

How hard is digital forensics?

CCL-Forensics' Mark Larson gives an insight into the complexities involved in digital forensic examinations and explains why it's best left to the experts.

The need for digital forensics is rapidly expanding and this growth shows no sign of stopping. This is very much a reflection of the penetration of computer and computer related communications technology pervading more and more aspects of everyday life. It is difficult for any of us to go through a typical day without interacting with several computers and communication devices. Each of these interactions leaves traces which, for a variety of reasons, may subsequently need to be analysed.

Digital forensics owes its existence, as do all branches of forensics, to the legal and law enforcement sectors. These sectors have the most compelling reason to use forensics - the need to identify, secure and exhibit evidence whether it be fingerprints, DNA or digital data.

"Digital forensics needs to be done properly"

This need to produce forensic evidence is therefore becoming more and more

important for legal professionals. Typical areas of law which are using digital forensics include civil litigation, employment tribunals and fraud. These, and many other issues, may all require the examination of digital data. Whether called forensics or not - if the purpose of the examination is to try and prove something - it is forensics, and that means it needs to be done properly.

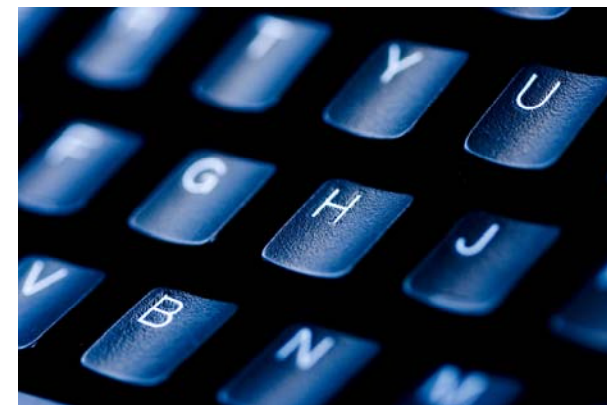
This requirement to examine digital data or devices is something that more and more solicitors are finding that they need to consider. You may begin to wonder why the examination of a computer should be carried out by a forensic examiner, when perhaps an internal IT department could help.

This article summarises the main reasons why a professional digital forensics company should be the first port of call if you feel digital evidence may be of use in your case.

1. Complexity - when did any of us last fire-up a hex viewer?
2. Data volumes - because life's (literally!) too short to comb through reams and reams of data.
3. Evidential procedures - forensic analysts do this every day, and know the procedures and pitfalls.

Firstly, existing IT staff have a 'day job' - keeping systems running and supporting the organisation. With the rapidly changing IT

landscape they are usually at full stretch just doing this. Secondly, but perhaps more importantly, there is very little synergy between running IT systems and examining them forensically. It's a common misconception in the computing world that because IT people know about computers they know about every aspect of computing but this simply isn't the case.



To give a more specific example - digital forensics practitioners will typically be examining data and data structures at a very low level - raw binary data from the disk. As an added complexity this data is usually dealt with in hexadecimal (i.e. base 16) format. Believe it or not this makes it easier to understand but in the normal IT world you never have to deal with data in this way. The binary / hexadecimal relationship is fundamental in digital forensics and you need to spend some time getting your head around it!

Sticking with the 'geek' theme for a minute we should perhaps look at some related reasons why you perhaps shouldn't try this at home.

“Digital analysts will typically be examining raw binary data”

One reason digital forensics is so useful in providing evidence is that it encompasses an examination of the entire physical media (such as a hard disk drive). This means that a digital forensics practitioner has access to ALL the data - not just what the ordinary user sees. Not only can an examiner see structures like disk partition and file tables (vital for computer operation but not normally viewable) but also all the unused areas of the media and this is absolutely critical.

Here's something to try. On your computer go to "My Computer" and look at the size (in gigabytes) of your hard disk drive. You can also see how much of the drive space is available - "Free Space". It is usual to think of this "Free Space" simply as part of the disk that you haven't used yet or are not currently using. You probably don't realize just how much data there is in these apparently 'unused' disk areas.

First of all there are deleted files - despite what they seem to tell you computers don't

delete anything. They just mark the storage areas on the disk that the data occupied as available for use. The data is still there and only disappears when it's eventually overwritten by other data. As most computers operate with a hefty amount of unused disk space or 'free space' at any one time - there's the potential for that data to be there months and even years later!

