

UNIT-III

Forensics analysis and validation

Forensic analysis:

Forensic analysis definition can be described as a detailed process of detecting, investigating, and documenting the reason, course, and consequences of a security incident or violation against state and organization laws.

Forensic analysis is often used for providing evidence in court hearings, especially in criminal investigations. It involves the use of a wide range of technologies and investigative methods and procedures. Forensic specialists gather different types of information by working with electronic devices.

Forensic validation:

Validation is the confirmation by examination and the provision of objective evidence that a tool, technique or procedure functions correctly and as intended. One of the most critical aspects of computer forensics is validating digital evidence because ensuring the integrity of data you collect is essential for presenting evidence in court.

Determining What Data to Collect and Analyze

Examining and analyzing digital evidence depend on the nature of the investigation and the amount of data to process. Criminal investigations are limited to finding data defined in the search warrant, and civil investigations are often limited by court orders for discovery.

Corporate investigators might be searching for company policy violations that require examining only specific items, such as e-mail. Therefore, investigations often involve locating and recovering a few specific items, which simplifies and speeds processing.

Scope creep: In which an investigation expands beyond the original description because of unexpected evidence you find, prompting the lawyer to ask you to examine other areas to recover more evidence. Scope creep increases the time and resources needed to extract, analyze, and present evidence.

One reason scope creep has become more common is that criminal investigations increasingly require more detailed examination of evidence just before trial to help prosecutors fend off attacks from defense attorneys. Because defense lawyers typically have the right of full discovery of digital evidence used against their clients, it's possible for new evidence to come to light while complying with the defense request for full discovery.

Examining and analyzing digital evidence depends on:

- Nature of the case
- Amount of data to process
- Search warrants and court orders
- Company policies

Scope creep

- Investigation expands beyond the original description

Using Access Data Forensic Toolkit to Analyze Data

FTK can perform forensics analysis on the following file systems:

- Microsoft FAT12, FAT16, and FAT32
- Microsoft NTFS (for Windows NT, 2000, XP, and Vista)
- Linux Ext2fs and Ext3fs

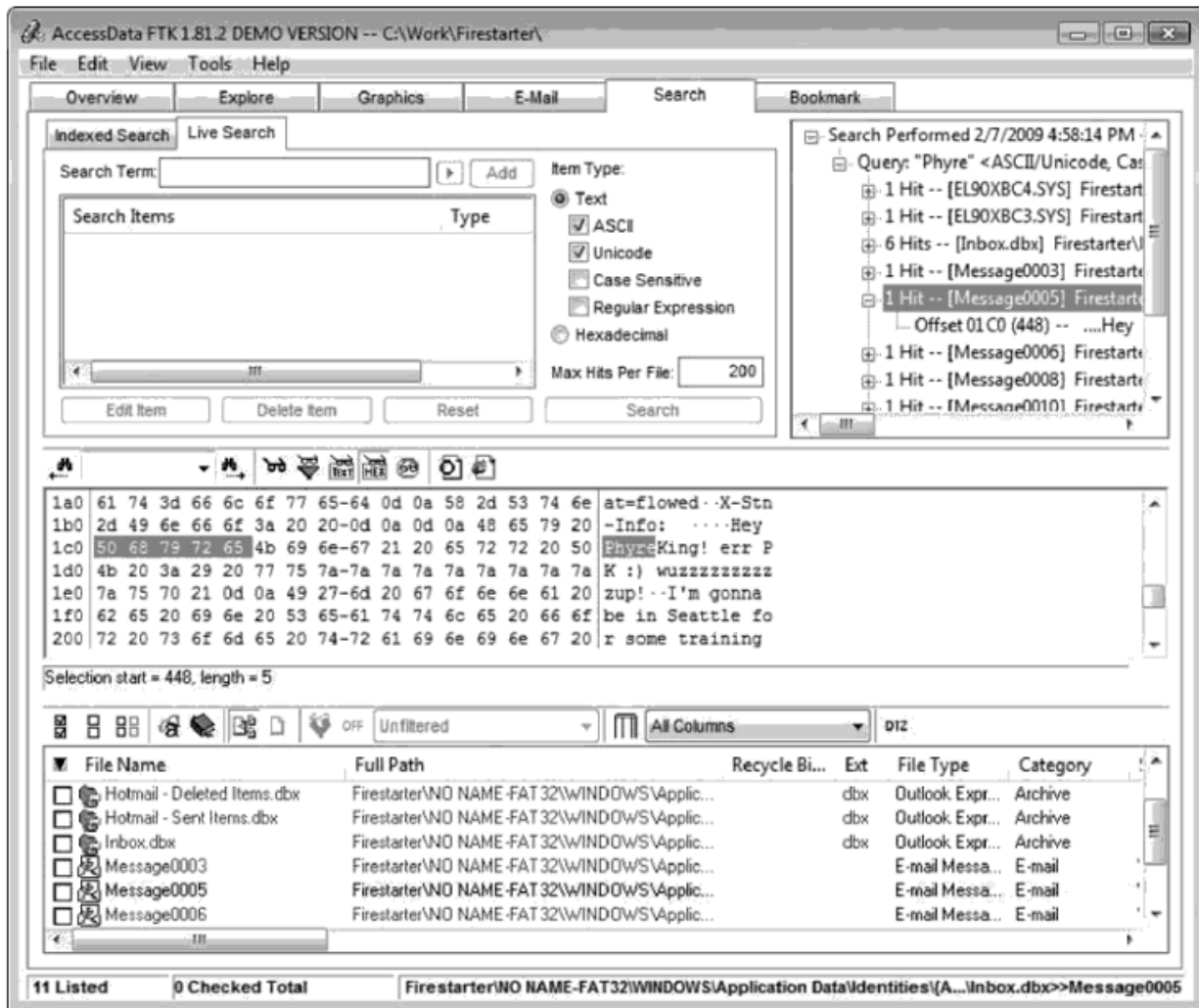
FTK can analyze data from several sources, including image files from other vendors. It can also read entire evidence drives or subsets of data, allowing you to consolidate large volumes of data from many sources when conducting a computer forensics analysis. With FTK, you can store everything from image files to recovered server folders on one investigation drive.

