

EDP AUDITING

CONDUCTING A COMPUTER FORENSIC EXAMINATION THAT WILL NOT LEAD TO TRIAL

Carol Stucki

INSIDE

Isolation of Equipment; Cookies; Bookmarks; History Buffer; Cache; Temporary Internet Files; Tracking of Logon Duration and Times; Recent Documents List; Tracking of Illicit Software Installation and Use; The System Review; The Manual Review; Hidden Files; How to Correlate the Evidence

INTRODUCTION

The nonliturgical investigation is one that is not foreseen to be taken to trial or involve litigation. However, one should always conduct an investigation as if one were going to trial, just in case one has to. Thus one will have all the evidence needed to prosecute the case already in structure, which will make the case easier to litigate if necessary without extra backtracking and rework.

One of the first things to consider: is there a need to isolate equipment or files? If yes, one must move quickly on this to preserve any possible evidence. What is preserved and found on the equipment, most likely a PC, will be the basis of the forensic examination.

ISOLATION OF EQUIPMENT

Should you need to isolate or quarantine equipment as a part of your investigation, you need to take a few steps to (1) ensure the protection of the equipment, (2) isolate and protect data from tampering, and (3) secure the investigation scene. First, you need to ensure that you have the authority to take the equipment. If you are taking any equipment, you should first get authorization from management. If you take working equipment, they will need to make arrangements to replace it while you conduct your investigation.

PAYOFF IDEA

This article reviews such topics as the isolation of equipment, isolation of files, tracking of Web sites visited, tracking of log-on duration and times, tracking of illicit software installation and use, and how to correlate the evidence one finds.

The first thing to do is ensure that the PC you are about to take as part of your investigation is the correct unit, the one actually used in the illegal activity, used by the employee under investigation. This can be done by checking the asset records, or the records that are kept in some corporations by the operations department. If you need to take an employee's PC, you need to have a witness and have the employee sign a form stating that you took the PC; record the serial number, make, and model, when you took it, and the reason. If you do not have such forms, ensure that you do record what action was taken, obtain the employee's signature, and secure the suspect equipment.

If you have to take an employee's PC, you must move quickly to ensure that the evidence is preserved intact and not tainted, altered, or even destroyed.

Once you have the PC in your possession, you need to preserve the "chain of evidence." You preserve the chain of evidence by making sure that neither you nor anyone else is left alone with the equipment. You should always record your actions with the equipment. A good way to record all the actions and whereabouts with equipment or any other piece of evidence under investigation is to keep a log. This log should show (1) who has access to the equipment, (2) who retains control over the log, and (3) where the log is stored. Additionally, you should record the when (dates and times), where, and why of your every action, so that every minute you have the equipment or data in your possession is accountable. Even if you put this PC in a locked cabinet or secured area, this needs to be recorded in the log.

One of the first things you should do with the PC is "ghost it." This means that you should back up everything on the PC. This way, you can ensure that you will not lose the data when you conduct your investigation. This also preserves the original data that might be disturbed during the investigation.

It is very important for the backup of any data under investigation that the programs used to perform this backup be independent and have integrity. That is, the programs should not be under the influence or control of any person or other program or system that is outside the investigation team. The integrity of the data and equipment needs to be ensured by the use of programs that will not alter the original data in any way, either intentionally or accidentally.

There are a number of programs used to perform such backups that are independent and have integrity. One such program is SafeBack, and it is freeware that is available on the Web.

Isolation of Files

Not all the data needed for an investigation will reside on a user's PC. Therefore, you need to gain access to the same files and directories that the user has access to. The first thing to do is to disable the user's ID. First,

ensure that the administrator verifies what action (or actions) will occur to the user's profile and accounts if the user's ID were to be disabled. Only after verifying that no data will be lost, altered, or destroyed by disabling the ID, should the administrator proceed to disable the user's ID.

You need to have someone with security or administration authority disable the users' ID. Operations personnel or a systems/data security office can do this. The easiest way to disable the user's ID is to change the password; but this is not the most efficient, as the user could regain access if he or she were to guess the new password. Ensure that the administrator disables the ID but does not delete it. In some security setups, deleting a user ID will cause data and files to be deleted as well. Because this is not what you want to happen, disable only the ID.

Once the ID is disabled, the next and most important step is to copy all the files to which the user had access. This provides a backup for your investigation, as the data cannot be quarantined. The confiscated data, however, cannot be used by the business for as long as you need to conduct your investigation.

Operations or security personnel should have paper files with access requests, and they can run a report that shows what the user had access to on the system. Make sure the list or report they give you contains the group access and public access files for the user. You need to investigate all of the places a user could have copied or hidden data. For the investigation, you might be able to ignore those files with read-only access, but it is always best to be sure and get it all.

Now that you know what the user had access to, request that operations personnel copy the files into a secure location that only you and your team have access to. Copy the file structure as well — all directories and sub-directories. Make two copies of the data: one as a backup and one for you to use in the investigation. This is similar to taking a picture of the crime scene before you start moving things around.

Now that you have a copy of the data to use, the following sections in this article provide various examples of potential investigative areas, and demonstrate how you can use the data collected as part of your investigation.

Tracking of Web Sites Visited

If your investigation requires that you track what Web sites have been visited by an employee, you need to begin by reviewing the following items

- Cookies
- Bookmarks
- History buffer
- Cache
- Temporary Internet files

Here we briefly define each of these items, where to find them, how to capture the findings, and how to evaluate what you have found.

COOKIES

Cookies are messages given to a Web browser by a Web server. The browser stores the message in a text file called *cookie.txt*. The message is then sent back to the server each time the browser requests a page from the server.

The main purposes of cookies are to identify users and possibly prepare customized Web pages for them. When you enter a Web site that uses cookies, you may be asked to fill out a form providing such information as your name and interests. This information is packaged into a cookie file and sent to your Web browser, which stores it for later use. The next time you go to the same Web site, your browser will send the cookie to the Web server. The server can use this information to present you with custom Web pages. Thus, for example, instead of seeing just a generic welcome page, you might see a welcome page with your name on it.

The name *cookie* evolved from UNIX objects called *magic cookies*. These are tokens that are attached to a user's ID or program and change depending on the areas entered by the user's ID or program. Cookies are also sometimes called *persistent cookies* because they typically stay in the browser for long periods of time.

You will find cookies on the PC's hard drive, usually the C: drive, under the Windows directory. Cookies is a sub-directory under the Windows directory. The best way to access the Cookies sub-directory and subsequent files stored there is via MS Windows Explorer (see [Exhibit 1](#)).

When you open this directory using Windows Explorer, you will find a listing of the Cookies for those Web sites that you have visited. If there are no files under this directory, they have been deleted. If there are files under this directory, you can view the dates and times they were last accessed. You will also see the ID that was used to access these sites on this PC.

Cookies can be deleted in several ways. One way is manually. The user can access the cookies folder and delete all information from the folder. If the deletion was done manually, one place to look for cookies is in the Recycle Bin. There is a Disk Cleanup program that comes with Windows 98 and higher that deletes the information in the following folders: Cookies, Temporary Internet, Downloadable Program Files, Recycle Bin, Old ScanDisk Files, and Temporary Files. See [Exhibit 2](#) for a look at the Disk Cleanup program. The Disk Cleanup program does not leave any place to look for deleted files. There are also Cookie Manager programs that will automatically delete old or expired cookies from your cookie folders. These programs allow users to set their own expiration

