

Chapter 3

The Liturgical Forensic Examination: Tracing Activity on a Windows-Based Desktop

Robert S. Greenfield, MCP

Gathering Evidence For Prosecution Purposes

One major guideline you need to follow when gathering evidence, whether it be files from a desktop, server, mainframe, or Internet-based external server is to preserve the integrity of the data. This means following careful procedures so you do not contaminate the subject data, and establishing a custodial chain for that evidence so that it is gathered in an approved, supervised, and legal manner for full admissibility in a court of law. Elsewhere in this book, such rules of evidence are covered; thus, we do not take the time here to further elaborate, other than to say that you must be conscientious about the manner in which such data is collected. Keep in mind also that initially you may not intend to prosecute, and are investigating purely for a corporate policy enforcement, and in the process of such investigation may come upon information that you will want to take legal action on. For this reason, it is critical that you treat all data carefully. Realizing too that if you are not in a “right to work” state, you may come under litigation from the targeted individual for an attempted wrongful discharge suit. If this happens, you want to have all your chain of custody and evidence handling procedures outlined and available for review so the courts will not find technical faults with your methods of gathering evidence.

Gathering evidence for prosecution purposes is really the mode you should consider operating in when a forensic examination is needed. For this reason, you should become familiar with the Federal Rules of Evidence, as well as your

local and state laws pertaining to the admissibility of evidence and what is required to provide “expert witness” testimony should that become necessary. You may not personally qualify as an expert witness in an area, so evidence gathered by you may be disallowed in one or more aspects of your testimony for which expert witness status is required.

The Federal Rules of Evidence are an umbrella under which the subsequent states add their own specific addenda. It is important that you check with your legal department regarding criminal and civil applicability with regard to evidential rules. Get to know the standards that are expected, and obtain if possible, the training to qualify as an expert witness in your state. You should also become knowledgeable as to who you can utilize that would be considered a valid expert witness should you need them. Be prepared with names of companies, individuals, and organizations as part of your overall action plan as you establish it. Make sure you are prepared to deal with possible civil or criminal prosecution needs well ahead of time. Make regular reviews of changes in laws that may require you to make changes in your action plan as well. Developing a corporate response plan to deal with these situations should be a top priority.

Gathering Evidence Without Intent to Prosecute

Of course, you should not let your intention not to prosecute sway your techniques in the gathering of evidence, as discussed in the previous section. However, you may have a situation wherein you are certain you will not have a case for litigation. While it is always preferable to have a complete evidential custody trail, and strict gathering requirements followed, your company may not have the funds, resources, or need to carry through at that level. Proper evidence gathering takes time and can involve a high degree of computer expertise in the more complex cases; so if you take this path, be aware that if you do find some illegal activity going on during the course of your investigation, you will want to immediately stop your activities, and should keep a log of everything you have done to the computer. It goes without saying that you should call the proper law enforcement authorities immediately, naturally. Having the log of activities performed on the computer will also aid in their subsequent investigation. Remember, even if you do not initially intend to prosecute, you may find it necessary in the course of your investigation.

The Microsoft Windows-Based Computer

In a corporate environment, it is best to monitor a computer remotely and trap data that you wish to examine for potential enforcement. This can be facilitated in a number of ways as discussed later. It is also important to remember that there are many areas one can examine on the computer directly. The Windows operating system and the programs that reside on it tend to leave lots of trails in different places that work to our advantage as we audit the computer files.

Depending on which Microsoft operating system is running on the desktop, certain things may be different. These are pointed out as needed where they occur. Some initial background on how things work on a Windows-based computer may be helpful as a primer to look at the items that will be discussed.

Operating Systems Versus Operating Environments

The Windows operating system under Windows 3.1, Windows 95, Windows 98, Windows 98/SE, and even Windows ME are all more technically operating environments. That is to say, they do not necessarily directly talk to your computer's hardware, but instead pass requests for things through the actual operating system, which in the case of the aforementioned platforms is MS-DOS (Microsoft Disk Operating System). Why is this important to know? Glad you asked. It is important because tools designed to work at the DOS level can be employed on these platforms that would not otherwise be available on systems running a true operating system that does not support all of DOS in exactly the same way. Examples of a true operating system would be Windows NT, Windows 2000, Linux, UNIX, and, of course, MS-DOS. All of these have direct communication layers within them that deal with handling memory, storage devices, and external peripherals such as the mouse, a scanner, the monitor, etc. These devices still use little programs called "drivers" that tailor the communications between the device and the operating system for that particular model, but that driver talks to the operating system in a standard way. Think of a driver as an interpreter that tells the operating system what the device can and cannot do, and how to make it do those things.

Storage Versus Memory

Another item that can cause confusion is the difference in storage and memory. You will often hear people not familiar with computers confuse the terms. It is important for you to understand how things are stored on a computer so that you can utilize the tools needed to examine them.

Memory

First and foremost, the term "memory" really refers to the amount of memory physically on computer chips inside the computer itself. If you bought your computer at a store and it came with 128 MB RAM, this means that the computer has 128 megabytes worth of chip memory. A byte is a single character of storage. So, the chip memory in this case could hold approximately 128 million characters of data. Not all of this memory is really available to the user because programs that make the computer run load up in memory when it is powered on. The moment power is cut, or the PC is turned off, regular chip memory is blanked out. This means that it is considered to be "volatile" memory because it does not store anything after you turn the computer off.

Storage

There are two basic kinds of storage: online and offline. Put simply, online storage is that which your computer can get to directly for permanently saving information. A hard disk is a form of online storage because it is always available and not something that can be taken away under normal conditions. As you are probably

already suspecting, offline storage is that CD-ROM, DVD, or diskette you use that can be popped in when needed and then taken out of the computer when finished.

Hard disk and floppy storage are subject to exploitation by advanced hackers who may have developed tools to utilize otherwise inaccessible areas of the hard disk for data storage. Techniques can be employed that take advantage of something called “slack space” in hard drive sectors. Basically, slack space is the unused space in a sector on the hard drive. Think of it as if the entire hard drive storage were divided up like the mail slots in a hotel lobby for each of the hotel rooms. When mail comes in (or in this case, a computer file to be stored is saved), it goes into the available mail slot reserved for it. If you have too much mail to fit in the single slot, it may have to overflow into the adjacent slot. The rule for this mailbox, however, is that once a slot contains a file, or part of a file, another file is not normally allowed to be stored in the remaining open portion of that mailbox (or sector in our case) even if there is plenty of room, and the next available mail slot is used. What happens to the potentially empty portion of space in the sector? Well, normally it goes to waste. That is why you can fill a hard drive up with lots of small files that do not add up to the rated storage capacity of the drive. The secret here is that low-level programs can be written to take advantage of these “slack” areas for data storage. Another thing to keep in mind is that data in a slack area may have belonged to an incriminating file prior to its deletion, and a smaller file was subsequently stored on top of it; thus, some of that incriminating information may be left behind in that “slack space.” A smart perpetrator can also take advantage of tools that supposedly wipe out information with multiple passes of file writes that write a series of binary 1s and 0s in a series of seven passes over the file area. While recovery of information wiped out in this manner is far more difficult, and in many cases impossible with any meaningful results, some recovery techniques exist that specialists can employ to retrieve some of the data. Factors such as the size of the hard drive, the accuracy of the mechanical system in the drive, the power with which the information was recorded, and even the length of time the information was left on the drive prior to wiping all will have an effect on the probabilities for recovery. Performing such recovery is available from companies that specialize in these tasks, but be advised that it is not inexpensive to have this done.

Detecting these sorts of situations requires a high level of expertise, and normally you will want to bring in a law enforcement agency, or forensic analysis consulting team, to get at that level of data obfuscation.

How Windows Uses Memory and Disk Storage

Windows uses memory in the computer and hard disk storage to run. It loads programs into memory that tell it everything from what kinds of devices are attached to the computer, to how to display a screen and sense and display mouse movement. Windows operating systems and environments are a set of interconnected programs at their low levels, and normally not all of it will want to fit into memory at a given time. This is especially true for things that are “in work,” such as a document, browsing the Web where a Web site page needs to be temporarily stored, etc. Windows will use part of the hard drive in a computer to enhance its ability to store data of an intermittent or intermediate nature.

Windows refers to this use of part of the hard disk as virtual memory because it is there to serve as a holding place for things either not yet saved permanently, or things that it uses only during the running of a program but that are not part of the final product.

General Guidelines To Follow

The following tips are important when making a review of a suspect computer and should be followed in any pursuit of suspicious activity, regardless of whether or not you intend to prosecute in a court of law.

Have a corporate action plan. This plan should be in place prior to ever needing to put it to the test. You should make sure you know in advance the various law enforcement agencies, groups, and consultants that can bring expertise to bear if needed. Make sure you have sufficient planning to cover incidents from both the nonskilled perpetrator and the advanced internal hacker. Remember that most corporate security precautions keep out most of the bad guys, that your real external threats will be from advanced hackers, and internal threats abound because those individuals are already behind your external security screens.

