

Computer Forensics: Implications for Litigation and Dispute Resolution

Written by Emily Virtue
April 2003

INTRODUCTION

Computer forensics is a specialised and fast growing field of investigation. Recent years have seen the expansion of discovery from traditional paper discovery to a search of computer records. This is the result of the increasing use of computer technology combined with the belief that valuable evidence can be found on computers in addition to evidence existing in paper form.¹

This paper seeks to answer the question “What is computer forensics” and to provide a brief overview of the legal issues as well as an outline of situations where the use of computer forensics may be beneficial. This paper will also identify the advantages and disadvantages associated with computer forensics. The paper will conclude with a few case examples which illustrate the application of computer forensics.

WHAT IS COMPUTER FORENSICS?

The term “computer forensics” is associated with a relatively new class of crime. Essentially computer forensics is used to describe the study of computer and storage devices for the purposes of obtaining legal evidence. The key element is that this evidence must be capable of being used in legal proceedings.²

Computer forensics involves the recovery of lost, damaged, hidden or password-protected data from a computer system after the system has crashed or been effected by a virus, or because of accidental, deliberate or

¹ W Mulligan & T Wright, *Recent Developments in the Substantive Law of Electronic Discovery*

² A Reid, *To Catch a Thief In the “Information Age”*, <http://www.asis.org.uk/news>

malicious file corruption or loss.³ As such, computer forensics can be described as the scientific process of preserving, identifying, extracting, documenting and interpreting data held on electronic storage media.⁴

THE COMPUTER FORENSICS PROCESS

Forensic computer examinations are unlike ordinary data recovery efforts. Forensic computer examinations use strict controls and procedures to ensure that all existing data is found, that the original data is preserved unchanged, and that any recovered data is admissible in court or other legal proceedings.

Deleted, disguised, hidden and password protected data can be retrieved in many instances. The forensic examiner is able to recover many forms of data which are not readily accessible. The recovered data would then be carefully documented, catalogued, analysed and recorded in exhibits, and reports would be presented to the client or the courts in compliance with the rules of evidence.⁵

Computer forensic examiners first make exact copies of all hard drives and disks using computer forensics software. The program automatically recovers deleted documents, emails and graphic images and displays them in an easy to read format. Each file's date and timestamp is displayed, making it easier to assemble a timeline related to when the file was created, saved or viewed.⁶

Every computer forensics examiner should employ a set of methods and procedures for all examinations. The examiner should be aware at all times during the investigation of all possible conclusions that their examination may lead to.⁷ This protects the examiner from allegations of bias.

³ Computer Forensics New Zealand Ltd, <http://www.data-recovery.co.nz/>

⁴ Competitive Advantage Solutions, <http://www.casglobal.com/services/cforensics.html>

⁵ Cyberlab Computer Forensics, <http://www.cforensic.com/pages/2cforensics.html>

⁶ US Newswire, *Computers Seized From al Qaeda Chief Should Yield a Mountain of Evidence Says Computer Forensics International*. Los Angeles, 3 March 2003 (<http://www.canberra.edu.au/library/dbases/index.html>)

⁷ F Horton, *Electronic Evidence*, <http://www.sinch.com.au/articles/2000/Fhorton1.htm>

During an investigation, the methodology which computer forensics specialists follow can be summarised as follows:

1. acquiring evidence without altering the original;
2. authenticating that the recovered evidence is the same as the original;
and
3. analysing the data without modification.⁸

THE LEGAL ISSUES

Computers have appeared in the course of litigation for several years. The arrival of computers in commercial disputes and in criminal cases did not create immediate difficulties as judges sought to allow computer-based evidence on the basis that it was not any different from traditional forms of evidence. However, a series of court cases in America questioned the admissibility of computer derived evidence. The main problem was that it was not always possible for a computer forensics expert to separate the legal issues surrounding the evidence from the practical aspects of computer forensics, such as the issues of demonstrating authenticity, reliability and completeness.⁹

The ultimate aim of a forensic investigation is that the evidence can be used in legal proceedings.¹⁰ As such, a computer forensics expert should have a sound knowledge of the law, particularly in the areas of legal jurisdictions, court requirements and the laws on admissible evidence and production.¹¹

Computer evidence must, like any other evidence, be:

- authentic;

⁸ S Sanborn, *Following the Digital Trail: Computer Forensics Experts Uncover Digital Evidence on Policy and Security Breaches*, (<http://www.canberra.edu.au/library/dbases/index.html>)

⁹ P Sommer, *Computer Forensics: An Introduction*, <http://www.virtualcity.co.uk/vcaforens.htm>

¹⁰ Ibid

¹¹ Ibid

- accurate;
- complete;
- convincing; and
- admissible.

