Chapter 8  Digital Forensic Analysis

Ian Kennedy with Ed Day

The definition of digital forensic analysis (DFA) will vary, but it normally includes aspects of the preservation, identification, examination and interpretation of digital information, intelligence and evidence. It is normally considered a ‘high level’ process (Carrier, 2003, p.1) – that is it involves deriving meaning from data rather than being simply descriptive. DFA is often a stage within a digital criminal investigation which itself might be part of a wider criminal investigation (see Chapter 6), normally following on from the recovery of data from a crime scene (see Chapter 7). With detailed knowledge of the investigative requirements, the officer in charge of the investigation (OIC) normally provides guidance on what is sought from the forensic investigation. This guidance should obviously be as detailed as possible to correctly steer the forms of analysis to be employed by the digital forensic investigators involved. Establishing the ‘five Ws and the H’ (the Who? What? When? Where? Why? and How?) of a criminal investigation will be at the forefront of the mind of the OIC (see Chapter 6). This chapter also includes explanations about how digital data is stored, and what sort of information is stored, mainly with respect to computers. The level of detail provided is necessary for understanding how such features can be used in the process of digital forensic analysis.

In practice the actual process of digital forensic analysis is usually performed with various dedicated software suites. Any hardware used (such as portable hard drives) tends to be either more rugged or powerful versions of consumer hardware, or specialist hardware such as write blockers. The processing and analysis of forensic evidence are typically performed on high specification PCs to cope with the large amounts of data that need to be indexed, searched or otherwise processed. Cellebrite’s UFED device is often used for the analysis of mobile devices (Cellebrite is a fully-owned subsidiary of the Sun Corporation, a listed Japanese company). Guidance Software's EnCase is
widely used for computer forensics cases in the UK as it allows for the automation of many of the processes during a digital investigation (Guidance Software Inc is a US-based and NASDAQ – listed company). Prior to the release of EnCase, law enforcement in the UK used various tools including DOS utilities, Norton Disk Edit, Disk Image and Back-up System (DIBS), and Vogon tools (Jones, 2009).

However many UK police forces now require dual tool verification in cases involving computers (ie ensuring that the results obtained with one tool can be verified using another). This is in part due to problems associated with the use of EnCase, such as the proprietary nature of its code preventing independent ‘white box’ testing, and its frequent software updates making verification difficult and costly. (A further reason is that the police have made widespread use of EnCase, and it has been noticed that suspects are beginning to deploy of a number of anti-forensics techniques). In the UK, AccessData's Forensic ToolKit (FTK) is now commonly used (the AccessData Group is a US-based company). Other commercial tools are also available, their popularity varying between country, for example X-Ways Forensics is commonly used by German investigators. Free and open-source digital forensic software is also available such as The Sleuth Kit and Autopsy. Other tools for specific technologies have also been developed and are widely used by law enforcement, for example Digital Detective's NetAnalysis for Internet Forensics, and products from RTL. Micro Systemation is also used for the examination of mobile devices (in addition to the Cellebrite tools mentioned earlier).

The location of digital evidence within a particular device will naturally be dependent on the type of device (see Chapter 7 above). The data of interest will depend on the investigation and may include image files, videos, document files, swap files, registry settings, event logs, print spooler files, temporary files, software, call information, address books, SMSs, location data, browser history and chat logs. Data may be easy to recover, but it may also be hidden, either deliberately or as a function of the operating system. An image file might be easily recoverable from a ‘Pictures’ folder, it might have been innocently deleted by a user yet still be recoverable, or a user might be deliberately hiding it via a variety of means, a simple one being renaming the file. Alternatively a suspect might have
attempted to erase data by using software or by degaussing (exposing magnetic media to a powerful magnetic field) (Kissel, Scholl and Skolochenko, 2006). It should be noted that not all software reliably removes all data. The increasing popularity of Solid State Drives (SSDs) however can be a disadvantage for investigators in that file erasure is much quicker and certain for SSDs (than for magnetic hard drives), and there is therefore much less chance of being able to recover deleted files (Bell, 2010). This is discussed in more detail in Chapter 10.

Digital evidence must be authenticated, documented and preserved. In the UK, the first ACPO principle (see Chapter 7) should be followed: a ‘copy’ must be made of the original data, and it is the copy that is analysed, not the original. The analysis of a hard drive is explained in detail below. We describe general and specific procedures that may be carried out on an entire hard drive image but the copy received by the analyst might be a subset of a drive, perhaps as small as a single file in which case not all the procedures described here would be relevant.

Analysis of PCs

A forensically important component of the PC is likely to be its hard drive (sometimes known as a ‘hard disc drive’ or HDD). Digital forensic analysis of the hard drive is always undertaken at the ‘logical’ level and sometimes also at the ‘physical’ level (although the distinction between the two forensic processes is somewhat artificial). The data contents of a hard drive are physically scattered throughout the drive but the data contents are presented to the user as a logical structure, consisting of drive letters, folder names.

