

Digital detectives

Digital forensics can be defined as the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law. It has evolved over the past ten years to become one of the primary methods of evidence in cases as wide ranging as murder and fraud.

When digital forensics comes to mind, most people will immediately associate the term with crimes which involve the use of computers, for example, the distribution of pornography or an online phishing scam. However, computers and mobile phones are often called upon to provide supporting evidence in cases which may previously have relied on other types of evidence such as eyewitness testimony.

Digital forensics can be split into two main areas; computer forensics and mobile phone forensics, with other devices such as PDAs, MP3 players and SatNav systems being subject to specialist analysis depending on their function and capacity.

Computer Evidence

Computer forensics can be used in a number of ways. It may be that a full analysis needs to take place, with the analyst producing a report on all aspects of the computer system including documents, emails and internet history. However, in some cases the analyst will be working to a very specific brief. For example, they will be asked to search for a particular keyword, website address or date and report back on their findings. This 'preview' investigation may then lead to a full analysis. A legal professional may also employ a digital forensics expert to examine a report which has been presented by the prosecution in order to get a technical perspective.

All reputable digital forensics laboratories will work within the guidelines set by the Association of Chief Police Officers (ACPO). These guidelines help to guarantee

evidential continuity and ensure that any evidence uncovered will be fair and therefore presentable in court.

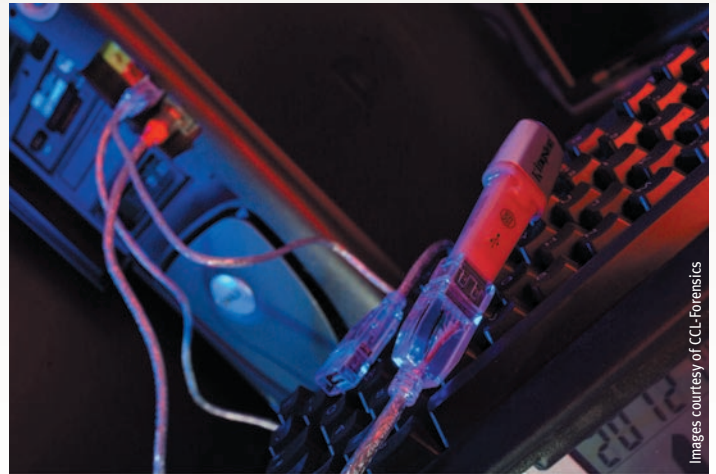
Indecent Images

Often, in defence cases, a forensic examination will take place in response to a report submitted by the prosecution as a result of their own investigations.

For example, the Police were informed by a cleaner working for a large company that she had found printed indecent images in the office of the suspect; hence a Police investigation began, with his PC and laptop being subject to analysis by an in-house team. The suspect had already stated that he had an alibi for a certain period of time as he had lent his laptop to a friend. His defence team therefore commissioned their own investigation of the computer by an independent computer forensics company, focused on the dates surrounding this period. The forensic analyst discovered that the source of the printed pictures found in the office was inside the period that the suspect had an alibi. The analyst also exposed the fact that software had been used to try to erase the images within this timeframe, as string text and partial images were discovered in unallocated space. This evidence was enough for any charges against the employee to be dropped; however another man was subsequently arrested and charged with possession of indecent images.

Mobile Phones

The other device that is frequently



Images courtesy of CCL-Forensics

put forward for digital analysis is the mobile phone. This small gadget can be home to reams of information and can be investigated in a number of different ways. A 'standard' examination will include looking at the handset itself, the SIM card (or both) to retrieve information including call records, text messages, images and videos. This type of investigation would usually aim to uncover who the suspect has been speaking to and when as well as, in the case of text messages, the nature of their conversation.

Another way in which mobile phones can be used as evidence is through the method of cell site analysis. This is the process of identifying, in real time or retrospectively, the location of a mobile phone when it was involved in certain activities, such as making or receiving a call or text message. When a mobile phone is being used, it is directed by the network to the nearest cell site, which has been allocated a reference number and name. By examining records of this information, an analyst is able to pin point a specific area where the suspect phone has been used.

In one recent case, a man was attacked outside a public house; he was seriously injured and his wallet was stolen. The victim had been involved in a long running feud with a neighbour and felt that he was responsible for the attack. Police arrested and questioned the suspect who denied any involvement; however there was sufficient evidence for him to be charged. The suspect's alibi was that he was

visiting his sister at her home over twenty miles away; therefore the police employed the services of an independent expert in order to prove to the court that this was not the case. The expert employed cell site analysis techniques to trace the whereabouts of the suspect's mobile phone at the time of the alleged attack. In this case, the report showed that the suspect had received a phone call in the vicinity of the public house just minutes before the attack took place. This evidence greatly helped the prosecution's case and the suspect was found guilty of GBH and theft.

According to Government National Statistics released in 2006, over 80% of 16-44 year olds using the internet on a regular basis, both at work and in their homes. Similarly, the increase in reliance on mobile phones, not just as communication devices, but as cameras, personal organisers and internet access providers has been a well documented trend. This technology helps keep a record of our lives and is being called upon with increasing frequency when allegations are made against an individual. Therefore it is vital that legal professionals are aware of the potential impact of digital forensic evidence, whether it is being used for or against your case.

■ **Beccy Smith is a communications executive at CCL-Forensics, an independent digital forensics laboratory. Please visit www.ccl-forensics.com for more information.**