FTK also produces a case log file, where you can maintain a detailed record of all activities during your examination, such as keyword searches and data extractions. This log is also handy for reporting errors to Access Data. At times, however, you might not want the log feature turned on.

FTK has two options for searching for keywords. One option is an indexed search, which catalogs all words on the evidence drive so that FTK can find them quickly. This option returns search results quickly, although it does have some shortcomings. For example, you can't search for hexadecimal string values, and depending on how data is stored on the evidence drive, indexing might not catalog every word. If you do use this feature, keep in mind that indexing an image file can take several hours, so it's best to run this process overnight.

The other option is a live search, which can locate items such as text hidden in unallocated space that might not turn up in an indexed search. You can also search for alphanumeric and hexadecimal values on the evidence drive and search for specific items, such as phone numbers, credit card numbers, and Social Security numbers. You can right-click a search hit to add it to your bookmarks, which includes the result in your final report.

Validating Forensic Data



One of the most critical aspects of computer forensics is validating digital evidence because ensuring the integrity of data you collect is essential for presenting evidence in court. Most computer forensic tools such as ProDiscover, X-Ways Forensics, FTK, and Encase provide automated hashing of image files. For example, when ProDiscover loads an image file, it runs a hash and compares that value to the original hash calculated when the image was first acquired.

You might remember seeing this feature when the Auto Image Checksum Verification message box opens after you load an image file in ProDiscover. Computer forensics tools have some limitations in performing hashing, however, so learning how to use advanced hexadecimal editors is necessary to ensure data integrity.

Validating with Hexadecimal Editors:

Advanced hexadecimal editors offer many features not available in computer forensics tools, such as hashing specific files or sectors. Learning how to use these tools is important, especially when you need to find a particular file, for example, a known contraband image.

With the hash value in hand, you can use a computer forensics tool to search for a suspicious file that might have had its name changed to look like an innocuous file. (Recall that two files with exactly the same content have the same hash value, even if they have different names.) Getting a hash value with a full-featured hexadecimal editor is much faster and easier than with a computer forensics tool.

Addressing Data-Hiding Techniques

Data hiding involves changing or manipulating a file to conceal information. Data-hiding techniques include hiding entire partitions, changing file extensions, setting file attributes to hidden, bit-shifting, using encryption, and setting up password protection.

