CHAPTER

Windows system artifacts 5

"You see, but you do not observe. The distinction is clear."
—Sherlock Holmes in *A Scandal in Bohemia*

INFORMATION IN THIS CHAPTER:

- Finding Deleted Data
- Hibernation Files
- Examining the Windows Registry
- Print Spooling Evidence
- Recycle Bin Operation
- Metadata: What It Is and How It's Used
- Thumbnail Images as Evidence
- Most Recently Used Lists: How They're Created and Their Forensic Value
- Working with Restore Points and Shadow Copies
- Examining Prefetch and Link Files

INTRODUCTION

Many say that the eyes are the window to the soul, but, for the forensic examiner, Windows can be the "soul" of the computer. The odds are high that examiners will encounter the Windows operating system more times than not when conducting an investigation. The good news for us is that we can use Windows itself as a tool to recover data and track the footprints left behind by the user. Because of this, it is imperative that examiners have an extensive understanding of the Windows operating system and all of its functions.

Love it or hate it, it's a Windows world. With Windows holding about 90% of the desktop market share (Brodkin, 2011), a forensic examiner will face a Windows machine the majority of the time. Getting cozy with Windows is an absolute necessity in this line of work. In the course of using Windows and its multitude of compatible applications, users will leave artifacts or footprints scattered throughout a machine. As you can imagine, this is pretty handy from an investigative perspective. These artifacts are often located in unfamiliar or "hard to reach" places. Even savvy individuals who are bent on covering their tracks can miss some of these buried forensic treasures.

Copyright © 2015 Elsevier Inc. All rights reserved.

The forensic challenge is to identify, preserve, collect, and interpret this evidence correctly. In this chapter, we'll take a closer look at many of these artifacts, their purpose, and their forensic significance.

DELETED DATA

For the average user, hitting the Delete key provides a satisfying sense of security. With the click of a mouse, we think our data are forever obliterated, never again to see the light of day. Think again. We know from Chapter Two that, contrary to what many folks believe, hitting the Delete key doesn't do anything to the data itself. The file hasn't gone anywhere. "Deleting" a file only tells the computer that the space occupied by that file is available if the computer needs it. The deleted data will remain until another file is written over it. This can take quite some time, if it's done at all.

MORE ADVANCED

FILE CARVING

The unallocated space on a hard drive can contain valuable evidence. Extracting this data is no simple task. The process is known as file carving and can be done manually or with the help of a tool. As you might imagine, tools can greatly speed up the process. Files are identified in the unallocated space by certain unique characteristics. File headers and footers are common examples of these characteristics or signatures. Headers and footers can be used to identify the file as well as mark its beginning and end.

Allocated space refers to the data that the computer is using and keeping tabs on. These are all the files that we can see and open in Windows. The computer's file system monitors these files and records a variety of information about them. For example, the file system tracks and records the date and time a particular file was last modified, accessed, and created. We'll revisit this kind of information when we talk about metadata later in this chapter.

HIBERNATION FILE (HIBERFILE.SYS)

Computers sometimes need their rest and can nap just like we do. Generally, a computer can go into three different modes or states when it sleeps. Those modes are: sleep, hibernation, and hybrid sleep. (Microsoft Corporation). The different modes are intended to conserve power and can vary from laptop to desktop. Through this "cybernap" process, more potential evidence can be generated, depending on how "deeply" the PC goes to sleep. "Deep sleep" modes such as hibernation and hybrid sleep save data to the hard drive as opposed to just holding it in RAM as in "sleep." As we know, data written to the drive itself are more persistent and can be recovered. It's possible that files deleted by a suspect could still be found here. How?

Let's say that the suspect is working on an incriminating document on Monday. She has to step away for awhile to make a phone call. She puts the laptop into hibernation mode, which causes the computer to save everything she is doing to the hard drive. When she returns 45 minutes later and brings the laptop back up, everything is just as she left it, including the incriminating document.

SLEEP

Sleep mode is intended to conserve energy but is also intended to get the computer back into operation as quickly as possible. Microsoft compares this state to "pausing a DVD player" (Microsoft, 2011; TechTarget, 2011). Here, a small amount of power is continuously applied to RAM, keeping those data intact. Remember, RAM is considered volatile memory, meaning that the data disappear when power is removed. Sleep mode doesn't do much for us forensically because all the data remain in RAM.

HIBERNATION

Hibernation is also a power-saving mode but is intended for laptops rather than desktop computers. It is here that we start to see some potential investigative benefit. In this mode, all of the data in RAM are written to the hard drive, where, as we know, it is much harder to get rid of data.

HYBRID SLEEP

As the name implies, hybrid sleep is a blend of the previous two modes and is intended mainly for desktops. It keeps a minimal amount of power applied to your RAM (preserving your data and applications) and writes the data to disk.

As with a page file, suspects bent on destroying evidence can overlook these hibernation files. Pedophiles or corporate crooks will often attempt to avoid detection by deleting or destroying evidence on their hard drives as investigations close in around them. These hibernation files, unknown to most users, are often missed during these last-minute "delete-a-thons."

REGISTRY

The Windows registry plays a crucial role in the operation of a PC. Microsoft's TechNet defines the registry as "simply a database for configuration files" (TechTarget, 2011). You could also describe it as the computer's central nervous system. In that context, you can see just how critical the registry is to the Windows computer.

