

Forensics on the Windows Platform, Part Two

Jamie Morris 2003-02-11

Introduction

This is the second of a two-part series of articles discussing the use of computer forensics in the examination of Windows-based computers. In [Part One](#) we discussed the wider legal issues raised by computer forensics and the benefits of pre-investigation preparation. In this article we will concentrate on the areas of a Windows file system that are likely to be of most interest to forensic investigators and the software tools that can be used to carry out an investigation.

Imaging

The first step in the forensic examination of a computer hard drive is almost always the creation of a "bit level" copy, or *image*, which includes every bit of information on the disk regardless of whether or not it is part of an existing file system. The creation of this image serves to provide a platform that can be subjected to in-depth analysis without fear of altering the original evidence. A number of tools are commonly used by investigators to perform forensic imaging, the following are some of the most popular:

- **EnCase:** EnCase is a fully featured commercial software package that enables an investigator to image and examine data from hard disks, removable media, and some PDAs. This image can be analyzed in a variety of ways using the EnCase program, common examples of which might include searching the data for keywords, viewing picture files, or examining deleted files. Many law enforcement groups throughout the world use EnCase; this may be an important factor for investigators to consider if there is a possibility that an investigation may be handed over to the police or used in a court of law.
- **SafeBack:** SafeBack is another commercial computer forensics program commonly used by law enforcement agencies throughout the world. SafeBack is used primarily for imaging the hard disks of Intel-based computer systems and restoring these images to other hard disks. It is a DOS-based program that can be run from a floppy disk and is intended only for imaging; in other words, it does not include the analysis capabilities of EnCase or Vogon's forensic software.
- **Data dumper (dd):** Imaging a computer's hard disk can be a lengthy process but it need not be expensive. dd is a freely available utility for Unix systems that can make exact copies of disks that are suitable for forensic analysis. It is a command line tool and requires a sound knowledge of the command syntax to be used properly. Modified versions of dd intended specifically for use as a forensic utility are also available.

Once an image has been made, how do we know that it was made correctly? How can we be sure that the copy is exactly the same as the original? The answer lies with an algorithm called MD5. This procedure results in the creation of a large number called a "message digest", the exact value of which is determined by the layout of data found on a disk (MD5 can also be used to create message digests for files). Crucially, if the disk contents were to be altered in any way, through deleting or changing a file for example, running the MD5 algorithm would result in a radically different message digest. This is true regardless of the extent of the alterations made; even a change to one bit of information on a large drive packed with data would result in a new message digest. md5sum is a freely available utility for creating MD5 message digests and by comparing message digests of original disks and copies thereof, can be used in computer forensic examinations to ensure that an image made is an exact replica of the original.

Searching the system

Once an image has been made, the task of searching for evidence can begin. Some of the commercial imaging tools that provide imaging capabilities also provide comprehensive image analysis facilities; however, for those looking for a freely available open source alternative, [TASK](#) and [Autopsy](#) are highly recommended.

The remainder of this section details a number of places where investigators often look when examining a Windows computer system.

When a user logs on to a Windows 2000 or NT system for the first time a whole directory structure is created to hold that individual user's files and settings. This structure has a root directory that is given the same name as the username that was used to log on (which in itself can be useful forensic evidence) and contains a number of folders and files of interest to the forensic investigator. For example, the file NTUSER.DAT (which holds configuration information specific to the user and is located in the root of the user's directory structure) is updated when the user logs out, thus enabling an investigator to pinpoint this logout time by examining the file's "last written" attribute.

The Cookies folder, which is used to hold data files stored by Internet sites that have been visited by the user, is yet another potential source of information for the investigator. Together with the temporary Internet history files described below, a fairly detailed picture of a user's Web surfing activities can usually be developed. A number of small utilities are available that can help display the contents of a cookie in an easily readable form; one to try is [CookieView](#), which is downloadable from [Digital-Detective.co.uk](#).

Files created by Windows operating systems to facilitate quick access to applications, files or devices or certain files created by the operating system for a range of other purposes are often termed *windows artefacts* and can be another important source of information for investigators attempting to recreate a user's activities (partly because they are often overlooked by those attempting to cover their own tracks). Common examples are the .lnk files created in the Windows Desktop, Recent, Send To and Start Menu folders. These files act as handy shortcuts that enable the user to access frequently used files or applications with a minimum of effort.

Examining these files can help to uncover the previous existence of files, folders, applications or devices that are no longer present on the system. This can be useful when files have been deleted and are no longer recoverable or where files were stored on a network drive. Furthermore, where a link exists to another storage device such as a Zip or Jazz Drive this can be an important indication to the investigator that other media needs to be located and analysed.

Other windows artefacts that can prove useful in an investigation are temporary files created during the installation or use of an application. These files are often removed when an application closes or the computer shuts down, but if an application crashes this process may not take place, leaving behind evidence of which the user is unaware.

Some of the most useful files (depending on the nature of the investigation) can be those created by a user's Web browser. Analysis of these files, together with files from the Cookies folder, can provide a wealth of information regarding a user's surfing activities. [NetAnalysis](#), another tool available from the [Digital-Detective.co.uk](#) Web site mentioned above, is a great tool for examining a Windows machine for evidence related to Web surfing. This tool isn't free but is full of great features, easy to use and well supported.

