Unit 2: Windows Forensics Analysis

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The process of Windows XP, Vista etc under forensics
- Forensic analysis of the NTFS Master file table
- Data access control and file deletion

1.2 INTRODUCTION

Despite the proliferation and growing popularity of other user interfaces, such as Macintosh OS X and Ubuntu (a flavor of Linux), Microsoft's Windows operating systems remain the most popular in the world. Sources have reported that over 90% of the computers in use today are running some version of the Windows operating system.1 This is not surprising given the almost endless variation that can be found in Windows products, their relative ease of use for the average computer owner, and the virtual stranglehold on marketing Microsoft has enjoyed for so many years (particularly before recent inroads by a resurgent Apple, Inc.). Microsoft operating systems have even found an audience in non-traditional quarters, as scores of Macintosh users have learned to use products like Apple's Boot Camp or Parallels virtualization software to run Windows on their Intel-based Macintosh hardware. Private users, Fortune 500 companies, and government agencies alike all overwhelmingly have chosen Windows systems as their primary technology infrastructures.[88]

In light of this, it should not be surprising that the majority of systems that digital investigators will be called upon to examine will be running a Windows operating system. The ease of use of Windows appeals to criminals and "evil-doers" the same as it does to the grandmother down the street. And both the longevity and popularity of Windows have made it a favorite target of virus authors, hackers, and industrial saboteurs. So, whether investigating child pornography, intellectual property theft, or Internet Relay Chat (IRC) bot infection, it is a safe bet that knowledge of Windows operating systems, and its associated artifacts, will aid investigators in their task.

1.3 WINDOWS XP

Windows XP has been a standard Microsoft OS for workstations for years. Since it hit the scene in 2001, millions of Windows users have grown comfortable with its user-friendly interface, comparatively efficient operation, and improvements over previous versions such as Windows 2000 and Windows ME. Windows XP comes in three primary editions (i.e., Home, Media Center, and Professional), which were targeted at different parts of Microsoft's work-station computing customers. From a file system standpoint, XP continues to run on top of the File

[88] Brill, A (2006b) The Brill files: An investigative report on data wiping utilities—Part two. Kroll Ontrack Newsletter, 4(6). Available online at <www.krollontrack.com/ newsletters/cccfn_0606.html>

Allocation Table (FAT) and New Technology File System (NTFS) structures with which examiners have grown familiar.[89]

There are many features in Windows XP that can be very useful for forensic examiners. Evidence of user actions is often recorded in areas (such as Internet history, Event logs, Prefetch files, thumbs.db files, and link files) that are easy to view for the trained digital investigator with the right tool. However, other challenges (such as analyzing restore points, analysis of data in the Windows registry, collection and analysis of memory, dealing with RAIDs and dynamic disks, overcoming Windows encryption, and documenting data destruction) can present a much greater challenge, even for more experienced digital investigators. Regardless of its utility, Microsoft stopped selling XP in 2008 but plans to continue support for this beloved Windows version until 2014, which means it will most likely be a big part of examiners' lives for many years to come.[90]

1.4 WINDOWS VISTA (AND RELATED SYSTEMS)

Windows Vista, which many still remember under its development code name of "Longhorn," was officially released in 2007 and, like XP before it, was intended by Microsoft to become the de facto OS for workstations. Vista, like XP (and the upcoming Windows 7), is available in multiple editions (i.e., Starter, Home Basic and Basic N, Home Premium, Business and Business N, Enterprise, and Ultimate), each with its capabilities and features; for example, Vista Home allows users to back up documents, and Vista Enterprise allows the creation of true-clone copies of the entire hard disk/partitions for later recovery or creation of identical systems.[91]

Also similar to XP, Vista, 2k8, and 7 take advantage of the NTFS file system and add the concept of Transactional NTFS (TxF). Implemented together with the Kernel Transaction Manager (KTM), TxF was designed to make NTFS more robust by treating file operations as transactions that can be rolled back or reapplied as necessary in the case of catastrophic system