The registry keeps track of user and system configuration and preferences, which is no simple task. From a forensic standpoint, it can provide an abundance of potential evidence. Many of the artifacts we look for are kept in the registry. Some of the potential evidence could include search terms, programs that were run or installed,

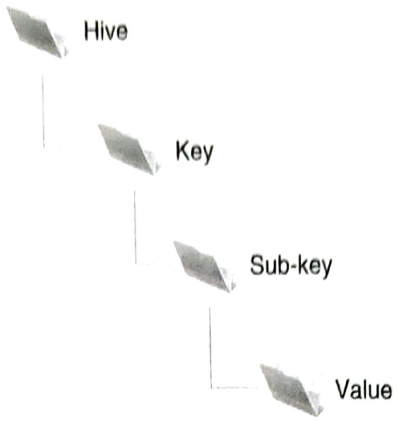

FIGURE 5.1

The Basic Structure of the Windows Registry.

web addresses, files that have been recently opened, and so on. As an added bonus, the registry can also hold the information we need to break any encrypted files we find.

REGISTRY STRUCTURE

The registry is set up in a tree structure similar to the directories, folders, and files you're used to working with in Windows. The registry is broken down into hives, keys, subkeys, and values. See Figure 5.1.

The Windows registry is comprised of five root-level keys. Each of these five bears the prefix of HKEY. Figure 5.2 shows these keys as seen through Regedit, the built-in registry editor in Windows. The five keys are classified as either derived or

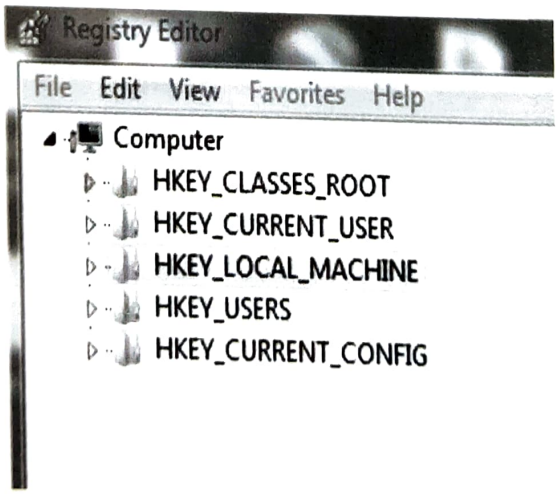

FIGURE 5.2

The Five Root-Level Keys as Seen in Regedit.

Table 5.1 The Five Root-Level Keys.

Key	Derived/Master	Brief Description
HKEY_CLASSES_ROOT	Derived	Links file types with programs (i.e., .doc file with Microsoft Word).
HKEY_CURRENT_USER	Derived	Configures the computing environment for individual users.
HKEY_CURRENT_CONFIG	Derived	Addresses the current hardware configuration.
HKEY_LOCAL_MACHINE	Master	Addresses all aspects of the computer's operation.
HKEY_USERS	Master	Computing environment settings for users that have logged on to the system.

master keys. If the key is derived, it's linked to the two master keys. Table 5.1 lists the five root-level keys along with a few details of each.

Inspecting the registry is done in nearly every forensic examination. Looking at the registry requires a tool that can translate this information into something we can understand. Two of the major multipurpose forensic tools, EnCase and FTK, do just that. FTK parses the registry for us, providing quite a bit of information. In addition, a separate application comes with FTK that is specific to the Windows registry. We can export registry files into Registry Viewer for a closer look (Figure 5.3).

As we've discussed, the registry holds quite a bit of information. Not all of it, however, will have any forensic value. A very handy feature in Registry Viewer is the ability to reduce the "noise" and show us only those areas that normally have some investigative significance. Registry Viewer calls these Common Areas and are displayed with the click of one button. Figure 5.4 shows us the software key with the Common Areas selected.

From the case files: the Windows registry

The Windows Registry helped law enforcement officials in Houston, Texas, crack a credit card case. In this case, the suspect's stolen credit card numbers were used to purchase items from the Internet. The two suspects in this case, a married couple, were arrested after a controlled drop of merchandise ordered from the Internet. Examination of their computer's NTUSER.DAT, Registry, and Protected Storage System Provider information found a listing of multiple other names, addresses, and credit card numbers that were being used online to purchase items. After further research, investigators discovered that these also were being used illegally without the owners' consent.

The information recovered from the registry was enough to obtain additional search warrants. These extra searches netted the arrest of twenty-two individuals and led to the recovery of more than (100,000 in illegally purchased merchandise. Ultimately, all of the suspects pleaded guilty to organized crime charges and were sentenced to jail time.