Hiding Partitions

One way to hide partitions is to create a partition and then use a disk editor, such as Norton Disk Edit, to delete any reference to it manually. To access the deleted partition, users can edit the partition table to re-create the links, and then the hidden partition reappears when the computer is restarted. Another way to hide partitions is with a disk-partitioning utility, such as G Disk, Partition Magic, System Commander, or Linux Grand Unified Boot loader (GRUB), which provides a startup menu where you can select an OS. The system then ignores other bootable partitions.

To circumvent these techniques, be sure to account for all disk space when you're examining an evidence drive. Analyze any disk areas containing space you can't account for so that you can determine whether they contain additional evidence.

For example, in the following code, Disk Manager recognizes the extended partition (labeled EXT DOS) as being 5381.1 MB (listed as Mbytes). The LOG DOS labels for partitions E through F indicate that they're logical partitions that make up the extended partition. However, if you add the sizes of drives E and F, the result is only 5271.3 MB, which is your first clue to examine the disk more closely. The remaining 109.8 MB could be a previously deleted partition or a hidden partition. For this example, the following code shows the letter "H" to indicate a hidden partition. Disk Partitions Cylinders Heads Sectors Mbytes Sectors 2 5111661663 5495.8 11255328.

Partition	Status	Type	Volume Label	Mbytes	System	Usage
D:	1		PRI DOS	109.8	FAT16	2%
	2		EXT DOS	5381.1		98%
E:	3		LOG DOS	109.8	FAT16	2%
	4	H	LOG DOS	109.8	FAT16	2%
F:	5		LOG DOS	5161.5	FAT32	94%

Windows creates a partition gap between partitions automatically; however, you might find a gap that's larger than it should be. For example, in Windows 2000/XP, the partition gap is only 63 sectors, so 109.8 MB is too large to be a standard partition gap. In Windows Vista, the gap is approximately 128 sectors.

Marking Bad Clusters

Another data-hiding technique, more common in FAT file systems, is placing sensitive or incriminating data in free or slack space on disk partition clusters. This technique involves using disk editor, such as Norton Disk Edit, to mark good clusters as bad clusters. The OS then considers these clusters unusable. The only way they can be accessed from the OS is by hanging them to good clusters with a disk editor.

Bit-Shifting

Some home computer users developed the skill of programming in the computer manufacturer's assembly language and learned how to create a low-level encryption program that changes the order of binary data, making the altered data unreadable when accessed with a text editor or word processor.

These programs rearrange bits for each byte in a file. To secure a file containing sensitive or incriminating information, these users run an assembler program (also called a macro) on the file to scramble the bits. To access the file, they run another program that restores the scrambled bits to their original order. Some of these programs are still used today and can make it difficult for investigators to analyze data on a suspect drive.

Start Notepad, and in a text document, type TEST FILE. Test file is to see how shifting bits will alter the data in a file.

Save the file as Bit_shift.txt in your work folder, and exit Notepad.

