Fields Associates
digital forensics consultants

Digital Evidence in Criminal proceedings

Considering the rate at which both the ownership of personal computing devices and the provision of high-speed internet have grown in recent years, it comes as no surprise that digital evidence is playing an important role in more and more criminal cases. In fact, when the Police now gather evidence from a suspect's residence, their personal computer is usually one of the first things to be collected for analysis.
Mobile phones are now more than capable of providing evidence that can contribute to a successful case. Through Cell Site Analysis the approximate location of a suspect at the time that a crime was committed can be determined. Such evidence will never be sufficient in itself, but it can, when used to supplement other items, be extremely influential.

A suspect's computer can also provide the prosecution with a wealth of valuable information. Emails, chat logs, even a user's internet history can be utilised in order to obtain a guilty verdict. Valuable data can also be gleaned from other sources such as smart phones and tablet devices.

Such evidence is now often crucial because the data contained on these devices has the potential to be extremely persuasive and even definitive in criminal trials. Consider, for example, how damning it would be if data directly referencing the crime could be recovered from any device owned by the defendant such as an email, an online chat log or other type of file. It is not unreasonable to suggest that such a piece of evidence could prove to be just as vital as DNA evidence in placing a suspect at the scene of a crime at a specific time.

However compelling the digital evidence in any case may appear to be, however, there is no guarantee that it will be admissible in court. Digital evidence is easily changed and not only does a strict chain of custody need to be adhered to, but any analysis also has to be conducted by an experienced and highly-qualified expert in order to ensure that any data is not compromised. When an individual analyses a drive and its

(continued on page 2)

Did your Client Really Create that File?

Only a few years ago solicitors and barristers representing individuals accused of having indecent images stored on their computer's hard drives would advise their clients to plead guilty irrespective of their client's protestations. To some, this will come as no surprise. A significant portion of the population would assume that any kind of digital file, whether an image, word document or other type of file could not be found in a device's storage media unless it had been created or downloaded by an end user – most likely the device's owner.

(continued on page 3)

Why Your Commercial Clients Need a Forensic Readiness Programme

(continued on page 2)

Fields Associates
digital forensics consultants

Digital... *(continuation)*

contents, they must ensure that they record every single act that is undertaken and every single way in which the files that are present on the drive may have been altered during their analysis. Put simply, if the analyses of the relevant devices are not conducted correctly, then either a successful prosecution or acquittal could be lost.
Employing the services of skilled data forensics such as Fields Associates will ensure that any evidence gathered is admissible in court and that the correct verdict is delivered.

Why... *(continuation)*

Over the last three decades, technological advancement has grown at a truly prodigious rate and, with a variety of devices now essential to the everyday business of the vast majority of organisations worldwide, it is no way surprising that most companies have practicable disaster recovery/contingency plans in place. Whilst such policies are well suited to addressing matters that may arise as a result of events which, whilst unlikely, are potentially catastrophic, little consideration is given to polices designed to address events which, whilst not necessarily disastrous, can be disruptive and occur far more regularly.
Common examples of such incidents include, but are in no way limited to, disputed payments, employee misconduct and the need to assist law-enforcement agencies with their investigations. In each of these – and many other – instances, it will almost certainly be necessary to provide and/or utilise some form of digital evidence; hence the need for companies to have an actionable Forensic Readiness Programme in place.
Digital evidence is notoriously volatile and can easily become worthless if handled incorrectly. In spite of this, few organisations have plans in place to allow them to preserve, identify and collect digital evidence in such a way as to ensure that it would be able to stand up to the vigorous tests to which it would be subjected in legal proceedings. This, of course, could prove costly should a company find themselves involved in various types of civil proceedings.

The need for organisations to provide various bodies with

admissible digital evidence will not only apply when they are directly involved in procedures either. Should a crime take place at a business, for example, then they will almost certainly be required to provide law enforcement agencies with video recordings or files that may relate to matters. Furthermore, institutions operating within the public sector are required to retain a variety of documents in order to adhere to stipulations set out within the Freedom of Information Act 2000. Financial and other institutions must also hold documentation on clients for set periods of time, also – something which, due to convenience, they are now likely to do through digital rather than physical means.

In order to form a workable Forensic Readiness Programme, organisations will need to utilise the skills and knowledge of their senior managements, legal advisers such as solicitors or digital forensics experts and their own systems administrators. The plan should focus on risk assessment whereby it will be identified what legal threats the organisation is most likely to encounter, the type of data that they are most likely to need to disclose as a result of these and cost-effective ways of backing up and securing this data so as to ensure that, should these records need to be accessed, this does not affect the organisation's day-to-day activities.

Fields Associates
digital forensics consultants

Did Your Client... *(continuation)*

It could be argued that the accused was not responsible for the presence of the data and that, as alluded to previously, it had been created by another individual who had access to the device in question. This is perfectly plausible, of course, but it is still extremely difficult to prove. But did you know that it is possible that illegal data could have found its way onto the relevant storage media without the intervention of either the device's owner or, indeed, anyone else with access to the device – at least not directly.

When an individual uses the internet, they are, if the correct security software is not installed on their device, susceptible to any number of viruses. Some of these viruses, known as Trojan horses or Trojans, can, if they infect the device in question, result in files appearing in a system without the user's knowledge.
Consider, for example, whether you've ever been told that you need to download a certain file before you can view a webpage, or if you've ever received a spam email from someone who you know and whose email address was in your address book. The former is a clear example of how a Trojan horse virus can find its way onto someone's hard drive whilst the latter shows the ease with which they can be circulated.

In some if not many instances Trojan horse viruses can be relatively innocuous. Many hackers utilise them solely to annoy end users by turning web pages upside down, affecting mouse movements or playing sounds repetitively. Some, however, utilise them in order to gather sensitive data such as passwords and debit/credit card information. Others afford hackers remote use of the infected device effectively turning its hard drive into a proxy storage device within which nefarious individuals could store any number of illegal images or other incriminating documents. All whilst the mechanism's owner is oblivious to the fact that illegal material is regularly being downloaded to their hard drive.

Quite literally any computer can become infected by a Trojan horse and the vast majority of people will have files that they have neither downloaded nor created lurking somewhere in their computer's hard drives. Fortunately, these files will rarely be incriminating and a relatively small number of people will face charges as a result of them. Those that do, however, will be hard pressed to explain their presence.

Sometimes files can appear in hard drives without the involvement of hackers, though. When you visit a website, the image files present on the page are stored in the device's temporary internet file. Now, imagine if you were to visit a site by accident – or were redirected to one – which contained illegal images. These images would be stored in your temporary internet folder until you removed them and, as this could potentially serve as proof of the fact that you created

indecent images, you could then be prosecuted under the Protection of Children Act 1978.
If either set of circumstances outlined above applied then an accused would not be guilty of downloading – and therefore creating – an indecent image as they would not have knowingly either viewed and/or downloaded such an image. In spite of this, many of these individuals would (and perhaps still will) be advised to plead guilty by their representatives.
On a final note, it must be added that there are numerous other reasons why an incriminating file may be present on any form of storage media without the appellant's knowledge, and under no circumstances should an individual that finds themselves accused of possessing illegal data be advised to plead guilty before significant investigations into the relevant media have been undertaken.