[89] Geiger, M (2005). Evaluating commercial counter-forensic software. In Proceedings of DFRWS 2005. Available online at <www.dfrws.org/2005/proceedings/geiger_ counterforensics_slides.pdf>

[90] Grand, J, & Carrier, B (2004) A hardware-based memory acquisition procedure for digital investigations. Journal of Digital Investigation, 1(1), 1742–2876. Available online at <www.digitalevidence.org/papers/tribble-preprint.pdf>

[91] Hargreaves, C, Chivers, H, & Titheridge, D (2008) Windows Vista and digital investigations. Digital Investigation Journal, 5(1–2), 34–48

failure.[92] Most of Microsoft's official literature suggests that Vista cannot be installed and run on FAT32. However, although this may be true from a simplistic or tech support stand-point, there are several tips and tweaks that will allow Vista to be installed on a FAT32 partition, so it is possible the digital investigator could encounter such a scenario. Before Vista was released, it was thought it would be based on a new file system (WinFS) under development by Microsoft. However, shortly before Vista's release, problems in development caused Microsoft to shelve the new file system temporarily, leaving Vista to utilize NTFS as its primary base.

1.5 OVERVIEW OF NTFS

While the world waits for WinFS, most modern Windows workstations and servers are using the much more familiar NTFS. NTFS is an alternative to FAT file systems (e.g., FAT12, FAT16, FAT32) and can be utilized by Windows NT/2k/XP/2k3/Vista/2k8 operating systems. The current version is NTFS 3.1, which has been used in Windows XP and later OS releases. Among improvements in NTFS file systems are increased file size potential (roughly 16TB versus 4GB for FAT32), increased volume size potential (roughly 256TB versus 2TB for FAT32), and the recording of Last Accessed times (in Windows NT/2k/XP/2k3, and Vista/2k8/7 if enabled). In addition, NTFS uses a data structure called the Master File Table (MFT) and entries called index attributes instead of a file allocation table (FAT) and folder entries in order to make the access and organization of data more efficient. These and other key features of NTFS of interest to forensic examiners are covered in this section.[93]

The primary internal files that NTFS uses to track data sometimes referred to as metadata files. The presence of these internal files on a system being examined (or traces of these files in unallocated space) should indicate to an examiner that the system was formatted as NTFS. It general, the dates and times associated with these files are set when the files are first created on the volume and do not change over time with the use of the system. As such, the dates and times of these internal files (particularly the Created Date) can be used as an indication of when the

[92] Kessler, M. (2007). Maintaining Windows 2000 peak performance through defragmentation. Microsoft Technet. Available online at <http://technet.microsoft.com/en-us/library/ bb742585.aspx>

[93] Lee, R (2008) VISTA shadow volume forensics. SANS Computer Forensics and E-Discovery Blog. Available online at <http://sansforensics.wordpress.com/2008/10/10/shadowforensics/>

volume was last formatted as NTFS. All of these files have their function and can be analyzed to the nth degree, but a few of them can be very useful to the investigator.

In ***Johnson vs Wells Fargo,***[94] a U.S. District Court in Nevada heard a motion on behalf of a defendant alleging that the plaintiff in the case reformatted two hard disk drives possibly containing evidence that the plaintiff falsified documentation to support his claims. The defendant informed the plaintiff of the intent to compel production of the hard disk drives in September 2007; however, the defendant's "forensic computer expert" (the label applied to the defendant's digital investigator in court filings) concluded, upon examination of the system files on the reformatted hard disk drives, that one of the drives was reformatted a mere five days after the plaintiff was notified that he would be compelled to produce it, and the second drive was reformatted only 10 days later. As a result, the Court found that the plaintiff destroyed potential evidence, and a jury instruction adverse to the plaintiff was ordered in the case as a result of his actions.