EXHIBIT 1 — Cookies Sub-Directory File Contents

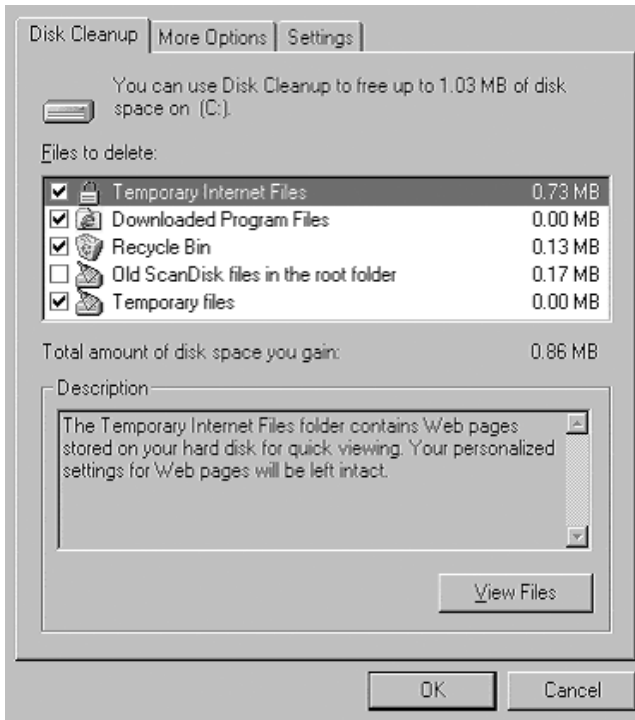
Address: C:\WINDOWS\Cookies

Name	Size	Type	Modified
anyuser@adl_impulsebuy(1)	1KB	Text ...	3/22/01 11:31 AM
anyuser@ads.link4ads(1)	1KB	Text ...	3/30/01 9:23 AM
anyuser@advertising(1)	1KB	Text ...	3/29/01 7:40 AM
anyuser@avenuea(2)	1KB	Text ...	3/28/01 8:13 AM
anyuser@bigcharts(1)	1KB	Text ...	2/4/01 8:44 AM
anyuser@dell(1)	1KB	Text ...	3/28/01 12:39 PM
anyuser@doubleclick(1)	1KB	Text ...	3/22/01 8:09 AM
anyuser@familysearch(1)	1KB	Text ...	2/4/01 8:45 AM
anyuser@fidelity(1)	1KB	Text ...	3/29/01 7:51 AM
anyuser@hc2.humanclick(1)	1KB	Text ...	2/16/01 7:28 AM
anyuser@icc(1)	1KB	Text ...	3/21/01 11:38 AM
anyuser@icc(2)	1KB	Text ...	3/27/00 7:31 PM
anyuser@icc(4)	1KB	Text ...	3/21/01 11:47 AM
anyuser@icpenney(1)	1KB	Text ...	3/27/00 7:15 PM
anyuser@marketwatch(1)	1KB	Text ...	3/21/01 11:33 AM
anyuser@mediaplex(2)	1KB	Text ...	3/22/01 11:51 AM
anyuser@msn(1)	1KB	Text ...	2/16/01 7:25 AM
anyuser@servedby.advertising(1)	1KB	Text ...	3/29/01 7:40 AM
anyuser@superstate(1)	1KB	Text ...	3/22/01 11:51 AM
anyuser@travelocity(2)	1KB	Text ...	3/28/01 12:19 PM
anyuser@wvwy(2)	1KB	Text ...	3/28/01 7:40 AM
anyuser@yahoo(1)	1KB	Text ...	2/4/01 10:20 AM
cstucki@0015580(1)	1KB	Text ...	12/19/00 8:18 AM
cstucki@70246539(1)	1KB	Text ...	1/2/01 4:30 PM
cstucki@70246539(2)	1KB	Text ...	10/3/00 8:42 AM
cstucki@ads.clickagents(1)	1KB	Text ...	11/2/00 10:44 AM
cstucki@ads.link4ads(1)	1KB	Text ...	10/3/00 8:44 AM
cstucki@amazon(2)	1KB	Text ...	10/23/00 5:04 PM
cstucki@amazon(3)	1KB	Text ...	3/5/01 5:08 PM
cstucki@avenuea(2)	1KB	Text ...	10/13/00 8:26 AM
cstucki@brfast(1)	1KB	Text ...	10/15/00 11:12 AM
cstucki@cobl(2)	1KB	Text ...	2/13/01 2:07 PM
cstucki@cnh(2)	1KB	Text ...	3/2/01 8:15 AM
cstucki@cnr(2)	1KB	Text ...	10/12/00 2:47 PM

100 object(s) 63.1KB (Disk free space: 2.72GB) My Computer

Start Preview and Enhance - C: Exploring - Cookies 9:27 PM

EXHIBIT 2 — Disk Cleanup Program from Windows 98



and archive dates. For example, the user can set the Cookie Manager to delete or archive all cookies more than five days old. Some of these manager programs put the deleted cookies into the Recycle Bin and some put them in a temporary archive folder. To find these archive folders, you would have to research the program and find the archive files.

For your investigation, you need to determine where each cookie takes you. Cookies can be named many things (see [Exhibit 1](#)); so by exploring and recording where each cookie takes you, you can determine what the user had been doing on the Web sites where the cookies came from. Note the date and time of each cookie; this is when they were created or accessed by the user for the first time for this site. However, some cookies are generated without a user having to actually access a particular site. These "magic cookies," which are generated without a user having to actually access a particular site, are often marketing gimmicks or ploys to get the user to go to their Web site. To determine where a user actually visited, you need to compare the cookies files to the history files. History files are described later in this article.

BOOKMARKS

A bookmark is a marker or address that identifies a document or a specific place in a document. Bookmarks are Internet shortcuts that users can save on the Web browser. Thus, users do not have to remember or write down the URL or location of Web sites they might like to revisit in the future. Nearly all Web browsers support a bookmarking feature that lets users save the address (URL) of a Web page so that they can easily revisit the page at a later time.

There are two places bookmarks or favorites are stored. One is in the Web browser under Favorites (see [Exhibit 3](#)). Another is on the C:, or hard, drive under the Windows folder, in the sub-folder called Favorites (see [Exhibit 4](#)).

The bookmarks or favorites are stored under the users' desired names. However, by clicking on these, you can visit each Web site the user has marked. Because bookmark names can be changed by the user, be sure to examine each one carefully. Be sure that you do not casually skip over a seemingly "tame" bookmark name simply because it does not look like it would be pointing to an unauthorized Web site (e.g., PrettyFlowers@Home). There is no real way to hide a bookmark, but users can bury a bookmark in a folder they create in the bookmark area. So be sure to open the folders you see in the bookmarks listing.

There is an added advantage to seeing the favorites listing from the user's C: drive view. You can see the dates and times when the bookmarks were created or modified. However, this does not provide you with a listing of times when the sites were actually visited, or how frequently.

HISTORY BUFFER

A buffer is a temporary storage area, usually in RAM. The purpose of most buffers is to act as a holding area, enabling the CPU to manipulate data before transferring it to a device (e.g., a printer, external device, etc.).

Because the processes of reading and writing data to a disk are relatively slow, many programs keep track of data changes in a buffer and then copy the buffer to a disk. For example, word processors employ a buffer to keep track of changes to files. Then when you *save* the file, the word processor updates the disk file with the contents of the buffer. This is much more efficient than accessing the file on the disk each time you make a change to the file.

Note that because your changes are initially stored in a buffer, not on the disk, all changes will be lost if the computer fails during an editing session. For this reason, it is a good idea to save your file periodically. Most word processors automatically save files at regular intervals.

On the other hand, a history buffer is a storage area on the Web browser of URL sites. What the history buffer shows you, from the Web

EXHIBIT 3 — Favorites from Web Browser (Explorer)

AT&T Business Internet Services - Home Page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss

Address http://www.attbusiness.net/ Go Links

Favorites

- Add... Organize...
- AT&T Business Internet Services - H...
- Toshiba America, Inc.
- WinZip@Home Page
- Links
- Search Engines
- Area Code Listing, by Number
- cXML.org
- Greatest Films
- My Documents
- Web Sites
- Yahoo! Maps and Driving Directions
- GSSI
- Yahoo! Yellow Pages
- Investor Home - MSN MoneyCentral
- Digital Marketplace Project
- Internet Explorer Update Reminder
- A Warm Wish Gift Baskets
- Headhunter.net (Job Details)
- Management Recruiting
- Registration Information
- AMM tool
- Disappearing Inc. - Enol Sert
- New Folder
- demo Download Instructions
- FamilySearch Internet Genealogy Ser...
- MarketMaker by PurchasePro
- https--ova.purchasepro.net-exchan...
- AT&T Business Internet Services

AT&T Business Internet Services

Global roaming in over 50 countries

Home Help Center Account Center Registration Center Software Center

The world is a very big place... Shrink It.

Global Roaming in over 50 Countries with AT&T Business Internet Services

advertisement info

Business

Careers

Computing

Entertainment

Weather & News

Reference

Shopping

Sports

Travel

Search

Assistant

Sign up now!

Global roaming in 50+ countries

Select Country

Worldwide Access

Access in over 50 countries!

Select Country

Service Tools

Access Numbers

Access Plans

Report a Problem

Contact Us

Top US & International Headlines

Thursday, April 20, 2001

Antarctic rescue plane en route for Chile...

CNN

Antarctic rescue plane takes off for Chile...

CNN

Plane takes off from South Pole with ill doctor on board...

Chicago Tribune

Algerian general in French torture case...

BBC

World bank must lend to middle-income states...

Financial Times

Ex-Senator Kerry Says Raid He Led in 69 Killed Civilians...

New York Times

19g

HEADLINES BY moreover

Featured News

Moulin Rouge Soundtrack Features Top Artists

April 2001 (Newstream) - Some of today's most cutting-edge artists and composers are working with filmmaker Baz Luhrmann to create what is expected to be one of the year's hottest soundtracks, for Luhrmann's epic,entine picture, Moulin Rouge.

