Digital Forensics and Selecting a Digital Forensics Expert Witness

What's the difference between an Expert in Digital Technology and a Digital Forensics Expert?

Technical knowledge is required by both, but that isn't enough to perform successfully in these two very different types of professions. Often service users will select the wrong kind of skill set for a particular task and the recipient, thinking of making money or out of ignorance, will accept the responsibility. This can have disastrous consequences in the long term as an expert in digital technology is not trained sufficiently to work in the legal sphere.

Digital forensics was born in the 1980s as computer forensics with the FBI's magnetic media programme, and the UK quickly followed suit with their own version. Digital Forensics, like all of the forensic sciences, is the application of science in the legal context. The four basics tenets cover four areas:

• Acquisition – a collection of data in a court defensible way in order not to alter the integrity of the storage medium or source memory that will produce a defendable evidential copy by creating a data HASH value which can be verified throughout the forensic process.

• Preservation – evidence, be it a mobile device or a hard disk, must be preserved in a way that it is defensible in court. The process ensures against loss, contamination or deleterious change whether it is accidental or intentional by those with malicious intent.

• Analysis – during the investigation the forensic copy, not the original (except in triage), is to be searched. The search is done using specialist tools so as not to alter the evidence file. Verification of the evidence can be performed at any time by comparing the evidence file against the original HASH created during acquisition. The examiner at this point will determine what is to be searched for and then run recovery and search for those categories of items.

• Presentation – the examiner, must clearly and accurately present their background, tools used, methods of verification, processes used for recovery, the findings and appendices containing the data to support the analysis.

The Sub-disciplines

As computers moved away from being isolated units to being networked and more varieties of digital mediums were invented the term computer forensics changed to digital forensics to encompass an umbrella of branches all dealing with digital evidence. As an ever evolving field the types and names for the sub-disciplines are also continually evolving. Some of the current sub-disciplines are:

• Audio Forensics – the collection, analysis and enhancement of any digital audio files. Poor quality audio can be 'cleaned up', transcribed, enhanced and analysed via spectrometry.

• Digital Camera Forensics – captured images from a digital camera either from an SD card or internal memory. These can be acquired, recovered if deleted and analysed not only for their content but for meta-data such as date/time and even location more recently.

• Digital Video and Photo Forensics – as with Digital Camera Forensics, video and photos can be collected, reviewed and analysed for a case.

• Games Console Forensics – a games console collects data such as logons, and a user may produce accounts which could be used as an alibi or to establish ownership.

• GPS Forensics – GPS in cars, ships and planes can yield information such as recently visited locations, favourite locations and other forensic artefacts which may determine the locations of the vehicle or device.

• Incident Response – is the discipline of network forensics looking at logs, network security, hacking, intrusion detection, breach analysis, Trojan horses and other malware.

• Media Device Forensics – thumb drives, iPods, SD memory card and everything in between can yield useful data or even be used to match up with activity on a computer.

• Mobile/Cell Phone Forensics – phones are ubiquitous in modern culture and not only are they used for calls and texts but also used for emails, messaging, social media, productivity and even hacking.

• Call Detail Record Forensics – Also referred to as Cell Tower Forensics relates to the communication towers that mobile devices utilise while in operation. These records can help to place devices within regions at certain times thus supporting, or refuting an individual's alibi.

• Social Media Forensics – social media both live and from the digital evidence can be harvested and presented for court.

The Expert in Digital Technology

An expert in digital technology, or sometimes referred to as a computer expert, may be someone who has more than a rudimentary knowledge of a computer or high-level corporate system administrator that designs and implements large-scale operations in blue chip environments. They may manage archive systems, maintain mobile devices, configure an enterprise network environment, install video surveillance systems, or any number of highly specialised fields within the digital technology landscape. A computer expert may as well have skills in maintaining, installing and repairing computer systems including data recovery capabilities in case of failure or other data loss events. Regardless of the technical abilities, the area often found lacking is the ability to do so in accordance with the requirements necessary to be qualified in a court of law.

The Digital Forensic Expert

A digital forensic expert, on the other hand, may not always have a system administrator background or indeed a lengthy background in computers. Many police officers start life as a 'bobby on the beat' and are side-lined to retrain as a digital forensic expert. Through additional discipline-specific training the technology background and associated credentials are received. The critical difference between the two professions is knowledge about the facts surrounding the data, not just the recovery of the data, evidence handling, investigation of the event and working towards presenting the findings within the law in an admissible manner.