In order to satisfy these broad tests for evidence, any computer forensics approach would need to include the following elements:

- well-defined procedures to address the various tasks;
- an anticipation of likely criticism by the other party on the grounds of failure to demonstrate authenticity, reliability, completeness and possible contamination as a result of the forensics investigation;
- the possibility of repeat tests to be carried out, if necessary, by experts hired by the other party; and
- an anticipation of any problems in formal legal tests of admissibility.¹²

However, there will be divergences from the expectations of more traditional areas of forensic investigation. The main reason for this is due to the rate of change in computer technology. For example, the deviser of a test for the presence of a prohibited drug, an explosive, fabric fibres, bodily tissues, etc can expect that over a period of time, the test may be improved or shown to be defective, but the actual need for the test and most of its essential detail will most likely remain unchanged. However, newness and obsolesence is normal in computer technology.¹³

COMPUTER FORENSICS SITUATIONS

Computer forensics can be used in various situations including:

¹² Ibid
¹³ Ibid

- documents - proving the authenticity of a document or demonstrating the forgery of a document.
- computer generated reports from human input. This is the situation where a series of original events or transactions are input by human beings but where after computer processing, a large number of reports can be generated. Examples include the order/sales/inventory applications used by many commercial organisations and retail banking.
- real evidence – machine readable measurements such as the reading of contents of magnetic strips and bar codes.
- electronic transactions - proving that an electronic transaction took place or proving that a presumption that it took place was incorrect. Typical examples include money transfers and ATM transactions.
- event reconstruction – to show a sequence of events or transactions passing through a complex computer system. Typical examples include computer contract disputes (for example, where a computer failed to deliver acceptable levels of service).¹⁴

These situations could result in a number of forms of litigation including:

- civil matters
 - o breach of contract
 - o asset recovery
 - o tort
 - o defamation
 - o employee disputes
 - o copyright and other intellectual property disputes
- criminal matters
 - o theft

¹⁴ Ibid

- o criminal damage
- o criminal offences concerning copyright and intellectual property
- o drugs offences
- o pornography offences

ADVANTAGES AND DISADVANTAGES OF COMPUTER FORENSICS IN LITIGATION AND DISPUTE RESOLUTION

The main advantage of a computer forensics examination comes from an ability to search through a mountain of data very thoroughly and quickly and in any language.¹⁵ This enables legal professionals to produce as evidence data which would otherwise be unable to be produced to the court. The ability to recover data which has been deleted, damaged, hidden or lost is of great advantage to legal professionals involved in litigation.

On the other hand, computer forensics does have some disadvantages.

The most common legal difficulty is having digitally based evidence accepted in court. Data collected for the purposes of evidence must be shown to be untampered with and fully accounted for, from the time of collection to the time of presentation to the court. Therefore, it must meet the relevant evidence laws.¹⁶

As such, computer forensics experts must have a good understanding of the legal requirements as well such as evidence handling, storage and documentation procedures.¹⁷

Another disadvantage is that there are substantial transactional costs associated with electronic discovery.¹⁸ Generally, each party bears its own

¹⁵ above n 6

¹⁶ Ernst & Young, *Computer Forensics*, eRisk Solutions Expert Paper, <http://www.ey.com.au>

¹⁷ above n 7

discovery costs. However, because the costs of producing electronic records can be substantial, it is not always appropriate to follow this rule. In America, legislation gives courts the power to limit the amount of electronic evidence which is to be discovered in order to reduce the costs for the producing party. However, the case law provides little guidance concerning the allocation of costs associated with the discovery of electronic records.¹⁹

In *Sattar v Motorola Inc*²⁰ the court allocated electronic discovery expenses equally among the parties. As such, it is arguable that the high cost of producing and preserving electronic records should result in parties pushing for cost-sharing in the onerous requests.²¹

Another disadvantage associated with computer forensics is that the disclosure of electronic documents presents the potential for inadvertently disclosing privileged documents.²² As a result, it would not be sufficient to rely solely on computer searches to identify any privileged documents. Therefore, it would be necessary to conduct a manual review of all the retrieved documents in order to identify any privileged documents which may be contained among them.

