

# **CSI For The Home PC**

Computer Forensics Inc.™

Television crime shows such as “Law and Order” and “CSI” show computer forensic examiners looking for the one computer clue that will put the perpetrator in the big house. Although the techniques portrayed in television investigations look complicated, here’s where an average computer user can put a little forensics into their life.

## **First Stage of the Investigation**

The first step toward investigating the use of your home computer is to understand the basic storage system used by Windows to manage Internet activity.

On your computer, go to a major news website, such as [www.cnn.com](http://www.cnn.com), [www.abcnews.com](http://www.abcnews.com), or [www.espn.com](http://www.espn.com). Notice how quickly the text of the first page appears. You will notice that the graphics take additional time to display properly on the system, generally appearing one at a time. This is because your computer system is asking another computer to send the files necessary to display the web page properly on your machine. Each web page is made up of numerous photographs, banners, and readable text that need to be transferred to your computer system. These files are stored in your Internet cache (for example, the Temporary Internet Files folder created by Microsoft’s Internet Explorer).

Web-based email, such as Hotmail and Yahoo Mail, is transmitted and displayed just like any other web page. This means that copies of these messages may be stored on the computer hard drive and may be viewed as files even after the computer is disconnected from the Internet.

By default, these files do not go away when you sign off the Internet. They stay buried in the directory structure of your hard drive. The contents of any type of web page you view may be stored on your computer’s hard drive.

## **Make Me a Cyber Sleuth**

There are a few simple procedures that any novice computer user can follow to track activity on their computer system. The sample procedures described are based on the Microsoft Windows platform. Of course, Windows is not the only operating system available, but it is the operating system we receive most often for examination in our forensics lab. We will also use Microsoft’s Internet Explorer as our example (sorry Netscape users) for the same reason. Note that these procedures are not true forensic procedures and should not take the place of a computer forensic examination, when warranted. They are, however, a handy way to learn where people have been.

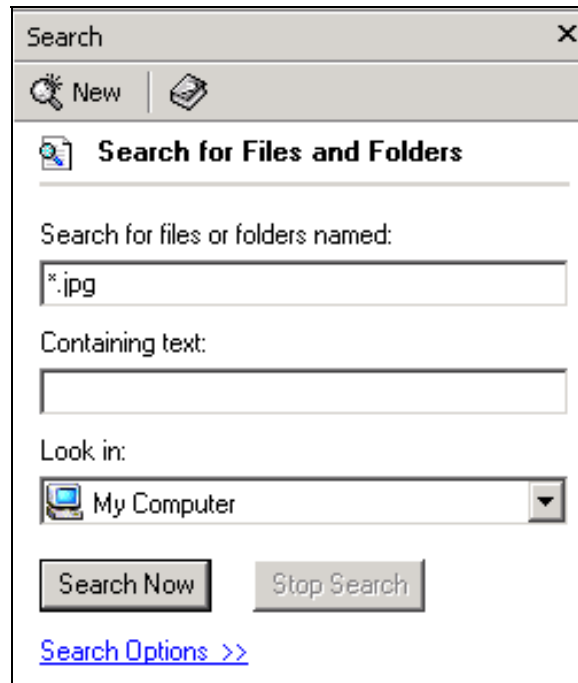
Our starting place is the Microsoft Windows search function. This simple tool, available as part of the Windows operating system, enables a user to perform advanced searches for images, programs, and email. Even if you don't know what you are looking for, the search tool has advanced features that allow you to locate files that may fit your criteria. The real power, however, of Windows "search" isn't in the software, but rather in the methods and terms you use to identify files and Internet activity.

### A Picture is Worth a Thousand Words

The majority of photographs viewed on the Internet are in a format known as "JPEG," which has an extension displayed as ".jpg." This is similar to the way Microsoft's Word files display a ".doc" extension, or a simple text file displays a ".txt" extension. When a user surfs the Internet, the graphics within each page are downloaded to the user's computer hard drive. These graphics are stored in the "Temporary Internet Files" folder and remain on the hard drive until the user or the operating system deletes the files. This folder contains both individual graphics and entire web pages that have been viewed from that computer.

Using the Windows "search" tool, you can run a search for "\*.jpg" (Figure 1) to locate all JPEG files in the directory structures of all drives connected to the computer.

Figure 1



Simply enter the file name as \*.jpg, choose to look in My Computer, and click on Search. After executing the search, use the View, Thumbnails feature of Windows XP Explorer to view folders of graphics in a “Thumbnails” or mini-picture mode. This not only makes it easier to view the graphics, but also eliminates the need to open each file. Click on the View tab and check the Thumbnails option.

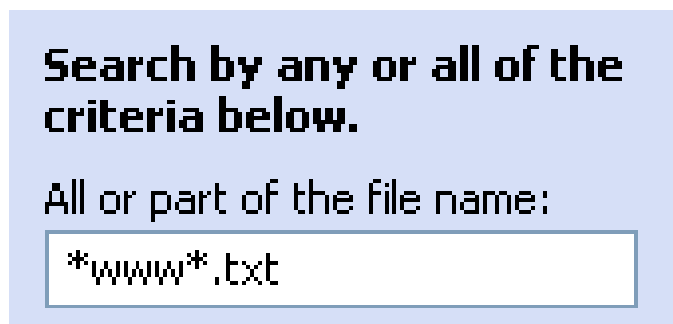
Another commonly seen graphic file type is a “Gif” file, or a file with “.gif” as an extension. These files are generally used to make web site banner ads advertising other web sites or products. As before, use the Windows search tool to find all occurrences of “\*.gif” on My Computer, and view them in thumbnail mode. Banner ads are a popular tool used by adult-oriented websites to lure viewers to additional sites containing the same type of material.

