by such change has not been unduly compromised.

3.2.3 Comply with the rules of evidence

The application or development of forensic tools and techniques should be undertaken with regard to the relevant rules of evidence. The WA Evidence Act (1986) enacts the rules of evidence applicable to our jurisdiction. It is outside the scope of this document to discuss the rules of evidence, and anyone interested in further light reading on this subject should refer to the WA Evidence Act (1986), specifically section 79C – Documentary evidence, admissibility of. However, one of the fundamental precepts of forensic computing is the need to ensure that the application of tools and techniques

does not lessen the admissibility of the final product. It therefore follows that the type of tools and techniques used, as well as the way they are applied, is important in ensuring compliance with the relevant rules of evidence.

Another important factor when complying with the rules of evidence is the manner in which the evidence is presented. Essentially, information should be presented in a manner that is as indicative of the original as is possible. That is, the method of presentation should not alter the meaning of the evidence.

3.2.4 Do not exceed your knowledge

The forensic computer specialist should not undertake an examination that is beyond their current level of knowledge or skill.

It is essential that the forensic computer examiner is aware of the limit of their knowledge and skill. On reaching this point, the examiner has a number of options:

- Cease any further examination and seek the involvement of more experienced and skilled personnel;
- Conduct the necessary research to improve their own knowledge to a point that permits a continuation of the examination; or
- Continue with the examination in the hope that all goes well.

The final option is without doubt the most dangerous. It is imperative that the forensic examiner be able to describe correctly the processes employed during an examination and to explain the underlying methodologies for such processes. Failure to explain, competently and accurately, the application of a process or processes can result in the expertise and credibility of the examiner being called into question in any subsequent judicial proceedings.

Another danger in continuing an examination beyond one's skills is the increased risk of damage – changes that the examiner is unaware of or does not understand and consequently may ignore. This is likely to be revealed when the examiner is giving evidence.

Essentially, only properly skilled and qualified staff that have the appropriate level of training should undertake complex forensic computer examinations. Additionally, given that technology is continually advancing, it is important that the examiner receives ongoing training.

3.3 Other Considerations

The four rules of forensic computing apply to the analysis of electronic evidence. However, some other points need to be considered in the overall investigative process.

3.3.1 Proceed from volatile to persistent evidence

Not all the evidence on a system will last for extended periods of time. Some evidence resides in volatile memory only while there is a consistent power supply; other evidence stored is continuously changing. When collecting evidence, always try to proceed from most volatile to least volatile and from most critical to least critical machines/systems. The possible presence of volatile evidence also needs to be taken into consideration when deciding whether or not to shut down a suspect machine. You may want to collect the raw data from volatile sources before you shutdown the system.

To determine what evidence to collect first, draw up an Order of Volatility – a list of evidence sources ordered by relative volatility. An example Order of Volatility could be:

1.	Caches	6.	Main memory
2.	Routing tables	7.	Temporary file systems
3.	ARP cache	8.	Secondary memory
4.	Process table	9.	Router configuration
5.	Kernel statistics and modules	10.	Network topology

3.3.2 Do not run any programs on the affected system

Since the attacker may have left trojaned programs and libraries on the system, you may inadvertently trigger something that could change or destroy the evidence you are looking for. Any programs you use should be run from your own read-only media, such as CD-ROM or a write-protected floppy disk.

3.3.3 Run unknown code in a controlled environment

If any unknown code is found, it should be treated as hostile binaries, or malware. The only place that you should attempt to run an unknown binary is in an 'isolation ward', on a throwaway machine disconnected from the network to limit any possible damage. After examining the binary, you should assume that the program might have damaged the test system in a way that you are unaware of, and the OS should be completely reinstalled.

3.3.4 Ensure that your actions are repeatable

Others should be able to repeat your actions and reach the same results. If they can't, this may once again provoke questions over the integrity of the duplicate evidence being examined, and the accuracy and reliability of both the examination process and results achieved.

3.3.5 Ensure that you collect the complete story

Your evidence must tell the whole story. 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 a suspect's actions, but also for completeness it is 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 an 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.

3.3.6 Be prepared to testify

If you are not willing to testify about the evidence you have collected, you might as well stop before you start. Without the collector of the evidence being there to validate the documents created during the evidence collection process, it becomes hearsay, and inadmissible. Remember that you may need to testify at a later time.

3.4 Evidence Collection – Freezing the Scene

Freezing the scene involves taking a snapshot of the system in its compromised state. A suitably qualified person must take this step, as the whole investigation is underpinned by the reliability and integrity of the original data. At the time of writing, the WA Police Computer Crime Investigation Unit utilise a software package called Encase to take a snapshot of a computer under investigation. Other suitably qualified investigators using other tools may also be acceptable.

Investigators not using Encase should consider the following points when gathering evidence:

- Use new media to write evidence to because it may appear that the evidence is faulty or contaminated if it is written over old information. As well, the old information is not part of this incident and it may not be appropriate for it to be available to any external party.
- All relevant computer files shall be copied onto removable media in an industry-standard format;
- A checksum digest for each file copied shall be generated, and the resultant digests documented and securely stored;
- All removable media shall be appropriately labelled and securely stored;
- The label shall contain such details as:
 - The date and time that the copy was taken;
 - The program or utility used to make the file copies;
 - The hostname and ip address of the computer from which the files were copied;

- The name and position of the person who made the copies;
- The investigator shall sign and date the labels of all media utilised and the signature countersigned by a witness; and
- The investigator shall establish written documentation that shall record all subsequent activity related to any labelled evidence that may be produced in court.

