Emerging Problems in Digital Evidence

Peter Sommer explains that computer forensics face the challenge of developing as quickly as new technology.

Evidence from computers has been used in legal proceedings as long as computers have been in service. Mostly, this appears to be a success story: many sorts of crimes, not just those with an obvious 'cyber' label, that have somehow during their commission left traces in digital form are routinely successfully prosecuted. Technicians and law enforcement officers have developed techniques and protocols for the preservation, analysis and presentation of certain forms of digital evidence. 'Computer forensics' has become an established set of disciplines. A community of vendors and consultants provide specialist products and services, sometimes of remarkable quality.

But closer examination shows that these achievements are limited to a relatively small subset of digital evidence – disk and network forensics. Disk forensics consists of making an exact copy of a hard-disk – 'forensic imaging' – and then analyzing it to the point where all manner of apparently hidden and deleted material is made manifest and where it is possible to produce detailed reconstructions of past activity. Network forensics is about reliably capturing activity on a network, matching it against what might be found on various individual computers and as a result being able to reconstruct activities and actions. In truth, however, it should really be called TCP/IP forensics as the techniques and tools are really only developed for that particular networking protocol.

There are many other forms of digital evidence which are routinely considered where high standards comparable to disk forensics simply don't exist but which law enforcement officers and prosecutors would nevertheless like the courts to accept.

These two subsets are undoubtedly highly important in terms of prevalence but we are now at an interesting point. There are many other forms of digital evidence which are routinely considered where high standards comparable to disk forensics simply don't exist but which law enforcement officers and prosecutors would nevertheless like the courts to accept.

The history of digital evidence tracks the history of computers, both as technological artefacts and as the locations of business, social and cultural activity. The earliest form of evidence from computers was print-out from large monolithic machines. There were two problems, eventually overcome by legal reform: admissibility and reliability.

It was in the early 1980s that matters really changed. IBM produced its first PC. Whereas it was impossible to visualize anyone seizing a whole mainframe or mini computer, a PC can be easily carried away. By the end of the 1980s the first products to make reliable complete copies of hard-disks were available (SafeBack in the US, DIBS in the UK); current software can carry out highly sophisticated analyses. It is possible to point to decisions in the Court of Appeal about the operation of our criminal law of 'making' photographs of the sexual abuse of children which were only possible because of the existence of reliable disk forensics (Sommer, 2002).

But the history of computing did not end with the creation of the stand-alone personal computer. PCs are now linked together via office-based Local Area Networks which in turn often feature central server computers. Since the mid-1990s we have the 'retail' internet to which individual domestic PCs can easily connect. Many technical and social institutions have grown up in just a few years – the world wide web, web-based ecommerce, streaming video, internet relay chat, peer-to-peer (P2P) file sharing. PCs have got cheaper and in particular the costs of data storage in the form of hard-disks has been for some time falling at a rate approaching 5% per month. PC operating systems and the applications to go with them become ever more sophisticated. The costs of solid state memory is dropping rapidly, giving rise to cameras, PDAs, media players and other devices with substantial power and the ability to store considerable amounts of data.

Let's start with large complex computers and networks. Should we not now be expecting the system to be 'imaged' in the way we do for single hard-disks so that defence experts are able to run as many verification tests as they wish? Do we have to make a forensic copy of the entire global network of a large global clearing bank and all its subsidiaries just of a suspected minor fraud in one branch? If you don't make such a copy — how much evidence should you provide? There are no easy answers.

What about internet activity? An individual internet-connected PC will contain a whole mass of information about the user's activities – applications, data files, configuration files, logs, material in the browser cache, and so on. That may be enough to convict someone once they have been identified. At an informal level there are plenty of ways of monitoring other peoples' activities live on the internet through various forms of eavesdropping. But often law enforcement will have to obtain warrants before they can legally do so – and how do we trust law enforcement's log files?

What about capturing information from a remote web-page? Possible reasons include suspicions of fraud, incitement, distribution of illegal material. At first sight this seems to be trivial; you call the page up via your web-browser and either 'save'or 'print'. Think again: what you see on your browser screen may have come from your internet service provider's cache, not from the suspect remote web-site. Again, many web-pages are dynamically created – they don't exist on the remote site but are created on the fly in response to a particular demand.

Computer-related cases are getting very big and complex, particularly where conspiracy is alleged. Large numbers of large computers may be seized – how long will the police investigation last? How do you 'serve' evidence on the court and defence? There are currently no protocols for this.

There is also a problem of expertise and its availability. Forensic science relies on testing and verification. The problem for those operating with information technology is the rate of change – DNA doesn't change, but computer hardware, operating systems, application programs do - dramatically over periods as short as five years. This is at odds with the normal timetables of academic peer-reviewed articles. Are we to hold back using a new investigatory technique until it has been properly tested – and give criminals a free ride in the meantime? Or do we offer to the courts our untested tools and run the risk that innocent people may be convicted?

Many cybercrimes are international in nature and the problems of international co-operation are acute. We now have the *Convention on Cybercrime*, issued in the name of the Council of Europe but also strongly supported by the United States and Japan. This aims to provide harmonized definitions of various computer-related crimes, so that mutual co-operation and extradition can be expedited. Most jurisdictions require some equivalence between their own laws and that of the country requesting assistance before they will grant it. The treaty also extends towards issues involving evidence, both in terms of warranting methods and actual procedures. So far so good. In the field of internet-based child pornography, co-operation has been very good, for example in Operations Cathedral and Avalanche (known in the UK as Ore). Elsewhere matters have been more difficult as individual nations have become concerned about sovereignty issues. There is a so-far little understood problem: the treaty in its current form does not appear to address problems of disclosure to the defence. In most countries defence lawyers are entitled to see all the evidence against their client. In the United Kingdom the prosecution is under a constant duty to disclose to the jury anything which might undermine the prosecution case; after receiving a defence case statement, the prosecution also has, under the *Criminal Procedures and Investigations Act, 1966*, to consider what might reasonably assist the defence. But what happens if that evidence was collected by an overseas law enforcement agency who feels that their obligations cease at their own borders? Expect some interesting test cases in the next few years.

Finally, there's a problem of careers and rewards in law enforcement. The computer forensics pioneers have had to remain at low ranks, because police promotion is often about management ability not investigatory skill. As a result, far too many specialised experienced officers are leaving for lucrative private sector jobs. ■

***Peter Sommer** is Senior Research Fellow at the Information Systems Integrity Group, London School of Economics.*

References

Convention on Cybercrime, Council of Europe, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Criminal Procedures and Investigations Act, 1966, plus Codes of Practice and Attorney-General's Guidelines, http://www.lslo.gov.uk/pdf/guide lines.pdf

Sommer, P. (2002) 'Evidence in Internet Paedophilia Cases'. *Computer and Telecommunications Law Review*, 8(7): 176-184.