### Follow the Cookie Crumb Trail

Cookies are more than a snack treat! They are also small files placed on a user’s computer hard drive by the web sites they visit. Have you ever returned to a web site and found that the site already knew your name? This is because a cookie was placed on your computer during one of your previous visits. These files contain complex identifying information that can be viewed by forensic examiners. The file names alone, however, usually point to the website of origin. Sites with adult-oriented material may be easily identified by name. Cookies are located in a folder labeled “Cookies” that is stored in the same general area as the Temporary Internet Files folder.

A search for cookies can be relatively easy. Cookies generally appear in the format: [USERNAME@www.websitename.com.txt](#). For example: a cookie might be labeled [SuziQ@horsesarefun.txt](#). To search for all cookies on a computer, enter the text “\*www\*.txt” (Figure 2) and click on Search. This search may not turn up all cookies in the computer’s directory structure, but it should locate most of them.

Figure 2



Look at the results of the search. If your computer is divided into multiple user accounts, you will be able to see which account was used to access the website that created the cookie on the computer (Figure3).

Figure 3



The example in Figure 3 shows cookies generated by Internet activity for the account holder “Tera”. Adult-oriented sites with obvious names can be easily located using this method. Other web site names may be harder to decipher, and may require further investigation, such as simply asking the account owner what the page really is.

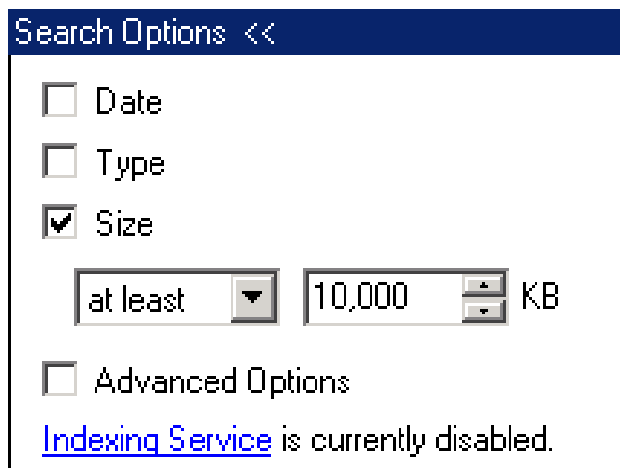
### Hide...and Seek

Image and movie files take up great amounts of space on a computer’s hard drive. Because of their size, they also take a lot of time to download to the computer hard drive. This is especially true when a dialup Internet Service Provider (ISP) account such as Earthlink or AOL is used, as opposed to a DSL or cable-modem connection. Smart users quickly learn that the downloaded files they want to view over and over are better kept on the hard drive, instead of having to re-download each time they go back to the web site.

A savvy computer user will typically hide adult-oriented files deep in the computer’s directory structure, counting on the fact that most users don’t explore the computer’s directory structure outside of the My Documents folder. A common place to hide pictures or movies is in the Windows system directories, side by side with Windows operating system files. The Windows operating system in most cases will disregard these unwanted directories because the system looks only for what it needs to operate correctly. An innocuously named folder full of photos and movies can be slipped in between the system folders and never noticed by other users of the computer.

Image and movie files take up significantly more space than average files. A search by file size (rather than name) can help locate out-of-place folders. Use the Windows search tool’s advanced features (Figure 4) to locate files based on size, rather than by file extension. Look for any large files that appear with adult-oriented names. Start looking for very large files, in excess of 10,000 KB, or 10 Megabytes in size. Files this large are likely to be movies.

Figure 4



### History's Mysteries

Microsoft Internet Explorer creates files named “Index.dat” and places these files in numerous locations in the computer’s directory structure. These files track Internet usage and can be viewed using Microsoft’s Notepad program. To perform a search for files named “Index.dat,” right click on the files and choose “Open With” the Notepad program. The text in an index.dat file looks like garbled junk; however, information about where the computer has been on the Internet can be buried among the seemingly random characters. After opening an index.dat file in Notepad, click on “Edit” and then “Find.” Enter the text “www” to search the file for website names. This may not be smoking gun evidence, however, a large number of suspicious or inappropriate names, combined with other findings, may give you a picture of where the user has been.

### Insects Frozen in Amber

Each time a user views Internet-based email they are looking at web pages. As noted before, the contents of a web page are downloaded to the hard drive for viewing with a web browser. As a result, the entire page contents are on the hard drive. These pages can still be viewed when the computer is disconnected from the Internet. Using the same search techniques noted earlier, a search for “\*.html” and “\*.htm” will locate the base component for the majority of pages viewed on the computer system. Use the View, Options tab and check “Details” to reveal information about each file—most importantly the “last modified date.” This date can give you an idea of when the page was last viewed.

**Be sure the computer is not connected to the Internet** when you look at the results of your “html” and “htm” searches. Choose “Work Offline” in the File menu before proceeding, otherwise, the computer will access the live web sites when you open each file.

A review of the static files on the hard drive will reveal how much information is stored on an individual computer system.

### **Think Before You Sleuth**

One piece of information gathered from a computer is not evidence of wrongdoing. Just as on “CSI,” all the evidence should be considered before reaching a conclusion. There are reasonable explanations for finding a few inappropriate files on a computer’s hard drive. We’ve all received popup banners or suggestive email from an unknown source. Spam and other unwanted material do get delivered to innocent systems routinely, so remember not to jump to conclusions too soon.

Many members of the household usually use home PC’s. Tell your children that your primary concern is to protect them from predatory behavior on the Internet. Tell them that you routinely check the system for “unwanted” material. As for adults, an open discussion of computer privacy expectations protects everyone from potentially embarrassing scenarios.