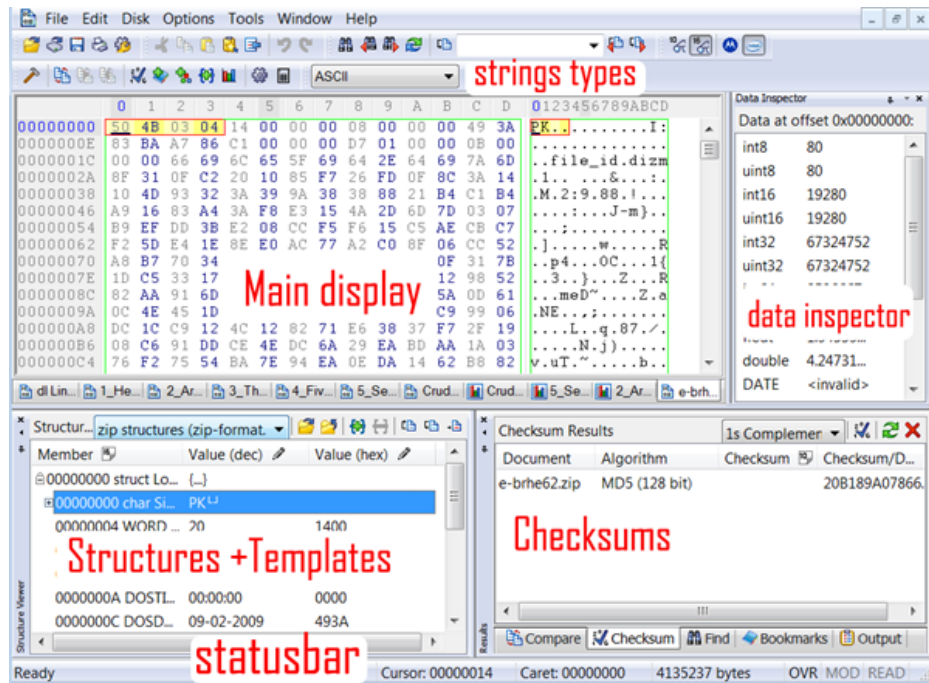


Fig: Hex Workshop

Start Hex Workshop. Click File, Open from the menu. Navigate to your work folder, and then double-click Bit_shift.txt. Bit_shift.txt open in Hex Workshop.

To set up Hex Workshop for the bit-shifting exercise, click Options, Toolbars from the menu. In the Customize dialog box, click the Data Operations check box, and then click OK.

Click the Shift Left button (<< icon) on the Data Operations toolbar. The Shift Left Operation dialog box opens, where you specify how you want to treat the data, the ordering scheme to use for bytes, and whether you shift bits for selected text or the entire file.

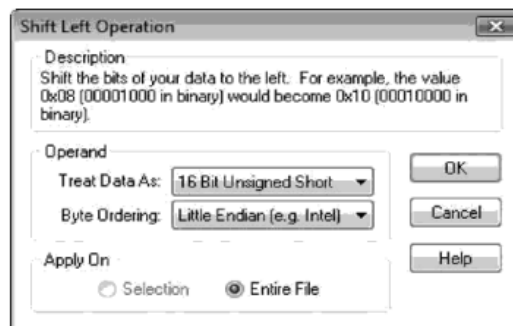


Fig: The Shift Left Operation dialog box

1. Click OK to accept the default settings and shift the bits in Bit_shift.txt to the left.
2. Save the file as Bit_shift_left.txt in your work folder. Above Figure shows the file in Hex Workshop, with the @ symbols indicating shifted bits.

Performing Remote Acquisitions:

Remote acquisitions are handy when you need to image the drive of a computer far away from your location or when you don't want a suspect to be aware of an ongoing investigation. This method can save time and money, too. Many tools are available for remote acquisitions; in the following sections, you use Runtime Software to learn how remote acquisitions are made.

Remote Acquisitions with Runtime Software

Runtime Software (www.runtime.org) offers the following shareware programs for remote acquisitions:

- DiskExplorer for FAT
- DiskExplorer for NTFS
- HDHOST

The above are designed to be file system specific, so there are DiskExplorer versions for both FAT and NTFS that you can use to create raw format image files or segmented image files for archiving purposes.

HDHOST is a remote access program for communication between two computers. The connection is established by using the DiskExplorer program (FAT or NTFS) corresponding to the suspect (remote) computer's file system. The following sections show how to make a live remote acquisition of another computer over a network. To use these tools, it's best to have computers connected on the same local hub or router with minimal network traffic.

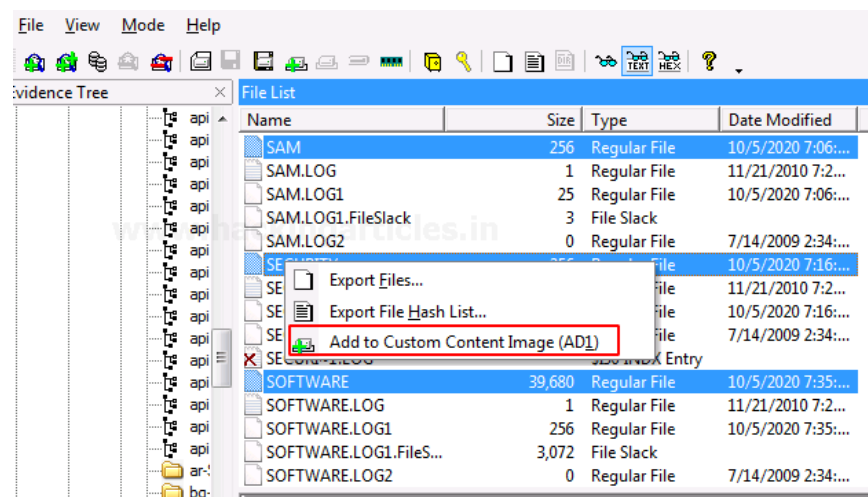


Fig: FTK displaying encrypted files

Network Forensics

Network forensics overview

Network forensics is the process of **collecting** and **analyzing** raw network data and tracking network traffic systematically to ascertain how an attack was carried out or how an event occurred on a network.

