



Computer forensics

By **Rodney McKemmish**,
Senior Manager,
KPMG

- ⑥ **What is computer forensics?**
- ⑥ **Elements of computer forensics**

1 Technology, the law and business

In many of today's criminal investigations and civil disputes, it is very rare not to find technology playing a part. In the world of criminal prosecution, computer technology is increasingly being used as either an aid in the examination of key evidence (eg forensic science) or as the primary source of evidence (eg computer forensics). In the world of civil dispute, computer technology is also playing a part in the examination and production of key evidence. Given therefore the important role that technology plays, it should come as no surprise to learn that for any evidence that is derived either in full or in part from these types of examinations, it is critical that the application of any computer technology be undertaken in such a manner that satisfies both the rules of evidence and expectations of the judicial process.

In the business environment the role of information is critical in not only the daily operations of the business, but also the decision-making processes so heavily relied upon. The value of information cannot therefore be overstated. Consequently it is critical that a business have available information that is both accurate and timely. Inaccurate information can lead to incorrect business decisions, whilst information that is not delivered in a timely manner can result in lost opportunities as well as poor business decisions. It is no wonder then that businesses invest heavily in their Information Technology (IT) infrastructure.

So what happens when critical business data is altered, deleted or false data inserted into a company's information holdings? How does a business prove that its information holdings have been deliberately tampered with? In these situations the first point of call is usually the company's own IT people. How the IT staff respond may prove decisive in any future legal

action taken, either by the company or, as often happens, against the company by an aggrieved third party who may have suffered a loss directly attributable to the company's actions. Actions which are derived in part from false or misleading data.

In response to these questions, and as a direct consequence of the needs of law enforcement, the field of computer forensics has emerged. Computer forensics bridges the gap between the law's need to establish the truth, and the seemingly complex nature of computer technology.

2 What is computer forensics?

Just as courts rely on properly qualified accountants to give expert and opinion evidence on accounting matters, so there is a need for experts to give evidence on matters relating to information technology. Hence the need for computer forensic experts. Computer forensics is more than IT support, it is a unique and distinct discipline in its own right which has been recognised internationally by both government and judicial entities. So what is computer forensics?

Computer forensics is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable in any legal proceeding (ie: court of law or other judicial or administrative hearing).

Simply put, forensic computing is:

'Data recovery with rules ... the rules of evidence'.

3 The four elements of computer forensics

Computer forensics essentially 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.
2. The preservation of digital evidence is a critical element in the forensic process. Given the potential likelihood of judicial



scrutiny in a court of law, it is imperative that any examination of the electronically stored data be carried out in manner that is at least intrusive as is possible.

3. The analysis of digital evidence is generally regarded as the main element of forensic computing. The extraction, processing and interpretation of digital data are all steps in the analysis process.
4. The presentation of digital evidence, being the final element, involves the actual presentation of the examiners findings before a judicial or administrative hearing.

4 The computer forensic dilemma

A unique feature of computer forensics that sets it apart from other IT related disciplines is the requirement that the final result must be derived from a process that is legally acceptable. Consequently the application of technology to the investigation of technological crime or information misuse must be achieved with due regard to the requirements of the law. Failure to do so can result in potential digital evidence being ruled inadmissible or at the very least be regarded by the courts as tainted. Whilst one can draw an inference from this statement that in every instance where a forensic examination of computer data is undertaken, the analysis results will end up being tested in court, in reality a large percentage of matters in which computer forensic evidence is generated do not make it to a court room. Despite this however it is critical for the computer forensic examiner to always work under the assumption that not only will the results of the examination be tendered in evidence, but also their processes and credibility will be challenged and tested.

Because not every instance of a forensic examination will be tested in court there has emerged a general belief that computer forensics is

The role of information is critical in not only the daily operations of the business, but also the decision-making processes so heavily relied upon.

simply about playing with computers, and as such any person with computer knowledge can perform a computer forensic examination. The real test however is not only in the results of an examination, as has been pointed out, but how those results would stand up to legal challenge. Obviously the key test will be the expertise and credibility of the computer forensic examiner who presents the evidence. The second test will be the processes and procedures adopted in the forensic examination, and the third and final test will be an examination of the technology used during the forensic examination process.

Given the potential therefore for computer forensic evidence to be challenged in a court, it is essential that the people chosen to be computer forensic examiners are suitably qualified, and experienced. For if they are not, the value of IT based evidence will be greatly diminished.