1.6 DATA ACCESS CONTROL

One of the key features of NTFS is its increased security over FAT file systems. This security manifests itself in many ways, but perhaps the most noticeable is an access control list (ACL) that governs read-write-execute access to Windows files and folders.[95] Security descriptors stored in the $Secure file, an internal NTFS file that is three data streams, details ownership and access information for files and folders on the file system. This ownership and access information is often quite important to an examiner attempting to determine who had access to (or who is responsible for) a particular data object. For example, an examiner seeking a clue as to which user account was used to download a particular pornographic picture usually need only look at the picture's owner in NTFS.

Although these ownership and access values in the $Secure file can be interpreted manually, it is fairly complex and requires data from several different internal NTFS files, so it is far easier for examiners to use a third-party tool.

[94] *Johnson v Wells Fargo* 635 F 3d 401 (9th Cir) [2011]
[95] Malin, C, Casey, E, & Aquilina, J (2008) Malware forensics Syngress Media

1.7 FORENSIC ANALYSIS OF THE NTFS MASTER FILE TABLE (MFT)

$MFT RECORD BASICS

Each MFT record has its data structure, to include slack that occurs between the end of the last attribute in the record and the beginning of the subsequent MFT record. Decoding the data in the records can sometimes be tricky, and is normally handled by a forensic tool, but it can be done by hand in the absence of one of these tools or for validation purposes.[96]

In addition to data such as the file status flag described earlier, which resides in each record header (normally the first 56 bytes of the record in XP and later), MFT records are composed of attributes that each have a specific function and structure. Each attribute has its header, which (among other things) identifies the attribute and gives the size of the attribute. It is also useful to understand that these attributes can be resident (meaning, they exist within a given MFT record) or nonresident (meaning, they exist outside a given MFT record, elsewhere on the disk, and are referenced within the record). Among these attributes, the Standard Information Attribute (SIA), Filename Attribute (FNA), and Data Attribute can be most helpful from a forensic perspective.

DATA-TIME STAMP DIFFERENCES BETWEEN NTFS AND FAT

NTFS date-time stamps differ from those recorded on FAT systems in several key ways. First, it is important to note that NTFS and FAT date-time stamps do not reside in the same locations; whereas NTFS uses the $MFT as a primary repository for date and time metadata, FAT systems record dates and times within folder entries. Another major difference is that NTFS date-time stamps are recorded in UTC, regardless of the time zone set for the system, whereas FAT date-time stamps are recorded in local time; this distinction is important, particularly when interpreting the date-time stamps manually. In addition, NTFS represents date-time stamps using the FILETIME format, which represents the number of 100 nanosecond intervals since January

[96] Mueller, L. (2009). Detecting timestamp changing utilities. Professional Blog. Available online at <http://www.forensickb.com/2009/02/detecting-timestamp-changingutlities.html>

1, 1601, and can be interpreted by most forensic tools, including free tools such as DCode by Digital Detective.[97]

The FILETIME format is different from the DOSDATETIME that is primarily used in FAT, which is 4 bytes and starts on January 1, 1980. To confuse matters, on FAT systems the resolution of create time on FAT is 10 milliseconds (additional bytes are used to record hundredths of a second), whereas write time has a resolution of 2 seconds, and access time has a resolution of 1 day, allowing the examiner to be less specific about when a file or folder was last accessed on the file system (Microsoft, 2009a). Even within NTFS, the use of Last Accessed date-stamps can vary. For example, NTFS delays updates to the last access date-time stamps by up to 1 hour after the last access (Microsoft, 2009a).

DATA ATTRIBUTE

An MFT record's Data Attribute can be very important to examiners, chiefly because it contains either the actual data itself (resident) or a pointer to where the data resides on the disk (nonresident). A resident Data Attribute contains the actual data of the file referenced by the MFT record; this occurs when the data the file contains is relatively small in size (usually less than 600 bytes), so small text files (such as boot.ini or Internet cookies) are often held as resident files. For larger files, the MFT contains a list of the clusters allocated to that file, called data runs.

