

# Forensic Computing

---

In 1965 Gordon Moore wrote in Electronics Magazine<sup>1</sup> his theory on the potential for computational evolution - 'increasing at a factored rate of double per year'.

Whilst his law has since been tempered based on actual industry development life-cycles, his prophetic statement still holds largely true and today there is almost no walk of life or industry where computers and information networks have not become deeply integrated — and criminals have moved in step with technical advances, discovering ways in which to leverage IT to facilitate the commissioning of offences. In many instances this is old, or conventional crime, perpetrated using new approaches that are reliant on technology. Postal fraud, for instance, has evolved to employ electronic communication channels, giving rise to waves of emails seeking to defraud recipients with promises of money and fictitious prizes (commonly known as '419 scams' as many of such notes tend to originate from the African continent and 419 is their penal code for wire fraud).

Studies into the cost of cyber-crime, commissioned independently by the Department of Trade and Industry (DTI)<sup>2</sup>, reveal alarming trends in the abuse and misuse of technology. The average cost per security incident has risen to over £160,000 and nearly one in four businesses in the UK have suffered a serious hacker attack or virus outbreak. The impact of an information security breach can be so devastating to business operations that one in ten never actually recover and the shutters close permanently. To counter this growing threat, security and law enforcement agencies have adopted fresh approaches for dealing with high technology crime.

Forensic Computing is a relatively young science when compared to contact forensics such as fingerprint recognition which have roots that can be traced back to Edmond Locard<sup>3</sup>, who in the early 1900s famously postulated the theory of evidence being left as 'mutual exchanges of contact'. Whilst various descriptions exist in relation to this practice, the international survey undertaken by Hannen et al., has been taken as the de-facto definition: 'Processes or procedures involving monitoring, collection, analysis... as part of 'a priori' or 'postmortem' investigations of computer misuse'. It is important to appreciate that this definition takes a wider view than the conventional reactive description, where forensics was regarded purely as an incident response function. Hannen et al. consider digital forensics as also taking a pro-active role in security, where it can be combined with intelligence and operational planning.

As a serious field of research, forensic computing studies only started to take real form in the early 1990s when, faced with ever increasing numbers of computers being seized at crime scenes and the potential for crucial evidence to be stored on a PC, various government agencies came together to host the International Conference on Computer Evidence (ICCE). Here many of the challenges facing law enforcement communities were aired and agreements forged to cooperate towards finding effective solutions.

---

<sup>1</sup> 'Cramming more components onto Integrated Circuits', Electronics Magazine, 19 April 1965.

<sup>2</sup> DTI Information Security Breaches Survey 2006: see [www.security-survey.gov.uk](http://www.security-survey.gov.uk)

<sup>3</sup> Dr Edmond Locard, Father of Modern Ridgeology: see [www.latent-prints.com/Locard.htm](http://www.latent-prints.com/Locard.htm)

Two years later, in 1995, the International Organisation for Computer Evidence (IOCE)<sup>4</sup> was formed, and a further two years later the member states that comprise the G8 subscribed to the mission of IOCE, pledging support for the organisation. This was the catalyst required to stimulate research and development, and since then great advances have been made in all spheres of digital evidence management.

When working on a matter where the case will rise or fall on the strength of digital evidence, for example where an allegation of possession of indecent images has been made, it is important to commission an independent forensic examination of all evidence and digital materials. This places the evidence into the wider context of the offence and enables barristers to make directions to the court based on a fuller appreciation of matter.

Assuming material has been seized by the authorities, the state will usually conduct their own forensic assessments (typically undertaken by the regional police hi-tech crime unit<sup>5</sup>), the results of which will be provided to legal representations. The mechanics of this process involve the 'imaging' of the 'target media' - the process of making a forensically sound duplication of digital materials of interest (e.g. the computer hard drive). During this duplication process a 'write-blocking' device will be employed to ensure the target media is not affected or corrupted in any capacity whilst its content is read and mirrored. The actual forensic analysis is then made upon the duplicated material, with the original placed into secure storage and maintained in the state in which it was seized. The forensic analyst will then peruse the imaged copy to identify materials of potential evidence value, extracting copies as necessary to form the basis of the expert report.

Looking at this from a defence perspective, a number of questions should be posed in relation to the digital evidence (based on the Daubert threshold test that evaluates the competency of evidence):

- whether the theories and techniques employed by the scientific expert have been tested;
- whether they have been subjected to peer review and publication;
- whether the techniques employed by the expert have a known error rate;
- whether they are subject to standards governing their application;
- and whether the theories and techniques employed by the expert enjoy widespread acceptance.