5 Rules of computer forensics

Given that the final product of the forensic process is subject to judicial scrutiny it is important that a number of rules 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. Given that the actual methodology employed in relation

to the various processes is determined by the individual forensic specialist, the actual process chosen should be applied in such a way so as not to compromise the relevant rule(s). Essentially the rules of computer forensics 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 computer forensics. Any examination of original evidence should be conducted in such a way so as to minimise the likelihood of alteration. Generally this rule is adhered to by the application of various duplication techniques. Essentially the original is, where possible, duplicated and the examination takes place on 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. Consequently, 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 same data, or parts of the same data, at the one time. This is especially important if specialist skills (eg cryptanalysis — password breaking) are required for various parts of the analysis process. Finally it ensures that the original is in the best state possible for presentation in a court of law.

Unfortunately whilst there are advantages to duplicating evidence, there are also a number of disadvantages. Firstly the duplication of evidence must be performed in



such a manner, and with such tools, so 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 can lead to questions being raised 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. This in-turn has resourcing and procedural implications. Additional resources are required to accommodate the duplicated data, and extra time is required to facilitate the duplication process. Furthermore the methodology being employed must be expanded to include the duplication process. Finally the restoration of duplicated data in a way that recreates 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.

Rule 2

Account for any change — where changes occur during a forensic examination, the nature, extent and reason for such change should be properly accounted for

During an examination it may be necessary for either the original or duplicate to be subjected to alteration. 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 the change. Additionally the examiner must be able to correctly explain the extent of any change and give a detailed explanation as to why change was necessary. As was stated earlier, this includes any examination whether it is conducted on the original or on a duplicate.

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 change. The ability of the examiner to correctly describe the change is directly attributable to his / her skills and knowledge. Whilst during the forensic examination this point may seem insignificant, it becomes a critical issue when the examiner is presenting his / her findings during judicial proceedings. Whilst the evidence may be sound, questions regarding the examiners skills and knowledge can affect both his / her credibility as well as the reliability of the process used. Hence, given sufficient doubt, the results of the forensic process can in the worst case be ruled inadmissible.

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 concepts of computer forensics is the necessity to ensure that the application of tools and techniques is carried out in such a manner so as not to 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. Whilst this is very much dependent upon the existing legislation, it is never the less necessary to ensure that the method of presentation does not alter the meaning of the evidence. Essentially the information should be presented

in a manner that is as indicative of the original as is possible.

Rule 4

Don't 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 computer forensic examiner is aware of their own limitations with regard to their current level of skills and knowledge. In effect the examiner must be able to recognise at what point the examination requires knowledge and skill beyond their own capabilities. On reaching this point the examiner has a number of options. The first is to cease any further examination and to seek the involvement of more experienced and skilled personnel. The second is to conduct the necessary research to improve their own knowledge to a point that permits a continuation of the examination. The third is to 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 correctly describe the processes employed during an examination. Additionally the examiner should be able to explain the underlying methodologies for such processes. Failure to competently and accurately explain 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 with continuing an examination beyond ones skills is the increased likelihood for damage. All too often in these situations, changes take place that the examiner is not aware of or does not understand. Consequently such changes are usually ignored. This in turn becomes a ticking time bomb, waiting to explode back in the

examiner's face. When it does, it usually occurs when the examiner is giving his / her evidence.

Essentially complex forensic computer examinations should be undertaken by properly skilled and qualified staff. The actual level of skill and knowledge will determine the complexity of the examination. To ensure that these conditions are met it is imperative that the examiner has undergone the appropriate level of training. Additionally, given that technology is continually advancing it is important for the examiner to partake in ongoing training.

6 Computer forensic technology — a short history

The technologies behind many of today's computer forensic techniques are directly derived from those technologies utilised in the field of data recovery. Over time however it became apparent that data recovery did not offer all the solutions, consequently some computer forensic practitioners began to develop their own tools and techniques. Today computer forensics has its own unique type of technology that has been developed to meet the evidentiary needs of the forensic process.

Whilst data recovery is essentially about accessing data that has been lost, damaged or rendered inaccessible, computer forensics is also about examining current data and eliciting key information about that data. In essence computer forensic technology analyses not only lost or damaged data, but also existing data in an effort to establish certain facts that may prove or disprove an event or action.

The majority of today's computer forensic technology has been influenced directly by the experiences of criminal investigations. Indeed, many of today's computer forensic software

Computer forensics, as a discipline, draws upon a multitude of technologies from other disciplines, bringing them together to form a complete solution.

and hardware developers have links, either directly or indirectly with law enforcement. Not surprisingly the majority of today's computer forensic research and development activity is being undertaken either directly by, or in conjunction with, law enforcement.

