

Prepared by Dr. Nermin Ewais

CYB 770  
IT Forensics

## Lecture 05



# Operating System Forensic

## Lecture 05

CYB 770  
IT Forensics

Prepared by  
**Dr. Nermin Ewais**

- Operating System and Operating System Forensic
- Kind of operating Systems
- Windows
- Linux Forensic

- An operating system (OS) is system software that manages computer hardware, software resources, and provides common services for computer programs.
- An operating system is a program which controls the execution of application programs and acts as an intermediary between the user of a computer and the computer hardware.
- A program which is being executed is also called a process or job.

**Definition:** Operating System Forensics is the process of retrieving useful information from the Operating System (OS) of the computer or mobile device in question.

- The most popular types of Operating Systems are Windows, Linux, Mac, iOS, and Android.

## Operating system Types

- Windows is a widely used OS designed by Microsoft. The file systems used by Windows include FAT, exFAT, NTFS, and ReFS.

- Linux is an open source, Unix-like, and elegantly designed operating system that is compatible with personal computers, supercomputers, servers, mobile devices, netbooks, and laptops. Unlike other OSs, Linux holds many file systems of the ext family, including ext2, ext3, and ext4.

- Mac OS X is the UNIX-based operating system that contains a Mach 3 microkernel and a FreeBSD-based subsystem. Its user interface is Apple-like, whereas the underlying architecture is UNIX-like.

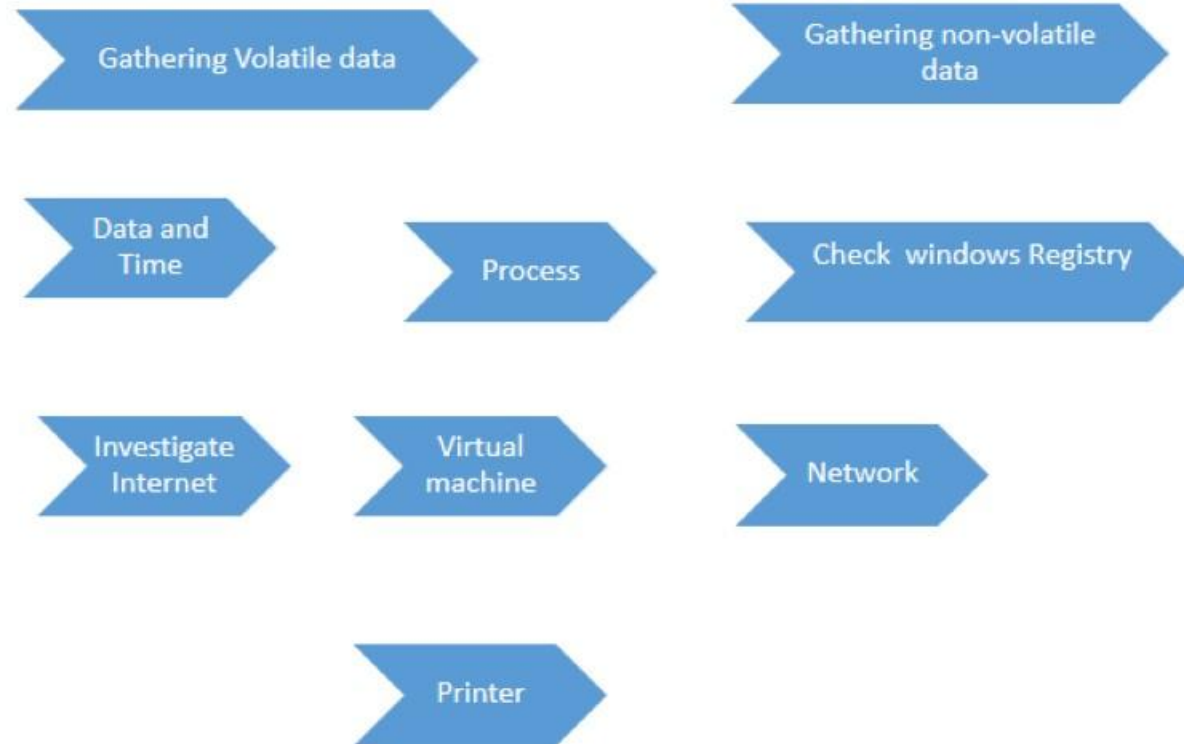
- Apple iOS is the UNIX-based operating system first released in 2007. It is a universal OS for all of Apple's mobile devices, such as iPhone, iPod Touch, and iPad. An iOS embedded device retrieved from a crime scene can be a rich source of empirical evidence.

- Android is a Google's open-source platform designed for mobile devices. It is widely used as the mobile operating system in the handsets industry. The Android operating system runs on a Linux-based kernel which supports core functions, such as power management, network infrastructure, and device drivers

## Windows Forensic

Some of the most crucial areas to check for evidence within volatile data , registers, physical and virtual memory, network connections, running processes, and system files.

# Windows Forensic analysis



## Coordinated universal time

- cmd
- Date /t & time /t

```
C:\Users\Nermin>date
The current date is: Mon 10/24/2022
Enter the new date: (mm-dd-yy)

C:\Users\Nermin>date/t
Mon 10/24/2022

C:\Users\Nermin>time
The current time is: 13:10:34.25
Enter the new time:

C:\Users\Nermin>time/t
01:10 PM

C:\Users\Nermin>
```