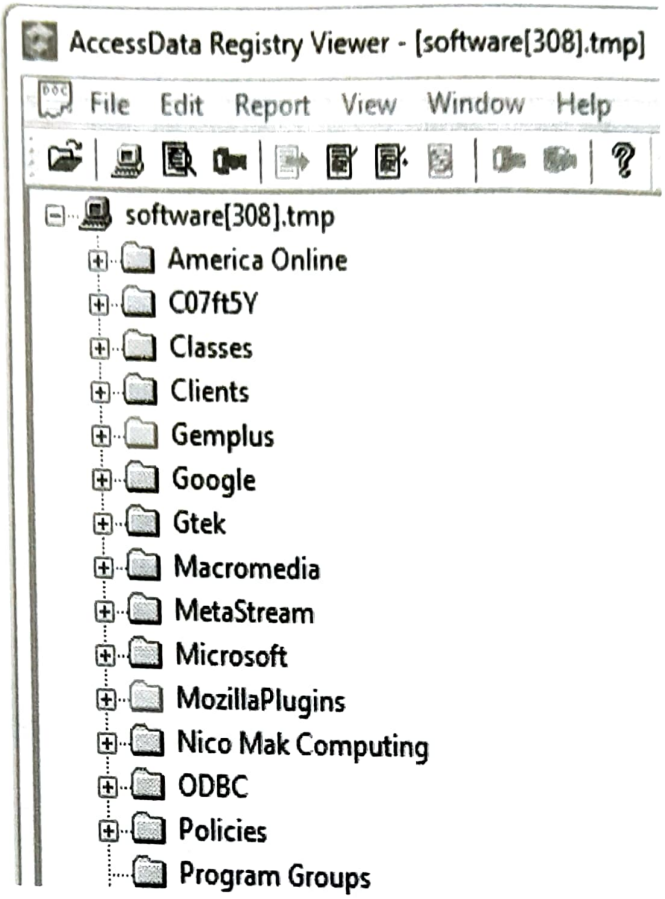

FIGURE 5.3

The Software Key in Access Data's Registry Viewer.

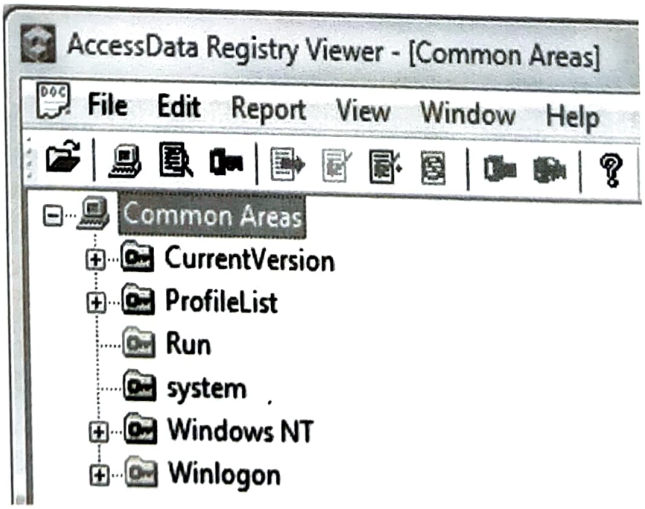

FIGURE 5.4

The Common Areas of the Software key in Access Data's Registry Viewer.

From the case files: the Windows registry and USBStor

In a small town outside Austin, Texas, guests at a local hotel called police after observing an individual at the hotel who was roaming around, mostly naked and appearing somewhat intoxicated. When the police arrived, they found the individual and determined that he was staying at the hotel. They accompanied him back to his room and were surprised by what they found. When the door opened, they discovered another individual in the room and a picture of child pornography being projected on the wall. The projector was attached to a laptop. Two external hard drives were found lying next to the laptop. The unexpected occupant said that the laptop was his but that the two external drives belonged to the other man and had never been connected to his laptop. All of the equipment was seized and sent for examination. Forensic clones were made of the laptop and both external drives. The initial examination of the external drives found both still images and movies of child pornography.

Next, examiners wanted to determine whether either of those drives had ever been connected to the laptop. The system registry file of the laptop was searched for entries in the USBStor key. Listings for external hard drives were discovered along with the hardware serial numbers from both external hard drives.

Next, examiners sought to validate their results. Using a lab computer system with a clean installation of Windows, they connected the defendants' external drives to the lab system. A write blocker was connected between the drives and the system to prevent any changes or modifications to the clones of the external drives.

The lab computer's system registry file was then examined and the USBStor keys showed the same external hard drive listings as the suspect's, with matching hardware serial numbers. These results proved that the suspect's external hard drives had, in fact, been connected to the laptop at one time. The suspect was eventually convicted of possession of child pornography.

ATTRIBUTION

Digital forensics can be used to answer many questions, such as "What terms were searched using Google?" We can find that. "Did Bob type those terms?" Houston, we've got a problem. Unfortunately, we can rarely put someone's sticky fingers on the keyboard when a particular artifact is created. We may need to uncover other evidence to connect those dots.

Tracking something back to a specific user account or identifying the registered owner of the system is a much easier task. A single PC can have multiple user accounts on the machine. In a technical sense, user accounts establish what that specific user can and can't do on the computer (Microsoft, 2011d). A PC will set up two accounts by default: the administrator and a guest account. Other accounts may be created, but they are not required. The administrator has all rights and privileges on the machine. The administrator can do anything with the machine. A guest account (which doesn't require any login) generally has less authority.

For example, a family PC could have separate accounts for Mom, Dad, and each of the kids. Each of these accounts could be password-protected.

Each account on the machine is assigned a unique number called a security identifier (SID). Many actions on the computer are associated with, and tracked by, a specific SID. It's through the SID that we can tie an account to some particular action or event.

