

Modern Forensic Evidence

Digital Forensics is the investigation and analysis of digital media in the interests of determining potential evidence and an invaluable tool in civil and criminal cases conducted by solicitors in the 21st Century

Computer Forensics was initially recognised in the mid 1990's, although the practices were not formally identified at this stage. These early explorations have since been developed by practitioners into a standardised, although by no means simple, process. All laboratories now work within the ACPO (Association of Chief Police Officers) Guidelines relating to computer based evidence. These describe how digital devices or media should be recovered by police officers and subsequently dealt with in the time leading up to analysis.

The forensic process involves taking a number of steps that ensure evidential continuity. For example, an analyst will take a forensic copy or "image" of the media, whether this is a hard drive, floppy disk or DVD to ensure that the data on the original media is not compromised. The analyst will then use the exact copy of the media to undertake their investigations.

A computer analyst will use forensic software to retrieve all information stored on the hard drive or flash drive, deleted or otherwise. It is then their task to work with the legal team and the case notes which they have been given to pull out the relevant information to assist the prosecution or defence with their case.

Digital Forensics has been 'traditionally' used in cases where a computer is required to commit the crime. The downloading of indecent images from the internet or online credit card fraud may be the types of crime that immediately spring to mind. However, it is now common practice for digital forensics to also be used in civil cases, such as theft of intellectual property or employee computer misuse.

Emails are commonly used as evidence as they can give clues surrounding the story of a relationship between two people in chronological order. A forensic analyst can often recover emails that have been deleted and these can be pieced together in order to create a complete account of events.

The other branch of Digital Forensics which has emerged much more recently is mobile phone forensics. There are three ways in which the phone can be used to provide evidence; the SIM card (where a lot of data, including the mobile phone number is stored), the handset itself or from the network provider (such as O2, Vodafone etc.)

Each mobile phone handset is different; therefore a number of different tools are required for the analysis, which can be a complicated process. The SIM card undergoes a similar examination procedure to a computer hard drive with a clone of the SIM being made before analysis takes place. This ensures that the SIM does not communicate with the network when it is activated and therefore that none of the evidence is altered. The information which can be extracted from these two pieces of equipment includes call records, contact lists, text messages, media messages and deleted information.

The network provider is able to provide what is called "cell site" information. This involves details of the location of the mobile phone at the time when a certain event occurs, whether it is a text message being sent or a voicemail message being picked up, providing a clear picture of the whereabouts of the phone (however it cannot give certainty as to who is using the phone at the time). This technology is commonly used to disprove or confirm

whereabouts and can be useful in criminal alibi cases.

It is essential to recognise the differences between the two types of evidence that can be presented. Mobile phone evidence is more familiar to courts and jurors and therefore can often be easier to understand, although it still needs to be presented carefully to have the desired impact. It is usually used as supporting evidence; to confirm or deny a person's movements, conversations and relationships within the context of the case.

Computer evidence is based around solid facts and it could be argued that it is more reliable as stand alone evidence, as there are a number of elements which can be pieced together to tell a more complete story.

Continuing developments in both technology and social behaviour mean that the use of digital forensics by both police and the legal profession can only increase in the coming years. With nearly forty million people in the UK now online and 47 million text messages being sent every hour, digital devices can give a vital insight into an individual's life and contain the key evidence needed to prove a case.



Beccy Smith
T: 01789 261200
bsmith@cd-forensics.com
www.cd-forensics.com