AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 118

What is Forensic Computing?

Rodney McKemmish

Developments in information technology have begun to pose new challenges for policing. Most professions have had to adapt to the digital age, and the police profession must be particularly adaptive, because criminal exploitation of digital technologies necessitates new types of criminal investigation. More and more, information technology is becoming the instrument of criminal activity. Investigating these sophisticated crimes, and assembling the necessary evidence for presentation in a court of law, will become a significant police responsibility.

This paper provides an overview of the new law enforcement field of forensic computing. It is an abridged version of a report prepared by the author during his Donald Mackay Churchill Fellowship. Its publication here reflects the Australian Institute of Criminology's continuing role in informing policy makers and the public about complex criminal activity.

Adam Graycar
Director

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. It encompasses *four key elements.*

1. *The identification of digital evidence* 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. Whilst many people think of personal computers as the sole focus of forensic computing, in reality it can extend to any electronic device that is capable of storing information, such as mobile / cellular telephones, electronic organisers (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 so that the appropriate technology can be used to extract it.

2. The preservation of digital evidence 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. 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.

June 1999

ISSN 0817-8542
ISBN 0 642 24102 3

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9200
Fax: 02 6260 9201

For subscription information together with a complete list of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au

or call AusInfo toll free on 13 24 47

3. The analysis of digital evidence—the extraction, processing and interpretation of digital data—is generally regarded as the main element of forensic computing. Once extracted, digital evidence usually requires processing before it can be read by people. 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.

4. The presentation of digital evidence involves the actual presentation in a court of law. This includes the manner of presentation, the expertise and qualifications of the presenter and the credibility of the processes employed to produce the evidence being tendered.

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 crime 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.

This can best be demonstrated by the situation where the forensic examiner utilises a third party software package to display and reproduce the data contained within a computerised document. As an example, consider a spreadsheet containing extensive financial data. If a third party product is used to reproduce the spreadsheet in its entirety, and that third party product does not accurately and concisely represent the location of each item of data, the entire meaning of the document may be changed. This in turn can have a significant impact should the document be tendered in evidence. Not only does it cast doubt over the processes employed during the forensic examination, but also over the skill and expertise of the examiner producing the document in evidence.

Primary Activities of Forensic Computing

Forensic computing is not a single activity, but draws upon many disciplines. It involves the application of information technology to the search for digital evidence and comprises the three primary activities listed below.

Media and electronic device analysis

The analysis of media relates to the examination of various types of storage media such as hard disks, removable storage media (e.g. floppy disks, ZIP disks) and specialist storage media (e.g. CD-ROMs, DVD). This requires a thorough understanding of both the physical structure and the operation of the media, as well as the logical structure and composition of the data as it is stored. Much of the complexity of this activity has now been removed thanks to the application of very efficient and intelligent data recovery tools. Consequently, much of the knowledge required to perform the task is encapsulated within the particular data recovery software.

"Electronic devices" refers to any electronic device capable of storing information of evidentiary value, including cellular phones, electronic organisers and various network communications devices such as routers and hubs. The analysis of such devices is somewhat more complex than the activity of recovering data from storage media and the hardware required is generally more specialised and complex.

The development of customised hardware devices has made the extraction of data from some types of electronic devices much easier, which in turn has allowed people without the relevant knowledge to perform data recovery on specific electronic devices.

Given the wide scope of this forensic computing activity, it comes as no surprise that a number of disciplines are involved. Software engineering, cryptography, electronic engineering and data communications are areas of expertise which, in combination, make the analysis of media and electronic devices possible.

Data communication analysis

Data communication analysis encompasses two separate activities:

- network intrusion or misuse
- data interception

Network intrusion or misuse is the main forensic computing activity when it comes to Internet based analysis. It consists of the following functions:

- intrusion detection;
- evidence capture and preservation; and
- event or activity reconstruction.

Intrusion detection generally involves the application of specialised software, and in some cases hardware, to monitor data communications and connections with a view to identifying and isolating potentially unlawful behaviour. Such behaviour includes unauthorised access and attempts at unauthorised access, remote system modification, and unauthorised monitoring of data packets.

Evidence capture and preservation generally occurs after an intrusion or abnormal behaviour is detected, so that the abnormal or suspicious activity can be preserved for later analysis.

The final stage, reconstruction of the intrusion or abnormal behaviour, allows a thorough examination of all data gathered during evidence capture.

To carry out these functions successfully, the forensic computer examiner(s) must be skilled in data communications and have the support of software engineers

and, where necessary, cryptographers.

Research and development

Research into, and the development of, new techniques and tools is vital to keep abreast of changes in technology. Time and resources must be dedicated to the research and development of new forensic techniques, not only to develop solutions to existing problems, but also to recognise emerging problems and find realistic solutions.

Unfortunately, the resources and skills required to maintain an effective research and development program are beyond the financial capacity of many computer forensic groups. And an additional restriction placed on any solutions derived from research is the requirement that they must be capable of satisfying the legal framework in which the forensic computer specialist works.