EXTERNAL DRIVES

Information has value—sometimes substantial value. The Coca-Cola Company doesn't keep the formula for Coke under lock and key for grins. Theft of intellectual property is a huge concern. One way that would-be thieves could easily smuggle data out of an organization is by way of one of these external storage devices, such as a thumb drive. As a result, examiners are often asked to determine whether any such device has been attached to a computer.

These devices can take a variety forms, such as thumb drives or external hard drives. In addition to stealing information, these devices can also be used to inject a virus or store child pornography. Whether such a device was attached can be determined by data in the registry. The registry records this kind of information with a significant amount of detail, including both the vendor and the serial number of the device.

PRINT SPOOLING

In some investigations, a suspect's printing activities may be relevant. As you might expect, printing can also leave some tracks for us to follow. You've probably noticed that there's a bit of a delay after you click Print. This delay is an indication of a process called spooling. Essentially, spooling temporarily stores the print job until it can be printed at a time that is more convenient for the printer (TechTarget, 2011). During this spooling procedure, Windows creates a pair of complementary files. One is the Enhanced Meta File (EMF), which is an image of document to be printed. The other is the spool file, which contains information about the print job itself.

There is one of each for every print job. What kind of information can we recover from the spool file? The spool file (.spl) tells us things like the printer name, computer name, and the user account that sent the job to the printer. Either or both of these files may have evidentiary value. The problem is they don't stick around long. In fact, they are normally deleted automatically after the print job is finished. However, there are a few exceptions.

The first exception occurs if there is some kind of problem and the document didn't print. The second is that the computer that is initiating the print job may be set up to retain a copy. Some companies may find this setup appealing if they have some reason to hang onto a copy.

Spool and EMF files can be used to directly connect targets to their crimes. Copies of extortion letters, forged contracts, stolen client lists, and maps to body dump sites are but a few pieces of evidentiary gold potentially mined from their computers.

RECYCLE BIN

The trash can has been a familiar presence on computer desktops starting with the early Macintosh systems. It's a really good idea, especially from the casual user's perspective. Users may not understand sectors and bytes, but most everyone "gets" the trash can. Sometimes, though, the trash can "gets" them. This is especially true when they count on the trash can to erase their evidence. They assume that their incriminating data have disappeared into a digital "Bermuda Triangle," never again to see the light of day. Unlike Amelia Earhart, that's definitely not the case. Using forensic tools such as Forensic Toolkit and EnCase, we can quite often bring those files back in mint condition.

ALERT!

RECYCLE BIN FUNCTION

Here's a quick question. Where is a file moved when it's deleted? I bet some of you said the Recycle Bin. That would make the most sense. I mean, that's where we put the unwanted files, right? But it would also be wrong. When you delete a file, it's moved to … wait for it … nowhere. The file itself stays exactly where it was. It's a common notion that, when deleted, the file is actually picked up and moved to the Recycle Bin. That's not the case.

Unwanted files can be moved to the Recycle Bin a few different ways. They can be moved from a menu item or by dragging and dropping the file to the Recycle Bin. Finally, you can right-click on an item and choose Delete. The benefit of putting files into the Recycle Bin is that we can dig through it and pull files back out. I've worked in places where digging through an actual office trash can be a pretty hazardous undertaking. Fortunately, things aren't nearly as dicey on our computers. As long as our files are still "in the can," we can get them back. However, emptying the Recycle Bin (i.e., "taking out the trash") makes recovery pretty much impossible for the average user.

Not everything that's deleted passes through the Recycle Bin. A user can actually bypass the bin altogether. Bypassing can be done in a couple of ways. First, if you press Shift+Delete, the file will go straight to unallocated space without ever going through the Recycle Bin. You can also configure your machine to bypass the Recycle Bin altogether. Your deleted files won't even brush the sides of the Recycle Bin.

The Recycle Bin is obviously one of the first places where examiners look for potential evidence. The first instinct suspects have is to get rid of any and every

incriminating file on their computers. Not fully understanding how their computers work, they put all their faith in the Recycle Bin. Now you know that's a bad move. Lucky for us, many folks still don't recognize how misplaced their faith is. As a result, the Recycle Bin is a great place to look for all kinds of potentially incriminating files.

MORE ADVANCED

RECYCLE BIN BYPASS

If an examiner suspects that the system has been set to bypass the recycle bin, the first thing they would check would be the registry. The "NukeOnDelete" value would be set to "1" indicating that this function had been switched on. (See Figure 5.5.)