Those engaged in unauthorised or illegal activity who use a computer to print documents may feel secure from detection if the documents are not saved to disk. However, even if the printed documents are only held in memory without being saved, it may still be possible to view the

printed documents by searching for the special files that are created by Windows during the printing process. These files, which have an .spl or .shd extension, contain a wealth of information about a print job, such as the name of the file printed, the owner of the file, the printer used, and the data to be printed (or a list of the temporary files containing such data).

Digging Deeper

Deleted Files

Many computer users believe that deleting a file, from within Windows Explorer for example, is enough to prevent that file from being accessed by others at a later date (especially if the "Recycle Bin" is also emptied). Fortunately for forensics investigators, the act of deleting a file in this fashion can still leave the data open to recovery. This is because when a file is deleted, the data itself is not removed from the system. Instead, the operating system simply marks the file as deleted and the area of the disk occupied by the file becomes available for storing other data. Until this area is overwritten, *the data belonging to the deleted file remains on the disk*. Using the appropriate forensic tools and methodology, this data can be recovered. Even in cases where the area of disk in question has been used to store data from another file, if the area occupied by the original file has not been completely overwritten it may still be possible to recover part of the deleted file.

If "deleted" data is still physically present on a system, how do we locate it? If we're lucky there may still be an operating system reference to its location, which we can use. In earlier Windows systems this may have been located in the File Allocation Table, in later systems within the Master File Table. If not, and we have some existing knowledge of what it is we are looking for, then the process of pattern matching can be used. Pattern matching can be used to search for occurrences of particular words or phrases (e.g. "drugs" or "firearms") or for file characteristics such as specific patterns at the start of a file known as "file headers" that identify particular file types.

The Recycle Bin

The Recycle Bin mentioned above, which is present on Windows operating systems, acts as a kind of halfway house for user-deleted files from which they may be undeleted by the user if required. The Recycle Bin is of great interest to forensic investigators because of a special file called INFO, or INFO2 on Windows 98 systems, which is used by the operating system to record details of files moved into the Recycle Bin. Amongst other details, the original location of files before they were deleted and the date and time of deletion are recorded in this file. When the Recycle Bin is emptied, this file is deleted along with the other files but, in exactly the same way as described above, it may still be possible to recover the file's contents if they have not been overwritten.

Sometimes the deletion of data takes place within an application other than a file manager, for example when deleting an email message from within an email client program. In these situations the ease of recovering the deleted data depends to a great extent on how it was stored within the application and what facilities, if any, are available for recovery. These facilities may be provided by the application vendor or, as is often the case, may be small utilities written by those working in the field of computer forensics.

In situations where a suspect no longer needs to gain access to a system and wants to hide some or all of the data contained therein they may be tempted to delete the partition and/or format the disk in an attempt to erase all stored data. However this is a fairly common misconception and whereas the act of deleting the partition or formatting the disk may indeed overwrite some areas of evidentiary value it will not destroy all previously existing data.

Users wishing to store data yet hide its true nature from others may do so in a number of different ways. One of the simplest is simply by changing the name and/or extension associated with a file. Thus a file called "naughty.jpg" might become "sales.txt" in an attempt to avoid suspicion. Whereas the part of the file name before the extension might yield few clues once changed, altering the file extension itself is detectable through a process known as signature analysis. In the same way that a particular type of file can be searched for based on its header, it is also possible to search for discrepancies between file headers and file extensions (that is, between what the file really is and what it claims to be). Where these two do not match, they may act as an indication to investigators that a more detailed analysis of the file is required.

Encryption

The use of encryption provides a different kind of challenge for the forensic investigator. Here, data recovery is only half the story, with the task of decryption providing a potentially greater obstacle to be overcome. Encryption, whether built in to an application or provided by a separate software package, comes in different types and strengths.

Some of the most commonly used applications provide encryption protected by passwords that can be readily defeated by investigators with the right tools and the time to use them. Other types of encryption, readily available to the general public, can be configured and used to create encrypted data that goes beyond the ability of the professional investigator to decrypt it using software. Nevertheless, in these cases it may still be possible to decrypt data by widening the scope of the investigation to include intelligence sources beyond the computer under investigation. For example, public key encryption can be used to create highly secure, encrypted data. To decrypt data encrypted in this fashion a private key and passphrase is needed. The private key may be found on the suspect's machine or backed up to removable media. Similarly, the passphrase may be recorded somewhere on the computer in case it is forgotten or may be written down somewhere and kept in a nearby location.

The Future

The practice of computer forensics differs from that of some other forensic disciplines in that it is not only the methodologies and tools that change over time but also, due to the pace of technological change in hardware and software, the underlying nature of the computer systems under investigation. The points raised above are intended to be of use to those thinking of carrying out a Windows investigation for the first time; but for those intending to embark upon a career in this field it is equally important to stress the value of being prepared for change. The lineage of the Windows family of operating systems clearly shows that each new generation comes equipped with a host of new features and capabilities. Unquestionably, those with less than honest intentions will use these advances in technology for their own ends. For those tasked with investigating hi-tech crime and misconduct, it is never too early to start preparing for the challenges ahead.

Jamie Morris is the owner of [Forensic Focus](#), a computer forensics news and discussion Web site.

Relevant Links

[Forensics on the Windows Platform, Part One](#)

Jamie Morris

[Privacy Statement](#)

Copyright 2006, SecurityFocus