Computer forensics, as a discipline, draws upon a multitude of technologies from other disciplines, bringing them together to form a complete solution. As highlighted previously, data recovery provides one valuable source of such technology. Other important areas that contribute to the development of computer forensic technology include data communications, electronics, cryptography, and software engineering.

For a more thorough examination of the benefits of computer forensic technology, I refer the reader to the case studies at the end of this paper.

7 Sources of electronic evidence

As has been stated previously, computer forensics is about evidence. Let us now examine where and how electronic evidence may be stored. Electronic evidence can occur in many different forms. Whether it is a word-processed file, or a fragment of data belonging to some previous file, the search for electronic evidence can involve varying degrees of technical complexity. Despite the methodology and technology used, electronic evidence can be located on a computer system in a number of different forms. Essentially data that may afford evidence of an act or event can be found either locally on the computer being examined, or remotely on another computer

system for which the local computer has remotely connected.

7.1 Local source of electronic evidence

Data that is stored on the internal hard drive of a computer can be regarded as being stored locally. This class of data by itself does not tell the computer forensic specialist anything special about the purpose of the data itself, but rather only raises issues of locality and access. What is perhaps more critical is the manner in which the data appears on the hard drive, and in what context it is stored. Merely locating a key sentence does not of itself imply that the computer contains critical evidence. It is the context in which the data is stored combined with the circumstances that will determine the worth of any such find. To this end it is critical that the computer forensic specialist be able to properly identify in what context the data is stored on the computer system. Essentially data can be stored in one of three key forms:

- **Current files**

Current files comprise all files residing on a computer system for which the user can readily identify and for which key attributes are readily determined (eg: creation time and date, modification date, access date). Essentially these are files and directories for which the user can see by means of a simple listing. Current files can take one of two forms, permanent files or temporary files. Permanent files comprise those files that reside on the hard drive permanently, and for which they can only be removed through the direct intervention of a user or program.



Documents, spreadsheets, program files, and graphics files are all examples of permanent files. Temporary files consist of those files that are created by a program or operating system, and reside on the hard drive for as long as the program or operating system requires them. Printer spool files, virtual memory, and rubbish bin files are all examples of temporary files.

- **Deleted files**

Deleted files consist of current files that have been deleted from the hard drive. Deleted files by their nature will retain many of the key attributes associated with them prior to their deletion, however reference to the file and its data is no longer possible due to the removal of key indexing information by the deletion process. Recovering data from deleted files is still an excellent means of locating electronic evidence, as much of the key attribute data associated with the file is still intact.

- **Residue data**

Data belonging to files that have been deleted and for which no logical association can be made to a file name or key attributes, can be considered residue data. Computers that have been used on a regular basis will accumulate large amounts of residue data. Typically this form of data is fragmented and, given the lack of key attributes, the context in which it was stored makes it difficult to ascertain when it was created and where it was stored.

7.2 Remote sources of electronic evidence

With the advent of networks, and in particular the Internet, data can be stored remotely on other computer systems. For the computer forensic specialist the remote storage of data presents a whole new set of challenges. The first, and most important, challenge is the ability to

For the computer forensic specialist the remote storage of data presents a whole new set of challenges.

identify from a local computer that data has in fact, or could in fact, be stored on a remote system. To achieve this the forensic computer specialist must firstly establish the nature and extent of remote connectivity available to the local machine. Whether it is by way of dial up access through a modem, or by means of a network connection, it is imperative that the computer forensic specialist be able to clearly identify the existence of such connectivity. Once having established the presence of remote connectivity, the computer forensic specialist must determine the location of potential repositories of remote data. Such repositories may either be in the form of 'mapped' network drives or remote Internet servers for which the user has both access to and storage space.

Whilst the identification of remote data may seem a simple process, it does in fact raise a whole range of issues that may impact on the subsequent admissibility of any remotely stored electronic evidence. Issues such as access to, and ownership of, the data, combined with a need to establish and maintain continuity and authenticity can impact on the forensic recovery of such data.

Case study 1 — when standard techniques can't cut it

An Australian company had entered into negotiations with a foreign government seeking a licence to produce and export primary produce from the country

concerned. Initially the negotiations were progressing well, the company had the pre requisite capital backing and production infrastructure to satisfy the governments requirements. As negotiations were drawing to a conclusion the company was informed that a competitor was to be awarded the relevant licence. Legal action was subsequently initiated. During the course of the legal action a laptop computer was retrieved from a company employee, who, it was suspected, had links to the successful competitor. The laptop was brought in for forensic examination in an attempt to establish if a nexus existed between the employee and the competitor, and if so, the extent of that relationship.