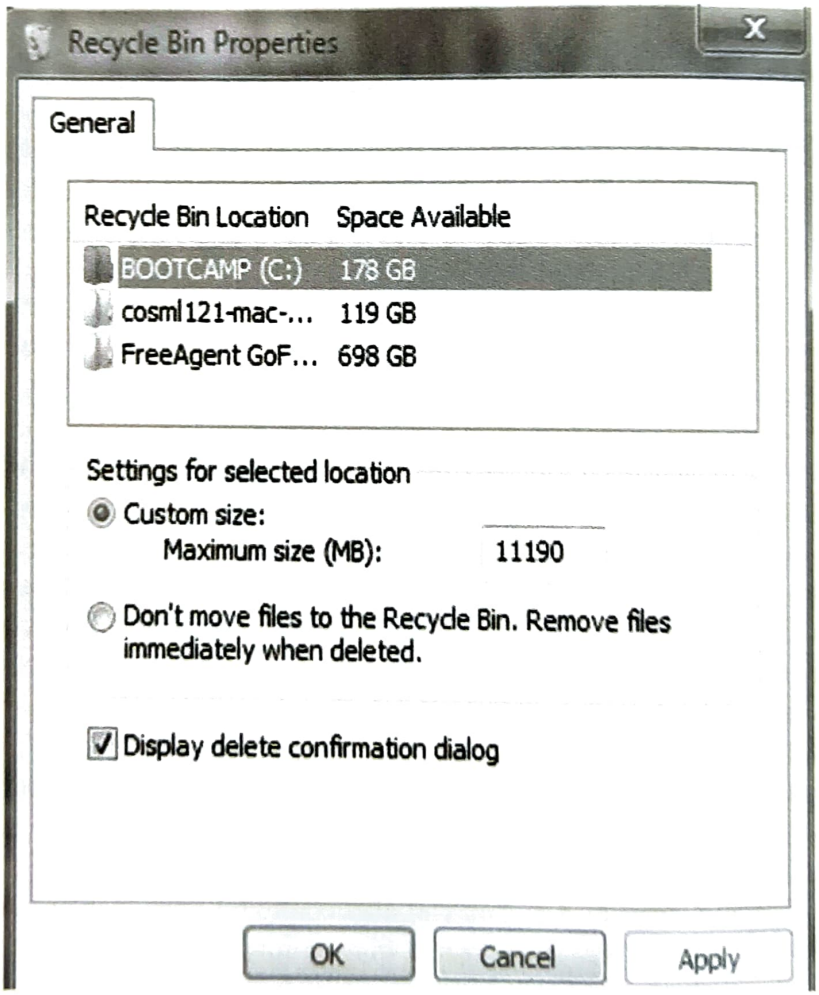

FIGURE 5.5

The recycle bin bypass option.

METADATA

Metadata is most often defined as data about data. Odds are you've come across metadata at some point, although you may not have known that's what you were looking at. There are two flavors of metadata, if you will: application and file system. Remember, the file system keeps track of our files and folders, as well as some information about them. File system metadata include the date and time a file or folder was created, accessed, or modified. If you right-click on a file and choose "Properties," you can see these date/time stamps as shown in Figure 5.6.

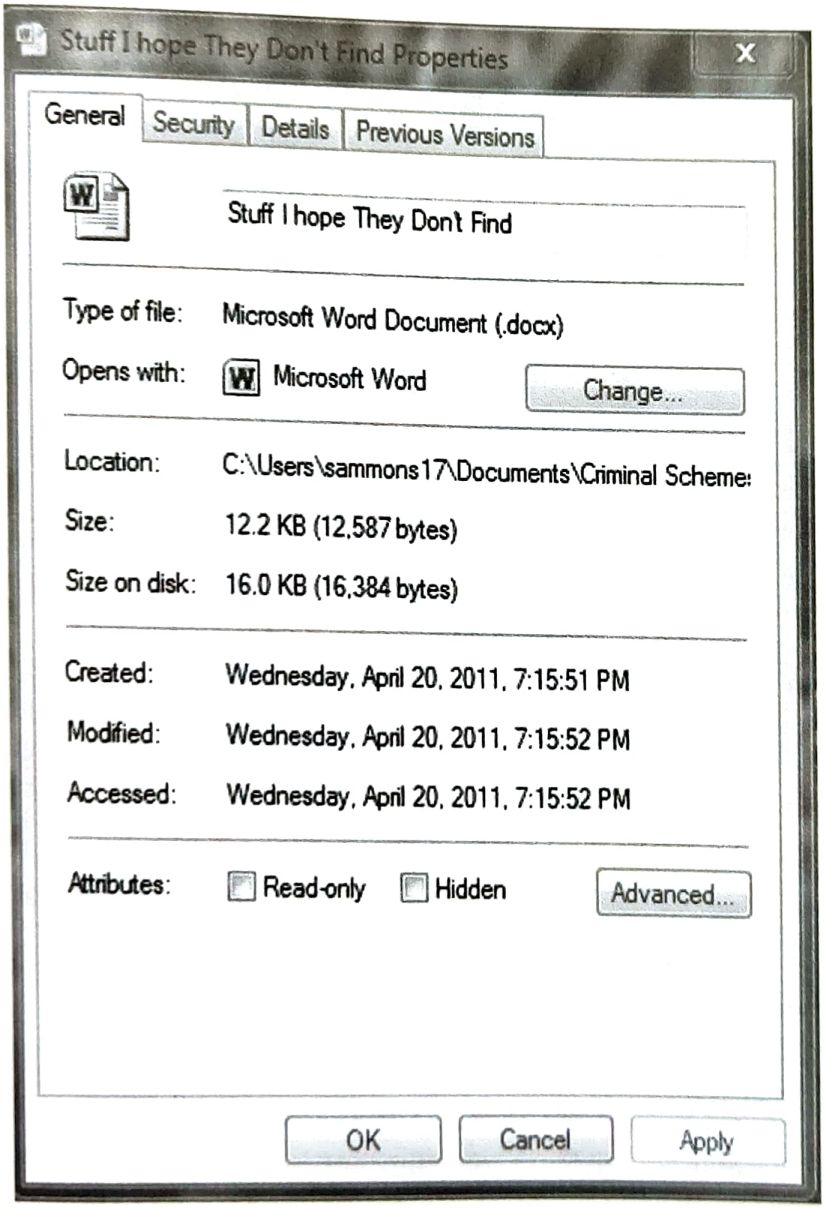

FIGURE 5.6

Metadata information as seen after right-clicking on the file and choosing "Properties." Note the created, modified, and accessed dates and times.