An initial step typically undertaken in a logical hard drive analysis is to identify the ‘operating system’ (OS) – for example, the Microsoft Windows 8 OS. A PC runs an OS that sits between application programs and the low level software and firmware on the machine. (Note that here we are using ‘PC’ as a general term, but others sometimes use it to differentiate a personal computer running a Windows-based OS as distinct from an alternative OS.) The OS controls the overall operation and resource management for the PC. There are a number of different OSs, for example Windows, Linux, Mac OS, iOS, Android and Java ME, but most PCs run one form or another of the Microsoft
Windows OS (netmarketshare.com, 2011). More recently the so-called tablet PCs are becoming more popular and these predominantly run versions of Apple’s iOS and Google’s Android. Here we will focus on Windows as it is the OS most often encountered by investigators (as a result of its popularity), but much of what is described here also applies or is at least similar for other OSs.

A frequently overlooked aspect of a PC investigation is the internals of the PC itself. If a suspect has opened the machine in order to upgrade it, or for another reason, their fingerprints or traces of their DNA may be found on surfaces inside the case. The serial numbers of components such as the RAM may also provide evidence that the machine has been upgraded, similarly for the CPU, motherboard and any other components. If the internals are dusty but a particular connector is clean this might suggest that something has been removed. The replacement of internal components (if shown to be performed by the user) would suggest that a user had a certain level of IT skills which might counter defences that depend on the user ‘not knowing what he was doing’ (Bryant et al., 2013).

The Registry

The Windows Registry (to be found in Windows XP, Windows 7 and now Windows 8) is storehouse of information, much of which can be of use to the forensic investigator. It is a special database that lists the computer’s OS and other system configuration details. The information in the registry can be visualised using a tool called Registry Viewer. Figure 1 shows a screen shot (AccessData 2011), with the installed operating system listed against ‘ProductName’, and the name of ‘RegisteredOwner’, (redacted for privacy).
Figure 1: The Registry Viewer
The date the operating system was installed on the computer is also shown as the ‘InstallDate’. In this example the date is stored as a 32-bit number, 0x450EB962, which the Registry Viewer tool helpfully translates to a date. As a means to verify this translation, the digital forensic investigator can use a second tool such as DCode (Digital Detective, 2011) to corroborate the timestamp. The procedure and the findings should be duly noted in the forensic investigator’s contemporaneous notes.

Figure 2 Converting raw data to time stamp values (image reproduced with permission of Digital Detective)
In addition to details concerning the machine’s configuration and application information, the registry also shows a list of all the users, and also the time each user most recently logged on and if a password was required (see Figure 3).

Figure 3 Access Data’s Registry Viewer

Other useful information in the registry includes the default number of days Internet Explorer retains internet history records for prior to deletion, the user’s wallpaper settings, an historical record of USB devices that have been attached to the computer (including the assigned drive letter and serial number in many cases) and recently saved files.
The registry also contains an encrypted/protected area known as ‘Protected Storage’ which stores sensitive information such as:

- data which has been typed for completing online forms (AutoComplete on Internet Explorer);
- passwords for protected websites;
- account identity information and passwords (including dial-up user accounts); and
- search criteria entered into web search engines;

The ‘TypedURLs’ area of the Registry can also be useful it contains records of any website address that has been manually typed into the Internet Explorer address box.

Records kept by PCs

Various actions can be performed on a file from its creation through to deletion, and this information is all stored, see Figure 5. The Windows operating system is a comparatively diligent keeper of records, monitoring who has accessed what, and when.
Figure 4: Some of the file information stored in Windows
A suspect may alter data to hide the provenance or function of the data, for example an image file might be renamed by changing its file extension so it appears to be a Word document. A user could also change a Word document’s metadata to make it appear that the file was created by someone else.

Useful evidence may also be created by OS automatic processes (not as a direct result of user action) and such evidence may reside in locations other than user-created folders. Windows XP and Windows 7 both allow the contents of a folder to be displayed in different ways, for example the ‘thumbnail’ view. This is often used for folders containing pictures, as shown here in figure 6.

![Figure 6 Thumbnail images](image)

Figure 6 Thumbnail images

When the thumbnail option is selected both Windows XP and Windows 7 create and save a separate and hidden file containing the small thumbnail sized versions of each picture. This will remain on the drive even if the main image files have been deleted. Most users are unaware that such a small thumbnail file continues to exist.

Another aspect of the Windows OS that allows for file recovery is the fact that Windows writes to what is known as a ‘swap file’. The swap file is typically used when RAM memory is getting low, and
data that has not been recently used is ‘swapped’ out to the hard drive, thus freeing up RAM. The
swapped out data is stored in a very large text file, and it may contain useful data for an investigation,
such as plain text passwords. However, there is no guarantee anything useful will be recoverable. In
modern Windows OSs, this file is named Pagefile.sys and normally resides in the root of the C: drive.
There may also be a file hiberfil.sys in the same location, which stores the data required for a
‘hibernating’ PC to resume function. This may also contain forensically useful data (Ruff, 2008).