1.8 NTFS FILE DELETION

In the same vein, it is quickly worth mentioning what happens in NTFS when a file is deleted (as opposed to being sent to the Recycle Bin). When a file is deleted in NTFS, many different things happen "under the hood," but among the observable behaviors important to examiners are:

- The deleted file's entry is removed from its parent index, and the file system metadata (i.e., Last Written, Last Accessed, Entry Modified) for the file's parent folder are updated. It is also possible that the metadata for the deleted file itself may be updated because of how the user interacted with the file to delete it (e.g., right-click on the file).

[97] Park, B, Park, J, & Lee, S. (2008). Data concealment and detection in Microsoft Office 2007 files Journal of Digital Investigation, 5(3–4), 104–114

However, examiners should exercise caution before drawing any conclusions from the metadata of a deleted file without other supporting, or related evidence found elsewhere on the file system.

- The two bytes located at record offset 22 within the file's MFT record are changed from \x01\x00 (allocated file) to \x00\x00 (unallocated file).
- The appropriate locations in $Bitmap are modified to show that both the space occupied by the MFT record and space previously occupied by the file itself is now unallocated and ready for reuse.

A recent investigation focused on a government server, which was found to be beaconing out to another country. The start date of the beaconing traffic gave investigators an approximate date for the compromise of the victim machine, as they began developing their timeline. However, during the forensic examination of the compromised system, the source of the beaconing was found to be a piece of malware (keylogger) whose File Created date-time stamp (as displayed by several different forensic tools) predated the beginning of the beaconing by almost two years.[98] Investigators began to wonder if the system had been compromised much earlier than they originally thought. But, upon more detailed examination of the file's MFT record, and manual translation of the dates and times held in the FNA for the malware and associated files, investigators confirmed that the malware had most likely been created on the system at a date and time that very nearly matched the start of the beaconing traffic, confirming their original timeline. This discovery led to suspicion of SIA date-time stamp alteration on the part of the intruder and the location of a date-time stamp modification utility.

Evidence of file deletion (as opposed to destruction/wiping) by a particular user presents its own set of challenges, particularly since no specific program or utility is required to delete a file in Windows. Simply sending a file to the Recycle Bin is not (by the most common forensic definition) actual deletion of the file; however, a user sending a file to the Recycle Bin is often viewed as legally significant in a case where the user was supposed to be preserving or protecting data. Further, a file in the Recycle Bin is usually easy to identify, and data provided by INFO2 records or $I files (Vista/7 Recycle Bin operation) can help the investigator pinpoint

[98] Parsonage, H (2008). The forensic recovery of instant messages from MSN Messenger and Windows Live Messenger. Available online at <http://computerforensics.parsonage. co.uk/downloads/MSNandLiveMessengerArtefactsOfConversations.pdf>

where the file was when it was deleted, as well as when the data was sent to the Bin and by which user account. Even if the Recycle Bin is empty, looking at the Last Written date-time stamp on the associated INFO2 record can provide the investigator with valuable data about the approximate time the Recycle Bin was cleared.

Forensic examiners can often recover data and associated metadata for deleted files, even when Recycle Bin information is not available. In particular, when dealing with NTFS, a recovered MFT entry can provide all the information a forensic examiner needs about deleted data. For digital investigators, knowing the mechanics is often a far cry from knowing who deleted the file and when. Most forensic suites have the ability to identify deleted and partially overwritten files, distinguishing them via different icons or information in the files' descriptions.

