E-Crime

A Guide to E-Crime Investigations

New Zealand
POLICE
Nga Pirihimana O Aotearoa

Produced by the Research and Development Group,

Training Service Centre.

This information is for Police use only.

Appendix A

Wording to be included in a search warrant

Computers, central processing units, external and internal drives and external storage equipment or media, terminals or video display units, together with peripheral equipment such as keyboards, printers, scanners and modems.

Any and all computer or data processing software or data including, but not limited to, hard disks, floppy discs, cassette tapes, video cassette tapes, magnetic tapes, integral RAM or ROM units and any other permanent or transient storage device(s).

The following records or documents, whether contained on paper in handwritten, typed, photocopied or printed form or stored on computer print-outs, magnetic tape, cassettes, discs, diskettes, photo optical devices or any other medium: access number(s), password(s), pass-phrase(s), personal identification numbers (PINS).

Any computing or data processing literature, including, but not limited to, printed copy, instruction books, notes, papers or listed computer programs in whole or in part.

Contents

Preface

This booklet supports the accompanying video and is designed to raise your awareness and understanding of electronic crime. The booklet will not make you an expert but it will provide you with some ideas on how to identify and deal with electronic crime (e-crime).

Note: If you come across any devices in the field that you are not familiar with or if you have any doubts about dealing with such devices, contact your nearest Electronic Crime Laboratory (ECL) at Auckland, Wellington or Dunedin. Your local Comms Centre has an after-hours contact list.

Additional copies of the video and booklet can be obtained from the Research and Development Group, Training Service Centre.

Virus attacks and worms: A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. Even a simple replicating virus is dangerous because it will quickly use all available memory and bring the system to a halt.

Some people distinguish between general viruses and *worms.* A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

Endnotes

[1] http://www.techweb.com/encyclopedia/

[2] Law Commission *Computer Misuse*, Report No 54, 1999, 54.

[3] http://www.pcc.philips.com/glossary/p-z.shtml

[4] http://www.techweb.com/encyclopedia/

PIN: Personal Identification Number.

Posting: An article or message posted to a newsgroup.

PUK code (PIN Unlocking Key): If PIN code has been entered wrong three times, the SIM card cannot be used before the correct unblocking PUK code has been given. If the PUK code is given wrongly 10 times the SIM card will be irrevocably locked.[3]

SIM card (Subscriber Identity Module): A smart card inserted into mobile phones that contains telephone account information.[4]

Smart card: A small electronic device about the size of a credit card that contains electronic memory, and possibly an embedded integrated circuit (IC). Smart cards are used for a variety of purposes, including:

- storing a patient's medical records
- storing digital cash
- generating network IDs (similar to a token).

Software: Computer instructions or data. Anything that can be stored electronically is software. The storage devices and display devices are hardware.

Spam: Electronic junk mail or junk newsgroup postings. Real spam is generally e-mail advertising for some product sent to a mailing list or newsgroup.

Usenet (also called netnews): A worldwide bulletin board system accessed through the Internet. Items posted to the system are tagged with topics and become known as 'newsgroups'. A news-reading program (newsreader) is needed to read or post articles to a newsgroup. Articles can also be archived or downloaded.

Introduction

Continuing advances in electronic technology and the growth of the Internet have seen computers and other electronic devices become commonplace both in commerce and in the home, with New Zealanders having one of the highest per capita rates of computer ownership and Internet access in the world.

Criminals have not been slow to adopt this technology for their own ends, both as a means to assist with the commission of traditional offences and to instigate a range of new offences. Accordingly, electronic evidence is now seen across the full spectrum of offending and you need to be able to deal with this evidence no matter what offence you are investigating.

With e-crime you have new questions to ask, new clues to look for, and new rules to observe in the collection and preservation of evidence.

This booklet is divided into four sections:

- Part I covers the Internet, what it is and how it works.
- Part II gives examples of investigations where electronic evidence helped gain convictions.
- Part III investigates electronic evidence, for example computer components, storage devices, disks, tapes and drives.
- Part IV looks at "best practice" in regards to the search, seizure and storage of electronic evidence.