## Process

- Running Jobs
- Task manager
- Tasklist

```
C:\Users\Nermin>tasklist
```

| Image Name          | PID  | Session Name | Session# | Mem Usage |
|---------------------|------|--------------|----------|-----------|
| System Idle Process | 0    | Services     | 0        | 8 K       |
| System              | 4    | Services     | 0        | 136 K     |
| Registry            | 124  | Services     | 0        | 113,488 K |
| smss.exe            | 576  | Services     | 0        | 1,088 K   |
| csrss.exe           | 824  | Services     | 0        | 5,736 K   |
| wininit.exe         | 956  | Services     | 0        | 6,460 K   |
| csrss.exe           | 964  | Console      | 1        | 7,664 K   |
| services.exe        | 352  | Services     | 0        | 9,676 K   |
| winlogon.exe        | 612  | Console      | 1        | 12,244 K  |
| lsass.exe           | 864  | Services     | 0        | 25,460 K  |
| svchost.exe         | 1120 | Services     | 0        | 37,252 K  |
| fontdrvhost.exe     | 1144 | Console      | 1        | 8,140 K   |
| fontdrvhost.exe     | 1152 | Services     | 0        | 2,808 K   |
| WUDFHost.exe        | 1216 | Services     | 0        | 21,756 K  |
| svchost.exe         | 1276 | Services     | 0        | 19,380 K  |
| svchost.exe         | 1336 | Services     | 0        | 8,444 K   |
| WUDFHost.exe        | 1380 | Services     | 0        | 9,648 K   |
| dwm.exe             | 1480 | Console      | 1        | 150,184 K |
| svchost.exe         | 1576 | Services     | 0        | 8,832 K   |
| svchost.exe         | 1592 | Services     | 0        | 11,424 K  |
| svchost.exe         | 1612 | Services     | 0        | 7,400 K   |
| svchost.exe         | 1660 | Services     | 0        | 10,524 K  |
| svchost.exe         | 1668 | Services     | 0        | 11,560 K  |
| svchost.exe         | 1776 | Services     | 0        | 5,864 K   |
| svchost.exe         | 1792 | Services     | 0        | 9,856 K   |
| svchost.exe         | 1876 | Services     | 0        | 15,176 K  |
| svchost.exe         | 1940 | Services     | 0        | 10,168 K  |
| svchost.exe         | 1948 | Services     | 0        | 11,704 K  |
| svchost.exe         | 1972 | Services     | 0        | 12,976 K  |
| IntelCpHDCPSvc.exe  | 1756 | Services     | 0        | 5,024 K   |
| svchost.exe         | 2060 | Services     | 0        | 8,436 K   |
| svchost.exe         | 2088 | Services     | 0        | 11,348 K  |

**What is the registry?**

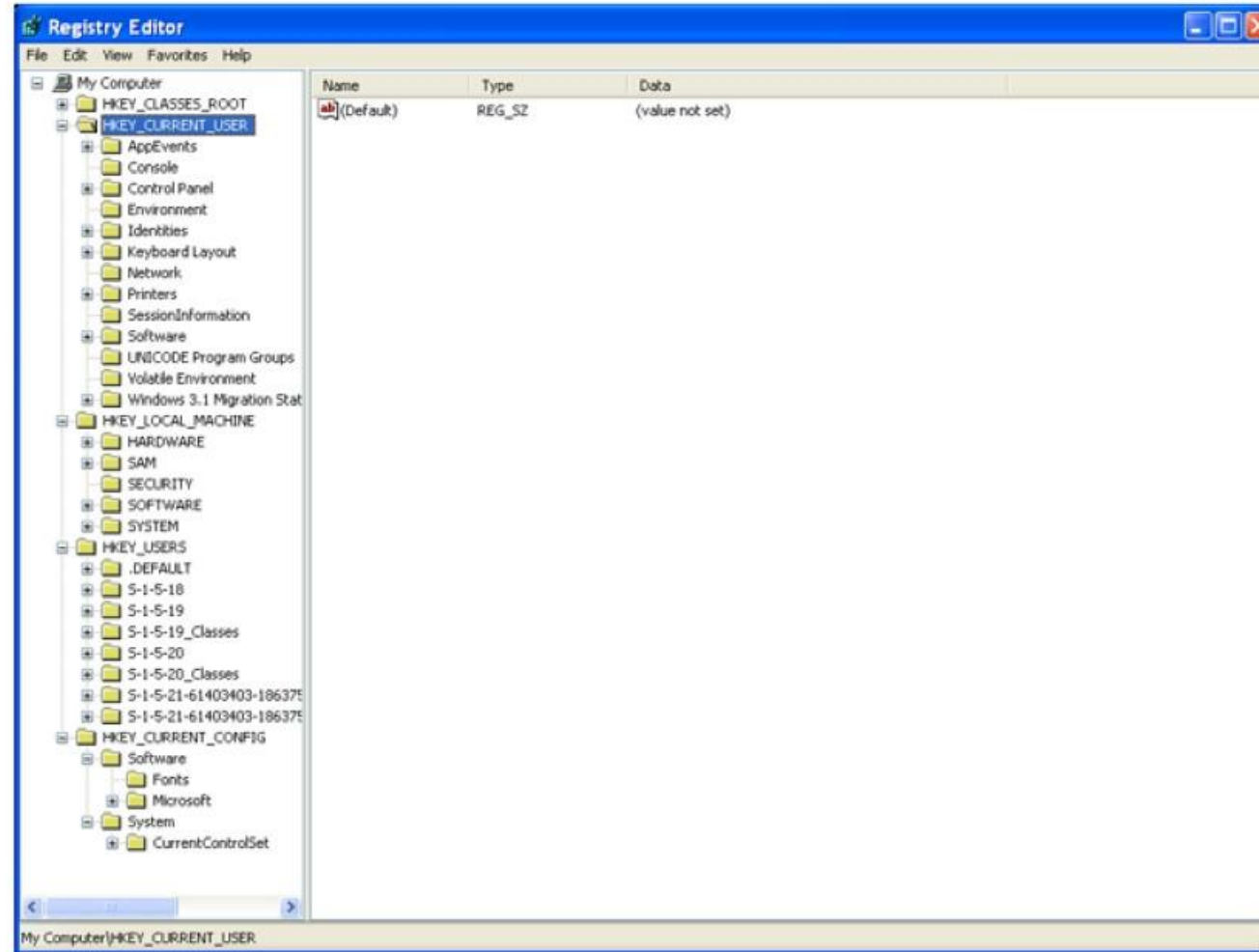
- Microsoft defines the registry as a central hierarchical database. This database is used to store configuration information about users, hardware devices, and applications.