Although this information can prove quite valuable to an investigation, we must keep in mind that all these date/time stamps may not be what they seem. One problem is that the system's clock can be changed by the user. Time zone differences can also cause some issues. Let's take a little closer look at the created, accessed, and modified date/time stamps.

Created—The created date/time stamp frequently indicates when a file or folder was created on a particular piece of media, such as a hard drive (Casey, 2009). How the file got there makes a difference. By and large, a file can be saved, copied, cut and pasted, or dragged and dropped.

Modified—The modified date and time are set when a file is altered in any way and then saved (Casey, 2009).

Accessed—This date/time stamp is updated whenever a file is accessed by the file system. "Accessed" does not mean the same thing as "opened." You may be asking how a file can be accessed without being opened, and that's a good question. You see, the computer itself can interact with the files. Antivirus scans and other preset events are just two examples of this automated interaction.

ALERT!

DATE AND TIME STAMPS

System date and time stamps should *not* be taken simply at face value. These settings are readily accessible and can be easily changed. Determining an accurate timeline can be further complicated if the case involves more than one time zone. Just because the metadata say a file was created at a certain date and time doesn't necessarily make it so.

Applications themselves can create and store metadata as well. Like the file system, they can track the created, accessed, and modified dates and times. But it doesn't stop there. They can also track a variety of application-specific attributes as well. Examples could include the name of the author, the name of the company or organization, and the computer name, just to "name" a few (Casey, 2009).

REMOVING METADATA

Although metadata used to be one of our best-kept secrets, it's not any more. The criminals aren't the only ones taking notice. Corporations, law firms, and private citizens are just some of the folks concerned about metadata and the information contained therein. These legitimate concerns are being addressed by actually removing the metadata before sharing those files with other people. Many tools exist for just that purpose. For example, law firms routinely scrub the metadata from all of their outbound documents, like those transmitted via e-mail. For the privacy-minded individual, the newer versions of Microsoft Word have the ability to detect and remove metadata. (See Figures 5.7 and 5.8.)

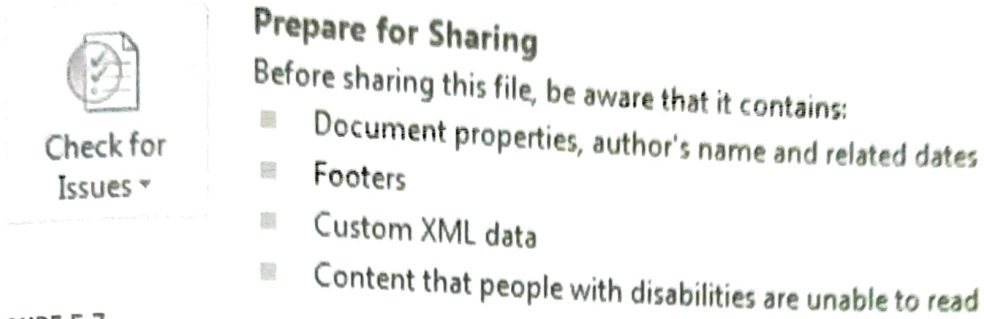

FIGURE 5.7

Menu item to choose for scrubbing inside Microsoft Word 2010.

Recovered metadata can be used to refute claims by a suspect that they had no knowledge of a file's existence. It's tough to claim you didn't know it was there when you not only opened the file but you changed or deleted the file as well. These dates and times can also be used to construct timelines in a case.

From the case files: metadata

Metadata can help investigators identify all the suspects in a case and recover more evidence. Take the case from Houston, Texas, regarding the production of counterfeit credit cards. The suspects in this case used "skimmed" card information in their card production process. Credit card skimming is when thieves grab the data from the magnetic strip on the backs of credit and debit cards. This often occurs during a legitimate transaction, such as when you use your card to pay for dinner at a restaurant.

After identifying their prime suspect, police arrested him and searched his computer. In the end, the search of the computer was disappointing. The search found one only Microsoft Word document that contained skimmed information. Furthermore, the search of the residence found no skimmer hardware and there was no skimming software on the computer. Not exactly the treasure trove they had hoped to find.

The exam didn't stop there. Further examination of the Word document hit pay dirt. A review of the metadata revealed the author of the document—a female. Further investigation found that she was the suspect's girlfriend and that she worked as a waitress in a neighboring town. This information gave investigators the probable cause needed to obtain a second search warrant for her apartment. During the second search, the skimmer (the piece of hardware used to extract the data from the

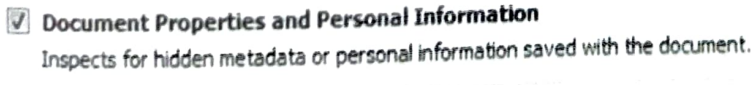

FIGURE 5.8

The option to scan for metadata in Microsoft Word 2010.

magnetic strip) was recovered. The examination of the computer found not only the skimming software, but additional lists of debit cards and related information. Fortunately, this information was seized before it could be used. Both suspects were eventually found guilty. Sammons, personal communication, 2011.

