Advanced Digital Forensics What Else is Possible?

by Simon Lang BSc (Hons). Digital Forensic Manager SYTECH - Digital Forensics

As the speed of personal technology and digital security advances, so must the techniques used in extracting and more importantly interpreting the essential evidential data found within and generated by modern digital device.

Case Example
A recent Digital Forensic assisted case involved a serial rapist whom attempted to murder a number of victims was caught and prosecuted due to the invaluable digital evidence gained and analysed.

This was a multi pronged examination which utilised the most advanced aspects of the Digital Forensic Disciplines described below.

Raw Facebook data was analysed which showed the defendant using various online accounts which were attributable to their mobile devices via the use of in-depth analysis. Cell-Site Analysis showed the "hunt" as he stalked his victims and randomly selected lone female victims at night, whilst locational data recovered directly from the handset showed numerous reconnaissance "missions" carried out by the suspect prior to these attacks.

The compelling evidence produced by this digital investigation assisted in the suspect being sentenced to life imprisonment.

Forensic Chip-Off Examinations
This is particularly useful and ground-breaking technique when it comes to recovering evidence from pin-locked or password protected BlackBerry devices and "smashed" phones, Solid State Hard-Drives and even USB Flash drives. Chip-off is a process that has been perfected over the years which uses a number of tools and complex techniques to access and decode this essential data.

Phone & Mobile Device Examination
Industry-leading forensic processes are used to extract every single item of data both live and deleted from the device, associated SIMs and memory cards. All of this information is presented to you in a format which is easy to understand and suitable to be used as Evidence no matter the type of case.

Latest breakthroughs currently being pioneered include that of a complex examination technique referred to as JTAG. This involves bypassing a mobile phones operating system and by using specialist equipment pulling both live & deleted data from the memory directly through the handsets circuit board. This is essential on Smartphone's which aren't supported by conventional forensic techniques as well as PIN/Password protected Android based phones.

The latest password protected Apple devices such as the iPad ,iPhone 4S/5/5S/5C are now accessible to various degrees of data extraction which until now have been inaccessible to evidence until the in-house R&D have thwarted this complex forensic problem.

Cell-Site – Mobile Phone Cell Site Evidence
Cell-Site Analysis is an invaluable branch of Digital Forensic based Services through which we can provide you

with the location of mobile devices when communications occur – and this can be any form of communication – whether calls, SMS or MMS.

This provides a reliable way for you to place individuals' mobiles in order that you can establish a picture of who was where, and when.

This evidence can be used within a legal case where a person's location is required, and this in turn can often help establish the guilt or innocence of an individual. Recent advancements in the analysis of GPRS (Mobile Data) packets and data analysis brings a whole new level of accuracy to the location of a device never before thought possible.

Computer Forensics

Computer Forensics is synonymous with materials of an indecent nature. However; Computer Forensics can be involved in absolutely any type of Criminal Investigation. By utilising advanced research methods on a daily basis tackle such complex investigatory matters such as the Encryption of valuable data or the use of TOR (The Onion Router) to anonymously traverse the Internet and gaining access to The Darknet which has recently often been referenced in News articles and offered referred to as the "Hidden Underbelly of the Searchable Web".

It is important to always be at the forefront of new and emerging technologies such as Bitcoin. Whereby it is now possible to carry out Bitcoin based Forensics & Recovery.

Attribution

Attribution of devices and data is offered used in all the above forensic disciplines. It is often best used in the differentiation of clean & dirty devices, or in the proving or disproving of alibis using complex communications patterns, location based data. And pattern of life analysis.

Often the best place to find this expertise is within the Private Sector, whereby essential and ongoing R&D is always utilised to its fullest, so the experts can always stay one step ahead. The speed of these examinations, production of findings and expert knowledge is an invaluable tool that private companies can offer and more importantly at a fraction of the internal cost. ■

Even in this state SYTECH were are able to extract both the live and deleted data held within.