**What about registry forensic investigator?**

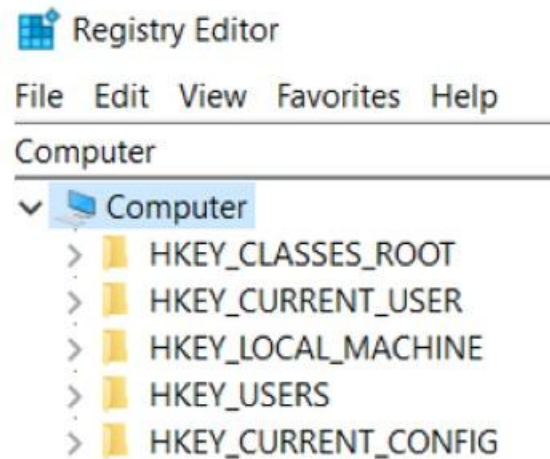
- Information in the registry will contain profiles for each user, installed applications, different document types, and property settings for folders and application icons.
- The registry will also contain information about the hardware on the system, to include networking information such as the ports that are being used.

## Understanding Windows Registry

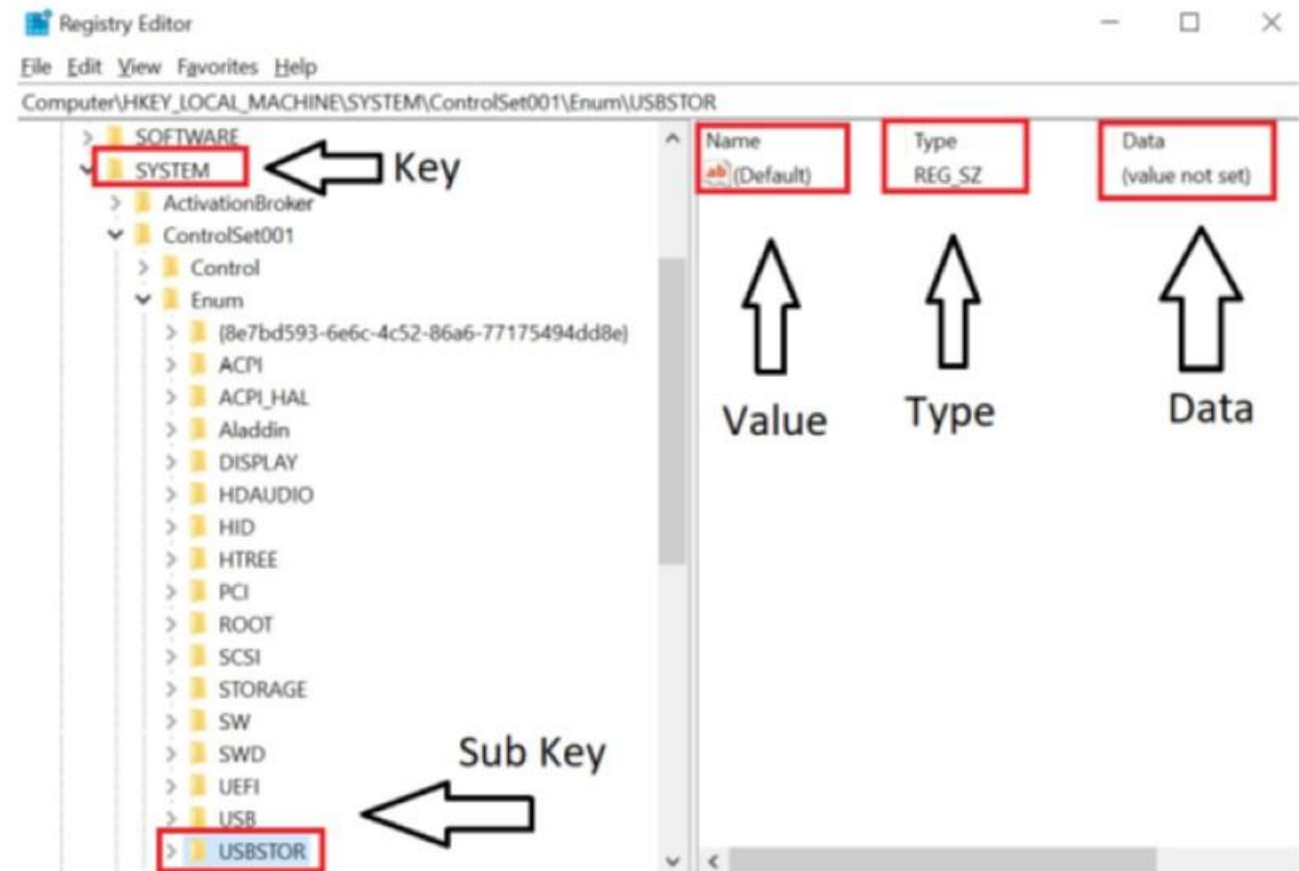
regedit



- In the search box on the taskbar, type regedit, then select Registry Editor (Desktop app) from the results.



- The comprises **subkeys** that contain the **Value**, **Type**, and specific **Data** or settings being saved.