Digital Forensic Expert versus Expert in Digital Technology

Many people and professionals may have skills which enable them to operate at a level above the layperson. In fact, they may be a highly trained specialist within their area of technological expertise. This, however, doesn't necessarily qualify them to be an expert in the eyes of the court. This can also happen if an expert, in a sub-domain of Digital Forensics, branches outside of their area of expertise.

For example, a mobile phone forensic specialist may not have the ability to perform audio forensic analysis. As a result, this may expose the individual as well as the instructing law firm to litigation due to bad processes. It is typically seen in the industry that a corporation or a law firm employ a computer expert to carry out tasks as their rates are often cheaper than that of a digital forensic individual or organisation. The relative cost of hiring a forensic expert over a general expert in a case that can mushroom to multi-million pounds is minuscule. The difference between winning and losing a claim is more than just whether the instructed person can interpret the results. They also need to develop the proper chain of custody, understand and explain the tools used, offer the repeatability of results through the application of the scientific process, and have credibility in court through their ongoing training and certifications in the field.

For example, a novice may be able to run a tool they found on the web and conclude, because an item was recovered, that an individual is responsible. A forensic expert can contemplate all the minor nuances to rule out or include them in their conclusion. Asking and answering questions while reviewing the evidence such as: Was the computer hacked? Who else had access? How many user accounts were administered on the system? Did the item arrive on the device because on an autonomous action such as a virus? Due to the volatility of digital evidence a digital forensic expert should be involved as soon as it is recognised that digital evidence is to be part of the case.

Comparison Scenario

An excellent example is if you had a client accused of deleting data after a litigation hold has been placed,

and file destruction software has been discovered then eliminated by the suspect. The laptop is given to a computer expert within the company with good intentions but no training in forensics to perform the examination. The individual installs commercial file recovery software to the disk and recovers deleted files. When the report is produced it states that the computer had wiping software installed however the files couldn't be opened. This was due to the software that was installed by the examiner overwriting the unallocated areas of the hard disk where the previously recoverable data resided. Additionally, during the seizure and examination, the examiner operates the machine, making more changes and leaves the device on the network, exposing it to the internet. This allowed the suspect to enter the device remotely through the network using a remote access software and wipe the entire disk. The neophyte examiner has no explanation of when, or if, wiping software existed. All that is left during trial is the examiner's word for the wrongdoing as the original evidence hasn't been preserved.

In the same case using a forensically trained computer forensic examiner, the laptop was taken off the network. The laptop hard disk was removed and placed into a write blocked copying device in order to preserve the data on the disk. One original copy and one working copy of the disk was made to two separate encrypted drives for security and redundancy. The examination takes place on the working copy of the data. The expert is able to determine that ccleaner was installed on the system in the past and deleted. The item is able to be identified as a cleaning software, and logs indicate its use. 'Zeroed out' areas of the disk are identified and are seen as typical, not of regular use, but of wiping of the free space. The client list, which was pertinent to the matter, was discovered downloaded, and although deleted it was present in the restore files when an inadvertent backup was made of the system. Using the filename of the client list, the working copy was keyword searched, and it was discovered that the document was emailed out to their Gmail webmail account. The expert can now form the opinion based on forensic evidence that the data signifies intent to hide actions and steal company data using a personal email address. The original disk was preserved and secured as were the forensic copies along with all developed work product throughout the process.

Differences

Both a technology expert and digital forensic expert may be able to recover data, but only the digital forensic expert would be able to produce a chain of custody, know how to handle the evidence and provide a resume outlining their experience and training in the specific field of digital legal interpretation in court. Technology experts do not have the need to understand the granular digital artefacts unwittingly produced by the system and a user during the operation of a device. They are trained in service, maintenance of a system or specific software function such as usage of QuickBooks for company accounts or Microsoft Office 365 for business applications.