Things you should think about as far as advance planning include what tools can be put in place to monitor employee activity if called upon to do so. Some are mentioned in the course of this chapter, but their mention is not to endorse any one company or product over another. There are many companies with many fine products out there. We hope to provide some starting points only. Indeed, the landscape changes far too rapidly to be able to provide an absolute recommendation of any one product in this book because, by the time this is written and goes to press, additional tools from other companies may well be available. It is for this reason that alliances should be formed by you with other corporate auditors to find out what they have done, and are doing. This personal networking of knowledge can lead to your most valuable arsenal of tools, advice, and awareness of services being provided by other firms.

Document everything you do. As an auditor looking for information, you may be called upon to testify as to your processes and procedures. Make sure that you keep a log with date, time, activity performed, and outcome of that activity. This log will come in handy as you proceed through your analysis. You should develop a standardized procedure that works for you in these cases, in accordance with your training and expertise in a given area, and then follow that as the template for your log of activities. This assures a consistent and thorough approach.

Leave ego at the door and do not overstep your training level. If you feel that the investigation will require someone with forensic analysis experience in computers, seek out a forensic analysis firm or your local law enforcement agency to assist. People with a high degree of understanding and technical know-how today can perform criminal activity on computers. Even your local company computer expert is not necessarily equipped to deal with this. Information is presented in this section relating to how data can be hidden, but such information should be looked upon as information that provides a better base of understanding; it is not a substitute for training in these areas of analysis.

Always assume that you are going to run into something of an illegal nature, and follow the rules laid out in the Federal Rules of Evidence. These rules exist

to make adjudication rulings against a victimized person or company less likely. Be aware that when you, or a company brought in to do the forensic analysis, fail to follow these Federal Rules of Evidence, you run the risk of having the case tossed out of court. Solid cases have been compromised on technicalities due to lack of adherence to these rules.

Always, ALWAYS assume that a computer has been set up by a potential perpetrator to destroy evidence if the computer is used in a “normal” manner. Programs called Trojans (as in Trojan horse lore) can be put in place that would activate upon start-up of the computer in a regular mode that could wipe out, or otherwise damage potential evidence. A Trojan horse is a program that masquerades as a legitimate program but is really sitting in wait to be activated by the unwary.

Always work only from backups of the data sources on a computer. This means bitstream backups of the hard drive, floppy diskettes, etc. Never work directly on the computer itself (other than to make the initial backups) because any potential damage that is done either by you, or by the booby trap of a perpetrator, could ruin your one and only chance of getting the goods on him or her.

Once you have made a backup of the data, make a backup of your backup and work only from that working copy of your backup. That way, you can retrieve information from your primary, protected backup should it become necessary.

When you make a backup, use a product that does a bitstream backup. Standard file copy or file backup programs will not perform these kinds of backups. It is critical that a bitstream backup be used so that data hidden in places on the hard drive can be preserved. A clever perpetrator may actually try to hide files in areas on the hard drive marked as bad when they are not. Files can also be encrypted, and you may only have ghosts of the original file in areas of the computer’s file system that are marked as deleted, when in fact they still physically exist. A bitstream backup will make an exact 100 percent mirror-image copy. Tools to do this were originally made for network administrators for the purposes of creating online backups and for distribution of mass installations of software throughout a corporate enterprise. These tools have been vastly improved over the years, and one of the standard tools in use by the FBI and other law enforcement agencies is called SafeBack; it is available from New Technologies, Inc. (www.forensics-intl.com) to authorized personnel. Other tools for making image backups exist from well-known companies such as PowerQuest Corporation (www.powerquest.com), which makes DriveImage Pro. This utility can make exact partition backups as well. Regardless of the product selected, and there are many other products from various vendors out there, you should *learn* how to use them long before you ever *have* to use them. The time to learn is not when you have a crisis and need to employ the tool. Always practice making backups with the tool and know its features. Questions about a product should not go unanswered. The only stupid question is an unasked one. Do not be afraid of asking anything of the appropriate support people. Some companies offer training in the use of their products, and even provide consulting services. While this book is a guide for the auditor wanting to investigate issues of compliance forensically, it is not a substitute for training and the use of experienced individuals, especially if criminal activity is involved. You may wish to bring in a forensics expert and work side-by-side with him or her through your first few incidents. In the corporate

environment, you should not work in isolation if at all possible. This gives you the support you will need at first, and it will add to the verifiability of activities performed.

If activity of an illegal nature is suspect, or if activity is suspected that is not in compliance with corporate computer use policy (if such a policy exists), and you want to maintain surveillance on the employee's computer use to further build a case, you must use caution when obtaining information so that the employee does not suspect any evidence gathering activity. Fortunately, especially in a network environment, tools exist today that allow such covert monitoring to be easily facilitated. Some of these tools are discussed later. In the case where a network is not present, or where technical expertise or finances to bring in such expertise is limited, you may need to examine files from the machine by first-hand inspection. This means that you will have to visit the machine and gather the evidence directly. When you do this, you will have to be very careful that you do not alter the files on the machine itself.

One of the tools this author recommends, if you do not have a network, is an external CD-RW or Iomega Zip or Jaz drive that connects to the computer via a USB connection. Most computers now have USB ports. If the suspect computer is running Windows 95 Revision B or later, support for this technology is already embedded in the operating system. These devices allow you to plug into the PC using the USB port, and then unplug, without having to reboot the computer. This is even truer of Windows 2000 machines, for which the USB support is exceptional. An external CD-RW drive is preferable because you are recording to a medium that does not provide for on-media alteration of a given file provided you are using CD-R media. CD-R media are blank CDs that allow you to write once and read many. The fact that you cannot erase them afterward, or rewrite files already placed on the CD, makes them excellent for preserving evidence that you may need to present in litigation. You should make your bitstream backups to the CD-RW drive.

The driver support for Iomega Zip drives is already native in Windows 95 Revision B or later, so you will not need to install additional drivers. Support of the external CD-RW drive may require installation of drivers. If this is needed, the author recommends that you make it a companywide project to install the drivers for it on each and every PC. The reason for this is twofold: (1) it will be readily available to anyone who needs to make a backup of something important; and (2) it will make it easier to perform covert archiving in the future. Making it part of the corporate standard on the desktop for computers not connected to the network also masks the fact that you may be interested in just a particular individual and in obtaining records from just one specific machine at the moment.

Adopting a corporate standard such as the CD-RW device drivers, and therefore requiring your company computers to be updated, also provides a window of opportunity for the installation of other software to aid in monitoring activity. Some of these monitoring products perform their surveillance over the corporate network; others do it on the machine itself; and others support a combination of these environments. One such monitoring product even allows for the covert e-mailing of screen captures and activity logs.

Let us examine some of the areas that are valuable to know about on a Windows-based computer. There are many different areas that the computer uses on a PC to store data, either permanently or temporarily, which can be of use

as you conduct a review of activities that have taken place on a given computer. We examine the following kinds of files and file areas on the computer that can provide insight: cookies, bookmarks (a.k.a. Favorites), history buffers, cache storage, temporary Internet files, the system registry, recent documents list, and hidden files. We look at each of these in turn, tell you about their purpose, and how you can exploit their existence for your benefit as an investigator. In the absence of a covert observation tool, it can be very handy to know about all of these areas. We also discuss how some of the covert observation tools work and how you can employ them.

Cookies

This is a term you have no doubt heard bandied about for quite some time. There has been a lot of information, both good and bad, as to what these files are and what they can do. Hopefully, this section will clear up that vague and often-misunderstood file type.

First, what exactly is a cookie? Simply put, a cookie is a file that usually holds things such as a user name and password for a given Web site, any custom settings that may have been put in place for a given Web site, and other data that the Web site may track with regard to the user's visit there. It could contain anything that the Web site has been programmed to store there. It may have, for example, the date and time of the user's last visit, how many visits the user made, and if the user likes to view the Web site with background music on or off. One of the things that cookies normally do not have in them is a complete history of where the user has surfed to on the Web before going to that site. It is possible, however, for it to have information about what site the user was at just prior to visiting the one the cookie is attached to. Other information that can be recorded is the IP address of the computer, and where, once the user was on the site, what pages were visited. Normally, cookies are used to enhance the visitor experience by allowing the site being visited to better customize the viewing experience and tailor it to the visitor. Privacy concerns with regard to the use of cookies are valid to the extent of how much the user wants to reveal to a Web site, and what that Web site has in the way of a privacy policy stating the terms of use. There are utilities out there that will allow the user to control the use of cookies on a computer, and the user can also determine, in the Web browser settings, whether or not to even allow the use of cookies.

From an auditing perspective, the presence of cookies can be great. Adult Web sites often use cookies for the capture of information and customization of site settings. As a result, one usually finds a cookie file for most popular adult Web sites. It should be noted that care should be used when implying that an employee is intentionally visiting adult Web sites on a corporate computer. For example, an employee may have wanted to go to the White House Web site and typed in `www.whitehouse.com` instead of `www.whitehouse.gov`. The address ending in `.com` is an adult Web site; the address ending in `.gov` is the official Web site of the White House in Washington, D.C. Corporate policies usually address the accidental visiting of a site such as the one mentioned above. By examining cookies, one can determine how often such "mistakes" are made, and thus reveal if there is a pattern. Someone who visits such a site and immediately

backs out of that site is probably not intentionally going to it; but someone with an established pattern of visits for any length of time may very well be abusing the resources of the company.