## Understanding Windows Registry

## Registry Editor

File Edit View Favorites Help

Computer

Computer

- > HKEY\_CLASSES\_ROOT
- > HKEY\_CURRENT\_USER
- > HKEY\_LOCAL\_MACHINE
- > HKEY\_USERS
- > HKEY\_CURRENT\_CONFIG

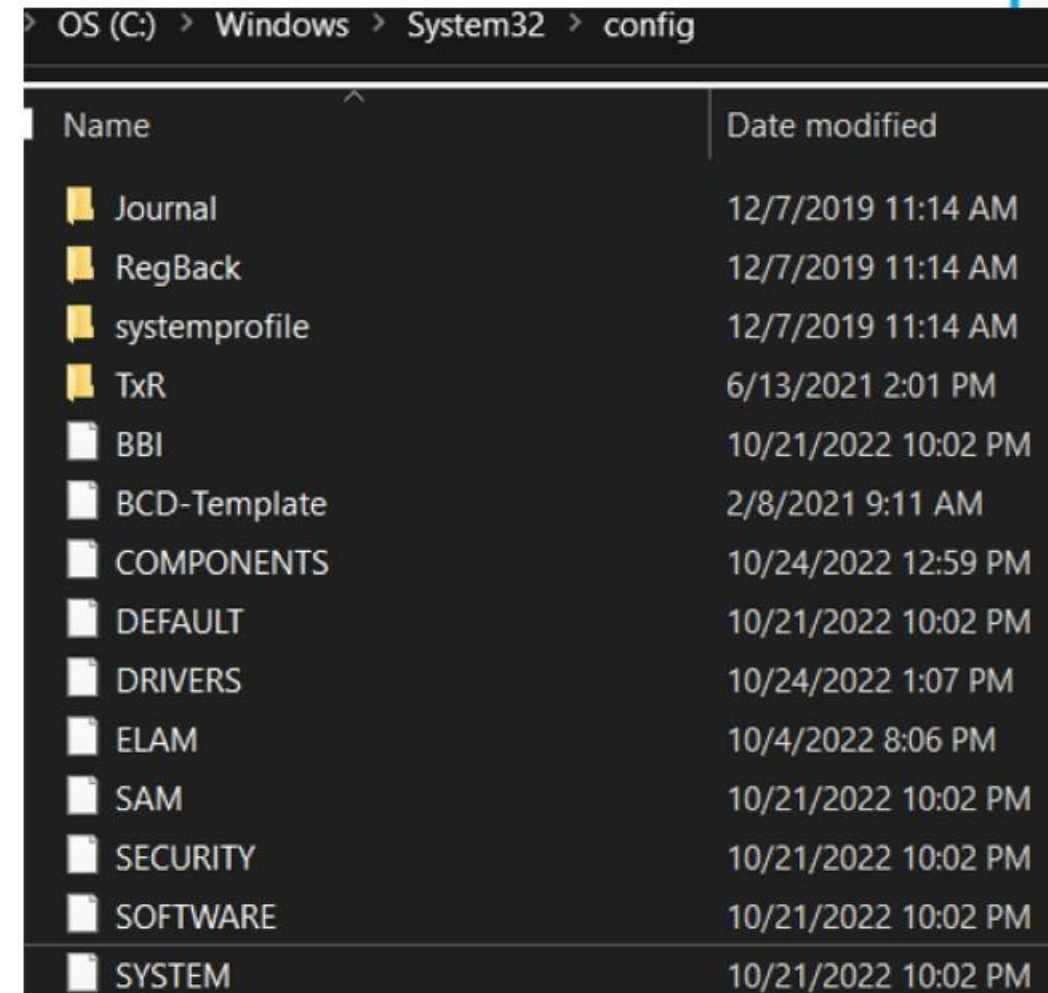
| Registry Key                     | Abbr.       | Associated files | Incorporates                                                                               |
|----------------------------------|-------------|------------------|--------------------------------------------------------------------------------------------|
| HKEY_LOCAL_MACHINE<br>HKEY_USERS | HKLM<br>HKU | NTUSER.DAT       | System settings<br>Settings related to all currently logged-in users                       |
| HKEY-CURRENT_USER                | HKCU        |                  | Both system and application Settings with regard to all currently logged-in users          |
| HKEY_CURRENT_CONFIG              | HKCC        |                  | Registry will be created at runtime and contains hardware settings and performance details |
| HKLM\SYSTEM                      |             | System           | File involves system settings about services and hardware                                  |
| HKLM\SOFTWARE                    |             | Software         | File incorporates configuration settings for all installed applications including windows  |
| HKLM\SAM                         |             | Sam              | Includes security info and user password hashes for all users on the system                |

### Registry file locations and purposes

| Filename and location                 | Purpose of file                                                                                               |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Users\user-account\Ntuser.dat         | User-protected storage area; contains the list of most recently used files and desktop configuration settings |
| Windows\system32\config\Default.dat   | Contains the computer's system settings                                                                       |
| Windows\system32\config\SAM.dat       | Contains user account management and security settings                                                        |
| Windows\system32\config\Security.dat  | Contains the computer's security settings                                                                     |
| Windows\system32\config\Software.dat  | Contains installed programs' settings and associated usernames and passwords                                  |
| Windows\system32\config\System.dat    | Contains additional computer system settings                                                                  |
| Windows\system32\config\systemprofile | Contains additional NTUSER information                                                                        |

# Understanding Windows Registry

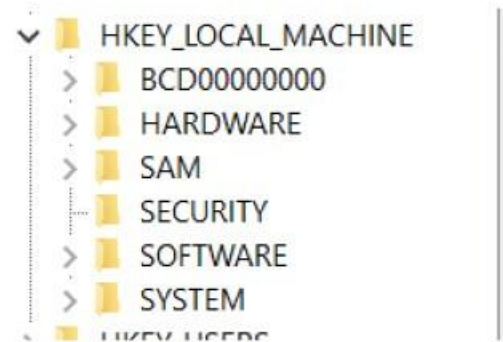
- The components of the registry are found in the **%SystemRoot%\System32\Config** folder and are called hive files. You will find the SAM, SECURITY, SOFTWARE, and SYSTEM hives:
- The **SAM** hive is the Security Accounts Manager and contains login information about the users.
- The **SECURITY** hive contains security information and, potentially, password information.
- The **SOFTWARE** hive contains information about application information and the default Windows settings.
- The **SYSTEM** hive includes information on the hardware and system configuration.