A glossary of terms is provided at the back of the booklet along with the wording to be used in a search warrant.

Part I The Internet and How it Works

Equipment to connect online

The online universe is made up of millions of interconnected computers. A computer connected to the Internet can transport you via your computer to just about anywhere.

To connect to the Internet (or go online) you need a computer, or other device, hooked to the Internet via a telephone line, cable or satellite connection. A group of networked computers can also share an Internet connection.

To access the Internet, specific “browser” software is needed to locate and display web pages, for example Microsoft’s “Internet Explorer”.

To make the connection there also needs to be an account with an Internet service provider (ISP), such as Paradise (provided by Telstra Saturn) or Xtra (provided by Telecom).

When the browser software is activated, a password is entered for the ISP account. The modem dials up the ISP and the user is assigned a unique identity, which is the Internet Protocol (IP) address.

By identifying the IP address you can trace back to the user account at any given point in time. However, these records are kept by the ISP for only a short period.

ISP (Internet Service Provider): A company that provides access to the Internet for a monthly fee. It provides the customer with a software package, username, password and access phone number.

Logic bomb: A nasty selection of codes that is covertly inserted into a program or operating system. It triggers some activity whenever a specific condition is met. The activity is generally destructive.[2]

Modem: A modem is a device or program that enables a computer to transmit data over telephone lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms.

Network: A group of two or more computer systems linked together. There are many types of computer networks, including:

* **local-area networks (LANs):** The computers are geographically close together (that is, in the same building).
* **wide-area networks (WANs):** The computers are further apart and are connected by telephone lines or radio waves.
* **campus-area networks (CANs):** The computers are within a limited geographic area, such as a university campus or military base.
* **metropolitan-area networks (MANs):** A data network designed for a town or city.
* **home-area networks (HANs):** A network contained within a user’s home that connects a person’s digital devices.

Newsgroup: Refer to **Usenet** below.

Palm pilot / PDA (Personal Digital Assistant): A handheld computer. A typical palm pilot can function as a cellular phone, fax sender, and personal organiser.

Flash Card: A small module that contains flash memory such as a PC Card, CompactFlash, SmartMedia or similar format.[1]

Hacker: A slang term for a computer enthusiast – a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s). The popular press has coopted the term to refer to individuals who gain unauthorised access to computer systems for the purpose of stealing and corrupting data.

Hacking: Unauthorised access into computer systems.

Hardware: Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips. In contrast, software is untouchable.

Internet Relay Chat (IRC): A chat system on the Internet that allows people to join live discussions online. To access IRC a special program is needed that connects to an IRC server. An IRC user can access 'chat rooms' and communicate with other users via text messages or web camera images.

Whenever someone joins or leaves a chat room a message is sent to the rest of the participants. Users can communicate with all the participants or send private messages to an individual. Users take on a nickname while in a chat room and anything they type is preceded by their nickname. The person behind the nickname can register other information about themselves, such as e-mail address, age and gender, that the other participants can access.

Intranet: A network belonging to an organisation accessible only by the organisation's members, employees, or others with authorisation. An intranet's web sites look and act just like any other web sites, but the *firewall* surrounding an intranet fends off unauthorised access.

The Internet

The Internet consists of the world wide web, Usenet newsgroups, Internet relay chat, and electronic mail (e-mail).

Wherever someone goes on the Internet, what they do and who they correspond with or how, it is likely that their computer will record some or all of those details. In many cases this process takes place without the user's intervention or knowledge and the resultant data ends up in areas on the hard drive to which the average user does not have easy access.

Reconstructing this data will often give an accurate picture of what has occurred. For this reason, if the circumstances warrant it, consider requesting the complainant to release their computer for forensic examination so that this material can be located and preserved.