Cookies are stored within a Web browser's file area, and on systems that provide user-by-user security and preference settings (Windows NT, 2000, and XP), they will be within the individual profile for that user within that user's cookies folder. For example, Exhibit 1 is what it would look like on a Windows NT or Windows 2000 machine if one were to display this using Windows Explorer.

Notice that the file extensions on the cookie files are **.txt**. That means that they are text files and that they can be opened using the Notepad application to examine the contents. While this sounds great, often doing so reveals little because the data is usually not directly readable in a meaningful manner. The reason is the way computers store numbers, and also the way those the numbers are subsequently displayed. Many times, the characters coming up mean very little except for the occasional cleartext message sometimes embedded. If there is an AOL cookie on a computer, for example, it may say inside it that the user needs to keep the cookie because the user has saved settings specific to his or her user identity. If the user opens one of these cookies using notepad, Exhibit 2 is what he or she might see.

As seen in Exhibit 2, not much is readable other than the URL from the Web site that placed it there. Utility programs are available that will allow the user to open and view the contents of a cookie in a somewhat more organized fashion, but for our purposes with auditing, the presence of the cookie and the Web site it is connected with is the most valuable portion. It proves that a visit to the site took place. Even if one of the available utilities is used, chances are that the individual other numbers stored in the cookie will have little meaning to anyone other than the Web site that created it. There is no fixed format requirement for a cookie, so it is difficult to obtain consistently useful information from cookies other than the originating URL and the creation date-time stamp, which indicates when the site had been visited initially. If the cookie gets updated or accessed, it may either get a new date-time stamp or it may have a new "modification" date. Using Windows Explorer, right-click on a cookie file and click on the Properties option that shows up. Under the "General" tab, the user will see something similar to Exhibit 3.

Notice toward the bottom of the window in Exhibit 3 the date created, the date it was last modified, and finally, the date it was last accessed on the computer. Be careful when checking this so as not to double-click on the file in question, but simply **right-mouse-click only** and bring up this property page. If you do accidentally double-click on the file, it will alter the Accessed: date. Be advised that the Accessed: date can also be modified if you perform a backup or copy of files from the system. See the suggestions for isolating the computer equipment from changes prior to performing any file operations.

Copy the files to your CD-RW drive to archive them. Another added advantage to the cookies is that they are named with the user ID of the person logged on at the time they were created. This is true of Windows NT, Windows 2000, and later computers as they provide the security by individual logon ID. On older Windows 95 or Windows 98 machines, the cookie files may not have any such identification, so you will have to correlate their creation and update dates with the individual's opportunity to imply a connection.

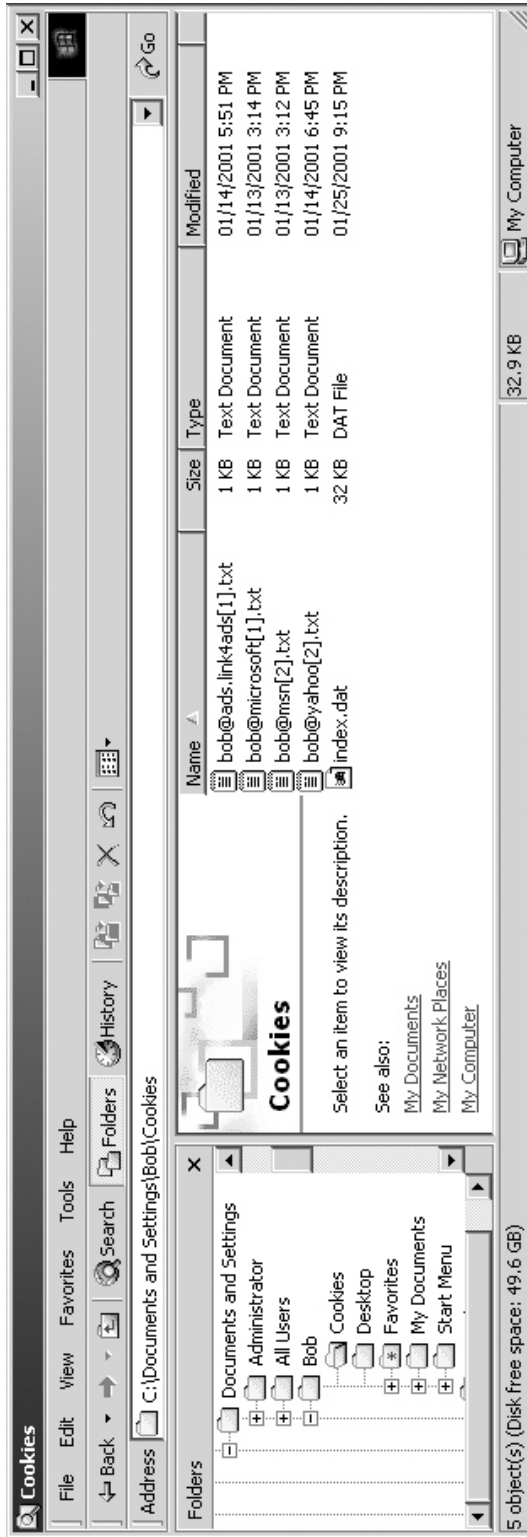


Exhibit 1. Windows Explorer Cookies Folder

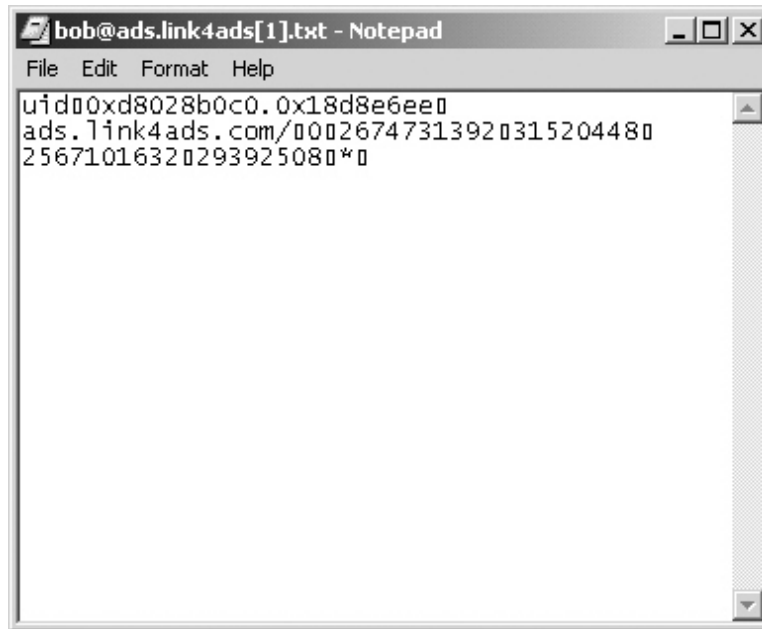


Exhibit 2. Advertisement Site Cookie

Bookmarks/Favorites

Depending on the configuration of the computer, it may have Microsoft's Internet Explorer (MSIE) Web browser or the Netscape browser. These are the two most common on corporate computers running Windows, although there are other browsers out there, such as Opera, or even some shareware or freeware Web-browsing tool. We will speak to the MSIE or Netscape tools in this book because they are prevalent.

A bookmark (the Netscape term) is the same thing as a Favorite (the Microsoft term). It is a record of the URL (uniform resource locator) that is the address on the Web of a given Web site. These URLs are held in special locations in each of these browsers and, in the case of Microsoft's Favorites, also become available in many other applications as well.

Netscape will have the bookmarks stored as part of a file (by default, it is called "bookmark.htm"). This file is actually stored in the same way as a Web page is written. You can look at the file to find out what places the individual likes to visit. When you are looking for these bookmark files, keep in mind that the user can customize several bookmark files under different names, and open them manually to get at the bookmarks. Also keep in mind that the user may be trying to hide the file by setting its file attribute to "Hidden," or calling it something other than "Bookmark." On Windows NT and 2000 machines, this file may reside in the individual's account area on the computer, but you should look for bookmark files in all areas on the computer.