Market Watch

Dow Jones Industrial Average

10,700

10,600

10,500

11 1 3

DJIA 10,697.14 ▲ 61.94

Nasdaq 2,034.97 ▼ 24.83

S&P 500 1,234.99 ▲ 8.23

3:09 PM ET 4/20/2001

©BigCharts.com

interactive charting

Book Travel Online

TRIP.com for Business Travel

Start

Exploring - cyber forensics

Inbox - Microsoft Outlook

AT&T Business Intern...

Preview and Enhance - C...

Internet

12:50 PM

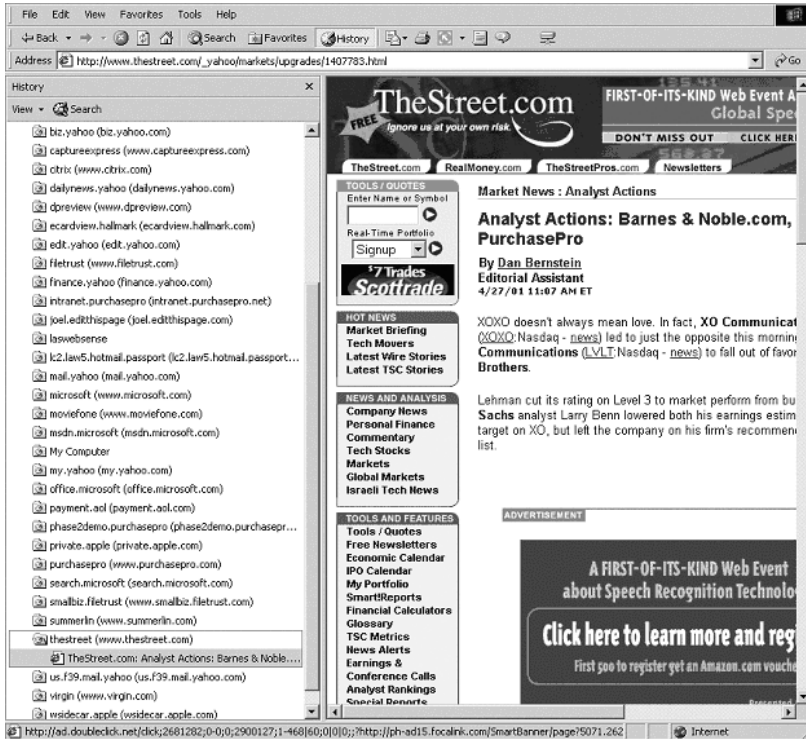
EXHIBIT 4 — Bookmarks from Hard Drive View

The screenshot shows the Windows Explorer interface with the Favorites folder selected. The main pane displays a list of bookmarks with the following columns: Name, Size, Type, Modified, Last Visited, and Last Modified.

Name	Size	Type	Modified	Last Visited	Last Modified
[Links]		File Folder	2/22/00 8:30 AM		
Search Engines		File Folder	3/15/00 4:37 PM		
A Warm Wish Gift Baskets	1KB	Internet Shortcut	8/11/00 9:21 AM		
AMM tool	1KB	Internet Shortcut	10/31/00 8:49 AM		
Area Code Listing, by Number	1KB	Internet Shortcut	2/8/00 9:35 AM		
AT&T Business Internet Services - Home Page	1KB	Internet Shortcut	2/22/00 8:17 AM		
cXML.org	1KB	Internet Shortcut	3/15/00 8:38 AM		
Digital Marketplace Project	1KB	Internet Shortcut	7/20/00 7:46 AM		
Disappearing Inc. Email Sent	1KB	Internet Shortcut	11/27/00 8:14 AM		
Greatest Films	1KB	Internet Shortcut	2/18/00 1:31 PM		
GSSI	1KB	Internet Shortcut	6/19/00 9:50 AM		
Headhunter.net (Job Details)	2KB	Internet Shortcut	9/14/00 9:11 AM		
Internet Explorer Update Reminder	1KB	Internet Shortcut	8/28/00 1:21 PM		
Investor Home - MSN MoneyCentral	1KB	Internet Shortcut	7/17/00 1:53 PM		
Management Recruiting	1KB	Internet Shortcut	9/25/00 8:40 AM		
My Documents	1KB	Shortcut	1/21/00 8:14 AM		
PurchasePro.com Intranet	1KB	Internet Shortcut	6/22/00 3:00 PM		
PurchasePro.Com, Inc. Specializing In Business To...	1KB	Internet Shortcut	12/15/99 6:04 PM		
Registration Information	1KB	Internet Shortcut	10/2/00 8:06 AM		
Toshiba America, Inc.	1KB	Internet Shortcut	2/22/00 8:18 AM		
Web Sites	1KB	Internet Shortcut	3/3/00 4:02 PM		
Wfn.Zip@Home Page	1KB	Internet Shortcut	2/22/00 8:18 AM		
Yahoo! Maps and Driving Directions	1KB	Internet Shortcut	2/8/00 9:23 AM		
Yahoo! Yellow Pages	1KB	Internet Shortcut	6/27/00 9:54 AM		

The status bar at the bottom of the window displays: 24 object(s) 6.06KB (Disk free space: 3.39GB) My Computer

EXHIBIT 5 — History Buffer from Web Browser



Browser's point of view, is what URLs or sites have been visited by day and what screens have been opened under each URL (see Exhibit 5).

To get to the history buffer, go to the Web browser. On the tool bar there is an icon or button called History (see Exhibit 5).

The history buffer can be cleared out by the user by simply highlighting and deleting the items in the list. The deleted contents from this list are not stored anywhere else in the browser, but they still exist in the hard drive history buffer.

The view of the history buffer from the hard drive point-of-view is a little different (see Exhibit 6). This view is found via the path Windows, History. Here you see the days of the week that the user actually accessed the Web. By opening one of the days of the week sub-folders, you can see the actual listings of the URLs visited by the user, and the time and dates the sites were last visited. By combining each day's lists, you can derive a pattern of visitation (and browser utilization) to each Web site.

Such information may document/prove that an employee (or at least the individual who sat at the particular PC under review) was accessing

EXHIBIT 6 — History Buffer from Hard Drive View

The screenshot displays the Internet Explorer interface with the History Buffer from Hard Drive View open. The window title is "Exploring - phase2demo.purchasepro (phase2demo.purchasepro.com)". The address bar shows "phase2demo.purchasepro (phase2demo.purchasepro.com)". The left pane shows the "Folders" tree with "History" expanded to "Today". The right pane shows a table of internet addresses and their last visited times.

Internet Address	Title	Last Visited
buy.asp?user=yRS19\mnphtl4&pass=HhVqJzaTZDCK6Z&um=MZqk3kdu...	buy.asp?user=yRS19\mnphtl4&pass=...	12/7/00 2:37 PM
sell.asp?user=yRS19\mnphtl4&pass=HhVqJzaTZDCK6Z&um=rz9xOvi...	sell.asp?user=yRS19\mnphtl4&pass=...	12/7/00 2:37 PM
index.asp?user=yRS19\mnphtl4&pass=HhVqJzaTZDCK6Z&um=rz9xO...	index.asp?user=yRS19\mnphtl4&pass=...	12/7/00 2:32 PM
productdetail.asp?user=yRS19\mnphtl4&pass=HhVqJzaTZDCK6Z&um=r...	productdetail.asp?user=yRS19\mnphtl4...	12/7/00 2:32 PM
classifieds_prod_subcat.asp?user=yRS19\mnphtl4&pass=HhVqJzaTZD...	classifieds_prod_subcat.asp?user=yRS...	12/7/00 2:31 PM
classifieds_prod_subcat.asp?user=yRS19\mnphtl4&pass=HhVqJzaTZD...	classifieds_prod_subcat.asp?user=yRS...	12/7/00 2:31 PM
classifieds.asp?user=yRS19\mnphtl4&pass=HhVqJzaTZDCK6Z&um=rz...	classifieds.asp?user=yRS19\mnphtl4...	12/7/00 2:31 PM
index.asp?user=yRS19\mnphtl4&pass=HhVqJzaTZDCK6Z&um=rz9x...	index.asp?user=yRS19\mnphtl4&pass...	12/7/00 2:26 PM
buy.asp?user=yRS19\mnphtl4&pass=HhVqJzaTZDCK6Z&um=rz9x...	buy.asp?user=yRS19\mnphtl4&pass=...	12/7/00 2:26 PM
emp_workarea.asp?user=yRS19\mnphtl4&pass=HhVqJzaTZDCK6Z&um...	emp_workarea.asp?user=yRS19\mnphtl...	12/7/00 2:26 PM
buy.asp?user=yRS19\mnphtl4&pass=HhVqJzaTZDCK6Z&um=rz9x...	buy.asp?user=yRS19\mnphtl4&pass=...	12/7/00 2:26 PM
login	login	12/7/00 2:26 PM
phase2demo.purchasepro	phase2demo.purchasepro	12/7/00 2:26 PM

the Web: (1) in violation of company policy; (2) during working hours instead of only during predetermined allowable times (i.e., lunch breaks); (3) on weekends or during other off-schedule, non-normal times when employees or other personnel should not be in the building/office; or (4) visiting unapproved or unauthorized sites.