A number of processes on a PC create temporary files, which often remain on the hard drive after the
process has completed; these may contain forensically interesting information. For example, the OS
creates temporary files when a user requests a file to be printed (in a process called spooling), which
may be retrievable from a machine’s hard drive (Sheldon, 2006). Other temporary files that may be
of interest (on Windows systems) list recently accessed files, and shortcuts to files, drives and external
media. Such files could be used as evidence when a user denies having accessed certain media or
devices. Other processes such as the installation of software may also result in a tell-tale trail of
temporary files, and again these can be used to refute a suspect’s denials. For example if a suspect
has removed a particular program that aids illegal file-sharing there may still be traces of this program
on his machine.

Data can also be concealed within partitions of hard drives, by for example saving data onto the D:
drive then de-allocating the partition (thus hiding it). When the user wants to retrieve the data the
partition is simply reallocated. There are two specific areas on a hard drive that can be used for hiding
data: the ‘Device Configuration Overlay’ and the ‘Host Protected Area’ that Windows cannot ‘see’.
Specialist low-level software is needed to write data to these areas (Battula et al, 2009).

Data can also be hidden using certain file formats such as the Office 2007 which uses a zipped
container, rather than the single document system found on pre-2007 versions of Office. The zipped
container holds a number of folders and documents, some of which can be edited in order to conceal
data (Park, Park and Lee, 2009).
One method of speeding up forensic examinations is by the use of known file filters (KFFs). This is available in some forensic software such as Access Data’s Forensic Toolkit (FTK). KFFs are databases of known files, either benign (such as Winword.exe), or of interest (such as known child sex abuse images), along with hash values that identify the files. The hash values are necessary since it is possible for a user to rename an illegal file as ‘winword.exe.’ for example. When FTK searches for illegal files it would consult its KFF when it encounters ‘winword.exe’ and check that its hash matches, and if they do not the file would be flagged as suspect. The KFF allows searches to be performed more quickly since benign files on the KFF can be ignored by the searching software (Davis, Kennedy, Pyles, Strickler & Shenoi, 2006).

**Metadata**

Some file types, such as Microsoft Office files, also contain ‘metadata’. This is data about the file (eg the author and when the file was created) as distinct from the file’s actual content. An example of file metadata is shown in figure 7. Note that the ‘Edit time’ value is recorded here as 4th January 1601 13:13. This means the total edit time for this document is zero years, 13 hours and 13 minutes (starting from the epoch 1601 date). In fact Windows stores this value as the number of 100 nanosecond periods that have elapsed since 1 January 1601 00:00:00.
A file’s timestamp may allow investigators to ascertain the temporal order of certain actions in relation to a file. This can be very important when determining who was likely to have been responsible for particular actions. For example, if according to its timestamp a file was created at a certain time then that can be checked against an event log in the registry (see above) to see who was apparently logged on to the machine at the time. This could provide information supporting the hypothesis that a particular user downloaded a particular file.

However the accuracy of any timestamps depends on a machine’s clock, which will depend on the time and the time zone set by the user, both of which may not be accurate. In addition, as for any clock the computer’s clock may run fast or slow (Willassen, 2008). It should also be noted that it is relatively easy to alter timestamps using hex editing software.

In addition to the computer’s clock, a file’s timestamp can also be affected by the file system, the methodology for storing, accessing and otherwise managing files on a partition. Most modern OSs provide support for more than one file system, but not all file systems store the same timestamps. The
New Technology File System (NTFS), for example, records the date and time the file was last accessed as well as the date and time any of the file’s properties were changed (Access Modified). However, neither of these timestamps are supported by the FAT32 file system. Therefore, it is not uncommon to see timestamps discarded when files are copied from a computer (using NTFS) to a USB pen drive (using FAT32). Files copied from a USB pen drive back to the hard disk in this scenario would bear a ‘zero’ timestamp.

The OS can also impact on a timestamp’s value. A Windows 7 computer running NTFS, for example, will stamp a file with a created date, modified date, access date and access modified date. As in this example, there can be a difference between the ‘Created’ date (see figure 5) and the metadata ‘Date Created’ values (see figure 7). When a file is copied to another device (such as a USB pen drive) the ‘Created’ date shown in figure 5 will record the date the file was copied to the device. However the file’s metadata including the ‘Date created’ (as in figure 7) is not automatically modified. The most likely reason for the discrepancy in this example is that the document was first created in 2004 and subsequently copied to another storage device in 2008.

Files containing digital camera or mobile phone generated pictures can also contain metadata. This can be read using a mainstream forensic tool such as EnCase, or specialist dedicated tools such as Exif Pilot which will present the information in a form more suitable for inclusion in a forensic report.