The Microsoft Favorites present a different issue. They are stored differently and can be customized at different levels. First, on Windows 95- and 98-based

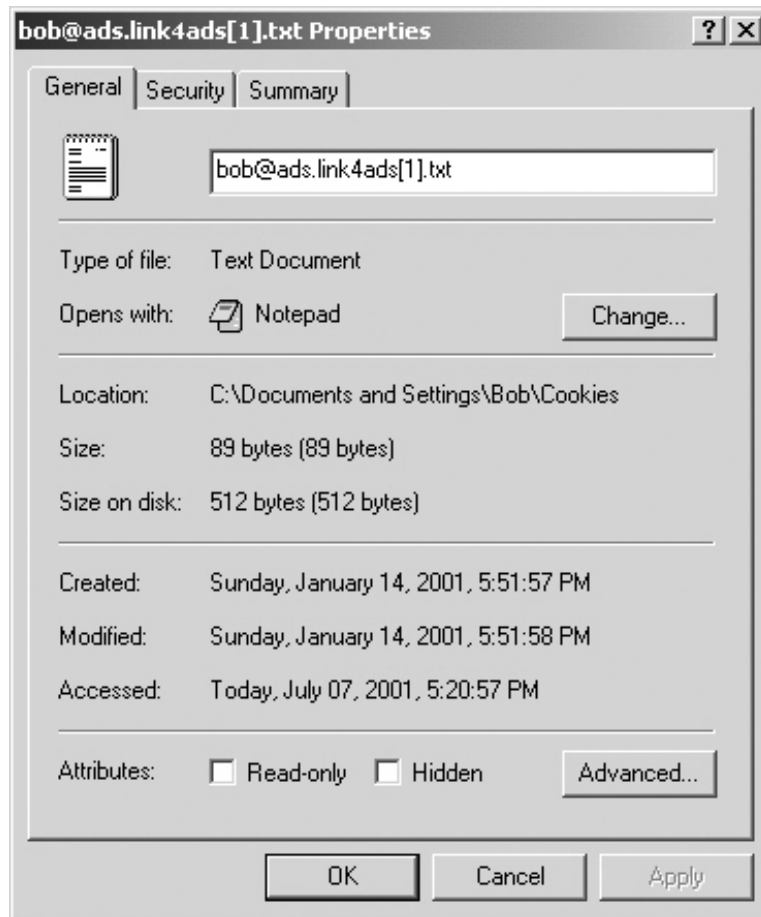


Exhibit 3. Windows Explorer File Properties

systems, there will be a folder on the computer called Favorites. Within this folder, you may find sub-folders that could be named for whatever the user wanted (category, topic, company name, etc.). And then within these sub-folders there may be additional sub-folders or actual files called Shortcuts, which are files that hold the URL information. On systems supporting multiple users (primarily, these will be Windows NT and Windows 2000 systems), you may have a Favorites folder under an All Users account, which are Favorites that will be available regardless of who is logged on. Under normal conditions, if the user does not have administrative rights (assuming this is a Windows NT or Windows 2000 machine), he or she will not be able to change the All Users folder contents, including the Favorites sub-folder. If this is a Windows 95 or Windows 98 machine, and a user wants to alter an All Users, Favorites folder contents, there is nothing to prevent its alteration. Make sure to examine each Favorites folder for its contents, and check the sub-folders all the way down the line. Keep in mind that individual files and folders could have the Hidden file attribute turned on. You will want to make sure that you use the Windows Explorer with its settings enabled to show hidden and system files. Also remember that you will need to be logged

on to that machine as the administrator (in the case of Windows NT and Windows 2000 systems) to be able to traverse across all the folders wherever they may be.

Internet Explorer's History Buffer

One advantage of the Microsoft Internet Explorer is that it keeps a history of where someone has surfed. By default, this option is enabled on Internet Explorer. The individual user can change the time span with which it will track this Web site visitation history, so you may not reap as much benefit from it, depending on how far back it is set to track. It will, however, track all sites visited. So, if a URL was typed into the browser's address bar, clicked from a Favorite entry, or clicked from a hyperlink on a Web page, it will be recorded in the history if it is enabled. Be aware that it is possible to set the history level to record 0 days of history, and to automatically clear all the browser cache upon exit. It is also possible for the user to manually clear the history by clicking on the option in the Internet Options dialog box within either Internet Explorer, or under Internet Options in the Start, Settings, Control Panel, Internet Options area, which brings up the same dialog.

If the contents of the history buffer are available, you hopefully will have a record of repeated use of the Internet in whatever form your company may consider to be abusive (surfing pornography, slacking off by excessive surfing, surfing non-business-related Web sites, etc.). You should look at the history buffer, either from a fresh restore or before you check out the other items in the Favorites list, because any new visits will generate additional entries into the history buffer.

Temporary Storage on the Hard Drive

Let's say you were typing a document in Microsoft Word. Very long documents with lots of pictures may not all fit into the available chip memory, so Windows uses the hard drive to fool the program into thinking you have more memory than you really do. Now, let's say you are working on a critical document. You cannot afford to lose the work being putting into it, so you have turned on the Auto Save feature of Microsoft Word. At a given interval, it will "flush" what it has in memory and virtual memory to a file on the hard drive in a temporary location. Microsoft Excel and Microsoft Word have these automatic save options. It is something to keep in mind in examing a system for files because some of these image files may be left over and could be examined.

When a document is being written, or a spreadsheet is being worked on, often times a file is created by the application making the document in what is called a "temp" area. This "temp" area is just that: a temporary area where files are located while they are being worked on and prior to being formally saved in some folder of the user's choice. On Windows-based computers, the area that is used by default is determined by settings stored in the computer. These settings are held in memory as a reference to where these temporary files should go. The memory reference is labeled with a variable name and is part of the environment within which the computer operates. The two environment variables involved

here are the TMP and TEMP variables. They are set to point at some given location on the computer. By default, on Windows 3.1, 95, 98, 98/SE, and ME systems, both will point to the location of *C:\Windows\Temp* or *C:\Temp*, depending on which operating system you are working with. On Windows NT/2000 platform machines, the values set for the TMP and TEMP environment variables will be set to a path sensitive to what user is logged on, so you would have to either try logging on as the individual, or, preferably, as that computer's administrator user and then locate the TEMP folders for the suspect user ID. To be sure where these variables are pointing, click the Start button, usually located in the lower left corner of the screen, and then click on Programs. Find the item in the menu labeled MS-DOS Prompt. Click on it and it will bring up a window that looks like the following:

In the window at the *C: />* Prompt, type the word Set and hit Return. The system will show you information about what is stored in the computer's Environment Variables. Make note of where the TMP and TEMP variables point as this directory (also known as a folder), holds residual files at times that may aid in the process of detecting use of the computer for illicit purposes.

On Windows NT/2000 systems, you can click on the Start button, then Run, and enter the word CMD into the Run window. It will bring up a box as shown in Exhibit 4. In the box, simply enter the commands SET TMP and hit the Enter button and SET TEMP and hit the button again. This will show the setting of these two Environment Variables. Exhibit 5 shows the values when logged on as the Administrative user on Windows 2000.

Temporary Internet Files

Just as with a Word or Excel document, a Web browser also uses a temporary location to hold all those graphics and other information on a Web site when you visit a particular location on the Web. In the case of Web browsers, they store data in temporary areas referred to as cache. This cache storage is functionally the same as the TEMP space described previously, but kept separate for the purposes of the Web browser's exclusive use. The idea here is that that if you have visited a particular Web page, downloaded that page, and gone to a subsequent page, it is faster, should you hit the Back button on the browser, to reload the page from hard drive than to download everything again. From an auditing perspective, this can be very useful because, if this area is not cleaned off, you can have the complete trail of what that person saw and downloaded on the Web and save copies of it for evidence. While the savvy Internet user may know to clean these off, or have the Web browser set to remove the files automatically, it is still an opportunity area that should not be overlooked. Most of the files that will be in this area will be HTML documents, graphics files, or perhaps some other Web-based scripting languages or programs. After archiving these files for safekeeping, you can make subsequent copies of them and view them using your own Web browser on your machine to open the HTML files directly and display the pages that were downloaded. Again, it is important to preserve the copies you made of the suspect machine intact and only work from subsequent copies so you do not alter or contaminate the evidence. It is also

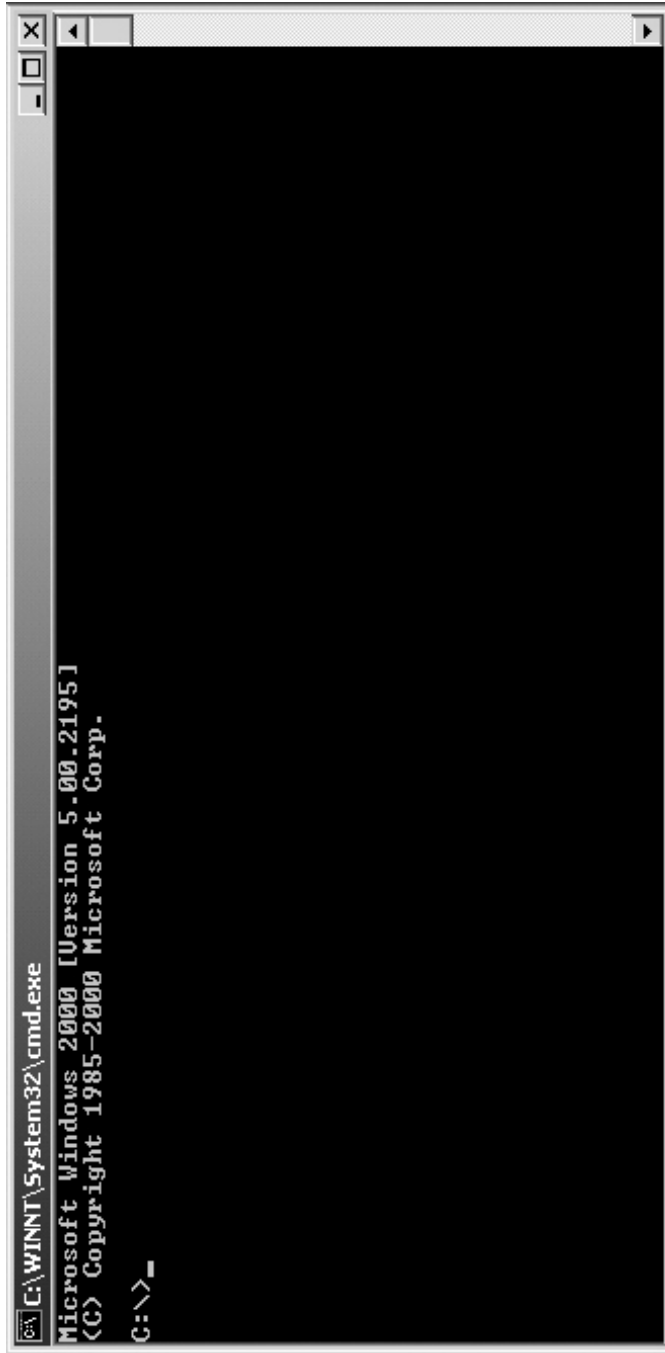


Exhibit 4. W2K Command Window



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C: > SET TMP
TMP=C:\DOCUMENTS\ADMINI~1\LOCALS~1\Temp