World wide web

The world wide web consists of thousands of websites. The websites are generally either electronic shop fronts set up to sell products and services or providers of information. Each website has a unique address known as uniform resource locator (URL). The URL for the Police website is www.police.govt.nz.

While there are many legitimate sites, criminals take advantage of the medium to operate **website scams**. Sometimes people try to find buyers for stolen goods on legitimate websites. Criminals can set up websites to collect credit card numbers and other personal information from customers who believe they are buying legitimate products or services. In reality nothing is ever delivered. The criminal then sells the stolen information or uses it for his or her own (illegal) purposes. This is becoming known as identity fraud/theft.

Questions to ask in a website investigation

1. What is the address or uniform resource locator (URL)?
2. How did the complainant become aware of the existence of the website?
3. When did the complainant contact the website?
4. Did the complainant print a copy of the screen image? If so, ask for a copy.
5. Did the complainant save a copy of the website in his or her computer? If so, ask for a copy on floppy disk.
6. Obtain the username, logon and password used to access the website.
7. Consider requesting the complainant to release the computer for forensic examination.

- **hard disk:** Hard disks can store anywhere from 20MB to more than 200GB. Hard disks are also from 10 to 100 times faster than floppy disks.
- **removable cartridge:** Removable cartridges are hard disks encased in a metal or plastic cartridge, so you can remove them just like a floppy disk. Removable cartridges are very fast, though usually not as fast as fixed hard disks.

Optical disks record data by burning microscopic holes in the surface of the disk with a laser. To read the disk, another laser beam shines on the disk and detects the holes by changes in the reflection pattern. Optical disks come in three basic forms:

- **CD-ROM:** Most optical disks are read-only. When you purchase them, they are already filled with data. You can read the data from a CD-ROM, but you cannot modify, delete, or write new data.
- **WORM:** Stands for ***w****rite-****o****nce, ****r****ead-****m****any.* WORM disks can be written on once and then read any number of times. You need a special WORM disk drive to write data onto a WORM disk.
- **erasable optical (**EO**):** EO disks can be read to, written to, and erased just like magnetic disks.

DVD (Digital Versatile Disc or Digital Video Disc): A new type of CD-ROM that holds a minimum of 4.7GB (gigabytes), enough for a full-length movie.

Encryption: The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text;* encrypted data is referred to as *cipher text*.

There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.

Glossary

Note: These definitions have been adapted from the Webopedia website http://www.pcwebopedia.com, except where indicated. Visit this site if you have any further questions regarding terms used in this booklet.

Browser: Short for *Web browser,* a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer.

CD-ROM: A compact disc made out of a polycarbonate with one or more metal layers capable of storing digital information. CD-ROMs are used to store computer data. They are *read-only*, which means that once the data has been recorded onto them, they can only be read or played.

Chat room: A virtual room where a chat session takes place. Technically, a chat room is really a channel, but the term "room" is used to promote the chat metaphor.

Chat session: A way of communicating in real time via a computer. Two or more parties type messages to each other, which are received immediately.

Disk: A round plate on which data can be encoded. There are two basic types of disks: *magnetic disks* and *optical disks*.

On magnetic disks, data is encoded as microscopic magnetized *needles* on the disk's surface. You can record and erase data on a magnetic disk any number of times, just as you can with a cassette tape. Magnetic disks come in a number of different forms:

- **floppy disk:** A typical 5¼-inch floppy disk can hold 360K or 1.2MB (megabytes). 3½-inch floppies normally store 720K, 1.2MB or 1.44MB of data.

Usenet and newsgroups

Another major aspect of the Internet is Usenet (also called netnews), which is made up of newsgroups. Newsgroups are like notice boards or discussion forums and are usually subject specific. Messages can be read from or posted to a newsgroup (a message posted to a newsgroup is called a posting). Copies of messages can also be downloaded onto a computer.

There are newsgroups that collect and distribute child pornography and advertise children available for sex. Thieves use newsgroups to advertise stolen goods for sale. Illicit drug manufacturers discuss production techniques and may purchase equipment online through these groups. For more information on Usenet and newsgroups, see the Glossary.