Figure 8 shows that the camera that was used to take the digital photo is recorded as a Sony ‘DSC-HXV5’, and also shows the date and time the photo was taken (‘DateTimeDigitized’).
DFA can involve comparing the various levels of recorded data. It is possible for example to corroborate data such as dates with those at another level, and any discrepancies could be an indication of an attempt to conceal actions by falsifying the data. By way of an example, consider the case of Dr Harold Shipman who was convicted of 15 counts of murder in January 2000 (but almost certainly responsible for many more). During the investigation, it became apparent that he had very likely altered the medical history records of his victims after they had died. The evidence supporting this was that the date on file metadata recording when an entry was made was different from (and
later than) the date originally entered by the user. (It is however possible for a knowledgeable user to change file metadata.)

**Example of a DFA-Forensic Investigation**

A recent investigation in the UK provides an illustration of the application of a number of the DFA methods described thus far. Following information provided to law enforcement, an individual was arrested during the early hours of a winter’s morning in a dawn raid, executed under a PACE 1984 search warrant. During the search a computer was seized and submitted for a forensic examination. The examination revealed that in excess of 5,000 indecent images of children were stored on the computer. In his defence, the suspect alleged that malware had infected his machine and that after the computer was seized, law enforcement had powered on the computer, thereby downloading additional indecent images of children. Such an action would be a serious breach of the ACPO guidelines on handling digital evidence, resulting in the entire computer exhibit being inadmissible in court (see Chapter 7). The first line of enquiry was to examine the computer for malware. The forensic image of the computer was scanned for traces of malware using multiple anti-malware products with the latest virus definitions installed. This identified two files infected with malware present on the system: a Trojan and a keylogger. The keylogger file was located in the temporary internet files area of the computer, indicating it had been downloaded from the internet. No evidence was found to show this file had been executed or placed in any other area of the computer. Furthermore, the date the file was created was later than the file creation dates of the illegally held pictures. The Trojan file was then examined and found to have been executed on a date that preceded the creation of the illegally held files. However, an examination of the file’s internal structure did not support the allegation that the Trojan was ‘responsible’ for downloading the files. Likewise when the Trojan was run in a sandboxed environment (a forensically secure means of running software and programs) no downloading activity was noted. An additional step was to restore the forensic image held to a clean hard disk and use this to boot the original computer. Monitoring the network activity of this machine demonstrated the Trojan in action. Again, no activity surrounding the alleged downloading of files was observed.
Turning to the allegation of the computer being powered on whilst in police custody, examination of the computer revealed that the date the computer was recorded as last being shut down did fall after the date it was seized by police. System logs kept by the Windows operating system were found to be corrupted and unreadable. By manually editing the file at a low level, it was possible to render these files readable once more and examine their content. Examination of these logs then revealed two entries recorded as taking place a week before law enforcement seized the computer. The first entry showed the computer’s clock being set forward by one month; the latter showed it being set back by one month. Both of these actions are very unusual and typically require user action. All of the recorded illegally activity had occurred during this one month period. This evidence did not support the claim that law enforcement personnel powered on the computer whilst in their possession. As a direct result of work undertaken by the DFA, the suspect was found guilty of these and related charges. He was subsequently convicted and sentenced to 12 years imprisonment. Furthermore, the allegations against the law enforcement agency were dropped and the Defence expert appointed was warned against making such strong and unfounded allegations in the future.
Traces Left by Users

From a legal standpoint in the UK, it is usually not enough to find an incriminating file on a computer, because this only demonstrates the guilty act (‘actus reus’). To evidence a guilty mind (‘mens rea’) it is usually necessary to demonstrate that a user had knowledge of an incriminating file. The actions the user performed in relation to the file are of key importance.

An appropriate place to start with this line of inquiry is the ‘Recent’ folder which shows the most recently opened files for a given user, of which the last 15 files are presented to the user in the “Recent Documents” menu shown in Figure 5. (The user may choose to delete the list of recent files, so it may be incomplete or empty.) The records in this list are actually small files known as ‘shortcuts’ or ‘link files’ which contain a record of when a corresponding file was opened, together with a copy of the file’s own creation, modified and last accessed dates. These additional copies of file dates also help to corroborate (or challenge) the dates stored against a particular file.

Figure 5: The Recent Documents folder

Furthermore, an independent record is kept of files that are opened with a ‘double-click’ action (such as Microsoft Word documents). This can be used to corroborate previously identified records and help to identify any attempts to falsify dates and times, as described above. Other software may also provide useful information in this regard, for example Windows Media Player may contain a list of
recently played media. Such a list could provide evidence supporting the points to prove in an indictment. For example, it could show that an individual has (a) knowledge of; and (b) has ‘made’ (ie: cause to be displayed) an indecent image of a child on the computer.