A preliminary examination of the word processor and spreadsheet documents on the laptop revealed nothing out of the ordinary. Attention was then turned to the e-mails. An analysis of the emails contained on the laptop again revealed nothing out of the ordinary. Indeed, the e-mails only went to confirm that the employee was meeting his responsibilities. As is normal under these circumstances a profile of activity was carried out on the laptop in an attempt to ascertain the extent and nature the laptops usage. The results indicated that in fact the laptop had been subjected to extensive e-mail and Internet usage. Immediately suspicions were raised, particularly with regard to the number of e-mails recovered from the system. Essentially indications were that there should have been significantly more e-mails than resided on the laptop at the time. Utilising commercially available data recovery software an attempt was made to identify and recover deleted email messages. This however proved fruitless. Finally a new forensic data recovery technique was applied. The results were immediate. Numerous e-mail messages were retrieved. These messages included communications

between the individual and the competitor, as well as detailed instances of corruption by officials of the foreign government.

Whilst standard commercial solutions were unable to lift the veil of secrecy hiding the crucial e-mails, the application of new and powerful forensic software, based on techniques specifically adapted for these situations proved successful. Derived from the knowledge and experience of the worlds leading law enforcement and military computer forensic groups, this new and advanced technology has already proven itself in Australia with regard to criminal prosecutions. In one recent case, standard forensic techniques were only able to identify some 400 child pornographic images on a suspect's computer. After applying the new technology in excess of 100,000 child pornography images were recovered.

Case study 2 — electronic discovery

All too often in civil discovery, the disputing parties focus on hard copy or paper based documents, often neglecting the electronic records and documents from which the paper based ones are derived. Often computer records and documents are placed in the too hard basket and ignored. Fortunately however, computer forensics is able to provide a flexible and thorough solution that can be tailored to the specific legal requirements of discovery. In one particular instance a large plaintiff company was in dispute with a competitor. During the course of this dispute a number of court orders were granted to facilitate the discovery process. As a result of one such order, the court gave permission for all computer records pertaining to the operations of the business to be copied. Utilising basic forensic technology and techniques, as used by Australian law enforcement agencies, the computer systems were

duplicated by non-destructive or intrusive means.

During the subsequent analysis of the data it became apparent that the business concerned operated multiple versions of its electronic books of account. Additionally to make things more difficult these electronic records were secured by means of encryption and passwords. In addition to the books of account, a large number of 'home-made' fictitious invoices were located on the computer, some of which had been deleted. Utilising knowledge of cryptographic schemes and elementary cryptanalysis techniques, the encryption process was determined and the passwords were retrieved. A low-level examination of the duplicated data resulted in a large number of genuine and fictitious invoices to be reproduced.

Ironically during the execution of the court order, very little hard copy documentation was located. Essentially the entire financial operations and history of the business could only be reconstructed from the computer records. Consequently the plaintiff was able to verify their claims and negate the respondents assertions.

Case study 3 — bringing forensic science and computer forensics together

For many years traditional forensic science techniques have been successfully used in detecting fraudulent behaviour. In particular the expertise and technology behind document examination have given investigators a powerful tool in the search for altered or fraudulent documents. Unfortunately with the advent of powerful desktop publishing and document creation programs, such as word processors, it is very easy for an individual to fraudulently create or reproduce a false document. Some would argue

that such capabilities make traditional document examination techniques ineffective in an electronic world. The reality however can be quite the reverse.

In a recent investigation a company suspected that a hard copy of a contract document had been fraudulently altered by one of their employees, in favour of the other named party. As the signed hard copy of the contract was the primary document, and subsequently in dispute, the company became concerned that the copy being tendered as an original was in-fact a fraudulent duplicate. The entire hard copy document was subsequently submitted to a qualified document examiner for expert analysis. Additionally, given that the company originally created the document, the computer being used by the suspected employee was discreetly copied and its content subjected to a forensic examination.

The primary focus of these examinations was to establish if the document was in fact a fraudulent representation, and if the suspicions surrounding the employee could be substantiated. The results of the computer forensic examination revealed a before and after copy of the suspect document. This was located, not in current files, but in residue data retrieved from the computer. These copies clearly showed the document in its original state as well as in its amended state. Further examination of the document properties helped establish when the alterations were made, and to which printer the document was printed from. Not surprisingly the printer used was the only one of its type in the office and was located in the employee's office. Suspicions were further confirmed when the document examination revealed that the page which contained the suspect alterations comprised a different paper type to that of the other pages within the document.