Questions to ask in a newsgroup investigation

1. Who is the complainant's Internet service provider (ISP)?
2. How did the complainant discover the existence of the newsgroup?
3. What is the name of the newsgroup?
4. What is the name of the posting?
5. Does the complainant have a printed copy of the posting? If so, ask for a copy.
6. Did the complainant download the posting onto their computer? If so, ask for a copy on floppy disk.
7. Obtain the username, logon and password used to access the newsgroup.
8. Consider requesting the complainant to release the computer for forensic examination.

Internet relay chat (IRC)

Internet relay chat is another major aspect of the Internet. It consists of thousands of “chat rooms” where people communicate in near “real time” using text messages.

Paedophiles meet in chat rooms to discuss their sexual exploits. Paedophiles and other sexual predators visit chat rooms catering for children and teenagers. They often pose as teenagers to lure young people into sexual relationships in the real world (off-line).

Fraudsters work in chat rooms developing relationships and looking for people who will fall for their phoney business opportunities and get rich schemes. For more information on Internet relay chat, see the Glossary.

Questions to ask in a chat room investigation

1. What is the name of the chat room or chat channel?
2. What is the name of the server the chat room is on?
3. What is the nickname, “handle” or screen name of the offender?
4. Did the complainant note the person’s Internet Protocol (IP) address next to their screen name in the users list? If so, ask for the IP address.
5. Did the complainant print a copy of the chat dialogue window? If so, ask for a copy.
6. Obtain the username, logon and password used to access the website.
7. Did the complainant save the chat dialogue on their computer? If so, ask for a copy on floppy disk.
8. Consider requesting the complainant to release the computer for forensic examination.

Conclusion

More criminals now commit their crimes electronically, including online via the Internet. It is quick, easy and assumed anonymous. However, the police know more than these criminals think.

By taking care to follow best practice, valuable evidence is more likely to be found. This booklet and accompanying video do not provide all the answers, but you will now have enough basic knowledge to deal with the situation and know when to call the ECL for their expert advice.

Key points

- Keep the suspect away from the computer or device.
- If the computer or device is ON, do not turn it off.
- If it is OFF, do not turn it on.
- For stand-alone computers, photograph or sketch a picture of the back of the computer. Number connections and cables.
- For business or networked computers, contact ECL for advice.
- Before submitting electronic items for fingerprinting or other forensic testing, contact ECL.

Electronic mail

Electronic mail (e-mail) is the transmission of messages or files over a communication network. Many organisations have an internal e-mail system (intranet) as well as access to the Internet and the ability to send e-mail messages world wide.

Criminals sometimes market their fraudulent scams through e-mail. This unsolicited, “junk” e-mail is called spam (although not all spam is illegal).

E-mail messages carry a source header that records the IP address of the original source and any subsequent transmissions of the e-mail. Usually, this information is not visible when the user views the e-mail.

Questions to ask in an e-mail investigation

1. What is the name of the Internet service provider (ISP)?
2. Does the complainant have a printed copy of the e-mail message (ideally including the complete header)? If so, ask for a copy.
3. Did the complainant save a copy of the e-mail message on their computer? If so, ask for a copy on floppy disk.
4. If the complainant does not have a copy of the e-mail message, is it still in the “computer mailbox” at the ISP? If so, ask for a copy on floppy disk.
5. What is the offender’s screen name and e-mail address?
6. What is the complainant’s username, logon and password.
7. What e-mail program was the complainant using?
8. Consider requesting the complainant to release the computer for forensic examination.

What attracts a lot of criminals to the Internet is the ability to remain anonymous. However, the irony is that it is almost impossible not to leave some sort of electronic trail.

Key points

- Computers record data from Internet use. This data can be located and preserved as evidence.
- Tailor your questions to the type of Internet use suspected.