As well as user-based files, it is also possible to demonstrate that a user had knowledge of and executed a particular application. When a user executes an application (such as a hacking tool) Windows will create a special copy of the program called a ‘pre-fetch’ file, a copy of which is stored in such a way that it speeds up the loading of the program the next time it is run (in much the same way as the internet cache is used to speed up internet browsing). By reviewing the pre-fetch files it is possible to determine if and when an application was executed. The deletion of files by a user can also be traced due to the way Windows stores and deletes files. Windows stores a file by first dividing it into ‘chunks’ which are then typically written onto the hard drive in separate storage locations called ‘clusters’ (generally 4kB in size). A typical file will occupy several clusters, which are then said to be ‘allocated’. When a file is written to a hard disk, there is no guarantee that it will occupy consecutive clusters. (This is a bit like a family trying to check in on a flight with seats together; they might not all be allocated adjacent seats). The locations of the clusters for each file are stored in either a File Allocation Table (FAT-based systems) or Master File Table (NTFS systems).

When a file is deleted on a PC using the Windows OS it is deleted in up to three stages. The first stage (which is optional) arises when a file is ‘deleted’ to the Recycle Bin (a special folder where the file is kept ready for ‘permanent’ deletion). All the dates and times together with the original location associated with the file are preserved by the OS, and a simple ‘Restore’ action by the user will bring the file back. A DFA will often locate suspect files within this folder. The defence typically offered is that the files were obtained accidentally and then immediately deleted. This could be corroborated in part by examining the pattern of files opened; but such a defence would be undermined if a repeated viewing of ‘unwanted’ and deleted files was revealed.

The second stage of file deletion arises when the Recycle Bin is emptied. Files deleted from the Recycle Bin (or deleted without passing through it) have the references (e.g. within the FAT) to the
file deleted. The deleted information includes the cluster numbers (storage locations) for each chunk of the file. These clusters are then no longer ‘allocated’ and hence can be re-used for storing chunks from other newer files. However, the file content within the clusters initially remains untouched. (In the analogy of the airline passenger list, emptying the Recycle Bin is analogous to removing the entire family from the passenger list without removing them physically from their seats on the plane. The seats are still physically occupied, but the booking system shows the seats as empty and available for re-booking.) The digital forensic investigator can search the ‘unallocated’ clusters for chunks of a previously extant file and attempt to recover it. (In the analogy, this is like walking through the plane to check the seats marked as unoccupied on the booking system, to see if they are really empty. The entire family might be found, and could then be rebooked into the same seats or allocated to other free seats.) If a computer has not been used much since the file was deleted, the prognosis for full data recovery is generally good.

The third stage of file deletion arises when files are partially (or fully) overwritten as the computer continues to be used. The clusters containing the chunks of the ‘deleted’ file are at risk of being used for other files, and the remaining data may be partially or fully overwritten. (Returning to the analogy, this is akin to new passenger being allocated to one of the seats that is listed as vacant but is still occupied by a family member; the family member would have to vacate the seat. So any attempt to find the entire family in their seats would now at best produce an ‘incomplete’ family.) Hence, the more the computer is used after a file is deleted, the worse the prognosis for data recovery - new files are created and allocated to clusters, thereby overwriting old data.

In addition if a file does not fill up a whole number of clusters there will be a residual amount of ‘slack space’ in the final cluster which will not have been fully overwritten. The slack space might contain remnants of a previously deleted file (Carrier, 2005) which can be recovered by using ‘file carving’ software. This software attempts to find certain characteristics patterns that can be used to distinguish different types of files. When it encounters a particular pattern in several fragments it will then attempt to rebuild the file (Pal and Memon, 2009).
Web browsers such as Internet Explorer, Chrome and Firefox can provide a number of traces of internet activity. This could prove useful to investigations into paedophile activity for example. Having identified one or more incriminating files, the digital forensic practitioner can examine the internet history records located on the computer to identify a timeline of browsing behaviour. The relevant files will vary with browser, for example Internet Explorer uses an index.dat file and ‘TypedURLs’ area of the registry (the latter also contains records sites that have been ‘copied and pasted’ into the browser’s address bar). In addition, temporary internet files (such as graphics from a page visited by a user) are kept by the Windows OS. However, most browsers also include a privacy mode that attempts to hide a user’s activity. These however have varying degrees of success, for example Firefox private browsing does not obscure Macromedia Flash Player history, so even if a user had been browsing in private mode there may still be a record of certain Flash video related sites (Aggarwal et al., 2010), and obviously this can be useful for an investigator.

As well as the website addresses visited, any keywords submitted to search engines such as Google or data entered into online forms can also be recovered. Records of access to both local and remote files (eg: files located on a network drive or USB device) can also be recovered from Internet history records.

Internet history is one of the most useful records of user activity as it can demonstrate both the likely intent (through searching) and probable action (through browsing/downloading) of the user. Each of these records is stored with the date and time against the user logged in at the time of the action. The small size of these records makes them quite resilient to being overwritten by other data: the recovery of deleted internet history records has been known to produce detailed records of user activity records going back a number of years.