| Name          | Date modified       |
|---------------|---------------------|
| Journal       | 12/7/2019 11:14 AM  |
| RegBack       | 12/7/2019 11:14 AM  |
| systemprofile | 12/7/2019 11:14 AM  |
| TxR           | 6/13/2021 2:01 PM   |
| BB1           | 10/21/2022 10:02 PM |
| BCD-Template  | 2/8/2021 9:11 AM    |
| COMPONENTS    | 10/24/2022 12:59 PM |
| DEFAULT       | 10/21/2022 10:02 PM |
| DRIVERS       | 10/24/2022 1:07 PM  |
| ELAM          | 10/4/2022 8:06 PM   |
| SAM           | 10/21/2022 10:02 PM |
| SECURITY      | 10/21/2022 10:02 PM |
| SOFTWARE      | 10/21/2022 10:02 PM |
| SYSTEM        | 10/21/2022 10:02 PM |

# Understanding Windows Registry

| Subtree                     | Filename                         |
|-----------------------------|----------------------------------|
| HKEY_LOCAL_MACHINE\System   | Windows\system32\config\System   |
| HKEY_LOCAL_MACHINE\Software | Windows\system32\config\Software |
| HKEY_LOCAL_MACHINE\Security | Windows\system32\config\Security |
| HKEY_LOCAL_MACHINE\SAM      | Windows\system32\config\SAM      |



- Some forensics tools, such as X-Ways Forensics, OSForensics, Forensic Explorer, and FTK, have built-in or add-on Registry viewers.

- The Windows Event Log is used by Microsoft Windows to store application and system logs. Typical Event Logs are: Application, System, and Security.
- Windows Server records events in the following logs:

#### ☐ **Application log**

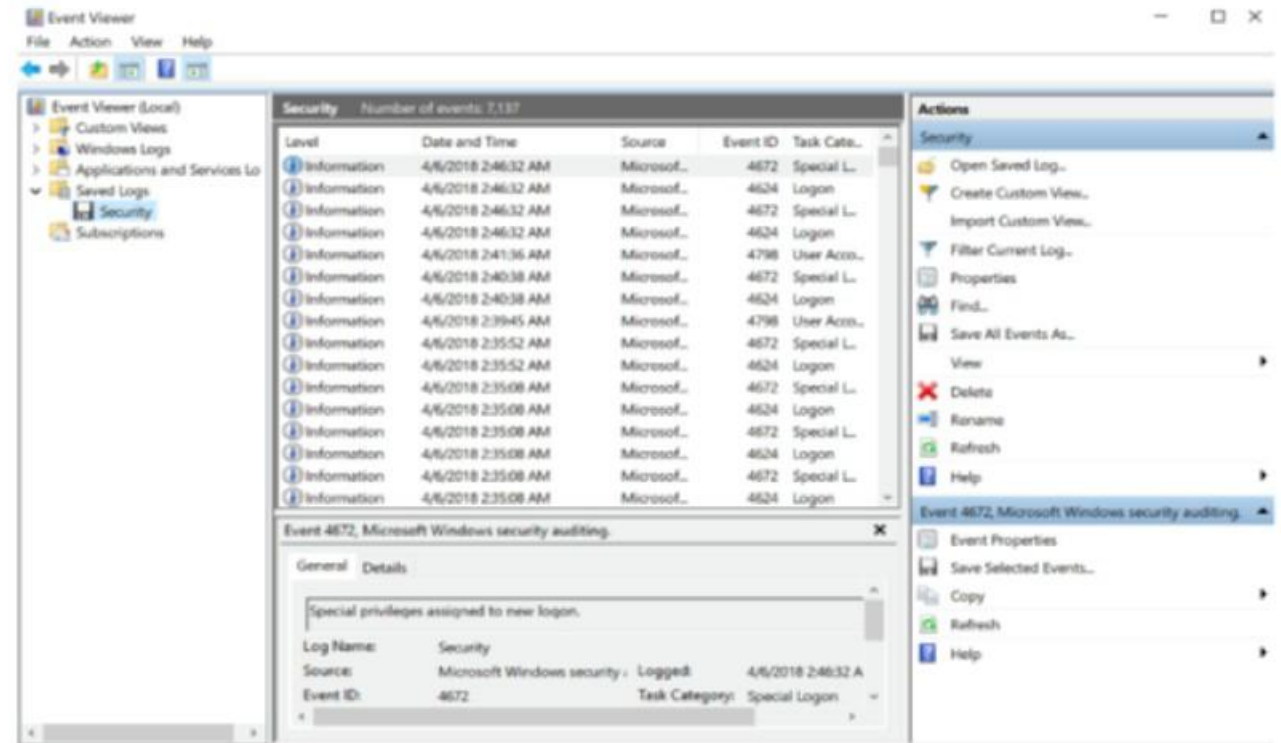
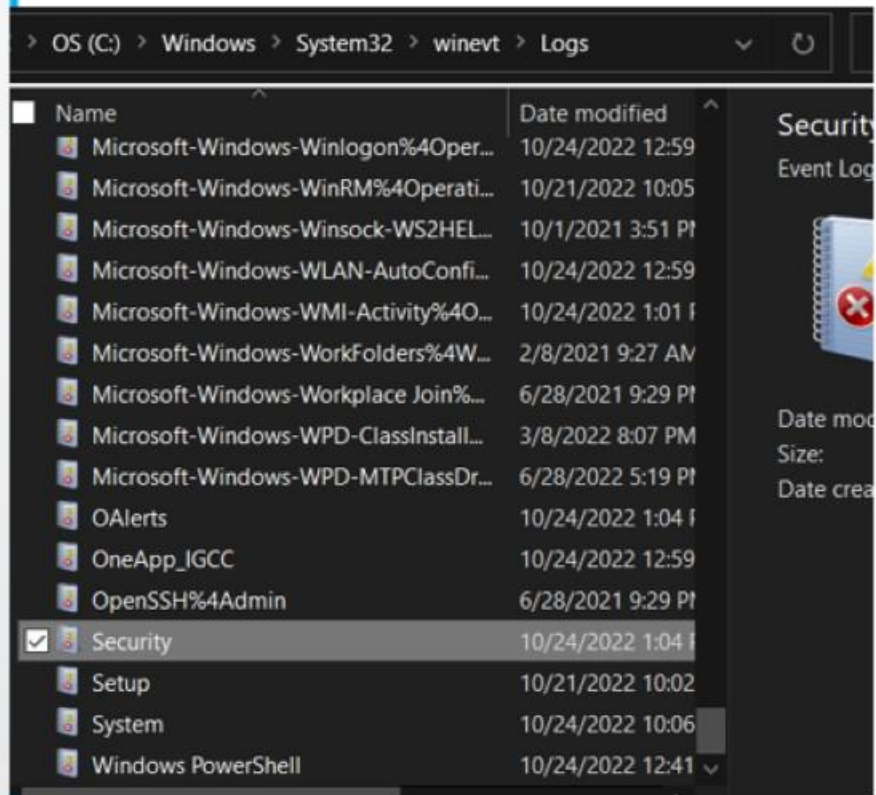
- The application log contains events that are logged by programs. Events that are written to the application log are determined by the developers of the software program.