CACHE

Cache can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching. A memory cache, sometimes called a cache store or RAM cache, is a portion of memory made of high-speed static RAM (SRAM) instead of the slower and cheaper dynamic RAM (DRAM) used for main memory. Memory caching is effective because most programs access the same data or instructions over and over. By keeping as much of this information as possible in SRAM, the computer avoids accessing the slower DRAM.

Some memory caches are built into the architecture of microprocessors. The Intel 80486 microprocessor, for example, contains an 8K memory cache, and the Pentium has a 16K cache. Such internal caches are often called Level 1 (L1) caches. Most modern PCs also come with external cache memory, called Level 2 (L2) caches. These caches sit between the CPU and the DRAM. Like L1 caches, L2 caches are composed of SRAM but are much larger.

Disk caching works under the same principle as memory caching; but instead of using high-speed SRAM, a disk cache uses conventional main memory. The most recently accessed data from the disk (as well as adjacent sectors) is stored in a memory buffer. When a program needs to access data from the disk, it first checks the disk cache to see if the data is there. Disk caching can dramatically improve the performance of applications because accessing a byte of data in RAM can be thousands of times faster than accessing the same byte on a hard disk.

When data is found in the cache, it is called a cache hit, and the effectiveness of a cache is judged by its hit rate. Many cache systems use a technique known as smart caching, in which the system can recognize certain types of frequently used data.

How is cache important to computer forensics? You can get the last set of instructions or data that was saved in the cache. This might be evidence you need to collect in your investigation. Unfortunately, capturing the cache information is tricky and can only be done with special programs.

TEMPORARY INTERNET FILES

Temporary Internet Files are those files that are “image captures” of each screen/site that you visit when you access the Internet or an intranet (see [Exhibit 7](#)). Temporary Internet Files is a sub-folder under the Windows folder on the C: drive or hard drive of the PC.

EXHIBIT 7 — Temporary Internet Files

Exploring - Temporary Internet Files

File Edit View Go Favorites Tools Help

Back Forward Up Out Copy Paste Undo Delete Properties Views

Address C:\WINDOWS\Temporary Internet Files

Folders	Name	Internet Address	Type	Size	Expires	Last Modified	Last Accessed	Last Checked
History	Cookie: cstucki...	Cookie: cstucki@hc2.humanclick...	Text Document	1 KB	9/29/01 11:49 AM	9/29/00 3:41 PM	10/3/00 7:42 AM	9/29/00 3:41 PM
Inf	70246539	Cookie: cstucki@hc2.humanclick...	Text Document	1 KB	10/3/01 3:51 AM	10/3/00 7:42 AM	10/3/00 7:42 AM	10/3/00 7:42 AM
Installer	Cookie: cstucki...	Cookie: cstucki@direct.travelocit...	Text Document	1 KB	11/9/00 3:59 PM	10/11/00 9:36 AM	10/11/00 12:17 PM	10/11/00 9:36 AM
Java	Cookie: cstucki...	Cookie: cstucki@travelocity.com/	Text Document	1 KB	12/31/00 3:55 PM	10/11/00 12:18 PM	10/11/00 12:18 PM	10/11/00 12:18 PM
hsp	Cookie: cstucki...	Cookie: cstucki@ads.link4ads.com/	Text Document	1 KB	12/31/00 3:59 PM	10/3/00 7:44 AM	10/12/00 1:43 PM	10/3/00 7:44 AM
Local Settings	Cookie: cstucki...	Cookie: cstucki@www.nutritionf...	Text Document	1 KB	10/16/01 9:34 AM	10/16/00 9:35 AM	10/16/00 9:35 AM	10/16/00 9:35 AM
Media	Cookie: cstucki...	Cookie: cstucki@www.norflax.c...	Text Document	1 KB	12/30/00 4:00 PM	10/23/00 12:41 PM	10/23/00 12:41 PM	10/23/00 12:41 PM
MsAgent	Cookie: cstucki...	Cookie: cstucki@amazon.com/	Text Document	1 KB	1/1/06 12:00 AM	10/23/00 4:04 PM	10/23/00 4:04 PM	10/23/00 4:04 PM
MsApps	50arcamaxlogo	http://www.arcamax.com/ezine...	GIF Image	3 KB	None	9/5/99 12:10 PM	10/24/00 7:50 AM	10/24/00 7:50 AM
msdownld.tmp	humor	http://www.arcamax.com/ezine...	GIF Image	8 KB	None	2/17/00 7:39 AM	10/24/00 7:50 AM	10/24/00 7:50 AM
NetHood	sm_ca25v1son...	http://www.arcamax.com/Image...	GIF Image	15 KB	None	8/21/00 5:15 AM	10/24/00 7:50 AM	10/24/00 7:50 AM
Offline Web Pages	001024	http://www.arcamax.com/ezine...	JPEG Image	38 KB	None	10/6/00 6:33 AM	10/24/00 7:50 AM	10/24/00 7:50 AM
Options	1009	http://us.a1.yimg.com/us.yimg.co...	GIF Image	5 KB	4/15/01 12:00 PM	4/14/04 4:00 PM	10/31/00 8:43 AM	10/31/00 8:43 AM
pctemp	1153	http://us.a1.yimg.com/us.yimg.co...	GIF Image	3 KB	4/15/01 12:00 PM	4/14/04 4:00 PM	10/31/00 8:43 AM	10/31/00 8:43 AM
Pit	signup_admin	http://www.ppweb.com/market...	Microsoft HTM...	3 KB	None	10/30/00 10:03 AM	10/31/00 8:49 AM	10/31/00 8:49 AM
PrintHood	btn_update	http://www.ppweb.com/market...	GIF Image	2 KB	None	10/17/00 9:32 AM	10/31/00 8:49 AM	10/31/00 8:49 AM
Recent	add_sidebar_bu...	http://a72.g.akamai.net/1/72/388/...	GIF Image	2 KB	None	5/11/00 9:34 AM	10/31/00 3:15 PM	10/31/00 3:15 PM
Samples	onair_contrib_...	http://a1.g.akamai.net/1/388/1/d/...	GIF Image	14 KB	None	12/13/99 4:34 PM	10/31/00 3:15 PM	10/31/00 3:15 PM
SendTo	video	http://a388.g.akamai.net/1/388/2/...	GIF Image	1 KB	None	9/28/99 1:36 PM	10/31/00 3:15 PM	10/31/00 3:15 PM
ShellNew	newarow	http://a388.g.akamai.net/1/388/2/...	GIF Image	1 KB	None	9/6/99 2:38 PM	10/31/00 3:15 PM	10/31/00 3:15 PM
spool	hdvide	http://a388.g.akamai.net/1/388/2/...	JPEG Image	1 KB	None	7/18/00 1:23 PM	10/31/00 3:15 PM	10/31/00 3:15 PM
Start Menu	crn.worldcom	http://a97.g.akamai.net/1/97/388/...	GIF Image	1 KB	None	4/21/00 9:52 AM	10/31/00 3:15 PM	10/31/00 3:15 PM
System	divide	http://a388.g.akamai.net/1/388/2/...	JPEG Image	1 KB	None	7/18/00 1:23 PM	10/31/00 3:15 PM	10/31/00 3:15 PM
System32	audio	http://a388.g.akamai.net/1/388/2/...	GIF Image	1 KB	None	9/24/99 8:19 AM	10/31/00 3:15 PM	10/31/00 3:15 PM
Tasks	si logo	http://a388.g.akamai.net/1/388/2/...	GIF Image	1 KB	None	8/6/00 6:48 AM	10/31/00 3:15 PM	10/31/00 3:15 PM
Temp	only	http://a388.g.akamai.net/1/388/2/...	GIF Image	1 KB	None	7/19/00 11:12 AM	10/31/00 3:15 PM	10/31/00 3:15 PM
Temporary Internet Fi	CNN.com.news...	http://a388.g.akamai.net/1/388/1/...	GIF Image	2 KB	None	8/6/00 6:48 AM	10/31/00 3:15 PM	10/31/00 3:15 PM
twain_32	fm logo	http://a388.g.akamai.net/1/388/2/...	GIF Image	1 KB	None	8/6/00 6:48 AM	10/31/00 3:15 PM	10/31/00 3:15 PM
Web	time.box.com	http://a388.g.akamai.net/1/388/2/...	GIF Image	1 KB	None	8/6/00 6:48 AM	10/31/00 3:15 PM	10/31/00 3:15 PM
Windows Update Setup F	crn_button3	http://a34.g.akamai.net/1/34/388/...	GIF Image	2 KB	None	12/31/99 7:22 AM	10/31/00 3:18 PM	10/31/00 3:18 PM
(D:) Proofdrive on 'Storage' (E)	election_spinr...	http://a3.g.akamai.net/1/3/388/1/d/...	GIF Image	16 KB	None	10/30/00 6:26 AM	10/31/00 3:18 PM	10/31/00 3:18 PM
Public on 'Storage' (F)	myelart2	http://a47.g.akamai.net/1/47/388/...	GIF Image	18 KB	None	10/30/00 6:27 AM	10/31/00 3:20 PM	10/31/00 3:20 PM
Tracker on 'Storage' (G)	Cookie: cstucki...	Cookie: cstucki@cnnaudience.com/	Text Document	1 KB	12/30/07 8:00 AM	10/30/00 7:44 AM	10/30/00 7:44 AM	10/30/00 7:44 AM

1,178 object(s)

The advantage of looking at the Temporary Internet Files over any other files is that this shows you the address of the site, and when it was last modified, last accessed, and last checked. This can be very useful when gathering evidence of too much Internet access, or inappropriate Internet access. These can also be useful in proving a pattern of logon and duration times.