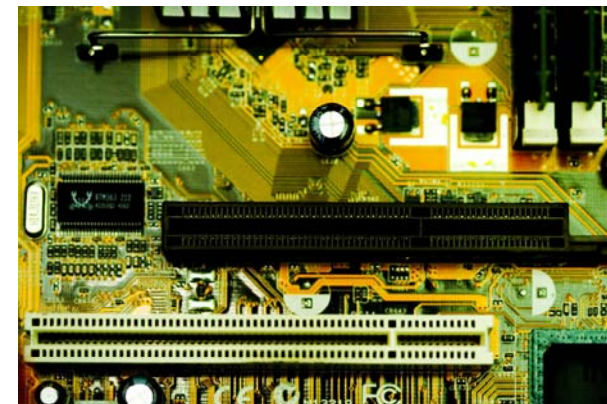
Your computer is also typically using this space to write data to all the time in normal operation - memory swap files and a range of temporary files (such as temporary Internet files - copies of the web pages you've viewed) are written to disk. Once deleted, the data remains but, specialist tools and skills are needed to recover them.

“There's the potential for that data to be there months and even years later”

Incidentally my computer disk usage is 44%. 56% of my disk is allegedly unused but as a forensic practitioner I am sure that 56% will contain an awful lot of information.

Data volumes and formats present an interesting challenge too. Most users find it hard enough to keep track of their own files. We've all had the miserable experience of searching through our folders looking for that report or presentation that we know is in there somewhere. Now imagine that that report or presentation isn't just in one of your folders

but that it could be anywhere on the computer - in system folders, other users' folders or, worse still, in part of the disk that you can't access - freespace! How do you go about searching for it? The Windows search function rather unhelpfully doesn't search freespace and neither do utilities like Google Desktop. If what you're looking for is deleted - you've got a problem. Digital Analysts, however, can retrieve this, providing it's not been overwritten by yet more deleted information.



There's also a lot of data to look through. As we touched on in our previous article "[An Introduction to Digital Forensics](#)" ([click to view](#)) - the Complete Works of Shakespeare are about 4.5 megabytes in data volume. If the data you wanted to find (whether it's your missing presentation or perhaps some important evidence) was lost on your hard disk and that disk was 4.5 megabytes in size then luckily you'll only have to trawl through

a volume of data equivalent to the complete works of Shakespeare to find it - easy!

Of course, who in the world has a 4.5 megabyte hard disk drive - nobody. A reasonably small hard disk drive at the time of writing is 80 gigabytes. Now to trawl through even this is the equivalent of leafing through a mere 17,777 copies of the Complete Works - not such an easy job - better keep the weekend clear (for the rest of your life!). And that's a modest drive - there are drives out with capacities of a terabyte or more - that's more than the equivalent of 222,000 times the volume of the Complete Works (best get some help because you quite literally will not live long enough to go through a fraction of that amount of data!). And, of course, what you want might be in 'freespace' - not the bit you can actually 'read'.

Ok, if this wasn't bad enough you'll also need to consider that the data isn't all in a form that can simply be read (a bit like Shakespeare too as I recall my schooldays!). Even simple text can be in a variety of forms that may make your search tricky. It could be in simple Unicode (not good if you're searching for standard ASCII text) or maybe compressed in a ZIP archive. And some of the interesting data won't be text at all - date and time data, often crucial as evidence, for example require decoding. Searching data is like searching a book for text where not all of the text is visible, where not all of the visible text is in a

language you understand and where some of the most crucial information may not be text at all.

Maybe that's enough geek stuff so let's take a look at another aspect.

Any computer, computer system, mobile phone or server that contains data that is required as evidence is in essence a 'crime scene'. We have all probably watched enough TV drama to understand that the first thing to do with any such scene is to preserve it. But how are you going to do that - especially if the crime scene is also a business critical server. Preserving, securing and handling evidence is an essential part of the evidential process and yet few people genuinely know how to do it in a way that will withstand challenge.

“Searching data is like searching a book for text where not all of the text is visible”

In fairness, you don't have to secure a crime scene everyday of the week but there are some fundamental issues with the events described above. First - never be tempted to have a look. You'll change data and crucially you may inadvertently overwrite some of the very evidence you seek. Second - you open yourself up to potential allegations that your actions at best tainted the evidence and at worst put it there. Third - you need to act in a timely way - this computer has been used and therefore changed on a daily basis and this has

seriously compromised the likelihood of it preserving the evidence.

Finally - you're just never going to be able to keep up to date with this rapidly changing technology unless you live and breathe it day in and day out.

This is what Digital Analysts do. So when you find yourself in a position where digital evidence forms a crucial part of your case, ensure it is handled properly by the experts. It could mean the difference between success and failure in court.

Mark Larson is Forensics Manager at CCL-Forensics, a leading supplier to law firms and law enforcement agencies.

For more information please contact Mark at mlarson@ccl-forensics.com or by calling 01789 261 200 and speaking to Mark - or Chris Booth in CCL-Forensics Sales.