DETERMINING TIME OF DELETION

A common mistake that forensic examiners can make is to assume that the Last Accessed date-time stamps of deleted files show when the files were deleted. Although it may seem logical in theory that a file would be accessed at the time, it was deleted, this is not always true. For instance, deleting an entire folder does not update the Last Accessed date-time stamp of the files it contains (try it!). As another example, when a user causes Internet Explorer to clear the Temporary Internet Files (e.g., Tools→Delete Browsing History…→Delete Files…, in Internet Explorer 7), it does not update the Last Accessed dates of the files. Without other supporting evidence, the only statement an examiner can safely make about a deleted file based solely on its Last Accessed date-time stamp is that it was not deleted prior to the date indicated by that piece of metadata.[99]

Determining who deleted the file can be even more difficult and often has to be obliquely proven by attempting to correlate system usage data (such as logged on users, etc.) with the last date-time stamps on the deleted file. A determination regarding who deleted a file can also be circumstantially supported by file permissions data (file owner, who has deletion rights, etc.), clues from the location of the deleted file (e.g., c:\Documents and Settings\<username>\My Documents), and link files and MRU registry data that pointed to the data in its active state, but

[99] Mueller, L (2008) Incident response—Recovering a BitLocker recovery password before system shutdown. Professional Blog Available online at <www.forensickb.com/2008/01/ incident-response-recovering-bitlocker.html>

the investigator must correlate and weigh each piece of evidence carefully before opining on the source of a file's deletion.

1.9 LET'S SUM UP

In this chapter, we studied the concept of Windows XP, Vista etc and the process of forensics with respect to it. We also discussed the new technology file system and data access control. Finally, we ended the discussion with forensic analysis of the NTFS MFT and the process of file deletion.

1.10 FURTHER READING

- Carrier, B. (2005). File system forensic analysis. Addison-Wesley.
- Dickson M. (2006). An examination into MSN Messenger 7.5 contact identification. Journal of Digital Investigation, 3(2), 79–83.
- Carvey, H. (2009). Windows forensic analysis (2nd ed.). Syngress Media.
- Geiger, M. (2005). Evaluating commercial counter-forensic software. In Proceedings of DFRWS 2005. Available online at www.dfrws.org/2005/proceedings/geiger_counterforensics_slides.pdf
- Hargreaves, C., Chivers, H., & Titheridge, D. (2008). Windows Vista and digital investigations. Digital Investigation Journal, 5(1–2), 34–48.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) **How are the evidence gathered by the examiners in Windows XP?**

There are many features in Windows XP that can be very useful for forensic examiners. Evidence of user actions is often recorded in areas (such as Internet history, Event logs, Prefetch files, thumbs.db files, and link files) that are easy to view for the trained digital investigator with the right tool.

2) **What is the key feature of NTFS?**

One of the key features of NTFS is its increased security over FAT file systems. This security manifests itself in many ways, but perhaps the most noticeable is an access control list (ACL) that governs read-write-execute access to Windows files and folders. Security descriptors stored in the $Secure file, an internal NTFS file that is three data streams, details ownership and access information for files and folders on the file system.

3) What is the process post deletion of files in NTFS?

When a file is deleted in NTFS, many different things happen "under the hood," but among the observable behaviors important to examiners are:

- The deleted file's entry is removed from its parent index, and the file system metadata (i.e., Last Written, Last Accessed, Entry Modified) for the file's parent folder are updated. It is also possible that the metadata for the deleted file itself may be updated because of how the user interacted with the file in order to delete it (e.g., right-click on the file). However, examiners should exercise caution before drawing any conclusions from the metadata of a deleted file without other supporting, or related evidence found elsewhere on the file system.
- The two bytes located at record offset 22 within the file's MFT record are changed from \x01\x00 (allocated file) to \x00\x00 (unallocated file).
- The appropriate locations in $Bitmap are modified to show that both the space occupied by the MFT record and space previously occupied by the file itself sis now unallocated and ready for reuse.

1.12 ACTIVITY

Explain the concept of forensic analysis in Windows XP, Vista and 7 along with the process of deletion of files in NTFS and the process of post deletion? Briefly explain the same with a relevant case study in the present era? (1000 words)