Care and submission of exhibits

Ensure that as far as is practicable none of the actions taken add, modify or destroy data stored on a computer, device or media.

Remember computers and related electronic equipment are fragile and sensitive to shock, temperature and moisture.

Items submitted to the ECL should be appropriately packaged and cushioned with bubble wrap and/or polystyrene. The external packaging should be clearly marked as fragile.

When submitting material to the ECL include the following items and information as appropriate:

- brief circumstances of the case
- the known history of the items submitted
- specific details of the examination required including any keywords to be searched against
- specific details of the items being submitted
- a copy of the warrant items were seized under
- a copy of the POL 268 form
- contact details of the submitter
- details of any other forensic testing proposed.

Contact the ECL before submitting electronic items for fingerprinting or other forensic testing if there is likely to be a requirement for these items to be examined by the ECL at some later date. This is because some of the treatments used by other forensic disciplines can damage or destroy electronic items.

In summary:

1. Sketch the rear of the computer.
2. Number each socket or port that has a cable connected to it and note this number on your sketch.
3. Attach the corresponding number to the end of the cable that is attached to the computer.
4. If the computer has cables attached to its front, sketch and label those as well.

If you have any doubts or concerns, contact the ECL.

Non-electronic evidence

Recovery of non-electronic evidence can be crucial in the investigation of electronic crime. Proper care should be taken to ensure that such evidence is recovered and preserved.

Items relevant to subsequent examination of electronic evidence may exist in other forms, for example written passwords and other handwritten notes, blank pads of paper with indented writing, hardware and software manuals, calendars, literature, text or graphical computer printouts, and photographs.

These items should be secured and preserved for future analysis. These items are often located near the computer or related hardware items. All evidence should be identified, secured, and preserved in compliance with General Instructions and district policy.

Part II
E-Crime Examples

These case examples show that time spent finding and preserving electronic evidence can pay huge dividends to the outcome of the investigation.

Operation Ono

This operation took place in Auckland City from August to December 1999. The electronic evidence found included an electronic diary and Vodafone cellphones. From that evidence Police extracted dates and times of drug sales and names of customers. As a result of the evidence five people were convicted for manufacturing methamphetamine, conspiracy to manufacture methamphetamine, and selling Class A, B and C drugs. The prison sentences ranged from 5 to 12 years.

Teenage Hacker Case

Staff from Paradise (an ISP) were contacted by a customer who had been unable to log on to the Internet. They established that someone else was using the customer's account and identified the originating phone number that had fraudulently accessed her account details. Paradise agreed to contact the investigators next time the offender was online. When the investigators were advised, they were ready to execute a search warrant within a couple of minutes. They found a 17-year-old hacker with the account holder's details on screen. Relevant computer items were seized.

The investigators discovered that the offender had distributed passwords to his friends and he and those friends were illegally accessing other accounts.

The offender was charged with “using a document” and was ordered to pay reparation, send letters of apology and do 80 hours’ community service. The friends were not charged due to their age, but were referred to Youth Aid.

Operation Godlee

This was a high-profile homicide investigation running from August to September 2000. Three members of a gang committed a homicide in the Christchurch Port Hills at Godley Heads.

In an attempt to become affiliated to an overseas gang, the leader of the Christchurch gang had surfed the web and e-mailed two gangs. A Canadian gang e-mailed back, asking for proof of how ‘bad’ he was before he could be accepted.