Another disadvantage is that the legal practitioners involved in a case where computer forensics examinations have been conducted must have extensive computer knowledge. This is relevant both to the solicitors and barristers involved as well as the judge or magistrate hearing the case. Without a comprehensive knowledge of computers, it would be extremely difficult for a solicitor to cross-examine a computer forensics expert. Similarly, it is possible that a judge or magistrate would be unable to provide an appropriate ruling without a thorough understanding of computer systems.

¹⁸ above n 1

¹⁹ above n 1

²⁰ 138 F.3d 1164 (7th Cir. 1998)

²¹ above n 1

²² above n 1

CASE EXAMPLES

The importance of utilising computer forensics experts is highlighted by the following decisions.

In one instance of computer forensics, the defendant in *United States v Tucker*²³ was found guilty of possession of child pornography. The conviction was strengthened by computer forensics evidence which was found in deleted internet “cache” files which were saved to the defendant’s hard drive.

A European murder case taken from <http://www.cyber-forensics.ltd.uk/> refers to a young girl who was murdered at a nightclub. The nightclub had a computerised ID system which recorded who had been at the club each night. The software recorded the time when the card was swiped but this information was not stored within the system. However, a computer forensics investigation was able to retrieve this deleted data.

A Hong Kong rape case taken from <http://www.canberra.edu.au/library/dbases/index.html>²⁴ refers to a girl who was involved in regular “chatting” with a man over the internet. After chatting to each other for some time they arranged to meet and the girl was subsequently raped. A computer forensics investigation was carried out on the girl’s computer and the address of the man was ascertained. A further examination of the man’s computer revealed the contents of his conversations with the girl. The man subsequently admitted his guilt.

In Australia, *Sony Computer Entertainment Australia Pty Ltd v Jakopcevic*²⁵ involved the infringement of two trademarks. The respondents were involved in manufacturing and distributing CD-ROMs bearing counterfeits of the Sony Trademarks. When the respondents became aware that they were going to

²³ 150 F.Supp.2d 1263 (D.Utah 2001)

²⁴ Xinhua News Agency, *Computer Crime Faces Computer Forensics*, Hong Kong, 7 October 2002, (<http://www.canberra.edu.au/library/dbases/index.html>)

²⁵ [2001] FCA 1520

be investigated, they deleted many business records from their computer. A computer forensics specialist was able to recover the deleted computer files.

CONCLUSION

With the increased use of computers in society, the necessity of electronic evidence in litigation has increased. Valuable evidence can be found on computers which enables legal professionals to produce evidence which had previously been lost, destroyed, hidden or deleted. While there are disadvantages associated with computer forensics, the advantages are far greater.

Reference List

Articles

Mulligan, W, & Wright, T, *Recent Developments in the Substantive Law of Electronic Discovery* (accessed from the Litigation and Dispute Processing WebCT page)

Reid, A, *To Catch a Thief In the "Information Age"*,
<http://www.asis.org.uk/news> (accessed 10 April 2003)

US Newswire, *Computers Seized From al Qaeda Chief Should Yield a Mountain of Evidence Says Computer Forensics International*, Los Angeles, 3 March 2003 (<http://www.canberra.edu.au/library/dbases/index.html>) (accessed 10 April 2003)

Horton, F, *Electronic Evidence*,
<http://www.sinch.com.au/articles/2000/Fhorton1.htm> (accessed 8 March 2003)

Sanborn, S, *Following the Digital Trail: Computer Forensics Experts Uncover Digital Evidence on Policy and Security Breaches*,
(<http://www.canberra.edu.au/library/dbases/index.html>) (accessed 10 April 2003)

Sommer, P, *Computer Forensics: An Introduction*, <http://www.virtualcity.co.uk/vcaforens.htm> (accessed 8 April 2003)

Ernst & Young, *Computer Forensics*, eRisk Solutions Expert Paper,
<http://www.ey.com.au> (accessed 8 April 2003)

Xinhua News Agency, *Computer Crime Faces Computer Forensics*, Hong Kong, 7 October 2002, (<http://www.canberra.edu.au/library/dbases/index.html>) (accessed 10 April 2003)

Web Pages

Computer Forensics New Zealand Ltd, <http://www.data-recovery.co.nz/>

Competitive Advantage Solutions,
<http://www.casglobal.com/services/cforensics.html>

Cyberlab Computer Forensics,
<http://www.ccforensic.com/pages/2cforensics.html>

Cases

Sattar v Motorola Inc 138 F.3d 1164 (7th Cir. 1998)

United States v Tucker 150 F.Supp.2d 1263 (D.Utah 2001)

Sony Computer Entertainment Australia Pty Ltd v Jakopcevic [2001] FCA
1520