TRACKING OF LOGON DURATION AND TIMES

If you need to review logon duration and times for a given user, you should contact the organization's network operations group (or similarly named/empowered department). This group can provide reports on any given IP address, user ID, and the times that the IP address and ID was logged into the network. Some of these reports can actually tell what addresses the user accessed and when. The most basic report should be able to tell when the ID was logged into the system and when it logged off. With some of the current system architecture, the reports track and log all user activity down to the keystroke. However, this detailed logging does pull down the performance of the servers, so the logging is not always done to this level of detail. You must ask your network operations personnel what type of reporting and subsequent information is available.

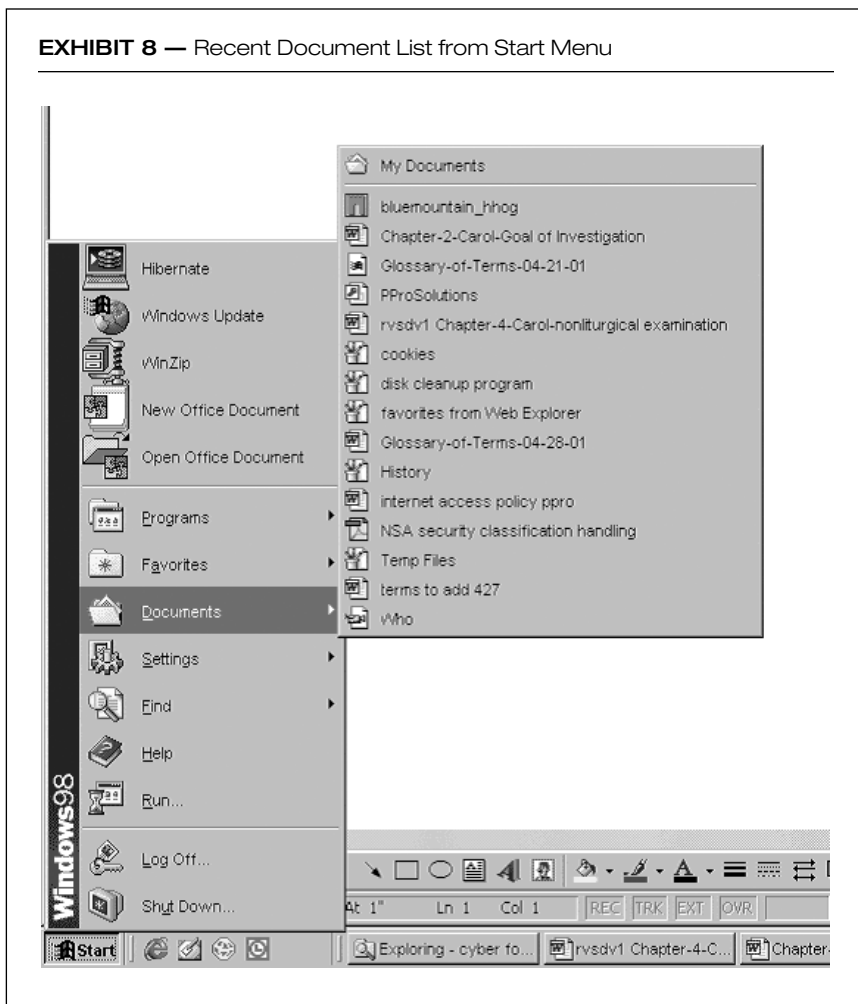
Ask for the entire detail report and see what they record; do not just ask for the basics; you might save time and effort if you ask for everything up front. What you ask for should include not only the activity but also the server monitor reports that pertain to the user, traffic monitoring, and site click-through reports. You want any report that exists that might show what a given user was doing at any moment. You might be surprised just how much information is available and how eager the operations staff personnel are to use their expertise.

Some of the evidence you can gather to help determine logon and duration times can be derived from the Temporary Internet Files and Recent Documents list. These files can help establish and support patterns of use. Although a smart user might clean up these files frequently using the disk cleanup utilities that Windows provides, it is always good to check to see what information is available. The cleanup utilities are in the Start Menu, Programs, Accessories, Disk Cleanup. This utility erases the Internet files, temporary files, and most cookies. See prior sections of this article on how to find and access Temporary Files.

RECENT DOCUMENTS LIST

The recent documents list can show you the latest documents that a user has accessed. There are two ways to see this list of documents, but only one shows you when the items on the list were accessed. First, you can see the documents from the Start menu, under the Documents "tab"/selection. You can click on any one of the documents listed and the docu-

EXHIBIT 8 — Recent Document List from Start Menu



ment is brought up on the screen (see [Exhibit 8](#)). You can also access the same list, via the Recent sub-folder under the Windows folder (see [Exhibit 9](#)). This view will give you the name of the document and when each was last modified. Windows 95 does not have this directory; only Windows 98 and more recent copies of Windows have a Recent directory.

TRACKING OF ILLICIT SOFTWARE INSTALLATION AND USE

If you are investigating a user who may be loading illegal, illicit, or non-work-related software on his or her PC, there are a number of places to check within the PC in question to prove or disprove these unauthorized (and maybe even illegal) actions. Some of these key places include the System Registry, System Information, and by simply viewing the hard drive's contents.

EXHIBIT 9 — Recent Documents List Hard Drive View

The screenshot shows a Windows Explorer window titled "Exploring - Recent". The address bar displays "C:\WINDOWS\Recent". The left pane shows the "Folders" tree with "Recent" selected. The right pane displays a list of recent documents with columns for Name, Size, Type, and Modified. The list includes files such as "AEC TFR list", "Agenda 1212", "APPENDIX A - Book Proposal ONLY", "Boggett - Applications Dev", "bluemountain_xmas", "Computer-Forensics-Book-Proposal", "Goal of Investigation", "H10466-2 PSM Web Link", "H10665-2 AUJ Web Link", "Parameters for PSM and AUJ utility", "PSM AUJ Home Page", "Strategic Development Meeting 120800", and "tpr priority list".

Name	Size	Type	Modified
AEC TFR list	1KB	Shortcut	12/9/00 4:14 PM
Agenda 1212	1KB	Shortcut	12/10/00 2:47 PM
APPENDIX A - Book Proposal ONLY	1KB	Shortcut	12/10/00 6:32 PM
Boggett - Applications Dev	1KB	Shortcut	12/10/00 2:39 PM
bluemountain_xmas	1KB	Shortcut	12/8/00 3:05 PM
Computer-Forensics-Book-Proposal	1KB	Shortcut	12/10/00 6:33 PM
Goal of Investigation	1KB	Shortcut	12/10/00 4:52 PM
H10466-2 PSM Web Link	1KB	Shortcut	12/9/00 3:44 PM
H10665-2 AUJ Web Link	1KB	Shortcut	12/9/00 3:44 PM
Parameters for PSM and AUJ utility	1KB	Shortcut	12/9/00 3:44 PM
PSM AUJ Home Page	1KB	Shortcut	12/9/00 3:44 PM
Strategic Development Meeting 120800	1KB	Shortcut	12/9/00 6:03 PM
tpr priority list	1KB	Shortcut	12/9/00 3:48 PM

13 object(s) 5.66KB (Disk free space: 3.39GB) My Computer

Before you begin this part of an investigation, you must first get a listing of all approved software that can reside on a given PC. This list most probably contains things such as Word, Excel, Microsoft Office, and other work-related software. There should be a master list (i.e., database) of what software resides on every PC that Operations maintains. However, with some site license agreements most of the software might be on a checklist, which Operations personnel use to set up new PCs. Not all these software programs might be on every PC.