C: > SET TEMP
TEMP=C:\DOCUMENTS\ADMINI~1\LOCALS~1\Temp

C: >
```

Exhibit 5. W2K Command Window

valuable to note the date-time stamp on these files and correlate them with the individual's use of the computer to further enhance the evidence chain.

Another consideration you may have to deal with is a multi-lingual suspect. Internet Explorer is particularly advanced in its ability to handle multiple language sets. Netscape provides this as well, although at the current time not to the same level as Internet Explorer. If the saved Web page appears to be unreadable and you bring up the HTML page using a program like Notepad, for example, it may be that the non-HTML portions of the page are in an alphabet other than English. You should therefore use the browser to examine the HTML files. Because you are working off of a bitstream backup, whatever languages were supported will be similarly supported in the computer you are using to examine the files. You may have to get a translator involved if you do not speak the language. Do not assume that the page being examined is of no consequence just because it is in Russian, Chinese, or Greek. Cybercrime now spans the globe, and the Internet facilitates it instantaneously. The larger a company grows, the greater the likelihood of having to deal with a multi-lingual situation. If your company hires people from abroad, you may well have to deal with languages from any of those countries because the suspect may well be conversing with people in his or her homeland via e-mail, or surfing to a Web site there, etc. The key here is to be prepared and assume nothing. This author once worked in a firm that brought in people from India, became good friends with a number of them, and learned that in just that group of people there were 15 different dialects of the same native language represented. And, to further complicate matters, some of these dialects were so divergent from one another that the only language that they could all consistently communicate in and be properly understood was English. Subtleties like this are things you may have to cope with. If you are dealing with someone as a suspect from abroad, it may not necessarily be enough to have someone familiar with just the general countries language, but be versed in the specific region's dialect as well.

System Registry

The system registry is a key set of files that allows the computer to track and make available certain key aspects of computer applications system level files. A registry entry may contain, for example, the path and filename of a particular file, and its version number. A program with such an entry can use that registry entry to check to see if maybe a system level file was changed over what it expected to see on the computer. Things such as the individual support components of a program, the program itself, and data pertaining to registration, licensing, use, and features of that application also may reside in the system registry. For example, your individual copy of Microsoft Word, Microsoft Excel, or some other piece of software, may put its registration information directly into the system registry and correlate this with a licensing monitoring program in your corporate structure.

What you as an auditor would be looking for in the system registry would be programs that may have been illegally installed on the computer, legitimate copies of software that may have been illegally installed on more than one computer, or other bootleg software that may open the company to litigation if licensing is not obtained from the vendor.



Exhibit 6. W2K Run Command from Start

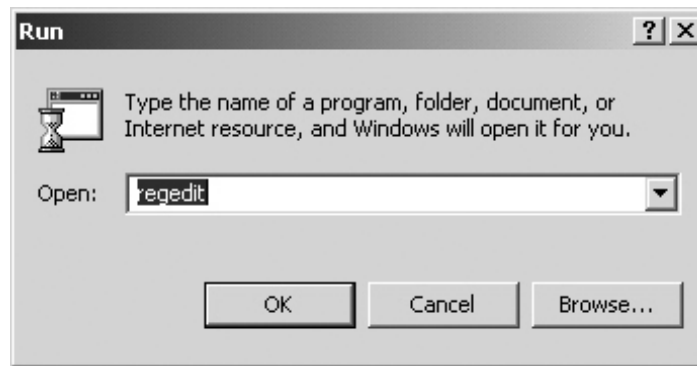


Exhibit 7. W2K Run Command Regedit

A computer-savvy perpetrator can use the system registry to hide or alter registration, or other information as well.

There are tools you can use to scan the system registry, many of which are shareware tools, but there is already a handy tool provided by Microsoft. It is called Regedit.exe (which is short for Registry Editor). You do not normally see it but it is there. If you left-mouse-click on your Windows Start button, you will see the pop-up menu appear (Exhibit 6). At the bottom of this menu is an icon that says Run beside it. When you click it, it will bring up a prompt for a command to run (Exhibit 7). Type in the word “regedit” and hit return or click the OK command button. This will bring up the Regedit program. It is very important that you work carefully so that you do not accidentally change a registry setting.

This program is designed for you to be able to actually look at registry entry settings, and, if you are knowledgeable, change settings. For our purposes, we utilize this merely as a tool to view what things are stored in the registry. The screen for the Regedit program looks like the one in Exhibit 8.

The left half of the window that appears shows the section of the registry you are viewing, and the portion on the right is the specific entry or entries that pertain to that section. The Regedit window works in a manner similar to the Windows Explorer, with a folder-based architecture. This architecture serves to compartmentalize entries in the registry based on function and applicability within that function. Registries can be huge, and you should be prepared to spend time sifting through this. You do not want to skip through something because that something you skip may well be an area that someone has hid something.

The best way to systematically go through the system registry is to print it out and scour the hardcopy. This way, you can check off each entry as you examine it. It is tedious, but this ensures that you have covered all your bases and it can further be utilized as an exhibit in court, provided the proper rules of evidence and chain of custody are observed. To print the registry, click the Registry menu item in the upper left corner to bring up the drop-down menu (see Exhibit 9). On the menu you will see the entry for Print... This will let you print the entire registry, or just the selected branch of that registry if you are highlighting just an individual portion of it.

Remember, registries are sometimes huge. So, when you are printing this, have patience and lots of paper on hand. I would recommend that you have a high-speed laser printer for this, due to the resulting print job size, but any Windows-based printer will do. As you scan through the printout, keep in mind that you are looking for something that is abnormal, hidden, or possibly look legitimate but pertain to a bootlegged piece of software. Remember also that a savvy computer user may have altered an entry to appear completely legal. You may need to correlate the software information you find with the licensing distribution database (if you have one), which should list who has what software, and what release levels and serial numbers should be present. If your company does not have such a listing, keep in mind that bootlegged software on an employee's machine can subject your company to hefty fines. Fines can be far in excess of the cost of obtaining a valid license.

When you click the Print... option, the panel in Exhibit 10 results. Note the bottom section of the central panel. This is where you have the option of printing all the registry, or just a portion. If you highlighted just a portion, you would see that branch of the registry in the Selected branch portion. You will want to use the All function, however. Make sure it is selected (as in Exhibit 10) and click the Print button at the bottom of the panel. Keep an eye on your paper supply and ink or toner cartridge so that you get a good, clean, legible copy.

The different top-level branches of the system registry are as follows.

HKEY_CLASSES_ROOT

This is where different file extensions become registered so programs can interact with them. For example, you might see an entry for .bmp. A file with a .bmp file extension would have an entry that designates it as belonging to the image class

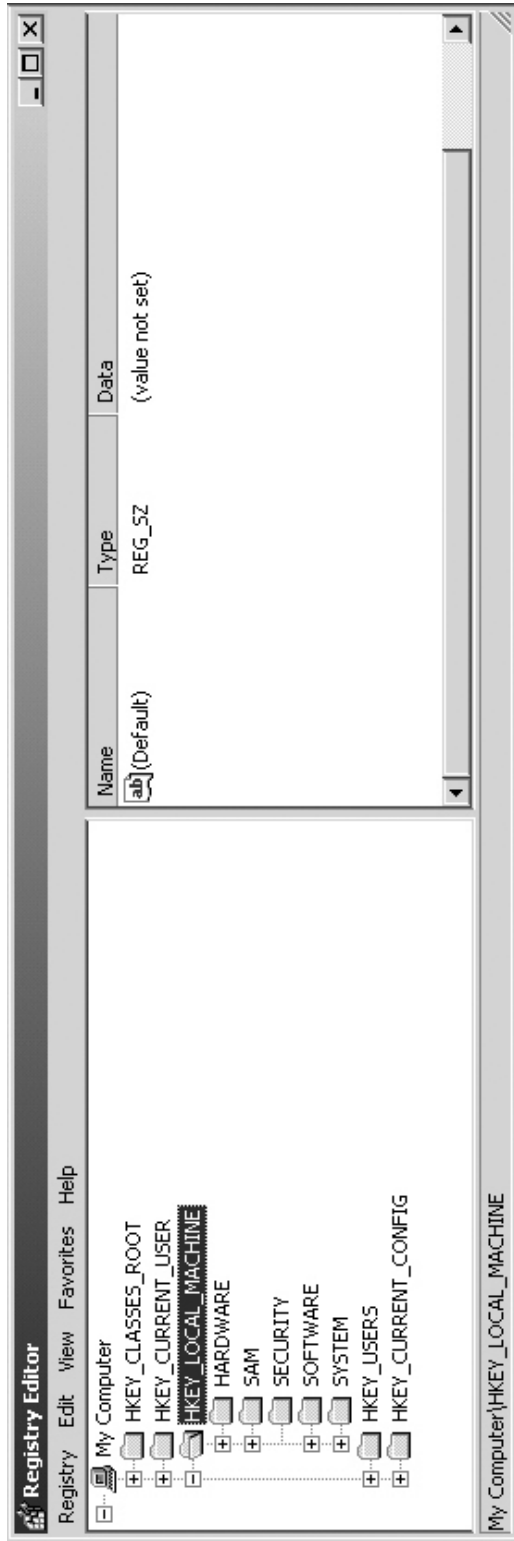


Exhibit 8. Regedit Screen Shot, with Registry Menu

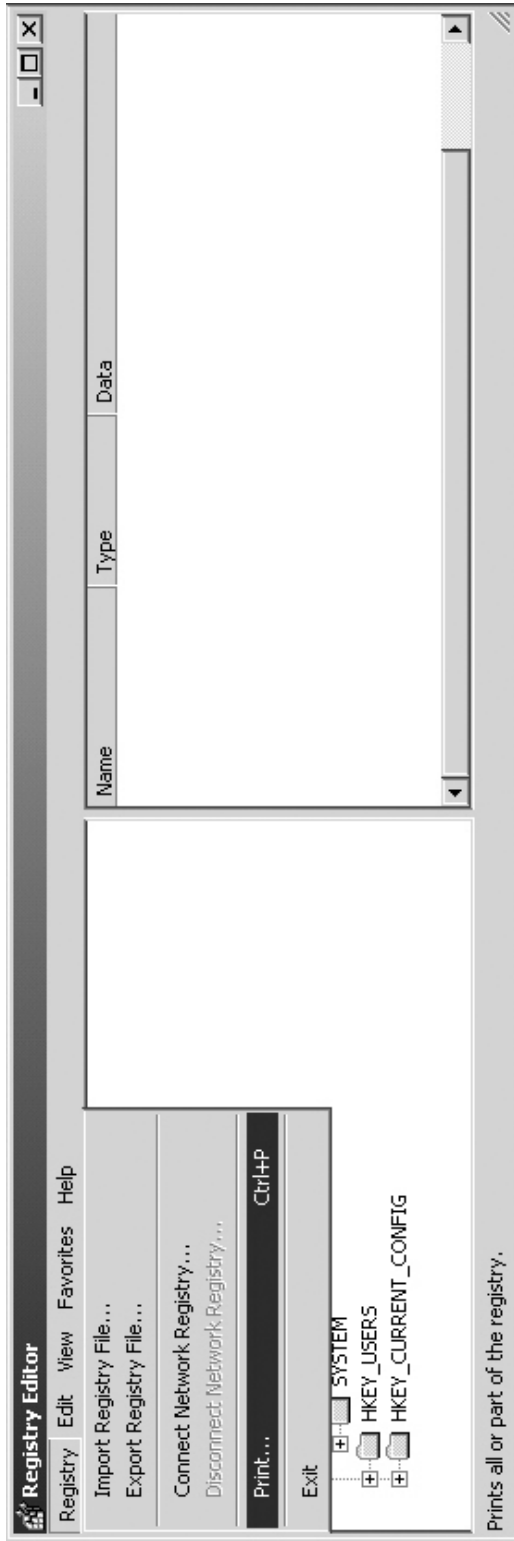


Exhibit 9. Regedit Printing Function

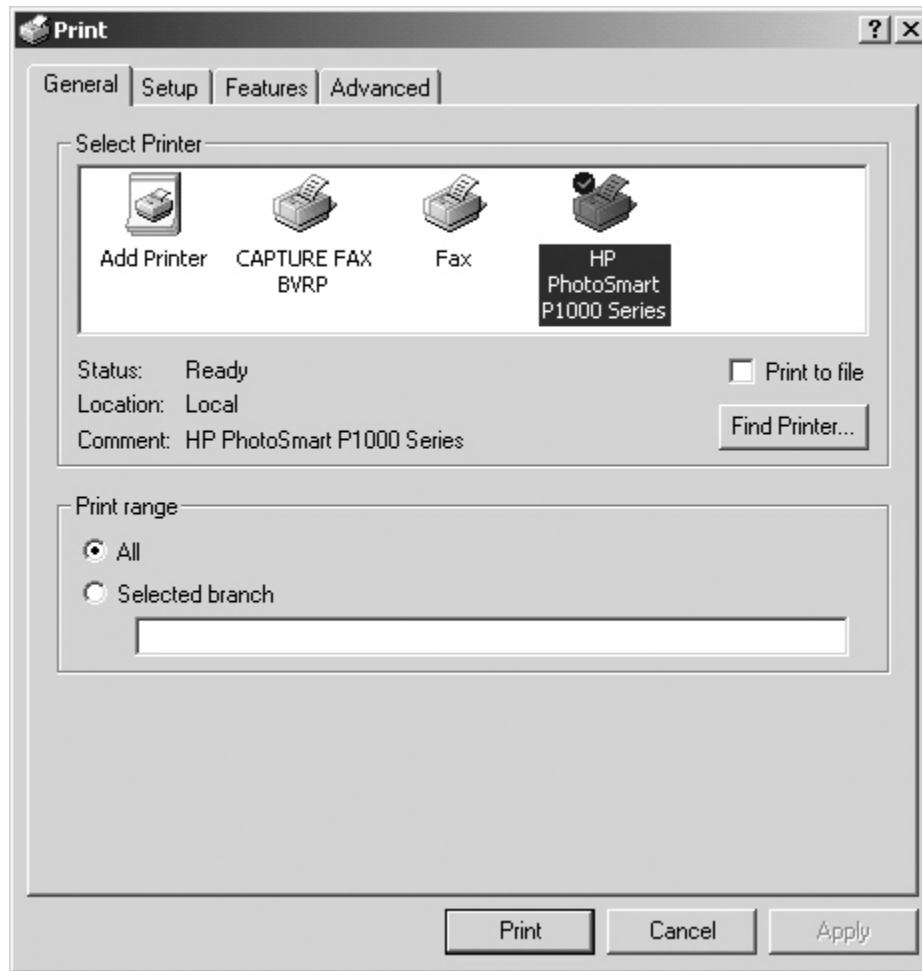


Exhibit 10. Regedit Printint Function

of objects. You may also see an entry for what program it is supposed to, by default, be opened with. Each known file extension on the system is registered this way. Find the entry for the .doc extension. It belongs to the “application” content type and, by default, is handled by the msword program, which is the file name for Microsoft Word program in the Microsoft Office Suite.

