Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

High Tech Crime Brief

2005

04

Evidence

Digital evidence

While the computer is sometimes likened to a smoking gun, it is much more a silent witness. Careful investigation is required to uncover and preserve what it might say, and sophisticated forensic analysis must be applied to relay that to the court. In fact, despite the impression sometimes conveyed in the media, it is not always easy to investigate or prosecute high tech crime. The main evidential difficulties are the ephemeral nature of records such as ISP data logs and the capacity for the internet to be used anonymously (AGEC 2000).

Each jurisdiction in Australia has its own law of evidence and the Commonwealth, the ACT, NSW and Tasmania have adopted a uniform model. While there may be some difficulties with the requirements for the proof of foreign business records (AGEC 2000), the laws in each jurisdiction facilitate the presentation of computer-based evidence (Ligertwood 1998):

- computer records and printouts may be tendered as documentary evidence or as business records to prove what they contain – this is an exception to the rule against hearsay, which would otherwise stop such material being relied on to prove the truth of its contents;
- it is possible to prove that particular processes are carried out on information and communications technologies (ICT) equipment and in some jurisdictions there is a rebuttable presumption that a computer works correctly; and
- under expert evidence provisions, experts can give evidence about the operation of computers.

Despite these facilitating provisions, there are a number of evidentiary problems that the investigator must face. For a detailed discussion see Smith, Grabosky and Urbas (2004).

Legal issues in uncovering evidence

Obviously law enforcement officers are constrained to follow the law. This is not always what happens however, whether through inadvertence, neglect or deliberate misconduct. Where there is a departure from general legal requirements in the gathering of evidence, the court may reject that evidence.

Search and seizure

Investigators need to take care to work within the terms of any warrant for search or seizure, and have the warrant extended or a fresh warrant issued where appropriate. Some of the potential problem areas are:

- where non-police are involved in the location of evidence of an offence – this may happen completely outside any warranted search or may compromise a warranted search;
- where evidence of a crime other than the one for which the warrant was issued is found in the course of a search, or on a data storage device after it has been seized; and
- where privileged information is uncovered, such as legal professional privilege in an email to or from a lawyer, because it is probable that a computer hard drive will contain a wide variety of material some of which may attract specific privileges.

Telecommunications interception

If the evidence is obtained in breach of the *Telecommunications Interception Act 1979* (Cwlth), then the evidence is automatically barred.

Assistance requirements

In some jurisdictions law enforcement officials have the power to require persons to assist them to gain access to data.

ISP information

Not all ISPs are required to retain data logs that are necessary to track data transfers in an investigation (Parliamentary Joint Committee on the Australian Crime Commission 2004). There is an ongoing difficulty in relation to the keeping of such records and facilitating their transmission to police in appropriate cases. Law enforcement agencies may be forced to rely on ISP cooperation and this is often more difficult or impossible to secure when the ISP is located overseas.

Practical issues in preserving evidence

Standards Australia has established a set of generic standards for managing electronic evidence. Electronic records are said to be volatile in that they can be immediately and deliberately or accidentally altered and expunged. Electronic records may also be automatically altered or deleted – usually to save storage media (Standards Australia 2003).

Safety

Obviously the safety of law enforcement officials in handling electronic equipment is of paramount importance.

Securing equipment

Protocols have been developed for handling equipment to minimise damage to, or alteration of, data. A pocket-sized best practice guide is available to officers.

Passwords/encryption

With proper regard for the rules for questioning suspects, the suspect may be a source of important information concerning the use of the computer and any passwords. Care needs to be exercised, however, as the suspect may deliberately mislead investigators.

Co-mingled data

Co-mingling may present problems in keeping a search within the terms of a warrant. This problem may arise when a data storage device is seized or where it is subject to authorised hacking or remote keystroke logging by law enforcement officers. The co-mingling of data is an increasingly important issue for investigators. Co-mingling may involve material that relates only to the suspect or it may involve a number of persons who share a computer, an email account or a data storage device, such as within a work group or family. This difficulty may be avoided by obtaining specific permission from other users to inspect or copy material.

The problem of co-mingling may require the investigator to make special arrangements for the safe custody of material seized, pending resolution of any competing claims regarding the legality of seizure.