**Countering the ‘pop-up defence’**

A DFA will normally be required in the circumstances of a suspect producing a ‘pop-up defence’: the claim that the existence of incriminating material on a computer was the result of malware rather than the suspect’s own actions. For example, in the UK an individual recently came to the attention of law
enforcement after downloaded images of child sexual abuse imagery were found on his computer. Following a dawn raid and the seizure of the computer, a total of 2,400 illegal images were recovered and produced as evidence. The quantity of material exceeded that required for indictments and so a representative sample was selected and the remainder of the material collated into what is termed a ‘roll-up’ charge. Following the initial prosecution report, a defence expert was engaged and a statement was produced. This introduced doubt about the provenance of the material recovered and suggested the material had come to be on the computer as a result of pop-ups during a normal browsing session.

The prosecution needed to establish the behaviour of the suspect around the time the incriminating files were created. On examination the computer was found to be running the Windows XP operating system. The Protected Storage area of the Registry was examined and ‘autocomplete’ data collected from web-based forms indicated that search terms associated with images of child sexual abuse had been used. Login details were also recovered for a number of password secured websites:

**Item:** http://xxx.xx.xx/:StringData

**Username:** <username>@talk21.com

**Password:** 3757121

**Item:** http://yyy.yy.yyy/:StringData

**Username:** <username>@talk21.com

**Password:** 3757121

**Item:** http://www.website.com/login/login.asp:StringData
Username: <username>@talk21.com
Password: 3757121

The ‘TypedURLs’ area of the Registry included the website <http://xxx.xx.xx> which was one of addresses found in the protected storage area of the registry with a username and password. This indicated that access to that particular web site was restricted and required the entry of a username and password or PIN number.

The internet cache was also recovered – this is an area created by a web browser (such as Internet Explorer) on the hard disk which in effect becomes a temporary storage area in which web pages (including embedded images) are stored as they are viewed. By examining the date and time the registry had been updated and then correlating it with the internet cache, it was possible to argue that the address had been manually entered moments before the page was rendered on the computer’s screen. To support this further the web page was extracted from the cache and reconstructed to show the court what would have been visible on the screen. The defence team had claimed the page was a ‘pop-up’, but it was in fact rendered following access through a login page.
To proceed beyond this screen, the user had to enter login credentials and press the ‘LOGIN’ button. Examination of the code ‘underneath’ this button showed that clicking the button would take the user to the URL <http://xxxxxxx-xxx.com/cgi-local/index.cgi?165158558;1031249585>.

The internet history entry immediately following the visit to the login page showed that the user was indeed taken to that URL, and the most likely explanation for this is that the user clicked the Login button. The date and time of this event (ie when the user logged in) correlated with the date and time the form-data was recorded in the registry. There were now two independent records of when the user logged into the web-site; the manual entry of data on the login form and the subsequent accessing of the URL.

It was then possible (again using the internet cache) to reconstruct the first page the user had accessed after the login process. It contained a number of links with names associated with different sexual activities. The internet
history showed that the user clicked on one of these within two seconds and was taken to a new page that contained further links to a number of video files.

The internet history also contained the following entry:

Visited: 17/09/2002 12:06:25 Tue
URL: http://xxxxx-xxx.com/cgi-local/videos2/video.cgi?raygolddance.mpeg

This showed that the user had then clicked on the raygolddance.mpg. Further examination of the internet history (in the temporary internet files location in the Registry) revealed numerous episodes
of browsing sessions over a period of time, and that the user had visited web-sites that appeared to contain images of child abuse.

The combination of manually typed URLs, the entering of credentials and the clicking on a sequence of links to eventually view a movie file on the screen together amount to activities that are not indicative of automated pop-up downloads. Furthermore, it was pointed out in the final report that there were 1,281 currently live indecent images and 1,199 located in unallocated areas, and that as the approximate size of the average picture was around 35Kb this amounted to approximately 84Mb of data in total. The computer was connected to the Internet via an ISDN connection which could run at maximum speed of 64Kb per second, and could therefore download no more than about 8Kb per second. To download all of the indecent images identified on the computer from the internet would have taken over three hours. The prosecution argued that this length of time is again not indicative of pop-ups, which by their nature are bursts of short-term unsolicited activity which are subsequently dismissed by a user. In light of the analysis presented in the prosecution’s response to the defence statement, the defence team withdrew their contention that the material that formed the indictment could have been produced as a result of pop-up activity. The defendant was found guilty and sentenced to a custodial term.

Analysis of USB-connected devices

As part of DFA, an investigator might need to test the hypothesis that a file located on a USB-connected device originated from a specific computer (or vice-versa). One of the ways of testing this would be to examine the records kept by Windows relating to the USB devices that have been plugged into the computer. When a USB device is plugged in for the first time a record is made of the date and time of the event, together with two codes representing the vendor and the product name of the device. Often the device serial number is recorded as well. By examining the original device in a forensically sound manner using specialist software (such as that produced by Nirsoft (2001)), this same information can be extracted from device itself, see Figure 12.
Figure 12: Examination of a USB device

Windows will also record the drive letter assigned to the USB device in the registry. This will allow the digital forensic investigator to create a timeline showing the insertion of a USB-connected device and user activity relating to files located on it.
Email forensics

As part of the DFA process a digital forensic investigator will often look for indications of communication between the suspect and other individuals (for example other suspects, or victims).

