

An introduction to Digital Forensics

CCL-Forensics' Marketing Manager **Andy Holmes** looks at how the world of digital forensics can help win litigation cases.

Imagine a world without computers. There are times when that's not an unattractive prospect. Remember that time when your Blackberry interrupted a dinner party with one of those "difficult" work emails? Or when you returned from a fortnight's holiday and had to wade through 900 emails ranging from snotty emails from your boss to the latest cure for embarrassing social problems?

But, as much as we may bemoan the invasion of computers into every aspect of our lives, it is not just difficult, but *impossible* to imagine living without them. That holiday you've just returned from, for example - even if you booked it at a travel agents, chances are that you checked out the online prices first. All those work emails you were faced with - you can't deny they were easier to deal with than a paper skyscraper where your in-tray once sat.

The advent of broadband means that these machines which dominate our lives can easily send vast amounts of information around the world in a matter of seconds. Little wonder then, that they are proving to be a cheap, fast and anonymous world for people who

want to manipulate them for their own illegitimate gains.

Actually, that's not strictly true. Cheap - yes. Fast - undeniably. But anonymous? The internet *is* anonymous isn't it? With the click of a mouse, surely you can delete information on a computer to cover your tracks. Can't you? Putting it bluntly - no. And that's where digital forensics comes in.

To give it a "proper" definition, digital forensics is "the application of computer investigation and analysis in the interests of determining potential legal evidence". It's not the snappiest definition in the world - but can be summed up as "finding stuff on computers and mobile phones to prove allegations". Or, of course, to DISprove them.



That makes it sound easy. We can all use computers - so if you suspect there's evidence on a particular computer, shouldn't you just switch it on, and have a look?

This document shows why that's the last thing you should be doing.

Digital forensics is not easy - far from it. It requires extremely careful handling of the evidence and the use of highly skilled analysts who know exactly where to search within the massive amount of digital data that these devices can store.

"Digital forensics is not easy - far from it"

Do you know how much your hard disk can hold? It's not the sort of thing that most computer users ever consider. It rarely gets full - unless you're using it as an archive. At the time of writing, the word "terabyte" is starting to enter common usage, along with its smaller siblings 'giga-' and 'mega-'. A terabyte hard disk can be bought online for a modest amount - but its data storage capacity is far from modest.

The complete works of William Shakespeare can fit into a file that takes up 4.5 megabytes - which doesn't sound like a lot. Especially considering how much space they used to take up in school libraries! Imagine our terabyte hard disk is equated to the size of the pitch at Wembley stadium. On this scale, the complete works of The Bard fits snugly into the centre spot - an area the size of a dinner plate. So there's a huge amount of space in the world of digital storage for hiding potential

evidence. It's just a question of knowing where to look.

"A forensic analyst can see through the digital disguise"

No suspect wants their activities to be found, so it's highly probable that they'll have tried to cover their tracks by "hiding" the potential evidence - by deleting the suspicious files, protecting them with passwords or trying to disguise them as something else. To an average computer-literate PC user, this is enough to keep this information from public gaze - but a forensic analyst can see straight through the digital disguise.

Next time you click "delete" anywhere on your computer - be it a file in a folder or an email in your inbox - ask yourself "is this machine REALLY doing what I'm asking it to do?". Again, and still rather bluntly, the answer is no.

It's a well known secret that computers don't really delete files, they just take it out of public view. The information is still on your computer - you just can't get at it. It sits in the unallocated area of the hard disk (which, considering our Wembley example, is pretty huge). Computers are quite lazy - they won't bother overwriting all that data, when there's so much empty space left on the hard disk. It's like a stereotypical

teenager's bedroom; tidying up just means shoving everything under the bed.

But with so much free space on a computer, there's a lot of room for deleted files. That doesn't mean it's easy to find it though - as you need not only highly specialized tools, but also an in-depth knowledge on how to use them. Digital forensic tools, as used by analysts, can recover these deleted files - provided they've not been overwritten. They can, with the skill of the analyst, crack password protected files and see through most of the, frankly, poor attempts that people use to cover their digital trail. This means the barrier between you and the evidence you need is removed.