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. Whilst these rules are general enough to apply to any process in forensic computing, adherence to them is fundamental to ensuring admissibility of any product in a court of law. As the methodology employed in relation to the various processes is determined by the individual forensic specialist, the actual process chosen should be applied so as not to compromise the relevant rule(s). Essentially, the rules of forensic computing are:

Rule 1—Minimal Handling of the Original

The application of forensic computer processes during the examination of original data 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.

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 computer specialists to work on the data, or parts of the data, at the 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 re-create the original environment, specific items of hardware etc. may be required. This again adds further complexity and time to the forensic process.

Rule 2—Account for Any Change

Where changes occur during a forensic examination, the nature, extent and reason for such changes should be properly documented.

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.

This is not to say that change shall not occur but rather, in situations where it is inevitable, the examiner has a responsibility to correctly identify and document the change—a process directly dependent on the examiner's skills and knowledge. 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 facilitate 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.

Rule 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.

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.

Rule 4—Do Not Exceed Your Knowledge

The forensic computer specialist should not undertake an examination that is beyond their current level of knowledge and 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 not aware of or does not understand and consequently may ignore. This is likely to be revealed when the examiner is giving evidence.

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

Current and Future Issues for Forensic Computing

Advances in technology give rise to new and exciting challenges but also present the forensic computer specialist with new problems. Advances in technology can also lead to more advanced solutions but unfortunately, whilst technology may change and adapt, the law is somewhat slower to change. Remembering that forensic computer specialists serve two masters, technology and the law, they must find an acceptable balance between the two.

Not all of the challenges faced by forensic computing are technical in nature. They must also deal with issues of resourcing, procedure and policy, training and organisational changes. This paper, however, focuses on the technical challenges.

Operating systems

Over the past decade we have witnessed rapid advances in operating system (OS) design and functionality—from the text based interface of DOS to the Graphical User Interface (GUI) of operating systems such as Windows and Unix (Xwindows). With the advent of the Graphical User Interface, operating systems have become larger, more powerful and more user friendly. It is the size and usability of the GUI operating system that presents forensic computing with a new challenge.

When DOS was the predominant operating system for the personal computer, things were much easier for the forensic computer specialist. The DOS based operating system could be installed on a floppy disk and a suspect's system booted via the floppy drive. Device drivers specific to the computer under examination would not be loaded but, given the simplicity of the operating environment, it did not generally matter. Today, the size of the GUI based operating system means that it cannot be installed in its entirety on a floppy disk. Whilst we can still boot to a text based interface, many of the important operating system features cannot be accessed.

In the laboratory environment the issue of size may not be relevant, primarily due to the development of alternate technologies, but in the field this proves to be the greatest hindrance.

Just as operating systems have grown in size, so too has their functionality. Of all the features incorporated into today's GUI based operating system, plug and play support provides the greatest danger to the forensic computer process. A plug and play supported operating system installed on a computer is configured to that computer. The operating system records the nature and configuration of all hardware installed on a computer. The subsequent addition or

removal of hardware is readily detected by the operating system, resulting in changes to the relevant configuration files. The impact of such intelligence has serious implications for the forensic examination process. Removing a hard drive and inserting it into another computer will inevitably result in changes as the operating system configures itself for its new environment. It does not even have to be the hard drive, but rather a restored binary image undergoing examination in the specialist's own system. Regardless of the approach, the possibility of change is significantly increased.

Data volume

Probably the greatest single challenge facing forensic computing today is the rapid increase in the capacity of today's storage media. The advent of new storage technologies, combined with increased demand for storage space by consumers and software developers, has resulted in a surge in the size of hard drives. Just as the capacity of hard drives has increased, so too has the volume of data being stored on such media. Increased use of multimedia, combined with the rapid expansion of the Internet, has resulted in greater demand for storage capacity. This in turn has led to an increase in the amount of information people store (whether permanently or temporarily) on their computers.

Being able to copy, store and process large volumes of data in a timely and accurate manner presents a unique challenge to forensic computing. The copying of data does not just refer to copying files, but includes the making of a binary image. Whilst the quantity of data resulting from a file copy is dependent on the number of files on the hard drive, the quantity of data resulting from a binary image is very much dependent upon the physical capacity of the hard drive itself. Even allowing for compression, the amount of data involved is substantial. For example, the binary imaging (without compression) of a 10 GB hard drive will result in a file, or files, totalling 10 GB in size. Copying such large amounts of data requires the use of very specialised tools in a specialised environment. The problem is compounded if the data is derived from a number of computers, or from a large file server or servers.