### ☐ Security log

- The security log contains events such as valid and invalid logon attempts. It also contains events that are related to resource use, for example, when you create, open, or delete files. You must be logged on as an administrator or as a member of the Administrators group to turn on, to use, and to specify which events are recorded in the security log.

### ☐ System log

- The system log contains events that are logged by Windows system components. These events are predetermined by Windows.



## 4624: An account was successfully logged on

|                                                         |                                                |                |                 |
|---------------------------------------------------------|------------------------------------------------|----------------|-----------------|
| Subject:                                                |                                                |                |                 |
| Security ID:                                            | SYSTEM                                         |                |                 |
| Account Name:                                           | DESKTOP-PM6C56D\$                              |                |                 |
| Account Domain:                                         | WORKGROUP                                      |                |                 |
| Logon ID:                                               | 0x3E7                                          |                |                 |
| Logon Information:                                      |                                                |                |                 |
| Logon Type:                                             | 2                                              |                |                 |
| Restricted Admin Mode:                                  | -                                              |                |                 |
| Virtual Account:                                        | No                                             |                |                 |
| Elevated Token:                                         | No                                             |                |                 |
| Impersonation Level: Impersonation                      |                                                |                |                 |
| New Logon:                                              |                                                |                |                 |
| Security ID:                                            | S-1-5-21-2734969515-1644526556-1039763013-1001 |                |                 |
| Account Name:                                           | jcloudy                                        |                |                 |
| Account Domain:                                         | DESKTOP-PM6C56D                                |                |                 |
| Logon ID:                                               | 0x11F43947                                     |                |                 |
| Linked Logon ID:                                        | 0x11F4390D                                     |                |                 |
| Network Account Name:                                   | -                                              |                |                 |
| Log Name: Security                                      |                                                |                |                 |
| Source:                                                 | Microsoft Windows security                     | Logged:        | 4/6/2018 05:26  |
| Event ID:                                               | 4624                                           | Task Category: | Logon           |
| Level:                                                  | Information                                    | Keywords:      | Audit Success   |
| User:                                                   | N/A                                            | Computer:      | DESKTOP-PM6C56D |
| OpCode:                                                 | Info                                           |                |                 |
| More Information: <a href="#">Event Log Online Help</a> |                                                |                |                 |

Internet has some issues that should be checked for evidence.

- History
- Temporary Internet files
- Cookies

- Knowing which networks, be they wired or wireless, the suspect has connected to might give you location information about their whereabouts at the time in question.
- The Wi-Fi document will be found at the following path:  
C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces

- Microsoft uses the same method to record a user's file activity and internet history as they use with the Internet Explorer/File Explorer/Edge browsers.
- It records local and remote file access. Most commercial forensics tools parse these files easily.
- Depending on the version, the history file will be located in the following areas:
  - ❑ IE6-7: %USERPROFILE%\LocalSettings\History\History.IE5
  - ❑ IE8-9:  
%USERPROFILE%\AppData\Local\Microsoft\WindowsHistory\History.IE5
  - ❑ IE10-11:  
%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV\*.dat

## Exploring History

| \\Users\\jcloudy\\AppData\\Local\\Microsoft\\Windows\\WebCache |        |
|----------------------------------------------------------------|--------|
| Name ^                                                         | Type   |
| .. = Windows (351)                                             |        |
| . = WebCache (24)                                              |        |
| V01res00001.jrs                                                | jrs    |
| V01res00002.jrs                                                | jrs    |
| V01.chk                                                        | chk    |
| V01.log                                                        | edblog |
| V0100016.log                                                   | edblog |
| V0100017.log                                                   | edblog |
| V0100018.log                                                   | edblog |
| V01tmp.log                                                     | edblog |
| WebCacheV01.dat (1)                                            | edb    |
| WebCacheV01.jfm                                                | jfm    |
| V01.log                                                        | log    |
| V01tmp.log                                                     | log    |
| WebCacheV01.dat                                                | dat    |
| WebCacheV01.dat                                                | hxx    |
| V01.chk                                                        | chk    |
| V01.chk                                                        | chk    |

## Temporary Internet files

- When you visit a website, your computer stores tiny pieces of data from the site so that its pages will display faster during return visits.
- Most computers store such files in a cache file or a folder called “Temporary Internet Files.” Occasionally the files can become corrupt or outdated and need to be deleted.

- Microsoft Internet Explorer (IE) uses temporary internet files to store copies of web content on a local hard drive.
- While it's useful for improving network performance, it can quickly fill the hard drive with large amounts of unwanted data.

- C:\Users\[username]\AppData\Local\Microsoft\Windows\INetCache:  
This temp files location is relevant in Windows 10 and Windows 8.
- C:\Users\[username]\AppData\Local\Microsoft\Windows\Temporary Internet Files: This is where temporary internet files are stored in Windows 7 and Windows Vista.
- C:\Documents and Settings\[username]\Local Settings\Temporary Internet Files: This is where Windows XP IE temp internet files are stored.