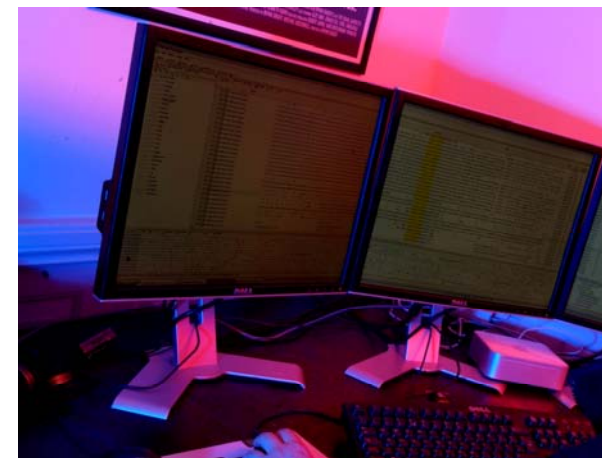
Effective digital forensic procedures are very complex - but they all start with a very simple mantra: "Secure the evidence".

"Secure the evidence"

Imagine the suspect's digital trail is a set of footprints in the snow. Fresh, clearly defined prints. If you were to do nothing, over a period of time, more snow would fall and this trail would disappear. This is the equivalent of repeatedly using a computer where you suspect there is evidence.

If you were to go in and investigate yourself, you too would leave a trail of footprints, and the more and more you investigate, the more complex this network of tracks will be - until there's no chance of seeing the original trail.

Securing the evidence, therefore, means "freezing" the initial set of prints, meaning they are completely unchanged, and can be investigated safely.



Digital forensic analysts do this by creating an "image" of the suspect device - whether a computer hard disk, mobile phone - or any other type of digital media. This can be USB flash drives, PDAs, iPods - basically anything that stores information in 1's and 0's.

This image leaves the original completely unchanged. The device in question doesn't even have to be switched on. (Even switching a computer on can modify more than fifty files, covering up potentially crucial evidence). Imaging creates a bit-for-bit forensic copy that can be analysed using highly complex specialist software. This should follow the precise guidelines set out by the Association of Chief Police Officers (ACPO).

Once imaged, the crime scene is in the hands of the analyst. It would be impractical to try to describe the analysis process in-depth, as it is an intricate, precise and highly secure procedure investigating all aspects of that digital media. Analysts are provided with a brief for each case, and spend hours scientifically combing through the data (even if it's been deleted, corrupted, fragmented or disguised) to locate that vital piece of evidence. That is, of course, provided the evidence is there; digital forensics can just as easily be used in defence cases as in prosecution.

“Once imaged, the crime scene is in the hands of the analyst”

Once analysed, the analyst's findings are presented in a clear easy-to-read format, which shows the relevant information, based on the initial brief. If the relevant guidelines have been followed throughout this procedure, this is admissible in a court of law - and can be backed up by an expert witness service, usually provided by the analyst who carried out the work.

What evidence can be recovered by digital analysts? The simple answer is: more than you may think. We've seen how promiscuous computers can be, and they can typically yield:

Emails	Internet Searches
Internet History	Chatroom Logs
Documents	Deleted Files
Images	Network Information
Videos	Internal metadata

Mobile phones, which are becoming more and more like mini-computers obviously store much less information, and because of the many varied designs can vary from model to model, but you can typically get

Contacts	Dialled calls
SMS (inc deleted)	Last cell location
Phone number	Subscriber info

from the SIM card alone. The actual handset can yield

Dialled/Received/ Missed calls	Images/Videos/Music files
SMS/MMS	Sound recordings
Contacts	Internet activity
Handset ID information	Internal metadata

And that's just computers and mobile phones. The expansion of digital media means that Digital Forensics Analysts are seeing a more

and more diverse range of devices that act like miniature computers. SatNav units for example hold a lot more information than you may think. It's been known for a SatNav to prove that a salesperson has been sunning themselves on a beach when they were supposed to be at a conference in London. MP3 players can act as file storage devices, making it possible to steal intellectual property right from under the nose of an unsuspecting workforce. Even games consoles have been used illicitly because of their file storage capability.

As a basic rule, if it works with digital information, and has some sort of memory, there's a chance that it could hold vital evidence for your next case - but only if it's handled properly. If you suspect it, secure it - and seek help from a qualified analyst.

So, next time you do anything on a computer, just think of the digital trail you're leaving behind - and ask yourself: does the 'delete' button actually do what it says on the tin?

The fact that it doesn't, could prove to be one of your most powerful tools in winning cases.

For more information on digital forensics, please call CCL-Forensics on 01789 261200 or email Andy Holmes at aholmes@ccl-forensics.com