Side-by-Side Comparison	
Digital Forensics Expert	**Technology Expert**
The ability to copy data in a forensically sound manner	Ability to install and set up computers, software, network in a secure manner and maintain operation of the item
Data recovery from the deleted areas of a disk, SQL databases, file slack, backups & other areas	Restoration of data following a disaster from backups
Understand that the workings of digital threats such as trojans, backdoors, viruses and malware have on the original system	Removal of harmful malware from infected computers, not the effect or explanation of such programs
Interpretation of left behind software after removal by a lay user by looking at deleted items and other artefacts	Troubleshooting and repairing computer problems
recovery and interpretation of internet and web-connected apps & the ability to export these so as to report on them	Software initiation and roll out for the client or employer
Granular level knowledge of operating systems especially Windows, Mac OS & Linux so as to be able to examine recorded artefacts & understand how changes made are recorded in the OS	Network setup in order for access to a server and/or the internet
Competent in the usage of a variety of different formats such as Expert Witness, DD Images and AD Logical Container Images for verification and production of a robust chain of custody.	The ability to work with conventional file systems relating to Windows, Mac and Linux
Competency in producing forensic images of entire digital media for the use of analysis	Can make backups using Clonezilla or similar including files directories but not usually deleted data as well. The purpose is for recovery of lost office items and the continuation of the business

Legal Expertise	
Digital Forensic Expert	**Technology Expert**
Ability to verify evidence and individual files	None
Production and maintenance of the chain of custody	None
Can manage eDiscovery projects and warrants	Only basic knowledge
Trial preparation skills	Not likely
Ability to testify in court	Can be used to testify but not as strong as a forensic expert
Sticks to guidelines required in handling digital evidence	Unlikely

Selecting an Expert

There is no international, or indeed a national body, that accredits a digital forensic examiner. In fact, because of the lack of knowledge of judges and legal professionals anyone with computer knowledge can call themselves an 'expert'. It is common for someone to call themselves an examiner despite his or her lack of abilities. Additionally, an examiner may be proficient in one or two domains of Digital Forensics but not others, such as at cell site analysis but not mobile phone acquisition and forensics. It is essential to look for relevant skills to that particular discipline prior to instruction of an expert. When instructing look for forensic specific training and certification in the field. Common certifications are ACE (Access Data Certified Examiner), CCE (Certified Computer Examiner), CFIP (Certified Forensic Investigations Practitioner), EnCE (Encase Certified Examiner) and X-Pert (X-ways Forensics Certified Examiner) to name a few.

If differing types of devices have been seized in a case, then it may be necessary to select experts according to the evidence that is available. If you have a mobile phone, a laptop and call detail records from the network it may be advisable to source a computer forensic expert, a mobile phone forensic expert and a cell site analyst all separately, if an individual doesn't exist with all those skills.

A service user must establish before hiring an individual:

• Do they have training, experience and certifications in the field?

• Does the examiner have experience in the type of case?

• What is the cost of the process?

Cost and scope are also something that the Digital Forensic Expert should be able to provide you with. While it isn't possible to be exact in the level of effort a matter will take, there should be some estimates that can be provided based on their experience with similar matters. As an example, legally aided work is capped at £74.00 an hour in the UK, elsewhere it may vary. In the private sector, costs can range from £150.00-£400.00 an hour (or even higher) dependant on experience. If the matter includes services such as analysis of one laptop including copying, data recovery, and search and reporting, then a ballpark figure of 10-20 hours would be a typical response. Mobile devices, cell tower data, in-vehicle systems, network access, and all of the rest will have their own cost and scope based on the expertise required and the level of effort necessary to perform the work. All of these factors should be discussed with the potential expert prior to any instruction or the expert gaining access to the evidence.

The Expert Report

The culmination of the entire process is typically delivered via an expert report. The expert report should include but is not limited to: a cover page, table of contents, introduction, case outline, qualifications of the expert witness, evidence verification results, use of appendices, separation of facts from opinion and have the judicious use of appendices. The content must be presented in plain English and have various terminology explained correctly. Dependant on the case in the UK the report must comply with Civil Proceedings (CPR), Criminal Proceedings (CrPR) or Family Proceedings (FPR) in terms of the expert declaration signed by the examiner appended to the report.

Regardless of the analysis performed thus far, if the expert is unable to present the findings in a factual, but compelling, way that outlines how their expert opinion indeed is the most likely scenario based on the evidence provided, then the exercise will have been for nought. Following the report, the expert may also be required to provide testimony directly to the courts. If written word of the expert is clear and concise, then the oral presentation of the findings should also be understandable to the courts.

At the end of the day, it is the role of the Digital Forensic Expert to review the data available in such a way that it is preserved as evidence, analysed to determine the facts and presented with the expert's opinion as to what those facts represent. Finding an expert, who is consultative in their process, to help walk you through the requirements of a Digital Forensic matter, is critical to your overall success.

For more information for legal professionals regarding digital forensics the book 'Daniel, Larry (2011). Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom. USA: Syngress.' is recommended.