Sam Patel, Head of Incident Response at AFENTIS, speaking at a recent legal seminar at the Liverpool Anglican Cathedral said: 'As the threat landscape has changed, so too have the countermeasures with specialists developing tools to aid in the recovery of sensitive data and to successfully isolate it so as to ensure it can be made admissible in a court of law.'

Putting abuses of technology on a statutory footing, Britain has a suite of legislation that can be invoked, from the Computer Misuse Act 1990<sup>6</sup> to the Regulation of Investigatory Powers Act 2000<sup>7</sup>.

<sup>4</sup> International Organisation on Computer Evidence (IOCE): Ref. [www.ioce.org](http://www.ioce.org)

<sup>5</sup> National Hi-Tech Crime Unit (NHTCU): Ref. [www.nhtcu.org](http://www.nhtcu.org)

<sup>6</sup> Computer Misuse Act 1990: Ref. [www.opsi.gov.uk/acts/acts1990/Ukpga\\_19900018\\_en\\_1.htm](http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm)

<sup>7</sup> Regulation of Investigatory Power Act 2000: Ref. [www.opsi.gov.uk/acts/acts2000/20000023.htm](http://www.opsi.gov.uk/acts/acts2000/20000023.htm)

Today digital forensics is an accepted science, and evidence duly secured in relation to best practices (in the UK these guidelines are outlined by the Association of Chief Police Officers) can be served in a court of law. Digital forensics are providing breakthroughs in all manner of high profile cases around the world, helping security and law enforcement agencies to catch offenders and secure convictions.

In the US, for example, the notorious BTK serial killer that had a reign of terror lasting over twenty five years in the Wichita areas, was ultimately tracked down after he sent a disk to a local radio station gloating at the police's inability to catch him. Unique digital footprints embedded within the files were extracted by forensic specialists, and like a lone fingerprint, investigators now had a powerful lead - all they needed was to match the file to the computer that had created it (much like having a fingerprint but not a suspect's hand to match it with). Wichita Police then conducted a house to house search, taking file samples from every computer encountered. Back in the laboratory, the file footprints were compared to the sample disk posted by the BTK killer, eventually finding a match. This tied the floppy disk to Dennis Radar's PC, a virtual smoking gun as far the prosecution were concerned. This digital evidence became a pivotal element of the State's case and ultimately helped secure a conviction.

In the UK the 2002 murders of Holly Wells and Jessica Chapman in Soham, Cambridgeshire, also saw digital forensics play a crucial, but largely unknown, role in the investigation. Technical analysts examined one of the girl's mobile phone to identify where it was located when it had been turned off. Information on the nearest network communication tower tends to be stored in a phone's memory and when the signal coverage of that tower is plotted, it is possible to identify the rough area (typically a few square kilometres) in which the phone was located when it was switched off. Having extracted this information from the handset, authorities had a rough idea of where to base their search; which ultimately led to the recovery of the two girl's bodies.

Speaking in an interview several years after his pioneering research on the Manhattan Project<sup>8</sup> where atomic reaction theory was developed, scientific visionary Oppenheimer explained that 'the scientist is free to ask any question, to doubt any assertion, to seek for any evidence'. This thinking holds especially true when applied to the discipline of forensic computing in a legal context. Here experts may be instructed by either the prosecution or the defence, however, in either instance, they have a higher duty to the court. They are instructed as experts, but experts for the truth. It is important therefore to ensure that the experts instructed are duly qualified, experienced and independent.

Commenting on the nature of digital evidence, Mandip Kumar, Partner at Russell Jones & Walker Solicitors, explained how the fragile nature of digital evidence can pose serious challenges to the investigator: 'digital material is extremely volatile - perhaps more delicate than its physical counterparts. It can be copied, amended, and transferred without almost any trace - only experienced and qualified specialists should be employed to work in a digital forensic environment if the subsequent findings are to withstand the scrutiny of a court of law'. When working on a matter where the case will rise or fall on the strength of the digital evidence, perhaps where an allegation of possession of indecent images has

---

<sup>8</sup> Manhattan Project: Ref. [www.atomicmuseum.com/tour/manhattanproject.cfm](http://www.atomicmuseum.com/tour/manhattanproject.cfm)

## Digital Evidence for Case Preparations

been made, it is important to commission an independent forensic examination of all evidence and digital materials.

Forensic computing and the securing of digital evidence is a powerful tool in today's fight against increasingly technically-savvy criminals. It is a discipline that continues to evolve and should remain high on the radar for both legal practitioners and law enforcement authorities.

AFENTIS FORENSICS - Expert analysis of mobile telephones, computer systems and all aspects of electronic evidence. AFENTIS runs frequent briefings across the UK on the changing face of technology and IT-related legislation. Find out more: [www.afentis.com](http://www.afentis.com) or contact Joanne Davies via email: [jdavies@afentis.com](mailto:jdavies@afentis.com)