You do not need to become an expert at reading every entry in the registry, and indeed, entire books have been written on just working with the Windows system registry; rather, you should become sufficiently familiar with things so that you can spot if something just does not look right. If you have any doubts about an entry, consult an expert, preferably one versed in forensics and cybernetic sleuthing.

HKEY_CURRENT_USER

Because you are logged on as the administrator (or an administrative level account), this registry branch will contain the settings that were based on the

preferences set up for that ID. This holds information such as what image is on the Windows background (a.k.a. wallpaper), what font is set as the users preference, etc. This is one entry that you can probably skip, but scan through it anyway, just in case someone made a new entry in there that may not belong.

HKEY_LOCAL_MACHINE

This is where you may hit some real paydirt. The areas within this branch are for the machine's configuration, including hardware and software loads, security, and other system level settings (see Exhibit 8 for the branch headers).

If bootlegged software or other nonauthorized software was loaded, it will, in all likelihood, show up in here in the Software branch. If the program is very old, it may not utilize the system registry for everything, but may instead depend on text files to retain setting information. These text files were referred to as .ini files (pronounced eye-en-eye), which stands for initialization files. This was the common form of program preferences recording and setup information in the early days of Windows 3.x and was still actively used well into the use of Windows 95. Most current programs do not use the .ini file concept, but work with the system registry due to it being the encouraged standard from Microsoft. It is for this reason also that you should look for these .ini files wherever they may be on the computer. Use the search function available from the Windows Start menu and search for all the files ending in .ini. While most programs do not use them for their system settings, some programs do still have them for backward compatibility, or because the developers of the software did not want, or perhaps did not need, the sophistication of the system registry to support their application in some areas.

HKEY_USERS

Under normal conditions, this portion of the system registry holds unique identifying information on various identities registered on the system. These entries are normally generated by the computer and do not normally contain information generated by the user directly. The information contained in this area will look very cryptic. This is also a potential hiding spot for things, so be on the lookout. It is difficult to say what a clever perpetrator might hide in here. Perhaps the perpetrator will keep a record of unique system identifiers so he can spoof things. Perhaps he will not even use the registry for this, but it is always a possibility that should not be ignored.

HKEY_CURRENT_CONFIG

Again, this area is generated by the computer and holds information about the current configuration of various system level elements of the computer. Among these system elements you may find certain switches for Microsoft products and Internet connections and options.

The author's advice is to look at system registry entries on corporate standard desktops that you know have not been compromised. Become acquainted with

what looks normal. Buy a good book on the system registry and read up on its usage and parts. You do not have to become a programmer by any means, but use the book as a guide for what is and is not supposed to be in an area. It will help you understand a lot more about how to spot abnormal entries or subtle changes that may indicate a problem.

Remember: if you are in doubt about an entry, it is best to involve an expert who can assist you. Such an expert should not normally be from within your company information systems group, but rather a person trained in forensic analysis as it pertains to computers. Your local law enforcement agency should be able to either assist, or provide guidance as to whom in your area may be qualified. Do not let ego stand in the way of a successful investigation.

Enabling and Using Auditing via the Windows Operating System

If you are lucky, and the suspect's computer is running either the Windows NT or Windows 2000 operating system, you may well be in luck in tracking activity on the suspect's computer. Part of these operating systems features includes an auditing feature that can be extremely useful.

Before getting too excited, there are some prerequisites and a caveat you should heed. First, setting up auditing properly and securely takes someone trained in the administration and security aspects of the operating system involved. Second, this will only work on the two operating systems if the suspect's computer is storing data on the hard drive where the hard drive is partitioned using the NTFS file system. It is possible that the suspect's computer could be running the same file system as Windows 95, Windows 98, or Windows ME, in which case no security would be available. The non-secure file system (FAT16 and FAT32) was never designed to store security attributes about a file or the users on the computer. On the Windows 95, 98, and ME operating systems, you could establish a "Windows Password," but all it does is store desktop preferences such as wallpaper and fonts, etc. A user can blast right past those logon screens by simply clicking the Cancel button on the logon prompt and have full access to everything on that computer. The only protection a file has on FAT16 or FAT32 includes the Read Only, Hidden, and System file attributes that could protect it a little from prying eyes. While this may be great for you as an auditor examining someone's computer running one of these computers, it is a gaping corporate security hole and does not afford any level of real protection, or auditing capability. Tools that people can buy that supposedly "lock down" the Windows 95, 98, or ME desktops are not really a deterrent. Those computers can still be booted from a floppy diskette and then full access to the hard drive is possible. Their methods of securely storing data usually involves setting up a series of Trojan files that redirect requests through a program to where the real file is located, usually with an altered name and file extension, and sometimes with altered file attributes to further try to hide the files.

As corporate policy, those computers capable of having the NTFS file system used on them should be switched over to them. New computer installations should use this when initially configured, and existing systems that do not yet have it

should be switched over. There are tools available that will allow you to easily change the partition file system without losing existing data or programs (although a thorough backup should always be done before such a switch) from companies such as PowerQuest Corporation (www.powerquest.com). Their product, Partition Magic, is one of the best in the industry and is the only one currently available that lets you switch both up to NTFS and back to FAT16 or FAT32, with data in place.

The NTFS file was designed to be secure. This file system also tends to be more resistant to file fragmentation. Remember the discussion of how the areas on a hard drive are like the hotel lobby mailbox system? Well, say you have a lot of mail (i.e., a huge file), and the available areas in the mailbox system (free places on the hard drive) are not contiguous in nature, meaning they have a spot free here and there scattered throughout the filing system. What happens to the file to be stored? Well, as you might have already guessed, it gets split up. It will become fragmented into as many pieces as needed, and the file system will keep track of where each piece is. The more fragmented a file becomes, the longer it takes to retrieve. This is often the cause of computer performance degradation over time. What makes NTFS resistant to fragmentation is that the file system management portion of the operating system will look at the size of the file to be stored and try to find the largest available contiguous block of space it can to put it. While it is not going to prevent fragmentation entirely, the degree of fragmentation is lower because of this more intelligent handling. The FAT16 or FAT32 file systems simply start storing at the first empty spot and work forward to store the file.