Acknowledgements

1. Defence Signals Directorate – various documents.
URL:<http://www.dsd.gov.au>
2. Braid, M. AusCERT. “Collecting Electronic Evidence After a System Compromise” August 2001.
URL: <http://www.auscert.org/render.html?it=2247>
3. McKemmish, R. “What is Forensic Computing?” 1999.
[URL:http://www.aic.gov.au](http://www.aic.gov.au)
4. McCarthy, T. Investigative Services Course documents – various. 2002.
5. Kruse II, W and Heiser, J. “Computer Forensics “. Pub: Addison-Wesley, ISBN 0-201-70719-5.
6. Rubidge, M. Detective, Computer Crime Investigation Unit, WA Police.
7. Guidance Software. “Forensic Methodology Training Manual”. 2001.
[URL:http://www.Encase.com](http://www.Encase.com)
8. Standards Australia. “HB171_2003 Guidelines for the Management of IT Evidence”.
9. George, R. Lawyer, Babington’s Lawyers.
10. Harraway, K. Manager – Critical Infrastructure Project, WA Fire and Emergency Services Authority
11. RFC 3227 – Guidelines for Evidence collection and Archiving, D. Bresinski & T. Killalea Feb 2002 [URL:http://www.fags.org/rfcs/rfc3227.html](http://www.fags.org/rfcs/rfc3227.html)
12. Information was also drawn from various papers and documents that are freely available on the Internet.

Appendix A Log of Events Form

Appendix B Seizure Forms

SEIZURE DETAILS – MACHINE

Incident # _____
Exhibit # _____

Seized From:

Address :	
Location In Premises :	
Date/Time Attended :	
Officers Present :	

Machine Isolation etc...

Status On Arrival :	On/Off() N/W() Modem()
Isolate – Modem :	Time() Method()
Isolate – N/W :	Time() Method()
Visible On Screen :	
:	
:	
:	
Active Tasks :	
:	
:	
:	
Floppy Saves :	
:	
:	
Shutdown :	Time() Method()

Describe Machine:

Make :	
Model :	
Serial :	
Case – Front :	
:	
Case - Rear :	
:	
Obvious Damage :	
:	
Photographs :	

Peripherals Attached:

Item	Seized (Y/N)	WACSIRT #

Sign and date :	
------------------------	--

SEIZURE DETAILS – PERIPHERALS

Incident # _____

Exhibit # _____

Seized From:

Address :	
Location In Premises :	
Date/Time Attended :	
Officers Present :	

Peripherals Details

NOTE: Data peripherals to be grouped based on location. Different media types may thus be grouped together.

WACSIRT #	Description (<i>Pics taken ?</i>)	Exact Location Found, Found by Whom

Sign and date :	
------------------------	--

Appendix C Chain of Custody Form

Evidence Chain of Custody

Incident # _____
Exhibit # _____
Sheet: _____ of _____

Evidence Description	
Collected from (specify source)	
Collected by (name, date and time)	
How Collected (specify any special procedures)	
Custodian (Name, Title, usual signature)	
Where Stored	

Date/Time	Reason for Access (include any procedure details)	Removed to (specify destination and attach receipt)	Person Accessing	Signature	Return Date/Time	Custodian Signature

Appendix D Guiding Principles During Evidence Collection

The following guiding principles during evidence collection are defined in RFC 3227 – *Guidelines for Evidence Collection and Archiving* published by the Internet Society. It provides guidance for frontline IT staff (e.g. system administrators) who are likely to be first responders to an IT security incident.

Principles

1. Adhere to your site's security policy and engage the appropriate incident handling and law enforcement personnel;
2. Capture as accurate a picture of the system as possible;
3. Keep detailed notes. These should include dates and times. If possible generate an automatic transcript. (e.g. on Unix systems the 'script' program can be used, however the output file it generates should not be to media that is part of the evidence.) Notes and printouts should be signed and dated;
4. Note the difference between the system clock and UTC (Universal Time Clock). For each timestamp provided, indicate whether UTC or local time is used;
5. Be prepared to testify (perhaps years later) outlining all actions you took and at what times. Detailed notes will be vital;
6. Minimise changes to the data as you are collecting it. This is not limited to content changes; you should avoid updating file or directory access times;
7. Remove external avenues for change;
8. When confronted with a choice between collection and analysis you should do collection first and analysis later;
9. Though it hardly needs stating, your procedures should be implementable. As with any aspect of an incident response policy, procedures should be tested to ensure feasibility particularly in a crisis. If possible, procedures should be automated for reasons of speed and accuracy. Be methodical;
10. For each device, a methodical approach should be adopted which follows the guidelines laid down in your collection procedure. Speed will often be critical so where there are a number of devices requiring examination it may be appropriate to spread the work among your team to collect the evidence in parallel. However on a single given system collection should be done step by step; and
11. Proceed from the volatile to the less volatile.