Because network attacks are on the rise, there's more focus on this field and an increasing demand for skilled technicians. Labor forecasts predict a shortfall of 50,000 network forensics specialists in law enforcement, legal firms, corporations, and universities.

Network forensics can also help you determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program, for example. A lot of time and resources can be wasted determining that a bug in a custom program or an untested open-source program caused the **"attack"**.

Being able to spot variations in network traffic can help you to track interruptions or attacks, so knowing your network's typical traffic patterns is important.

Network forensics examiners must establish standard procedures for how to acquire data after an attack or intrusion incident. Typically, network administrators want to find compromised.

Typically, network administrators want to find affected machines, get them offline, and restore them as quickly as possible to minimize downtime.

Securing a Network:

Network forensics is used to determine how a security breach occurred; however, steps must be taken to harden/secure networks before a security breach happens, particularly with recent increases in network attacks, viruses, and other security incidents.

The National Security Agency (NSA) developed an approach, called the defense-in-depth (DiD) strategy. DiD have three modes of protection:

- People
- Technology
- Operations

People:

The people as a mode of protection means organizations must hire well-qualified people. And organizations should make sure employees are well-trained in security procedures and are familiar with the organization's security policy.

Technology:

The technology mode includes choosing strong network architecture and using tested tools, such as intrusion detection systems (IDSs) and firewalls.

Operations:

The operations mode addresses day-to-day operations. Updating security patches, antivirus, software, and operating system.

Performing Live Acquisitions

Live acquisitions done before taking a system offline are also becoming a necessity because attacks might leave footprints only in running processes or RAM. For example, some malware disappears after a system is restarted. The information in RAM is lost after you turn off a suspect system.

The problem investigators face is the order of volatility (OOV), meaning how long a piece of information lasts on a system. Data such as RAM and running processes might exist for only milliseconds; other data, such as files stored on the hard drive, might last for years.

The following steps show the general procedure for a live acquisition,

Step 1: Create or download a bootable forensic CD, and test it before using it on a suspect drive. If the suspect system is on your network and you can access it remotely, If not, insert the bootable forensics CD in the suspect system.

Step 2: Make sure you keep a log of all your actions; documenting your actions and the reasons for these actions is critical.

Step 3: A network drive is ideal as a place to send the information you collect. If you don't have one available, connect a USB thumb drive to the suspect system for collecting data. Be sure to note this step in your log.

Step 4: Next, copy the physical memory (RAM). Microsoft has built-in tools for this task, or you can use available freeware tools, such as **mem fetch** (www.freshports.org/sysutils/memfetch) and **Back Track**.

Step 5: The next step varies, depending on the incident you're investigating. Such as creating an image of the drive over the network, or shutting the system down and making a static acquisition later.

Step 6: Be sure to get a forensic hash value of all files you recover during the live acquisition to make sure they aren't altered later.

Several **bootable forensic CDs** are available, such as **Helix**



Performing a Live Acquisition in Windows

Live acquisitions are becoming more necessary, and several tools are available for capturing RAM. ManTech Memory DD (www.mantech.com/msma/MDD.asp) can access up to 4 GB RAM in standard did format. Another freeware tool, Win32dd (<http://win32dd.msuiche.net>), runs from the command line to perform a memory dump in Windows. In addition, commercial tools, such as Guidance Software Winen.exe, can be used.

Another popular tool is Backtrack (www.remote-exploit.org/backtrack.html), which combines tools from the White Hat Hackers CD and The Auditor CD (see Figure 11-3). More than 300 tools are available, including password crackers, network sniffers, and freeware forensics tools.

Backtrack has become popular with penetration testers and is used at the annual Collegiate Cyber Defense Competitions.



Fig:Some of the tools available in BackTrack

Developing Standard Procedures for Network Forensics

Network forensics is a long, tedious process, and unfortunately, the trail can go cold quickly. A standard procedure often used in network forensics is as follows:

- Always use a standard installation image for systems on a network. This image isn't a bit-stream image but an image containing all the standard applications used. You should also have the MD5 and SHA-1 hash values of all application and OS files.
- When an intrusion incident happens, make sure the vulnerability has been fixed to prevent other attacks from taking advantage of the opening.

- Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off.
- Acquire the compromised drive and make a forensic image of it.
- Compare files on the forensic image to the original installation image. Compare hash values of common files, such as Win.exe and standard DLLs, and ascertain whether they have changed.

In computer forensics, you can work from the image to find most of the deleted or hidden files and partitions. Sometimes you restore the image to a physical drive so that you can run programs on the drive.

In network forensics, you have to restore the drive to see how malware attackers have installed on the system works.

For example, intruders might have transmitted a Trojan program that gives them access to the system and then installed a rootkit, which is a collection of tools that can perform network reconnaissance tasks (using the ls or net stat command to collect information, for instance), key logging, and other actions.

Using Network Tools

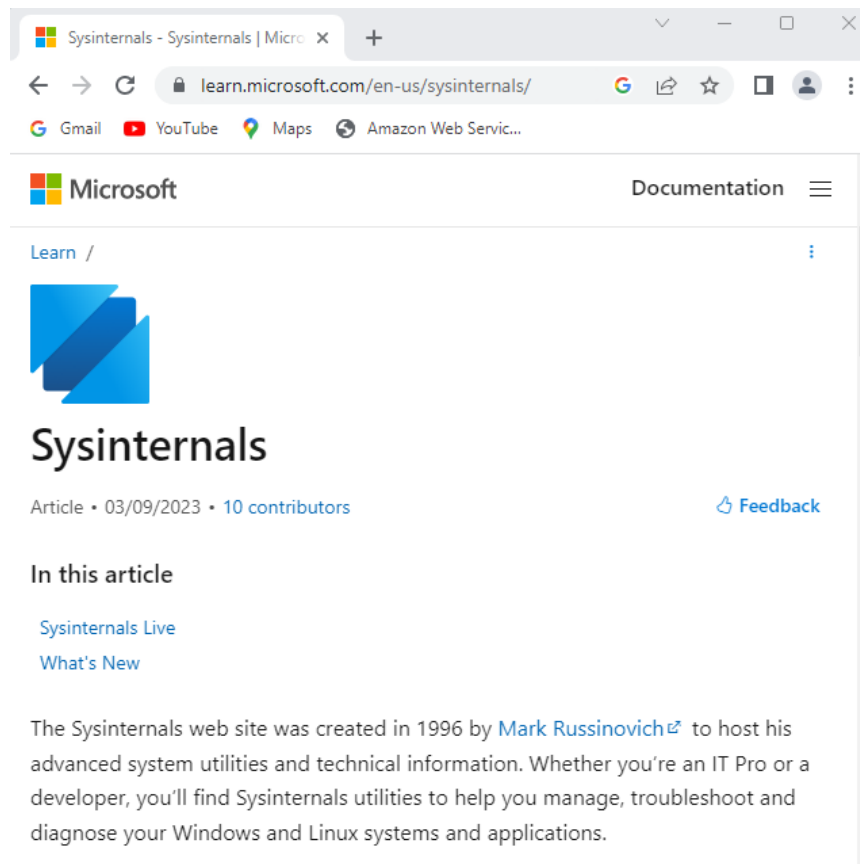
A variety of tools are available for network administrators to perform remote shutdowns, monitor device use, and more. The tools are freeware and work in Windows and UNIX. **Sysinternals** (www.microsoft.com/technet/sysinternals/) is a collection of free tools for examining Windows products. They were created by Mark Russinovich and Bryce Cogswell and acquired by Microsoft.

Sysinternals

A collection of free tools for examining Windows products.

The following list describes a few examples of the powerful Windows tools available at Sysinternals:

- RegMon shows all Registry data in real-time
- Process Explorer shows what files, and Register Keys are loaded at a specific time.
- Handle shows what files are open and which processes are using these files.
- Filemon shows file system activity.



Far too many tools are available to list here, but you should take some time to explore the site and see what's available. One in particular that's worth investigating is PsTools, a suite created by Sysinternals that includes the following tools:

- **PsExec**—Runs processes remotely
- **PsGetSid**—Displays the security identifier (SID) of a computer or user
- **PsKill**—Kills processes by name or process ID
- **PsList**—Lists detailed information about processes
- **PsLoggedOn**—Displays who's logged on locally
- **PsPasswd**—Allows you to change account passwords
- **PsService**—Enables you to view and control services
- **PsShutdown**—Shuts down and optionally restarts a computer
- **PsSuspend**—Allows you to suspend processes