Fragmentation can make low-level data recovery efforts more difficult because of the need to track down all the pieces. This is yet another reason to be using the more secure and more intelligently managed NTFS file system in your organization.

One other feature available only on the Windows 2000 operating system is something called Folder Redirection. This feature lets you have a hard drive folder, or even an entire hard drive, located somewhere other than the user's local computer. This feature can be made transparent to the user and is best used on desktop systems. Laptops that are potentially undocked and redocked (or repeatedly disconnected and reconnected to the network) are not suitable for this entire drive redirection because the location of the drive, not being local, would require synchronizing the files back to the laptop over the network before undocking, and again once it was docked. The time involved to do this level of synchronization is impractical. It is recommended, however, that you consider redirecting the section of the system that contains the Event Logs so that the logs for a computer are actually stored on a secure, remote server. This prevents tampering and provides an easier way to make ongoing examinations of a given system. Setting this up will require some expert administration skills; the details of this setup are beyond the scope of this text. Be aware, however, of the capabilities and look into implementing this audit tracking and remote storage of the logs if at all possible.

When you enable auditing, you cause entries to be made to an event log. On Windows NT and Windows 2000, the Event Log Viewer (see Exhibit 11) is used to observe the entries made by the auditing of activities. Event Logs are divided into three or four sections: System Messages, Application Messages,

Event Viewer

Security Log 1,587 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Success Audit	07/08/2001	9:37:31 AM	Security	Object Access	562	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:31 AM	Security	Object Access	562	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:31 AM	Security	Object Access	562	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:31 AM	Security	Object Access	560	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:31 AM	Security	Object Access	560	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:31 AM	Security	Detailed Tracking	593	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:31 AM	Security	Privilege Use	577	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:31 AM	Security	System Event	515	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:31 AM	Security	Detailed Tracking	592	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:31 AM	Security	Privilege Use	576	Karen	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:31 AM	Security	Logon/Logoff	528	Karen	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:31 AM	Security	Account Logon	680	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	9:37:15 AM	Security	Detailed Tracking	593	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	8:33:16 AM	Security	Detailed Tracking	593	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	8:32:00 AM	Security	Detailed Tracking	592	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	8:31:44 AM	Security	Detailed Tracking	593	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	8:30:29 AM	Security	Detailed Tracking	592	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	8:30:13 AM	Security	Detailed Tracking	593	SYSTEM	TBJD6E11ZP93Q57
Success Audit	07/08/2001	8:28:58 AM	Security	Detailed Tracking	592	SYSTEM	TBJD6E11ZP93Q57

Exhibit 11. Event Log Viewer General Screen

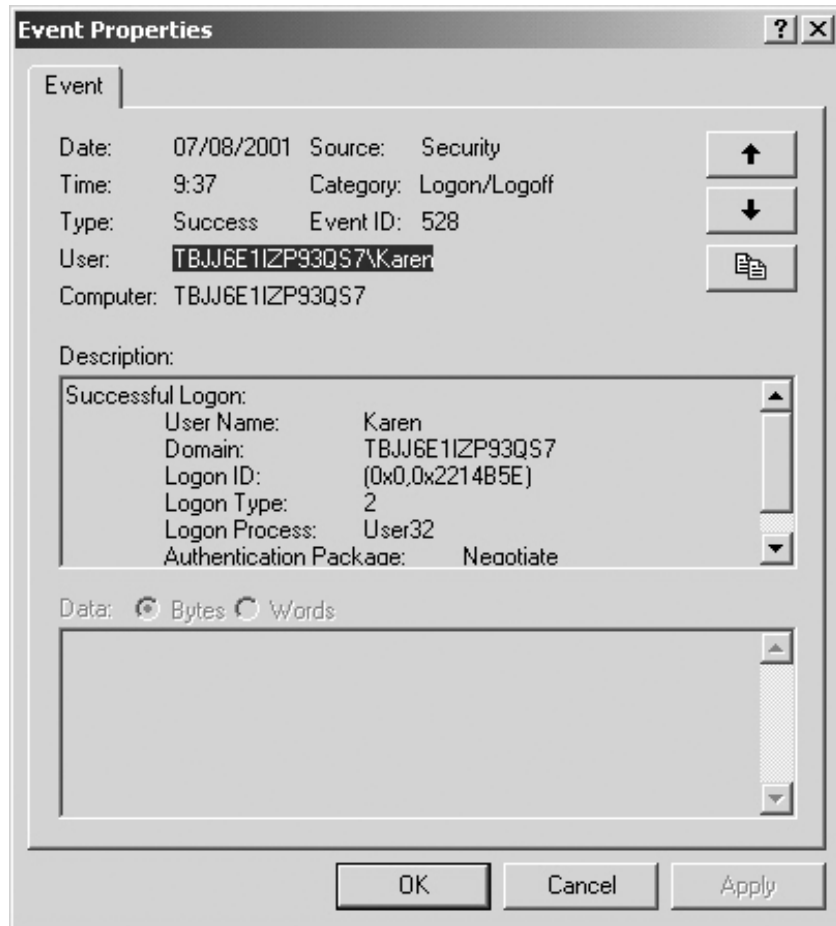


Exhibit 12. Event Log Viewer Logon Item Details

Security Logs, and possibly IExplore (which contains auditing information on Internet Explorer Events). The event viewer program is used by an administrator-level account on either Windows NT or Windows 2000 to bring up these logs. The event viewer is split into two panes, with the logging areas and the individual events listed. The amount of time an event log is kept depends on the settings for the logs, which tell the computer when to overwrite the oldest entries. If you are going to be monitoring someone over an extensive time frame, you may need to make this a fairly large value.

As you can see from the screen capture of a sample system in Exhibit 12, the auditing function can capture as high or as low a degree of event granularity as you wish. Specific file and application access can be audited, as well as logon and logoff times and other user activities. The entry highlighted in Exhibit 11 shows a logon on event for a user on the computer. If you want to view the exact contents of that event, you simply double-click to get more information about it and the detail view will appear for that entry.

As seen in Exhibit 12, this particular entry shows a successful logon of the user under the account shown. You can view the details of any event regardless

of which portion of the logs they are in. If you are auditing the use of a given application, for example, you can find out who invoked the program, when it was started, etc.

The success of your auditing will depend on the expert invocation of the auditing feature, the establishment of proper security configurations in your organization, and the vigilance with which such monitoring of a suspect is carried out. Do not limit event logs to too small a size when tracking someone for possible infractions of policy or the law. Such trespasses may not occur on a daily or even weekly basis, so be prepared to maintain logs over a long monitoring duration. Do not forget that these logs need to be backed up also. Separate backups should be made onto CD-R media and that media should be kept tucked away in a secure, controlled environment with full chain of custody provisions as per the federal and other local Rules of Evidence. Most default settings for logs will make them overwrite after a few days or a week. The idea behind most default auditing is not that of enforcement, but of debugging problems with a given computer system. It is up to you and your corporate security team to ensure that monitoring via the auditing capability of the events log is made efficacious.

More food for thought. You may actually have to initiate covert monitoring of someone in your own group or on the corporate security team. Make sure you have sufficient processes and policies in place to be able to monitor anyone. Remember: the computers in an organization belong to the company and are corporate resources. The rights to privacy in the workplace and on the computer are very limited, especially if your company gives notice to users when they log on that they are subject to being monitored. If you suspect that the person who needs monitoring is a highly skilled security expert, you are probably going to have to get expert help from an outside forensics and security firm.

Confiscation of Computer Equipment

When you confiscate a computer, you should keep in mind all factors relating to Rules of Evidence and establishing a custodial chain. From an evidential perspective, you will want to have the computer isolated and secured as quickly as possible. There are a number of factors to consider when impounding the equipment. First and foremost, make sure that when you impound it that you have a secure location to bring it to. All your hard work will be for naught if it can be intimated in court that unauthorized persons gained access to the computer and might have tampered with it.

Make certain you document the original state of the computer. This can and should include taking date/time stamped photographs of the computer and its attached peripherals from all angles. If the system is powered up when you arrive, photograph the screen. Make sure that you do this quickly, as a password protected screen-saver may come on that will inhibit your ability to make a proper shutdown of the system. Shut down the system following the normal Windows shutdown process. Keep in mind that a clever individual may have put a Trojan horse program in place to destroy parts of the system or evidence. This is another reason to have employed covert monitoring ahead of time.