- Cookies are text files with small pieces of data — like a username and password — that are used to identify your computer as you use a computer network.
- Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience.
- Data stored in a cookie is created by the server upon your connection. This data is labeled with an ID unique to you and your computer.

- Microsoft Edge to store cookies is similar to the Chrome cookies location. All the cookies are also stored in a single file called Cookies. Launch File Explorer and insert the following path into the address bar:

"C:\Users\Your\_User\_Name\AppData\Local\Microsoft\Edge\User Data\Default"

- Mozilla Firefox stores all the cookies from every website you visit in a single file called cookies.sqlite. the following path in File Explorer's address bar:  
"C:\Users\Your\_User\_Name\AppData\Roaming\Mozilla\Firefox\Profiles"

- **IECookiesView**

IECookiesView is a forensic utility that is used to display the details of all cookies that are stored by Internet Explorer. It provides the capability to sort cookies according to name and date. Additionally, it provides a search function that can find a cookie in the list by just specifying the name of a website.

- **IE History Viewer**

Any URL that is typed into the address bar or any link that is followed in Internet Explorer automatically causes the address to be stored in the history index file. The IE History Viewer parses all data from the history file, and prints the list of all visited URLs. This application provides the ability to save the list of addresses as a text, HTML, or XML file.

- Netstat -ano

Collect information about the network

- Ipconfig

Know IP address and DHCP

```
C:\Users\Nermin>netstat
```

```
Active Connections
```

| Proto | Local Address   | Foreign Address       | State       |
|-------|-----------------|-----------------------|-------------|
| TCP   | 127.0.0.1:49673 | DESKTOP-UAC9DLD:49674 | ESTABLISHED |
| TCP   | 127.0.0.1:49674 | DESKTOP-UAC9DLD:49673 | ESTABLISHED |
| TCP   | 127.0.0.1:49677 | DESKTOP-UAC9DLD:60115 | ESTABLISHED |
| TCP   | 127.0.0.1:49677 | DESKTOP-UAC9DLD:60116 | ESTABLISHED |
| TCP   | 127.0.0.1:49678 | DESKTOP-UAC9DLD:49679 | ESTABLISHED |
| TCP   | 127.0.0.1:49679 | DESKTOP-UAC9DLD:49678 | ESTABLISHED |
| TCP   | 127.0.0.1:59988 | DESKTOP-UAC9DLD:59989 | ESTABLISHED |
| TCP   | 127.0.0.1:59989 | DESKTOP-UAC9DLD:59988 | ESTABLISHED |
| TCP   | 127.0.0.1:60115 | DESKTOP-UAC9DLD:49677 | ESTABLISHED |
| TCP   | 127.0.0.1:60116 | DESKTOP-UAC9DLD:49677 | ESTABLISHED |

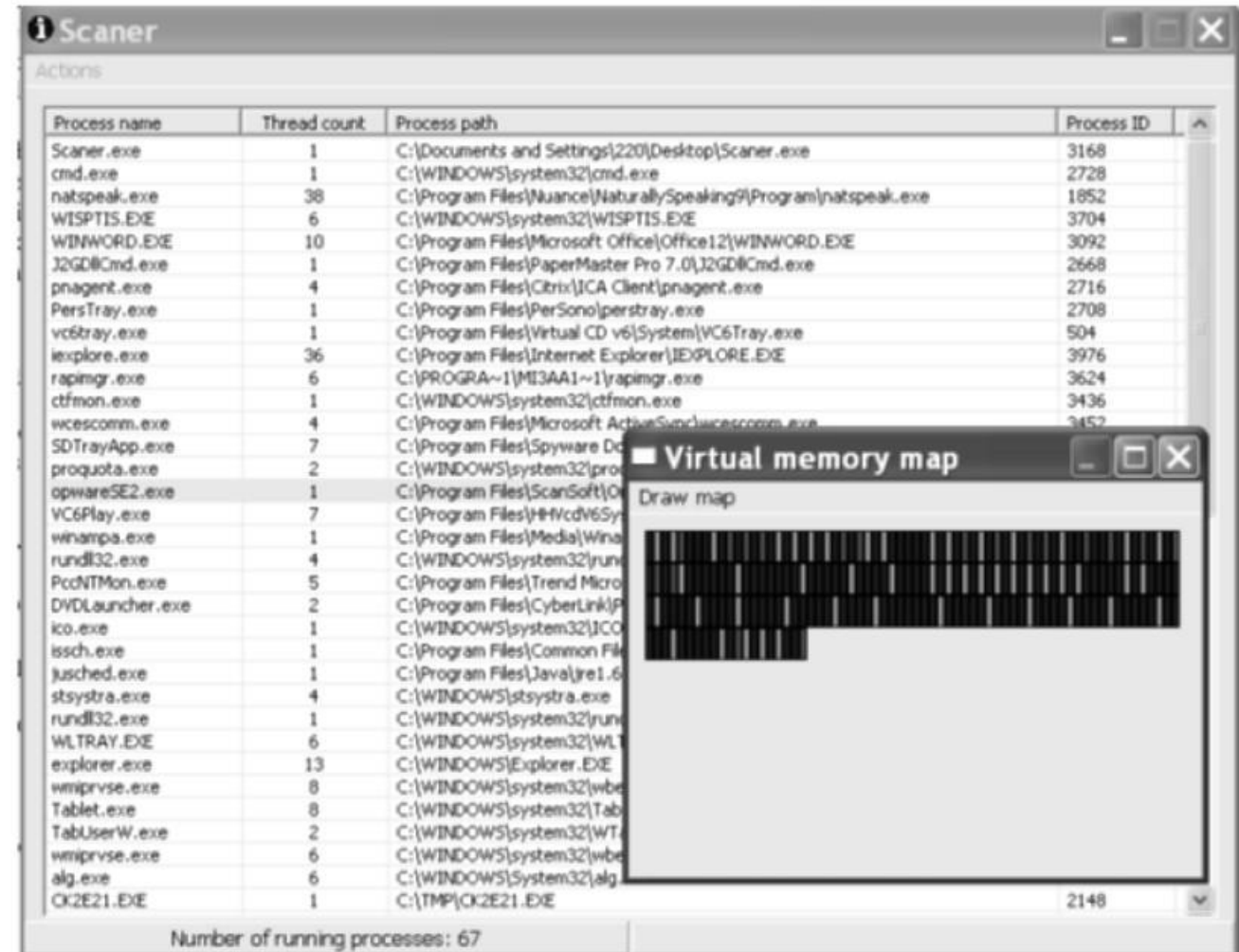
## What Is Virtual Memory?