The company policies and procedures should have an outline of the software that is not permitted to be loaded on a company-owned PC. The most recognizable programs that are usually not work related are games. When looking for these types of programs, look carefully at the names of the files; users often change the names to avoid detection. To double-check the programs' legitimacy, actually launch all **.Exe** files to ensure that you get accurate information about what is actually behind the file's name and residing on the PC. Remember: this procedure should be carried out on the mirror-imaged, working copy data, and not on the original PC — both to avoid corrupting seized data as well as disrupting networked services or other legitimate data that may reside on the PC in question.

As you are checking the software list, you should also note all the serial numbers and registration numbers of all software that resides on the PC. These numbers should be compared to the software licenses held by the company to ensure that the loaded software is both legal and authorized. For example, a user might have MS Access on his or her PC, but the company might not have authorized or actually loaded this on that user's PC. The user might have obtained certain software packages in some manner, however, not complying with company procedures and thus it has been illegally installed on the PC. This is the most common type of illegally installed software on company equipment today. This is most risky to a company because software license infringement can be expensive to a company if it is discovered and not corrected.

Okay, how do you actually begin to search for this evidence? First, you need your lists of what can be on any given PC and what is registered to be on the specific PC you are investigating. You are also looking for a list of all information that pertains to the PC under review; specifically, information such as verification of assignment of the PC to a specific employee and, if available, all software licensed for the given PC. You should then check and compare the information on these lists against the master list maintained by Operations.

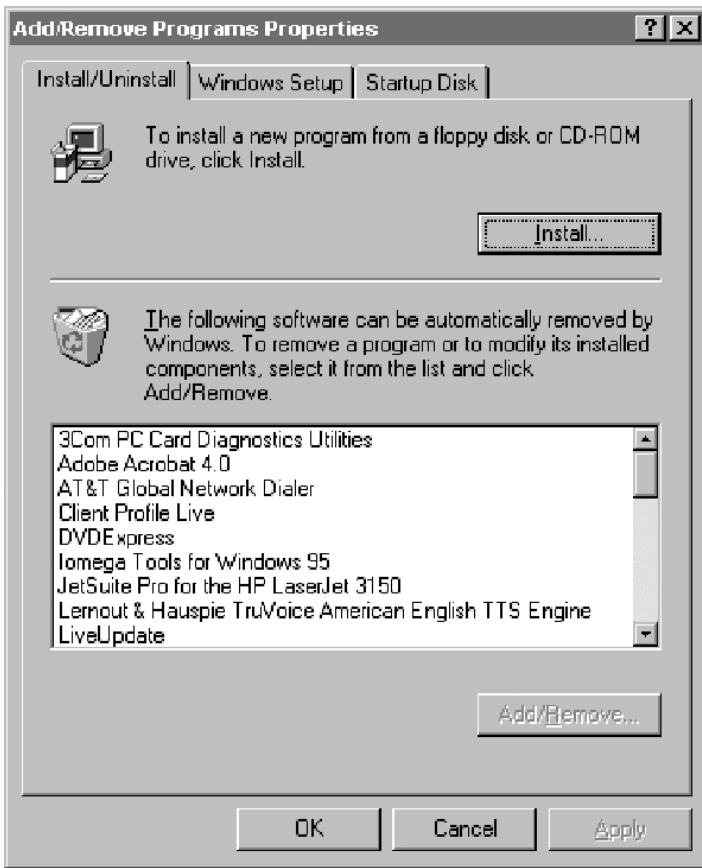
Next, you need to list all the programs that currently reside on the PC. There are several ways to accomplish this. One method is to use the System Registry files; we refer to this as the System Review. Another method is to review all files via the PC directories (i.e., Explorer); we refer to this as the Manual Review. Both methods are discussed briefly in the following paragraphs.

THE SYSTEM REVIEW

The system review can be conducted using some automated methods. One of these methods is to use the System Registry files. There are several System Registries. We discuss the two primary Microsoft registry files. One is a list of all software loaded on the PC; the other is a more comprehensive list of what is loaded, when it was loaded, and how it is configured. Both can be used to verify that illegal or non-work-related software or hardware was loaded onto a given PC.

The more simple list of what has been loaded can be viewed by accessing the path from the Control Panel, to the Add/Remove Programs icon (see [Exhibit 10](#)).

EXHIBIT 10 — Add/Remove Programs Software Listing



A more comprehensive list of software and hardware that have been loaded onto a PC can be obtained via the Microsoft System Information panels. The following path can access these: Start, Programs, Accessories, System Tools, System Information (see [Exhibit 11](#)). This screen shows the basic system information of the PC being investigated. The most useful information about a PC can be found under the Components directory. This is where you will find some history — when things were loaded and last modified (see [Exhibit 12](#)).

There are three levels of information shown on this screen: Basic, Advanced, and History. All three can provide needed information in an investigation, depending on what you are looking to prove.

The Components/System/Basic Information can help determine if illegal or non-work-related software was loaded onto a PC (see [Exhibit 12](#)). To determine if there is illegal software or non-work-related software on the PC using this list, first you need a list of all legal software that should be on the machine, along with any serial or license numbers for the software. This list should be available from the Operations department that distributes and fixes the PCs. Next, take this list and verify what software is on the machine; be sure to check the serial numbers. The Components/System/Basic Information list tells you what software is on the machine and when it was loaded. But the serial numbers will be in the “about” information or start-up screen for the software. If the software is not work related, it will not be on your list from the Operations department. You must check company policies about loading non-work-related software on company PCs.

Another view to see if software has been loaded onto the PC from the Web is available via Windows Explorer, in the Windows Directory under the Download Program sub-folder (see [Exhibit 13](#)).

The Components/System/History information can show when a component (piece of hardware or firmware) was loaded and when it was last modified (see [Exhibit 14](#)). However, many components are modified when the user reboots or turns on the computer. The “red herring” items to look for in this history would be things that were not issued with the computer and the user added himself. These might include graphics cards, emulators, or sound cards. The Component/History files are not much different in the information that they provide (see [Exhibit 14](#)).

[Exhibit 15](#) shows what has been updated in the last seven days. The Complete History file shows when items were loaded or when they were modified since last being loaded.

THE MANUAL REVIEW

One of the reasons for conducting the Manual Review as well as the System Review is to ensure you have covered all of the bases. What the

EXHIBIT 11 — System Information Base Screen

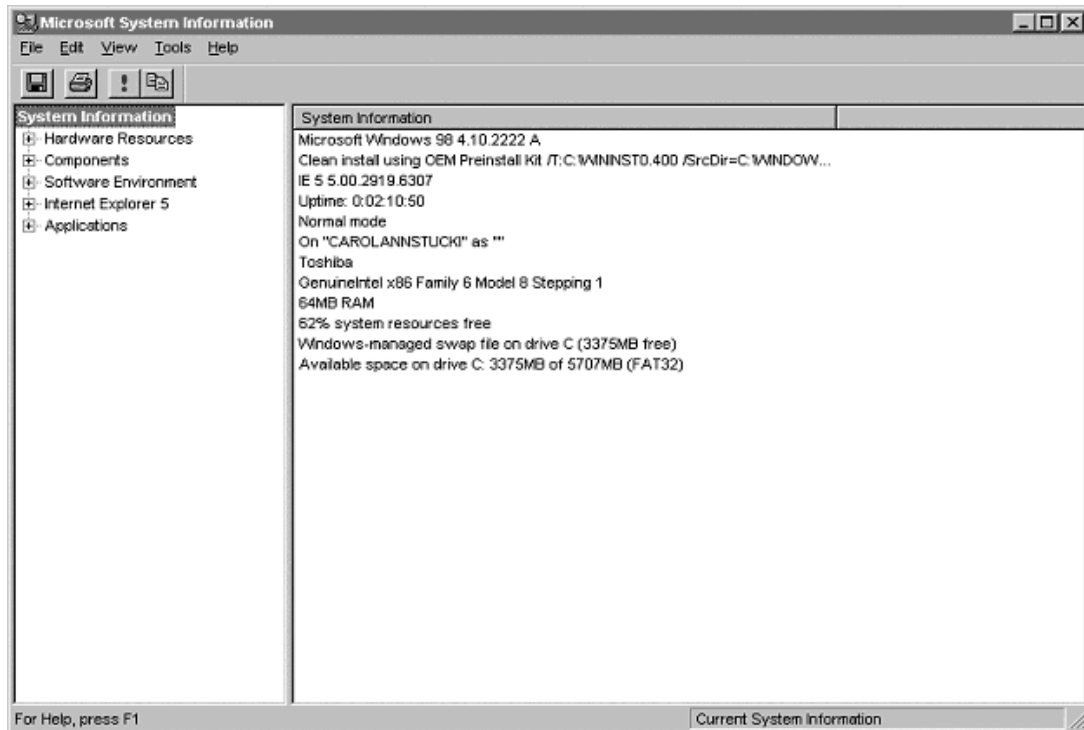


EXHIBIT 12 — System Information/Components/System/Basic Information

The screenshot shows the Microsoft System Information application window. The left-hand pane displays a tree view of system components, with 'System' selected under the 'System' category. The right-hand pane displays the 'Basic Information' tab, which is divided into several sections: Processor support, Plug and Play Software Device Enumerator, Advanced Configuration and Power Interface (ACPI) BIOS, System board, Toshiba GSXS Device, SCI IRQ used by ACPI bus, and Composite Power Source. Each section lists system resources and drivers with their respective file names, dates, times, and sizes.

