Computer forensics - bringing back the deleted

Rodney McKemmish

Imagine someone sitting down at your work or home computer and slowly piecing together where on the Internet you have been surfing, what documents you have created and deleted, and with whom you have been communicating. Welcome to the world of computer forensics. Just as forensic scientists are able to reconstruct the events of a crime scene, so to the computer forensic expert is able to reconstruct what a person has been doing on a computer. Computer forensics has been described as the process of "identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable." In simple terms, computer forensics seeks to reconstruct past events by examining the relationship between the computer and the person(s) who have used it.

So how is it that a computer forensic expert is able to peel back the binary layers to build a picture of past activity.

The answer is a simple mix of technical knowledge, and how operating systems behave. Knowing how a computer behaves under differing circumstances, and knowing where to look, allows the computer forensic expert to zoom in on the electronic trail with relative ease. By way of example, let us consider what happens when a person creates a suspect document using Microsoft Word on a Windows computer, and then later deletes the document to avoid their actions being detected. When a document is first created Microsoft Word also creates a temporary instance of the document. This temporary instance is, in most cases, a near identical copy of the original document. The temporary copy of the document is usually deleted when the original file is saved and closed. However, as will be explained shortly, this temporary instance can itself be brought back to life. Sometimes, however, the temporary instance of the file is not deleted, thereby leaving a trace of the original or source document, even after it is long gone.

When the source document is placed in the Windows recycle bin, and the recycle bin emptied, further traces of the source document are created. The act of placing the file in the Windows recycle bin results in a further copy of the file being created within the recycle bin folder. And when the recycle bin is emptied, the copy of the file is deleted. At this point we have three possible instances of the one document leaving a trace on the computer; the original file, the temporary file and the rubbish bin copy.

Even after all of this, how is it that we can still bring back to life the source document? The answer resides in the way data is stored on the computer. When a file is created, the file name and its associated properties (i.e. creation date, modification date, last access date and location) are recorded in a large index table maintained by the operating system. The index table points to one or more areas on the internal hard drive that contains the body of the file. When a file is first created or copied onto a computer, the operating system uses the index table to identify areas of the hard drive that are free for use. Once sufficient space has been identified, the operating system stores the file in the free space, and updates the index table accordingly.

When a file is deleted, all that happens is that the file storage information in the index table is cleared. Consequently, the operating system sees the area occupied by the file as being free for use. Despite this, however, the original file data remains in

Continued page 8

Courts and technology...cont.

A less obvious technological development in the Supreme Court has been a major revision of the security system operating in Darwin. The CCTV cameras have all been replaced with more modern equipment, and the number of cameras has been doubled.

The courts are striving to keep up with technological developments, and to ensure that we maintain pace with such developments both within the profession, and in other courts around Australia. To this end the court established the Court and Technological Strategy Committee (CATS) some years ago. The committee welcomes suggestions from the profession and from the public as to how we may improve services. Such suggestions can be directed to the Director of the Supreme Court, Chris Cox, or to myself.

of this behaviour that the computer forensic expert is able to search for evidence of the original file in the areas of the hard drive marked as being free for storage. Making the chances of recovery even more likely, is the fact that not one, but at least three instances of the same file may exist on the same hard drive. This explains why the computer forensic expert is often able to bring back from the deleted seemingly lost data.

In terms of criminal investigations, civil litigation and electronic discovery, the ability to recover deleted data has shown its worth time and again. However, recovering data is only half the story. For it is not uncommon for the authenticity of a computer file to be challenged. Particularly when there is a question over when, or where the original file was first created. It is at this point that the computer forensic expert begins to apply their knowledge of operating system behaviours to better understand whether the file that has been recovered is, in fact, an originating document. In part, this process is made a little easier by the existence of the temporary copy and the copy recovered from the recycle bin. By examining the various file properties, such as dates and times, for each instance of the file, the forensic computer expert is able to compare the observable sequence of events with that expected for a file that has been created in the ordinary course of user activity. Any variance immediately gives rise for suspicion. And when such suspicion arises, the forensic computer expert interprets the observed behaviours and extrapolates out the most probable sequence of events.

So what does all of this mean? In terms of electronic evidence, the days of merely identifying a file on a computer are long gone. Computer forensics have evolved to such an extent that reconstructing the electronic trail has become more of a science rather than a simple process of finding hidden or missing data. The ability to apply reconstructive techniques, such as that highlighted above, can add significant evidentiary advantage to matters where the authenticity or reliability of electronic data is under suspicion. Other types of reconstructive forensic techniques that can be applied, include:

- Rebuilding past Internet surfing activity.
- Identifying past instances of external storage devices, such as memory sticks, being connected to a computer.
- Reconstructing the copying of data onto an external storage device.
- Differentiating human initiated Internet activity from virus initiated activity.
- Reconstructing unauthorised access to computer systems and/or computer data.

Given these techniques, it is not surprising to find matters involving allegations of theft of intellectual property, inappropriate employee behaviour, unfair dismissal, falsification of documents and emails, as being areas where reconstructive techniques have been successfully employed. Indeed, with recent advances in computer forensics, there is now a growing demand for such techniques to be used when assessing the reliability or authenticity of suspicious electronic evidence.

About the Author

Rod is the Head of e.Forensics for <e.law> Australia. Prior to joining <e.law> in March of 2006, Rod was the practice leader of KPMGs Forensic Technology team for 6.5 years and a computer forensic specialist in law enforcement for 8.5 years. Rod has extensive experience in providing expert evidence in relation to Computer Forensic and IT issues in both criminal and civil matters. Intellectual property disputes, electronic discovery, employment law, trade practices, and criminal prosecutions are areas where Rod has provided expert reports and opinion. A casual lecturer at the Queensland University of Technology, and regular guest lecturer at the University of New South Wales, Rod is also co-author of the book, Computer and Intrusion Forensics, published by Artec House.