One such source of communication evidence is email. An email examination can also produce evidence of when and from whom a file was obtained, or demonstrate that it was distributed to a third party.

Broadly speaking, email evidence exists on a computer in two forms: multiple email messages stored within a single file (also known as a 'container' file, as used by Microsoft Outlook), or in multiple files (often the case for Web based email such as Yahoo or Hotmail). Emails in container files are typically stored in a similar way to how files are stored on a disk, so references are used internally to identify where each individual email is stored. The forensic practitioner is thus able to search not only for deleted email container files, but individually deleted emails within such files.

Email messages themselves can contain a wealth of information about their provenance. An examination of an email’s underlying code (the ‘header’) can provide clues to both the source and route taken by the message in its delivery, see figure 13.
Generally speaking, the path an email has taken can be determined by reading upwards the list of servers identified in the email header. The most reliable of this information is located at the top, where the recipient’s own email server is identified. (The further down the entry, the greater the risk that the email header has been fabricated.

Figure 1 above shows an email with the line (indicated by an arrow):

Received: from [219.108.113.213]

This is the recorded source Internet Protocol (IP) address of this email. On the internet an IP address functions much like a telephone number, with each address being allocated to an Internet Service Provider (ISP). Publicly available databases such as Centa1Ops (Hexillion 1997) can be interrogated to identify an organisation assigned to a particular IP address. The use of other online tools such as
ip-adress.com (2004) can provide an approximate geographical location of the email source as shown in figure 14. In this example the ISP is located in Japan.


**Figure 14: Tracking an IP address**

In the UK, powers granted by the Regulation of Investigatory Powers Act (2000) permit law enforcement bodies to approach the ISP and require them to provide details of the individual business or organisation using the IP address on the date and time in question.

**Social Network forensics**

Instant messaging (IM) software such as Windows Live Messenger or the IM facility in Facebook can leave a number of forensically useful artefacts on PCs (Van Dongen, 2007), and also on mobile phones (Husain & Sridhar, 2010) and smartphones. Images, sound recordings, video and chat logs may all be recoverable. Instant messaging allows users to conduct one-to-one conversations whereas
chat allows for many-to-many conversations. Many of the IM and chat programs available record the contents of each conversation between individuals by default, for example, Yahoo! Messenger for PC does this, unless the user has selected the option ‘Do not keep a record of my conversations’, (Yahoo, 2013). Typically, these records are stamped with a time and date and can support the hypothesis that one individual knew another, or even provide a confession of a crime, as in figure 15.
Messenger Plus! Chat Log
Session Start: 21 December 2000

[Chat log content]

Do u have CVV
No I'm out of the game

Hey

What's a CVV number?
It's a code on the back of your credit card.

I heard u could have 2 CVV numbers for each card. I think
It's the security code on the back of your credit card.

Do they ever lose it?
Yes, but they are closer to death for a while.

I'm out of the game.

I need to find it.

I need some 4-9 cvv like that.

Hey, do you have one in mind that I can use?

I need money but I don't want jail.

I can send a few dollars.

I have some contacts with Fed's here in India.

We'll get it to ya.

Don't happen again.

I will be.

That's great.

I'm in a cab right now.

Please give them some money.

Good night and that's the truth.

We do have any money?

I always get some things.

But now nothing.

So what a show

I'm not a show.

Stay safe.

I hope.

Alright do u have the US.

you want log in, password and pth for LIT.

u do have UK money

of course

I heard they screw box.

I need some money to pay my attorneys.

I've been suspended with many bogus

World trade Logins.

and

US PCs is down.

I got DVR not

kiosk

all are Commercial win's box.

so I'll log a screen if you need.

u can see it and you're

how much you need

TH&B

Moments.

I need to call and send a day

I have Wednesday to do this.

Please boxes.

send over TH&B boxes.

and u will give a screen to my ZRIS.

u can see it like you're.

Please box.

So you have ZRIS and you're broke

you

NOTES

how old are you

ST

I'm 40 and I own my own house, I own my own business and I don't owe anyone a thing.

All bought for cash.

Just TH&B is not a big thing for a

key phone will be a need in next phone.

Ok bye.

If u want to send me to LIT please.
Mobile Device Forensics

The situation for digital forensics for mobile phones is very different from that of the PC, mainly due to the fast paced changes in the mobile phone market. For example recent statistics suggest that in the first quarter of 2011, only three years after the first commercial Android handset was released, over 36,000,000 Android handsets were sold (Gartner, 2011). Mobile phones tend to have a shorter life than PCs and have a wider variety of OSs and architectures, and it is therefore difficult for manufacturers of forensic tools to keep pace with the fast changing technology.