Microsoft System Information

File Edit View Tools Help

System

Basic Information Advanced Information History

Processor support

System
 Alloc resources: None
 Driver: update.sys 4/23/1999 10:22 PM Size: 60592

Plug and Play Software Device Enumerator

SYSTEM
 Alloc resources: None
 Driver: streamcl.dll 4/23/1999 10:22 PM Size: 20480
 ks.sys 4/23/1999 10:22 PM Size: 98432
 swenum.sys 4/23/1999 10:22 PM Size: 3296

Advanced Configuration and Power Interface (ACPI) BIOS

System
 Alloc resources: None
 Driver: vpowerd.wd 9/28/1999 6:35 PM Size: 37547
 power.drv 4/23/1999 10:22 PM Size: 1920
 pci.wd 8/11/1999 8:41 AM Size: 65919
 acpi.sys 4/23/1999 10:22 PM Size: 83136

System board

System
 Alloc resources: None

Toshiba GSXS Device

System
 Alloc resources: None

SCI IRQ used by ACPI bus

System
 Alloc resources: Logical Configuration 0
 IRQ: 9 Mask: x0200

Composite Power Source

System
 Alloc resources: None
 Driver: battc.sys 4/23/1999 10:22 PM Size: 6432

For Help, press F1 Current System Information

EXHIBIT 13 — Downloaded Programs Viewed from Windows Explorer

The screenshot shows a Windows Explorer window titled "Exploring - Downloaded Program Files". The left pane shows the "All Folders" tree with "Downloaded Program Files" selected. The right pane displays a table of installed files.

Program File	Status	Total Size	Creation Date	Last Accessed
Button.webabutton	Installed	96 KB	7/30/99 10:04 AM	7/6/00
CV3 Class	Installed	256 KB	3/21/00 2:55 PM	4/24/00
DirectAnimation Ja...	Installed	608 KB	10/16/99 8:53 PM	10/16/99
InstallControl Class	Installed	256 KB	10/26/00 1:54 PM	1/24/01
Internet Explorer Cl...	Installed	128 KB	10/16/99 8:53 PM	10/16/99
Microsoft XML Par...	Installed	192 KB	10/16/99 8:53 PM	10/16/99
PWImageControl ...	Installed	256 KB	3/30/00 1:13 PM	6/15/00
Shockwave Flash ...	Installed	32 KB	8/17/00 6:43 PM	4/16/01
webascn.WebAd...	Installed	960 KB	10/2/99 5:32 PM	7/6/00
Win32 Classes	Installed	704 KB	10/16/99 8:53 PM	10/16/99

10 object(s)

EXHIBIT 14 — System Information/Components/System/History

The screenshot shows the Microsoft System Information application window. The left-hand pane displays a tree view of system components, with 'System' expanded and 'History' selected. The right-hand pane displays the 'History' tab for the System component, showing details for Processor support, Plug and Play Software Device Enumerator, and System board.

Microsoft System Information

File Edit View Tools Help

System

Basic Information Advanced Information **History**

Processor support
 Last Change Tue Dec 26 09:44:01 2000
 Driver: update.sys 4/23/1999 10:22 PM Size: 60592
 Original Configuration Thu Oct 07 10:11:59 1999 to Tue Dec 26 09:44:01 2000
 Alloc resources: None
 Driver: update.sys 4/23/1999 10:22 AM Size: 60592

Plug and Play Software Device Enumerator
 Last Change Tue Dec 26 09:44:01 2000
 Driver: streamci.dll 4/23/1999 10:22 PM Size: 20480
 Driver: ks.sys 4/23/1999 10:22 PM Size: 98432
 Driver: swenum.sys 4/23/1999 10:22 PM Size: 3296
 Original Configuration Thu Oct 07 10:11:59 1999 to Tue Dec 26 09:44:01 2000
 Alloc resources: None
 Driver: streamci.dll 4/23/1999 10:22 AM Size: 20480
 Driver: ks.sys 4/23/1999 10:22 AM Size: 98432
 Driver: swenum.sys 4/23/1999 10:22 AM Size: 3296

Advanced Configuration and Power Interface (ACPI) BIOS
 Last Change Tue Dec 26 09:44:01 2000
 Driver: vpowerd.vxd 9/28/1999 6:35 PM Size: 37547
 Driver: power.drv 4/23/1999 10:22 PM Size: 1920
 Driver: pci.vxd 8/11/1999 9:41 AM Size: 65919
 Driver: acpi.sys 4/23/1999 10:22 PM Size: 83136
 Original Configuration Thu Oct 07 10:11:59 1999 to Tue Dec 26 09:44:01 2000
 Alloc resources: None
 Driver: vpowerd.vxd 4/23/1999 10:22 AM Size: 37523
 Driver: power.drv 4/23/1999 10:22 AM Size: 1920
 Driver: pci.vxd 4/23/1999 10:22 AM Size: 65895
 Driver: acpi.sys 4/23/1999 10:22 AM Size: 83136

System board
 Original Configuration Thu Oct 07 10:11:59 1999 to Date
 Alloc resources: None

For Help, press F1 Current System Information

EXHIBIT 15 — System Information/Component/History/Last Seven Days

The screenshot shows the Microsoft System Information application window. The left-hand pane displays a tree view of system components, with 'History' selected under the 'System' category. The right-hand pane shows the 'History' tab, which is set to 'Last Seven Days'. The main content area lists several system components with their last change dates and driver information:

- Dial-Up Adapter**
Last Change Tue Dec 26 09:44:01 2000
Alloc resources: None
Driver: pppmac.wxd 4/23/1999 10:22 PM Size: 235585
- Processor support**
Last Change Tue Dec 26 09:44:01 2000
Driver: update.sys 4/23/1999 10:22 PM Size: 60592
- Plug and Play Software Device Enumerator**
Last Change Tue Dec 26 09:44:01 2000
Driver: streamci.dll 4/23/1999 10:22 PM Size: 20460
Driver: ks.sys 4/23/1999 10:22 PM Size: 98432
Driver: swenum.sys 4/23/1999 10:22 PM Size: 3295
- Advanced Configuration and Power Interface (ACPI) BIOS**
Last Change Tue Dec 26 09:44:01 2000
Driver: vpowerd.wxd 9/28/1999 6:35 PM Size: 37547
Driver: power.drv 4/23/1999 10:22 PM Size: 1920
Driver: pci.wxd 8/11/1999 9:41 AM Size: 65919
Driver: acpi.sys 4/23/1999 10:22 PM Size: 83136
- Toshiba GSXS Device**
Original Configuration Tue Dec 26 09:44:01 2000 to Date
Alloc resources: None
- Infrared Communication Device**
Original Configuration Tue Dec 26 09:44:01 2000 to Date
Alloc resources: None
Driver: IrXfer.cnt
Driver: IrXfer.hlp
Driver: Ir_Nonwxdbr
Driver: IrSmall.dll 4/23/1999 10:22 PM Size: 45056
Driver: IrXfer.exe 4/23/1999 10:22 PM Size: 102400
Driver: Irmon.exe 4/23/1999 10:22 PM Size: 135168
Driver: infrared.cpl 4/23/1999 10:22 PM Size: 16896
Driver: infrared.cnt

At the bottom of the window, there is a status bar with the text 'For Help, press F1' on the left and 'Current System Information' on the right.

Manual Review will tell you, that the System Review will not, is what actual applications reside on the PC.

The first step in the manual review is to locate all executable programs/applications on the PC. To do this on the PC, start Explorer — not the Web Browser Internet Explorer, but the Microsoft Explorer. Once there, from the top menu select Tools, Find, Files and Folders. This gives you a pop-up box where you can identify what you want to search for. In this case, we use a wild card query to find all files ending with **.Exe**, or all executable files. Set the “Look in” field to the drive you are investigating; this is usually the C: drive. Select option to look at **all** of the C: drive. See [Exhibit 16](#) for an example of the results of this search.

This can be quite an extensive list. However, you should check each of these references to ensure they do belong to authorized programs. Most unauthorized programs are put under the Programs directory, but do not assume anything; check them all. You can check them by actually launching them. You can do this by clicking on the file from the Find screen. However, to record your findings, it might be best to print this screen and manually check off each item on the list as you verify it.