A sudden power down can be potentially damaging to the computer due to the loss of data from the memory buffer that was not committed to the hard

drive. Normally, a Windows shutdown writes all unsaved buffer and disk cache to the hard drive as part of its shutdown process. Once the computer is powered down, leave it off until you have made your bitstream backups. You should work only from a similar computer that you set up from the restored bitstream backups made from the suspect computer. Leave the suspect computer off if at all possible. If damage is to occur, it will happen to the computer you are working off of, and that system can be restored again from the bitstream backups if need be.

Tag all connections into the computer and even draw a diagram of the connections so that the system can be put back together identically in the secure location. You will want to tag not only the wire leading into the computer, but also the socket it goes into. Photographing the connection is also a good idea once the tags are in place.

Make sure you protect the floppy diskette or other media drives. It is important that the read/write heads of the floppy drive or other media not be misaligned due to handling damage. Many diskette drives come packaged from their manufacturers with a cardboard insert, especially on older drives, to protect the heads. If possible, use one for the floppy drive. If not, make sure the computer is wrapped carefully (after fingerprints are taken if necessary), with shock-absorbent foam padding or thickly wrapped in bubble wrap on all sides, prior to transport.

Make sure all personnel handling the equipment ground themselves first before touching the chassis, components, and media. They should wear rubber-soled shoes and not wear any clothing made of synthetic materials that can attract, or even generate, static electricity.

Remember that transporting the computer equipment is a prime area where the chain of custody must be properly maintained. Transport should be performed by more than one person, and should be direct from the suspect's site to the secure storage location. No single part of the equipment should be let out of the sight and possession of at least two trusted and duly trained and authorized people for even a moment. If you intend to go to court, you have to be able to prove that no opportunity existed for the tampering, damage, or substitution of the evidence.

Make sure that once the equipment is brought to the secure location, that it is kept secure. Tampering and damage prevention are critical, and the physical security of the lockup area must be maintained. Video surveillance of the lockup area is recommended and should be in use while your examination of the system is performed. This will help ensure that the defendant can perpetrate no claims of poor process control or other bungling. If such surveillance is not feasible, then having an expert witness present during your examination to cross-check your findings is also a valuable resource.

Once your examination of the suspect's system is completed using the parallel computer, you should fire up the suspect's computer and cross-check your results as a further point of evidence.

Other Methods of Covert Monitoring

Many computer programs exist that can spy on every keystroke, every window brought up, and every e-mail sent, all without the knowledge of the person operating the computer. Such utilities work at various levels and have a wide

range of prices. One of the newest entries into the fray for this is a program called SpectorSoft, made by SpectorSoft, Inc. (www.spectorsoft.com). The program, which costs less than under \$100 as of this writing, takes intermittent snapshots of what is being done on a computer. It maintains these logs of activity in great detail. One version of this company's software will even covertly e-mail out the logs to an account you designate on a regular basis. While it is not 100 percent unbreakable in terms of finding it, one would have to know exactly when it was installed to be able to find it, and even then, it would be quite a chore to locate. It is just one more weapon to consider in your arsenal of analysis and monitoring for illicit or illegal activity.

Other tools exist to monitor usage profiles of everything from Web browsing habits to e-mail. Another vulnerability that new programs are also taking into account in their monitoring capabilities is that of anonymous e-mail services available via the Web. Someone with a Hotmail or Yahoo! e-mail account could send company-sensitive data out using these services and until now, there was no good way to easily track and prosecute that. This is changing, thanks to these new tools. It is difficult to block the use of Web-based e-mail due to the fact that many of the uses for such e-mail systems are perfectly legitimate. A contractor might use such an e-mail account to keep in touch with his or her company, for example. Such communications may be of a sensitive nature between that individual and the company, and using a service such as Yahoo! or Hotmail keeps their mail off the company's servers, reducing corporate workload and keeping corporate privacy intact.

While your corporate firewall may not allow it, many companies do not block the protocols or ports in the firewall to disallow communications via a chat program like AOL's Instant Messenger, Yahoo! Messenger, ICQ, MSN Messenger, PowWow, IRC chat clients, or NetMeeting sessions. If your company allows such messaging services to pass through the corporate firewall, remember that a file can be sent out or received directly through these tools and it will bypass your e-mail scanning protections. Corporate secrets could be revealed very quickly using these tools, and because it is done without e-mail, yet a typed message is sent, it is easier to covertly send out messages like this, but can be just as damaging as if someone picked up the phone and told it to the recipient directly. A program that can capture keystrokes and screen shots will capture evidence of activity like this, and can further enhance your stack of evidence. It should be used in conjunction with the other tools mentioned, such as auditing through the operating system.

One other tool exists that can capture all data in or out of a computer. That tool is called a sniffer. A sniffer can trap data packets as they are sent out from the computer and as they are received. It is literally an intercept of the information traveling down the network wire, although it does not prevent the transmission of such data in either direction. While it will not capture purely locally stored information (information that never leaves the confines of the PC itself), anything that goes out of or into the computer will be caught. Windows 2000 Server and Windows NT Server come with a program that can remotely monitor any computer address and trap the data to and from it. While designed as a tool for performance and trouble monitoring, it can be put into play for such monitoring tasks. All that is needed is the Internet Protocol address (i.e., IP address) of the computer to be monitored. Check with a trained Windows NT or Windows 2000 Administrator



about information on this tool and its use. It comes with the Server versions of both Windows NT and Windows 2000.

Advanced spy equipment also exists that can monitor the minute electromagnetic fluxes coming from the keyboard or the communications port of the computer. Such equipment, when used properly, is another way to trap all data going into or coming out of a computer. This kind of equipment is not inexpensive, and it will not work against computers hardened against electronic eavesdropping (the government refers to this as an equipment's Tempest rating). But your average computer will send out tons of impulses that can be captured from the wires and keypad buttons on the keyboard and mouse, to the fluxes in the monitor screen and wires leading from the graphics port of the computer.

An awareness of the tools available for the purposes of monitoring and collecting data is half the battle of getting up and running effectively. Hopefully, this chapter was of aid in bringing about such awareness and helping guide you to a successful implementation of your forensic detection and investigation skills.