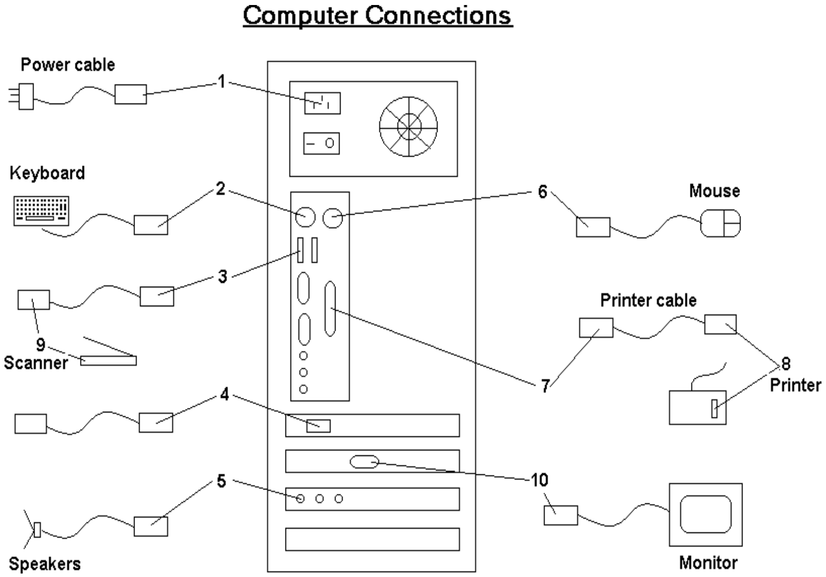
As a result the leader decided to kill one of the other gang members. He and two others took the victim to Godley Heads, carried out the murder, then sent a text message saying “Done”. The day after the murder, the leader e-mailed the Canadian gang and asked them whether they could get a copy of the Christchurch Press as the murder he had organised would be in it. This e-mail pre-dated any press releases or articles relating to the homicide.

The investigators were able to find electronic evidence in the form of e-mails, text messages and messages sent through chat rooms. All three men were found guilty of murder.

If the other end of the cable can be unplugged from an external unit (eg printer, monitor, scanner), unplug it, give that end of the cable its own number and, if possible, show on your diagram what the cable was attached to.

By using numbers it doesn’t matter if you are unsure what type of socket or port a particular cable connects to. If you can identify the external units the cable connects to, such as mouse, keyboard and printer, those details will be helpful.

An example of this type of sketch is shown below.



If you are out of town, make an assessment as to the seriousness of the offence and the kind of information likely to be on the phone. Obviously, if a cell phone is found at a homicide scene then it should be transferred to the nearest ECL as soon as possible.

Collect all contract documentation with the warrant, for example PUK codes, and any other documentation related to the cell phone.

Other devices

Apply the same basic rules as for cell phones. If it is off leave it off, if it is on leave it on. Be aware that battery powered devices will die when the battery is exhausted, which may activate a lockout or data loss.

Computer Diagramming

When you submit a seized computer to the ECL, you must have ensured the ECL experts can reassemble the computer ***exactly*** as it was found. It is essential the ECL knows where the various cables were attached. One reason for this is that many systems have multiple sockets or ports that are for the same purpose. For example there may be two monitor ports, or two sets of audio connections. The ECL needs to know which sockets or ports were in use on an individual system.

An easy method to document the cabling is to sketch the rear of the computer and on the diagram number each socket that has a plug in it. Physically attach the *same number* to the end of the cable that is plugged into the computer. This number can be attached with a sticker or by tying a label to the cable.

Hawkins Case

An 8-year-old girl sparked a paedophile investigation when she complained of being indecently touched and violated. In the evidential interview the victim told of how she was shown photos of naked people on a computer. The investigators seized the offender's computer, computer-related items and a digital camera.

The hard drive revealed thousands of pictures downloaded from the Internet and 54 pictures of a second victim that had been taken with the digital camera, downloaded to the hard drive then saved on a floppy disk.

The offender was convicted with three charges of rape and 22 charges of sexual offending. He was sentenced to 11 years' jail.

Part III Electronic Evidence

In the New Zealand Police there are specialist forensic examiners and analysts at the Electronic Crime Laboratory (ECL) in Auckland, Wellington and Dunedin who carry out the examination of devices.

Electronic evidence can be latent in the same sense that fingerprint or DNA evidence is latent. Latent evidence is evidence that is not easy to "see", so specialist equipment and/or software is needed to make the evidence visible. Files can be created, such as documents, e-mail messages, database information, photo files and video files. However, the computer also creates files that document the use of the device, such as date and time stamps, history files of websites visited, and temporary files for unsaved documents. Some electronic evidence is time sensitive and as such this class of evidence should be dealt with promptly.