A quick review of the items in the list might narrow your investigation. If you see icons on the far left that represent something suspicious, you might investigate these first. Suspicious items might include game or playing card icons. See [Exhibit 17](#) for an example of an excerpt of the full list.

[Exhibit 17](#) shows an item on the list with a Playing Card icon — see the freeplus item? This is actually a game, and for most companies and systems may be a violation and should not be installed on the PC.

Another thing to watch out for on your listing of files are Hidden files (see discussion below). You need to check the system standards and settings to determine if the file manager allows you to see these or not before assuming your file list is complete.

HIDDEN FILES

A hidden file is a file with a special hidden attribute turned on so that the file is not normally visible to users. For example, hidden files are not listed when you execute the DOS DIR command. However, most file management utilities allow you to view hidden files.

DOS hides some files, such as MSDOS.SYS and IO.SYS, so that you cannot accidentally corrupt them. You can also turn on the hidden attribute for any normal file, thereby making it invisible to casual snoopers. On a Macintosh, you can hide files with the ResEdit utility.

Why are hidden files important to your investigation? If you do not have the settings on the Folder Options set to allow you to view hidden files, you might miss evidence. To review the settings on the PC you are

EXHIBIT 16 — Find Files Named: *.exe

Find: Files named *.exe

File Edit View Options Help

Name & Location | Date | Advanced

Named: *.exe

Containing text:

Look in: (C:)

Include subfolders

Find Now

Stop

New Search

Browse...

Name	In Folder	Size	Type	Modified
Fileicons	C:\WINDOWS\Application Data\Microsoft\Installer\00...	11KB	Application	12/14/00 11:07 AM
Fileicon	C:\WINDOWS\Application Data\Microsoft\Installer\20...	64KB	Application	12/14/00 11:27 AM
misc	C:\WINDOWS\Application Data\Microsoft\Installer\20...	28KB	Application	12/14/00 11:27 AM
Quick Search	C:\WINDOWS\Favorites\Links	44KB	Application	12/29/99 2:36 PM
Toggle Images	C:\WINDOWS\Favorites\Links	30KB	Application	12/29/99 2:36 PM
Agentavr	C:\WINDOWS\Mesagent	269...	Application	10/13/98 8:08 PM
tssetup	C:\TOSHBA	24B	Application	11/19/99 5:00 PM
tdiags	C:\TOSHBA	27KB	Application	11/19/99 5:00 PM
Srvpw	C:\TOSHBA	3KB	Application	11/19/99 5:00 PM
Tver	C:\TOSHBA	84B	Application	11/19/99 5:00 PM
Mouse	C:\WOUSE	103...	Application	11/18/99 8:37 AM
Setup	C:\WOUSE\UNINSTAL	123...	Application	8/6/99 12:34 PM
Em_execc	C:\WOUSE\SYSTEM	38KB	Application	11/18/99 8:37 AM
Crdswitx	C:\WOUSE\SYSTEM	24KB	Application	11/18/99 8:37 AM
Kbdtray	C:\WOUSE\SYSTEM	20KB	Application	11/18/99 8:37 AM
dsuninst	C:\Program Files\YAMAHAYAMAHA OS-XG Driver	97KB	Application	10/15/99 2:03 PM
Units32	C:\Program Files\YAMAHAYAMAHA OS-XG Driver	43KB	Application	9/21/99 6:01 PM
Cx32	C:\Program Files\WebMeeting	5KB	Application	12/14/00 11:26 AM
Conf	C:\Program Files\WebMeeting	630...	Application	12/14/00 11:26 AM
Web32	C:\Program Files\WebMeeting	5KB	Application	12/14/00 11:26 AM
Sysagent	C:\Program Files\Plus!	38KB	Application	4/23/99 10:22 PM
Cncagent	C:\Program Files\Plus!	248...	Application	4/23/99 10:22 PM
Themes	C:\Program Files\Plus!	112...	Application	4/23/99 10:22 PM
Noconp	C:\Program Files\Plus!\SYSTEM	71KB	Application	4/23/99 10:22 PM
wabnig	C:\Program Files\Outlook Express	35KB	Application	11/21/00 2:24 PM
wab	C:\Program Files\Outlook Express	23KB	Application	11/21/00 2:24 PM
msimn	C:\Program Files\Outlook Express	42KB	Application	12/14/00 11:27 AM
msimn	C:\Program Files\Outlook Express	72KB	Application	12/14/00 11:26 AM

400 file(s) found

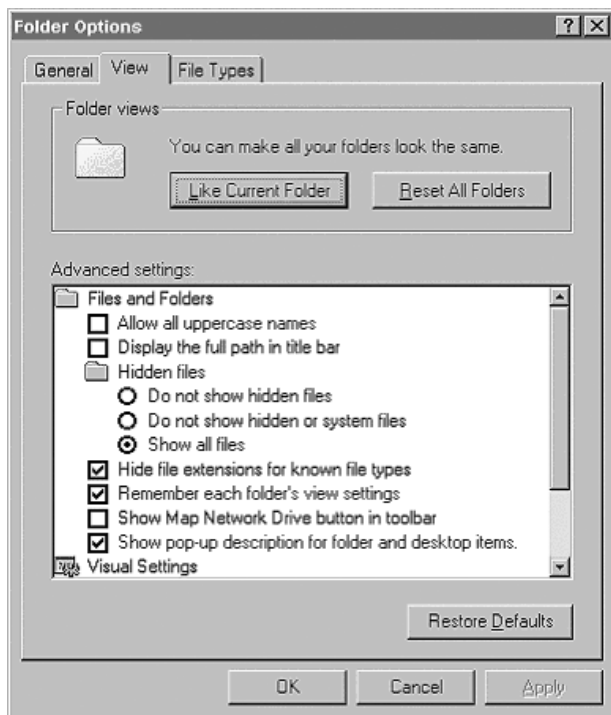
EXHIBIT 17 — Find Files Named: *exe Excerpt of List

Name	In Folder	Size	Type
Network Diagram Wizard	C:\Program Files\Visio\Solutions\Network Diagram	837...	Application
Network Database Wizard	C:\Program Files\Visio\Solutions\Network Diagram	1,0...	Application
Network Equipment Information	C:\Program Files\Visio\Solutions\Network Diagram	69KB	Application
Unwise	C:\Program Files\treeplus	70KB	Application
treeplus	C:\Program Files\treeplus	121...	Application
ringstart	C:\Program Files\omega\Tools	19KB	Application
lowwatch	C:\Program Files\omega\Tools	21KB	Application

investigating to ensure that you see hidden files, you need to launch Explorer. From the top menu within Explorer, select View, Folder Options, and the View Tab on the pop-up box (see [Exhibit 18](#)).

If the radio buttons are marked so that the hidden files are not to be shown, you will not see all the files. You should reset these so that you can see the hidden files and ensure that you have a complete list.

EXHIBIT 18 — Folder Options to See Hidden Files



HOW TO CORRELATE THE EVIDENCE

Now that you have captured the file evidence and the data, you can graph an access pattern or list the illegal software and when it was loaded. Next, you need to check the access and download dates and times against the timesheets, surveillance, and other witness accounts to ensure that the suspect under investigation actually had the opportunity to engage in unauthorized acts using the PC in question.

In other words, you need to ensure that the employee under investigation actually had access to the equipment on the dates and times listed in the evidence. For example, if the employee had a desktop PC and did not come to work on the date that illegal software was downloaded on his PC, then you might need to look for other supporting evidence (e.g., access logs indicating potential access from an external/remote location). Be advised that the investigator must obtain solid evidence that the employee under investigation actually had an opportunity and was actually using the PC at the time that the unauthorized action took place. Failing to link the employee to the PC and to corroborate and substantiate the evidence, in an irrefutable manner, will result in an inability to hold the employee accountable for his or her actions and further to prosecute the employee via the existing legal system.

When reviewing the evidence you have gathered, you need to follow and show the facts — and only the facts. If you have to make leaps in your logic to get from point A to point B, then you do not have enough evidence to substantiate a claim.

Also, you need to ensure that you can adequately explain how the employee under review was able to commit the offense, illegal act, unauthorized action, etc., and also be able to present evidence/proof of how it was done. This proof should be simple to follow so that there is no doubt that the offense was committed. Someone's career, in addition to their legal freedoms, could be on the line as a result of your findings, as well as the organization's liability (for a wrongful or unsubstantiated accusation). Thus, you want to be sure.

Notes

1. Webopedia, www.webopedia.com, Computer Terms and Definitions Web Site.
2. Tinnirello, P., Ed. *Handbook of Systems Development 1999*, Auerbach Publications, Boca Raton, FL, 1999.

Carol Stucki is working as a technical producer for PurchasePro.com, a rapidly growing dot.com company that is an application service provider specializing in Internet-based procurement. Carol's past experience includes working with GTE, Perot Systems, and Arthur Andersen as a programmer, system analyst, project manager, and auditor.