THUMBNAIL CACHE

To make it easier to browse the pictures on your computer, Windows creates smaller versions of your photos called thumbnails. Thumbnails are just miniaturized versions of their larger counterparts. These miniatures are created automatically by Windows when the user chooses "Thumbnail" view in using Windows Explorer. Windows creates a couple of different kinds of thumbnail files, depending on the version being used. Windows XP creates a file called thumbs.db. Microsoft Vista and Windows 7 create a similar file called thumbcache.db.

Most users are completely unaware that these files even exist. The cool thing about these files is that they remain even after the original images have been deleted. Even if we don't recover the original image, thumbnails can serve as the next best evidence. Their mere existence tells us that those pictures existed at one point on the system.

MOST RECENTLY USED

Windows tries to make our lives, at least on our computers, as pleasant as possible. They may not always succeed, but their hearts are in the right place. The Most Recently Used (MRU) list is one such example of Microsoft thinking of us. The MRUs are links that serve as shortcuts to applications or files that have recently been used. You can see these in action by clicking on the Windows Start button through the File menu in many applications. (See Figure 5.9.)

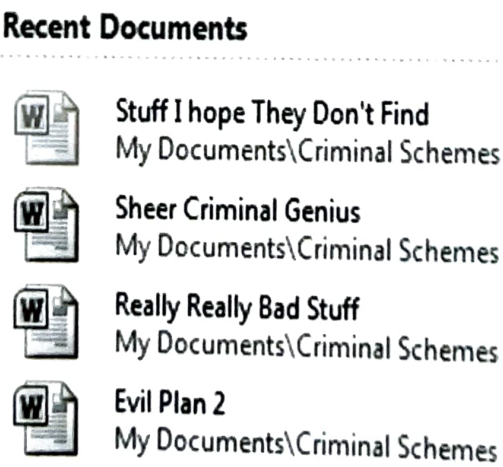

FIGURE 5.9

An MRU in Microsoft Word 2010.

RESTORE POINTS AND SHADOW COPY

Do you ever wish you could go back in time? We're not there yet, but lucky for us, Windows is. There may come a time when it's just easier (or necessary) for our computers to revert back to an earlier point in time when everything was working just fine. In Windows, these are called restore points (RPs), and they serve as time travel machines for our computers.

RESTORE POINTS

Restore points are snapshots of key system settings and configuration at a specific moment in time (Microsoft, 2011c). These snapshots can be used to return the system to working order. RPs are created in different ways. They can be created by the system automatically before major system events, such as installing software. They can be scheduled at regular intervals, such as weekly. Finally, they can be created manually by a user. The RP feature is on by default, and one snapshot is automatically produced every day.

Before you start looking around for your RPs, you should know that Microsoft has taken steps to keep them from your prying eyes. They are normally hidden from the user.

These RPs have metadata (data about the data) associated with them. This information could be valuable in determining the point in time when a snapshot was taken. If the RP contains evidence, this can tell us exactly when that data existed on the system in question.

Digging through the RPs may reveal evidentiary gems that don't exist anywhere else. For the average person trying to conceal information from investigators, RPs are likely not the first place they would start destroying evidence. Obviously, that works in our favor.

From the case files: Internet history and restore points

A defendant accused of possessing child pornography claimed that he had visited the site in question on only one occasion, and that was only by accident. To refute this claim, examiners turned to the restore points for the previous two months. Examination of each of the registry files found in the various RPs told a significantly different story. The evidence showed that not only had multiple child pornography sites been visited, but the URLs had been typed directly into the address bar of the browser, destroying his claim that the site was visited by accident. Confronted with this new evidence, the defendant quickly accepted a plea deal.

SHADOW COPIES

Shadow copies provide the source data for restore points. Like the RP, a shadow file is another artifact that could very well be worth a look. We can use shadow files to demonstrate how a particular file has been changed over time. They can likewise hold copies of files that have been deleted (Larson, 2010).

From the case files: restore points, shadow copies, and anti-forensics

Officers from the Texas Office or the Attorney General (OAG) Cyber Unit, responding to a tip, served a search warrant at a suspect's residence. The OAG Cyber Unit obtained the search warrant after being were alerted that the suspect was uploading child pornography to the Internet. When the officers served the search warrant, they found the house unoccupied. Officers called the suspect, letting him know they were in his home and that he should come home immediately and meet with them. When the suspect arrived, officers interviewed the suspect and searched his vehicle. Inside the car in which he arrived was a laptop computer.

All items seized were taken to the OAG offices for forensic examination. During the exam of the suspect's laptop, an alarming discovery was made. It appeared the suspect, on the drive home to meet the officers, used a wiping tool to get rid of not only incriminating images but the Internet history from his laptop. While the initial exam found no child pornography on the laptop, other compelling evidence was recovered.

For example, the examiner was able to recover logs from the wiping program itself, showing that it had indeed been run. That wasn't all. Since the operating system was Windows Vista, the examiner decided to check the shadow copies found on the machine. Remember, these shadow copies (or System Restore Points) are essentially snapshots of data at a given point in time.