Recognising the potential evidence that may exist on an electronic device could be vital to the successful resolution of the crime.

Sources of evidence

All computers, whether a stand-alone PC or a laptop, contain one or more hard drives. A huge amount of data can be stored on the hard drive. It is a prime source of evidence. The hard drive can be taken out of the computer and hidden elsewhere.

If a suspect or any other person is in attendance at the scene, question them to obtain information, such as the owners and/or users of the electronic devices found at the scene, passwords, usernames, encryption codes and ISP.

Other electronic devices can contain valuable evidence associated with criminal activity. Unless an emergency exists, the device should not be accessed. Should it be necessary to access the device, all actions associated with the manipulation of the device should be noted to document the chain of custody and ensure its admission in court.

Cell phones

If the cell phone:

- ➨ is off, leave it off
- ➨ is on, leave it on
- ➨ is on, photograph the display or write down the information on the screen
- ➨ is on and you are near the ECL, take the phone straight to the ECL
- ➨ is on and you are far from the ECL, attach the phone to a battery recharger
- ➨ rings, do not answer it.

If the cell phone is on, be aware that turning it off or letting the battery run flat may activate a security lock-out device that will make it almost impossible for the ECL to turn the phone on again.

3. Using sticky labels or similar, label the components and existing connections at the back of the computer. Label all connectors and cables at each end. This will enable reassembly if needed.

4. Photograph the back of the computer or sketch a diagram. For information on computer diagramming see page 26.

5. Place tape over each drive slot.

6. Collect all removable storage media and documentation.

7. Obtain all logons, usernames, passwords and PIN numbers.

Note: It is common for people to write their passwords down and leave them on or near the computer. Keep an eye out.

Networked or business computers

If the computer is networked or a business computer consult the ECL for further assistance. If possible, call the ECL before you execute the warrant. Pulling the plug could severely damage the system and disrupt legitimate business leaving the Police open to official complaint and the possibility of civil action.

Remember: Keyboards, the computer mouse, disks, CDs, and other components may have fingerprints or other physical evidence on them that should be preserved in the usual manner.

Data can also be stored on various other removable storage devices, including disks, drives and tapes. These can be small and are portable, making them easy to hide or disguise. A CD-Rom containing evidence can be disguised as a music CD.

The amounts of data on modern devices can be huge. When you require ECL staff to examine a device you must give them specific details of what you are looking for. The more detailed your information, the more efficient the search.

Note: To give you an idea of the size of the search task, if the contents of a full 40GB hard drive were printed out as text it would produce a stack of A4 pages 1,500 metres high. This is over 4½ times the height of the Auckland Sky Tower. Even a 3½" floppy disk can carry enough information to print in excess of a ream of paper. Therefore, it is important to be as detailed as possible in your search request to an ECL.

Remember: A computer and its related storage devices are not the only electronic devices from which evidence can be collected. Most electronic devices contain some kind of memory function that may be accessible and hold useful information. Ask for logons, usernames and passwords for these devices as appropriate.

Electronic devices that exist today include:

Cellular and mobile telephones
SIM cards
Digital cameras and videos

Scanners
Palm pilots or PDAs
Facsimile (fax) machines
Electronic diaries and organisers
Pagers
Flash cards
Smart cards
Photocopy machines
Removable media storage devices (there is a multitude of different types)

These devices come in a range of shapes and sizes and can be easily disguised.

Key points

- Many electronic devices have memory devices that can hold useful information.
- Electronic evidence can be time sensitive – you must deal with it promptly.
- The hard drive is a prime source of evidence.
- The recovery of electronic evidence requires specialised knowledge and technology.
- Give ECL staff specific details of what you are looking for.