The storage of such large volumes of data also presents the forensic examiner with a new set of problems. Many forensic specialists have turned to a network solution. Essentially, network servers become very large storage repositories. In order to hold such large volumes of data in one location, forensic computer analysis networks require exceptionally large storage capabilities. In terms of hard drive space, these inevitably exceed many corporate based network servers. However, server storage only provides a short-term solution—data cannot reside on the server forever. Consequently, longer-term storage solutions have to be found. Currently, tape backup and CD-ROMs provide the most popular solution, but both have their shortcomings. CD-ROMs can only hold 650 MB of data so, given a 10 GB drive, some 16 CDs would be required to accommodate an uncompressed image. Tape provides greater storage, but its reliability with regard to long-term storage is questionable. Additionally, tape is more susceptible to damage than CD-ROM. One emerging solution is the Digital Versatile Disk (DVD), but at present its acceptance within forensic computing is very limited.

The accurate and timely processing of these large volumes of data provides the final challenge to the forensic computer specialist. Identifying the required information, and retrieving it in a form that is legally acceptable, requires the expenditure of time and effort beyond that normally associated with similar processes. The use of binary imaging, combined with a need to extract specific items of information, means that specialised tools are needed and there are extra steps within the examination process.

Digital devices

Recent advances in microelectronics have allowed microprocessors to become more powerful and physically smaller. Not only has the microprocessor become faster and more capable, but storage chips have increased their capacity significantly. Such improvements are having a significant impact on the forensic analysis process. Small personalised electronic devices, such as electronic organisers, are able to store and process significant quantities of data, which in turn may have intelligence or evidentiary value in an investigation.

The advantages of the forensic examination of such devices can best be illustrated in drug related investigations. Increasingly, suspected drug dealers are using personal electronic organisers to store contact names and numbers of both clients and drug contacts. The electronic organiser allows for the storage of large quantities of data, which can be secured by means of a password. Additionally, these devices are easily concealed. It is no surprise that lawful access to the information contained in such devices can present law enforcement agencies with an Aladdin's cave of incriminating information.

These technologies have given rise to an application of microelectronics that is set to have the single greatest technological impact on our society to date: the smart card. The ability of smart cards not only to store significant quantities of data, but also to process and secure that data in a single "chip", adds significant complications to the forensic computer examination process. Just as smart card technology is sophisticated, so too are the forensic processes and tools required to analyse and extract

the data, requiring a level of research and development beyond the resources of many of today's forensic computer units.

Encryption

Improvements in processing technology combined with advances in cryptographic techniques mean that today's encryption schemes are relatively secure for the everyday user. However, there has been a recent increase in the use of encryption by offenders in Australia and overseas.

Recent experience has seen the use of encryption spreading from what has traditionally been the domain of the hacker community to other criminal activities. In particular, paedophiles frequenting the Internet have turned to encryption to hide illegal images of child pornography. A Victorian based paedophile was discovered in possession of a quantity of computer images depicting child pornography. Some were encrypted with a commercially available product to disguise their nature during transmission, via the Internet, to an associate and, to further assist the subterfuge, file names were changed to represent data other than a graphic image.

Advances in communications technologies, such as the Internet, have made complex encryption products widely accessible, presenting the forensic computer examiner with a significant barrier. Regardless of the encryption process used, if the user is required to open cipher text by way of a password or key (whether secured by an asymmetric or symmetric encryption algorithm), the encryption process can almost always be attacked by using brute force techniques. Whilst this may seem like the answer to breaking all encrypted data, it is sometimes impractical. The use of strong keys (long key lengths) can result in a brute force attack lasting many years or decades—not a viable proposition for most criminal investigations.

Improvements in the processing power of microprocessors, combined with such technologies as distributed computing, have allowed many forensic computer specialists to use the brute force approach in different situations.

Unfortunately, just as the forensic specialists have become aware of the advantages of improved processing power, so too have those who design and implement encryption algorithms. Today there is a move towards multi-implementation of an encryption algorithm within security products. This in turn has the effect not only of securing the data more strongly, but also of significantly slowing down the encryption and decryption process.

Conclusion

Given the increasing opportunities for computer based crime in contemporary Australia, a number of related emerging issues need serious consideration by Australian law enforcement. Many agencies throughout Australia must recognise the contribution that forensic computing can make in the investigation of crime, and in turn must ensure that such a contribution is supported and positively promoted. Failure to do so will see those agencies falling behind technologically competent criminals who readily recognise the advantages of using new technologies in the commission of crime.

A number of Australian law enforcement agencies command impressive forensic computing resources, and the Computer Crime Program of the Australasian Centre for Police Research (formerly the National Police Research Unit) is assisting law enforcement agencies in the exchange of knowledge and technology. Through efforts such as this, Australia can become a world leader in the adoption of technology to analyse electronic evidence.

Senior Sergeant Rodney McKemmish is the Officer in Charge of the Forensic Computer Examination Unit, Queensland Police Service. He has performed duties as a police officer and forensic computer examiner with the Victoria Police Force and Queensland Police Service and currently chairs the Australasian Computer Crime Managers Group.

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.