Another difficulty is that mobile phones cannot be imaged in the same way as PC hard drive. It is possible to make an exact copy of a PC hard drive without changing data on it, but the data retrieval process for phones requires a two way communication with the device. This does not provide an exact copy of all data and can potentially alter data on the device, in apparent contravention of the UK’s recommended practice (ACPO’s first principle – see Chapter 7). The National Institute of Standards and Technology (NIST) in the US have produced guidelines on ‘Cell Phone Forensics’ (Special Publication 800-101). However, NIST explain that the guidelines do not prescribe how law enforcement should actually analyse mobile devices (Jansen and Ayers, 2007, p.1). Furthermore, due to the variety of handsets on the market the currently available forensic software it is not capable of examining the various types of devices, so investigators may have no choice other than to manually examine the device and photograph or video their findings (ACPO, 2012).

A decision will need to be made concerning the degree of DFA to conducted on a suspect’s mobile phone (in the UK reference is made to Levels 1 to 4). The examination could range from the relatively simple check of phone number against billing information to support
identification, to the much more complex, technically demanding and expensive removal and examination of on-board memory modules. The degree of analysis conducted is likely to depend on the seriousness of the alleged offence. There are also a number of ‘layers’ to a mobile phone that are forensically important. These are (Owen and Thomas, 2011, p. 136):

- the ‘hardware layer’ consisting of a processor chip (for example in the Samsung Galaxy S, the ARM Cortex-A8 CPU);
- the RAM;
- the ROM;
- antennae (such as GPS, wifi, Bluetooth) and other hardware for input and output of data;
- the Original Equipment Manufacturer (‘OEM’) layer (proprietary software of the manufacturer e.g. Apple) used for booting, configuration files; and
- the ‘application layer’ which includes internet browsers, word processing applications.

Once accessed much of the evidence on a mobile phone is similar to that on a PC. Just as with computers, phones can contain videos, images and documents, and of course they can also be used to browse the internet. Phones also have address books and call histories (Curran, 2010), and many have GPS capabilities which can be used to determine where they have been used. Removable SD cards are often used for data storage on phones, and these can be thought of in much the same way as PC hard drives. But other information is much harder to retrieve than on PCs, due to the variety of OSs used on mobile devices, and so on occasions it might be necessary to examine mobile data at the level of hexadecimal code.

The mobile phone network for the UK follows the GSM/UMTS standard which requires phones to have a SIM card. One important piece of information stored on the SIM card is the International Mobile Subscriber Identity (IMSI) which identifies the person or corporation that has an account with
the NSP (Willassen, 2003). This allows for portability of SIM between handsets (Jansen and Ayers, 2007) and handsets between SIMs. This is interesting forensically since a number of phones can be linked to the same person or group of people, thus potentially providing evidence of associations between individuals.

**When examining a phone**, a decision will have to be made on what to do first, since removal of the SIM card normally requires battery removal which can lead to the alteration of data on the device. Also a password or PIN number might be required for access when the machine is switched back on. Connection to a phone by cable is by far the most preferable method as it is more secure (ACPO, 2007), but wifi, Bluetooth, or infrared could also be used.

**Location data** is also available from mobile phones, and this may be used to determine suspects’ movements and help determine event timelines. It is possible to ascertain the location of Global Positioning System (GPS) enabled phones, although the accuracy depends on a number of factors including how well the phone ‘sees’ the satellites which send signals to the phone (the phone uses these to determine its location). An alternative location method is Cell Site Analysis which uses data about which cell phone mast the phone was connected to at a particular time (Denby, Oussar and Ahriz, 2008). Such data was used in the investigation of the 1998 car bomb attack in Omagh in Northern Ireland in the UK, which resulted in 31 deaths. A series of phones were linked to the incident using cell site data (Cormack, 2010).

Emerging technologies provide other ways to track phone locations, for example phones can act as carriers and readers in Radio Frequency Identification (RFID) systems. (RFID systems allow contactless communication between devices that carry data and readers; the Oyster cards and Oyster readers on London’s public transport systems work this way.) Location Based Services (LBS) can use RFID technology, for example particular adverts can be sent to a phone when it is in the vicinity of a shop selling the relevant product (Denby, Oussar and Ahriz, 2008), thus leaving a record of the phone’s location at a particular time. Near Field Communications (NFC) are very close range RFID communications for which the devices must be generally be no more than 20cm apart. It is expected
that NFC technology will become widespread in mobile phones and may lead to significant increases in the use of phones as payment devices (Finkenzeller & Müller, 2010). In the future, the data relating to such ‘touch payments’ could be used by investigators to retrospectively track the location of a particular phone.

Many aspects of the investigation of mobile phones can be automated using commercial tools such as Paraben’s device seizure, Radiotactics’ XRY, Oxygen’s Forensics Suite, AccessData’s FTK Phone Examiner and Guidance Software’s EnCase Neutrino/Smartphone Examiner. Some of these tools are exclusively software whereas others such as XRY include hardware for use in tasks such as cloning SIM cards.