Device types

Stand-alone, non-networked computer

Note: If the screen is blank do not automatically assume that the computer is off, it may have gone into “hibernation” mode. You should determine whether the computer is actually on or off by moving the mouse – if the computer is on the screen should reactivate.

DO NOT TOUCH THE KEYBOARD OR MOUSE BUTTONS.

If computer is off, DO NOT TURN IT ON.

If computer is on, DON’T TURN IT OFF.

If there is material on the screen about which you are unsure, call the ECL before you take any further action.

Then

1. Consider photographing the screen if the material on the screen is relevant.

2. Pull out the power plug from the back of the computer first and then from the wall. If the computer is a laptop you will also have to remove the battery, look for a large latched panel usually marked with a battery icon. Do not replace the battery once you have removed it.

   This will instantly stop the computer if it is on and remove the possibility of someone restarting it.

1. Freeze the scene

Freeze the scene for potential fingerprints and other forms of forensic evidence. Immediately restrict access to the computer and other electronic devices and related material (for example floppy disks). Do not attempt to access information on the computer at this stage.

Do not allow the suspect near the computer or device as electronic data can be altered or destroyed within seconds. Criminals write “logic bombs” that can cause a computer to crash and destroy data if the correct sequence of keystrokes is not used.

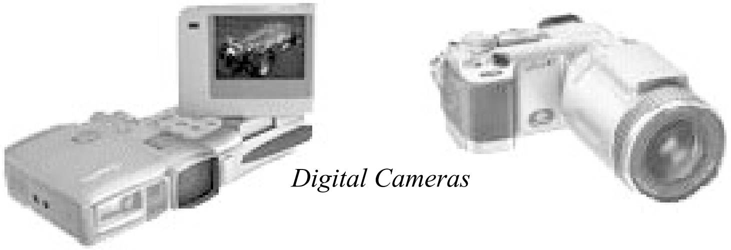
2. **Locate** and **secure** the evidence

Isolate the computer from telephone lines, as data on the computer can be accessed remotely. Identify telephone lines attached to devices such as modems and caller identification (ID) boxes. As the computer end of a telephone cable appears very similar to a network cable it is better to disconnect telephone lines from the wall rather than the device where possible.

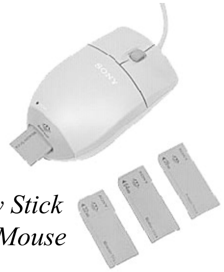
Secure the computer as evidence.

Turning a computer on or off can alter the components of evidential files, such as date and time stamps and modification, deletion or user name attributes. In effect, this alters the evidence and affects its admissibility in court.

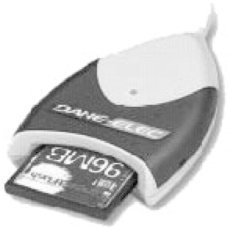
Examples of Electronic Devices



Digital Cameras



Memory Stick Reader Mouse

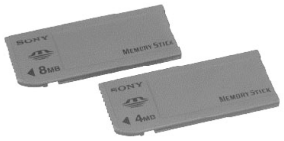


Flash Card Reader

Electronic Organisers

Flash Card

Smart Card



Memory Sticks

Facsimile

Photocopier

Pager

Scanner

ZIP Drive

Cellphone

Part IV
Best Practice

Electronic evidence is delicate. It is easily altered, damaged or destroyed by improper handling or examination. It is important to know when to call in experts from the ECL.
Any attempt to access data or run a computer program can jeopardise the integrity of the evidence. Electronic evidence, like all other evidence, must be handled carefully and in a manner that protects its evidential integrity.

Note: If you are planning to execute a warrant and have concerns about what you may find or how to handle electronic equipment call the ECL *before* you execute the warrant. Wording to include in the warrant is outlined at the end of this booklet.

First response

Freeze – locate – secure – document – protect

As a first responder, it is necessary to:

1. freeze the scene
2. locate and secure the evidence
3. document any action taken to ensure the evidential trail
4. protect perishable data physically and electronically.