Next, the forensic image (clone) of the suspect's laptop was loaded into a virtual environment. This enabled the examiner to see the computer system as the suspect saw it. The examiner exported out the restore points from the suspect's laptop, then imported those same files into the forensic tool. This process allowed the examiner to use his tools to extract images and other information from the suspect's system RPs. This procedure hit pay dirt. More than 3,000 images of child pornography were recovered. In addition, log files were found showing searches and downloads of those same files. When it was all said and done, the suspect pleaded guilty and is currently serving ten years in a Texas state prison.

PREFETCH

Speed kills. In the case of computers, it's the *lack* of speed that kills. Developers at Microsoft know this and work hard to squeeze every millisecond out of the system. Prefetching is one of the ways they try to speed up the system.

Prefetch files can show that an application was indeed installed and run on the system at one time. Take, for example, a wiping application such as Evidence Eliminator. Programs like this are designed to completely destroy selected data on a hard drive. Although we may not be able to recover the original evidence, the mere presence of Evidence Eliminator can prove to be almost as damning as the original files themselves. Stay tuned for more discussion on Evidence Eliminator.

LINK FILES

We all love shortcuts. They help us avoid road construction and steer clear of traffic jams. They save us time and make our travels easier, at least in theory. Microsoft Windows also likes shortcuts. It likes them a lot.

Link files are simply shortcuts. They point to other files. Link files can be created by us, or more often by the computer. You may have created a shortcut on your desktop to your favorite program or folder. The computer itself creates them in several different places. You've probably seen and used these link files before. Take Microsoft Word, for example. If you look under the File menu, you'll see an option called "Recent." The items in that list are link files, or shortcuts, created by the computer.

Link files have their own date and time stamps, showing when they were created and last used. The existence of a link file can be important. It can be used to show that someone actually opened the file in question. It can also be used to refute the assertion that a file or folder never existed. Link files can also contain full file paths, even if the storage device, such as a thumb drive, is no longer connected.

INSTALLED PROGRAMS

Software that is or has been installed on the questioned computer could also be of interest. This is especially true if the same application has been removed after some relevant point in time (i.e., when the suspect became aware of a potential investigation). There are multiple locations on the drive to look for these artifacts. The Program folder is a great place to start. Link and prefetch files are two other locations that could also bear fruit.

SUMMARY

The computer records a tremendous amount of information, unbeknownst to the vast majority of users. These artifacts come in a variety of forms and can be found throughout the system. For example, it's possible to identify external storage devices, such as thumb drives, that have been attached to the system. Items moved to the Windows Recycle Bin can tell us when they were deleted and by which account.

Even if a file has been deleted or overwritten, copies of the file could still exist on a drive in multiple forms. These often-overlooked copies are generated by print jobs and hibernation functions, as well as restore points. These files can also be found in the swap space, a specific portion of a hard drive that is used when the system is out of RAM.

One major takeaway from this chapter is that valuable evidence of specific files, actions, or events can be recorded in multiple locations. As such, truly getting rid of such material can be a highly technical process beyond the reach of most crooks.

Even deleting data and defragging your hard drive won't get rid of all data. The computer stores data in a way that permits fragments of older files to be carved out

for further analysis. The partial files removed from the slack space could contain just enough information to become a useful piece of evidence. Attribution is a major challenge in digital forensics. Saying with absolute certainty that a specific individual was responsible for a given artifact is often impossible. Identifying the account is often the best that can be done.

The system and the applications we use generate data about data. This information, known as metadata, can tell us when the file was created, accessed, modified, and deleted. Knowing what software has been installed and run could be relevant to an investigation. Drive-wiping software, for example, could be of particular interest. The Windows registry and the prefetching function are two sources of this potentially relevant information.

REFERENCES

Brodkin, J., 2011. Windows on Verge of Dropping Below 90% Market Share. Retrieved from: <http://www.networkworld.com/news/2011/011311-windows-on-verge-of-dropping.html> (accessed 11.05.11.).

Casey, E., 2009. Handbook of Digital Forensics and Investigation. Academic Press, Burlington, MA.

Doyle, A., 1891. Sherlock Holmes A Scandal in Bohemia. The Strand Magazine, United Kingdom.

Larson, T., 2010. Windows 7 Current Events in the World of Windows Forensics. Retrieved from: <http://digital-forensics.sans.org/summit.../12-larson-windows7-forensics.pdf> (accessed 11.05.11.).

Microsoft Corporation, 2011a. How the Recycle Bin Stores Files. Retrieved from: <http://support.microsoft. com/kb/136517> (accessed 11.05.11.).

Microsoft Corporation, 2011b. Sleep and Hibernation: Frequently Asked Questions. Retrieved from: <http://windows.microsoft.com/en-us/windows7/sleep-and-hibernation-frequently-asked-questions> (accessed 11.05.11.).

Microsoft Corporation, 2011c. System Restore: Frequently Asked Questions. Retrieved from: <http://windows.microsoft.com/en-us/windows/system-restore-faq#1TC=windows-7> (accessed 11.05.11.).

Microsoft Corporation, 2011d. User Accounts Overview: Microsoft Corporation. Retrieved from: <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/usercpl_overview.mspx?mfr=true> (accessed 11.05.11.).

TechTarget, 2011. Spool: Whatis.com. Retrieved from: <http://whatis.techtarget.com/definition/0,sid9_ gci214229,00.html> (accessed 11.05.01.).