Connecting the accused with the offence

It is said that the computer should be treated as a crime scene. Regard should also be had to the physical crime scene in which the computer is located. Physical exhibits, including other devices such as printers or scanners, may be of crucial significance. There may be handwritten information about passwords, encryption or printouts that document online activity. Any information showing the suspect's use of the computer could be important to prove that it was the suspect using the computer at a particular time. Other obvious items of relevance are guides to hacking, printouts of child pornography, or writings that may be associated with suspect online activity.

Following the traces of behaviour

In many investigations it may be necessary to prove the timing, source and routeing of data transmissions. Time is of the essence in obtaining ISP records, as these may not be kept for extended periods.

Software to preserve and recover data

Various software products are available to investigators to secure and recover data. This technology appears to be widely accepted. It is essential that investigators follow procedures for the use of such tools to avoid having the resulting information rejected for a failure to do so.

False records

The investigator needs to be conscious of the possibility that a sophisticated offender may use various security weaknesses to hide their own tracks or lay false trails to divert attention from themselves. Tip-offs and leads need to be carefully scrutinised to avoid the hijacking of investigations.

Experts

Every investigation should be approached on the basis that the prosecution will be put to the test and required to formally prove its case with expert evidence. Persons with appropriate levels of expertise need to be involved in the investigation from the earliest possible date (Thomson 2004).

Technical issues in interpreting evidence

While a convincing trail might be established through computer forensics, it will be of no use against a particular defendant unless the connection can be made between that trail and that defendant.

Connecting a suspect with the offence

Using digital evidence to link a suspect with a particular action can involve a painstaking job of connecting aspects of the digital evidence to other evidence. Sometimes technical evidence may prove that material relied on by the defence was created at a later time than it is made to seem. This was important in the UK prosecution of Dr Harold Shipman for the murder of his patients in relation to his computer files (Halliwell 2004). The Independent Commission Against Corruption (ICAC) relied on similar date time stamp evidence from a computer to find documents had been falsified (ICAC 2001).

The Trojan horse defence

An important vehicle for the commission of offences against computers is Trojan horse software. This is software that can be transmitted from one computer to another and which allows an infected computer to be controlled remotely. A number of cases have recently been argued on the basis of a defence claim that either a Trojan horse is to blame for material appearing on a defendant's computer or that the prosecution has failed to exclude that possibility (Rasch 2004). The prosecution may be able to call evidence that no Trojan horse or trace of one was found on the computer or that other evidence ties the suspect to the criminal use of the computer – referred to as evidence of habituation (Halliwell 2004).

Encryption

Where the investigator is faced with the use of data encryption, early lawful use of key logging software may provide the means to decrypt data. In some cases the lengthy process of decrypting data may need to be undertaken.

Conclusion

Computers have revolutionised the investigation of traditional crime and have opened up a new sphere for the investigation of high tech crimes where ICT equipment or data are the object of offending or the tool for the commission of an offence. Those who investigate high tech crime are faced with many opportunities and challenges. The biggest problems are not to do with the laws of evidence but rather with search and seizure, the scale of material that is available, the volatility of data and the degree of anonymity available using ICT.

Contact
Australian Institute of Criminology
GPO Box 2944 Canberra ACT 2601
Phone: 02 6260 9200 Fax: 02 6260 9201
Web: www.aic.gov.au

Project no. 0074 ISSN 1832-3413

<AHTCC>

The Australian High Tech Crime Centre
funded this research.

Further reading

Action group into the law enforcement implications of electronic commerce (AGEC) 2000. *Issues paper: evidence and the internet.* Canberra: AGEC

Halliwell E 2004. Footprints on the disk. *The guardian.* 5 February

Independent Commission Against Corruption 2001. *Report on investigation into matters concerning John Kite and the National Parks and Wildlife Service.* Sydney: ICAC

ISO PDTR 18044. *Information security incident handling guidelines*

Ligertwood A 1998. *Australian evidence* (third edition). Sydney: Butterworths

Parliamentary Joint Committee on the Australian Crime Commission 2004. *Cybercrime.* Canberra: Parliament of the Commonwealth of Australia

Rasch M 2004. The giant wooden horse did it! *The register.* 20 January. http://www.theregister.co.uk/content/56/34985.html

Smith R, Grabosky P & Urbas G 2004. *Cyber criminals on trial*. Cambridge: Cambridge University Press

Standards Australia 2003. *Guidelines for the management of IT evidence.* Sydney: Standards Australia

Thomson I 2004. *Vital e-crime evidence is often destroyed.* http://www.vnunet.com/News/1152379

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government, the AIC or the AHTCC