- In order to copy virtual memory into RAM, the operating system divides virtual memory into pages.
- Each page contains a fixed number of addresses that are stored on disk until called by the operating system.
- When pages are called by the operating system they are copied from disk memory to RAM, a process which translates virtual addresses into real addresses.
- This process is known as mapping. The process of copying virtual pages from disk to main memory is known as paging or swapping.

# What Is Virtual Memory?

## System Scanner

System scanner (available from [www.codeproject.com/w2k/system\\_scanner.asp](http://www.codeproject.com/w2k/system_scanner.asp)) is designed as a replacement to the Task manager



The screenshot shows the 'Scanner' application window with a table of running processes. A 'Virtual memory map' dialog box is open in the foreground, displaying a 'Draw map' button and a grid representing memory usage.

| Process name    | Thread count | Process path                                                    | Process ID |
|-----------------|--------------|-----------------------------------------------------------------|------------|
| Scanner.exe     | 1            | C:\Documents and Settings\220\Desktop\Scanner.exe               | 3168       |
| cmd.exe         | 1            | C:\WINDOWS\system32\cmd.exe                                     | 2728       |
| natspeak.exe    | 38           | C:\Program Files\Nuance\NaturallySpeaking9\Program\natspeak.exe | 1852       |
| WISPTIS.EXE     | 6            | C:\WINDOWS\system32\WISPTIS.EXE                                 | 3704       |
| WINWORD.EXE     | 10           | C:\Program Files\Microsoft Office\Office12\WINWORD.EXE          | 3092       |
| J2GD8Cmd.exe    | 1            | C:\Program Files\PaperMaster Pro 7.0\J2GD8Cmd.exe               | 2668       |
| pnagent.exe     | 4            | C:\Program Files\Gibix\ICA Client\pnagent.exe                   | 2716       |
| PersTray.exe    | 1            | C:\Program Files\PerSono\perstray.exe                           | 2708       |
| vc6tray.exe     | 1            | C:\Program Files\Virtual CD v6\System\VC6Tray.exe               | 504        |
| ieexplore.exe   | 36           | C:\Program Files\Internet Explorer\IEXPLORE.EXE                 | 3976       |
| rapimgr.exe     | 6            | C:\PROGRA~1\MI3AA1~1\rapimgr.exe                                | 3624       |
| ctfmon.exe      | 1            | C:\WINDOWS\system32\ctfmon.exe                                  | 3436       |
| wscntcomm.exe   | 4            | C:\Program Files\Microsoft ActiveSync\wscntcomm.exe             | 3452       |
| SDTrayApp.exe   | 7            | C:\Program Files\Spyware Doctor\SDTrayApp.exe                   |            |
| proquota.exe    | 2            | C:\WINDOWS\system32\proquota.exe                                |            |
| opwareSE2.exe   | 1            | C:\Program Files\ScanSoft\OpwareSE2.exe                         |            |
| VC6Play.exe     | 7            | C:\Program Files\Hewlett-Packard\VC6Play.exe                    |            |
| winampa.exe     | 1            | C:\Program Files\Media\Winampa.exe                              |            |
| rundll32.exe    | 4            | C:\WINDOWS\system32\rundll32.exe                                |            |
| PcdNTMon.exe    | 5            | C:\Program Files\Trend Micro\PcdNTMon.exe                       |            |
| DVDLauncher.exe | 2            | C:\Program Files\CyberLink\Power2Go\DVDLauncher.exe             |            |
| ico.exe         | 1            | C:\WINDOWS\system32\ico.exe                                     |            |
| issch.exe       | 1            | C:\Program Files\Common Files\Microsoft Shared\Speech\issch.exe |            |
| jusched.exe     | 1            | C:\Program Files\Java\jre1.6\jusched.exe                        |            |
| stsysstra.exe   | 4            | C:\WINDOWS\system32\stsysstra.exe                               |            |
| rundll32.exe    | 1            | C:\WINDOWS\system32\rundll32.exe                                |            |
| WLTRAY.EXE      | 6            | C:\WINDOWS\system32\WLTRAY.EXE                                  |            |
| explorer.exe    | 13           | C:\WINDOWS\explorer.exe                                         |            |
| wmiprvse.exe    | 8            | C:\WINDOWS\system32\wmiprvse.exe                                |            |
| Tablet.exe      | 8            | C:\WINDOWS\system32\Tablet.exe                                  |            |
| TabUserW.exe    | 2            | C:\WINDOWS\system32\TabUserW.exe                                |            |
| wmiprvse.exe    | 6            | C:\WINDOWS\system32\wmiprvse.exe                                |            |
| alg.exe         | 6            | C:\WINDOWS\System32\alg.exe                                     |            |
| OK2E21.EXE      | 1            | C:\TMP\OK2E21.EXE                                               | 2148       |

Number of running processes: 67

This process occurs when a computer prints files in a Windows environment. When a user sends a print command from a computer to the printer, the print spooling process creates a “print job” to some files that remain in the queue unless the print operation is completed successfully.

C:\windows\system32\spool\printer\

SPL: files are created in the printer spooler on your computer when you send documents for printing and are used to store the contents of the documents.

SHD files contain details for the print job.

SHD file is a 'shadow' file that contains information about the print job including owner, the printer, the name of the file printed and the printing method (EMF or RAW)

- SPL and SHD files are stored in the "Printers" spooler folder on your hard disk.
- In RAW format, the .SPL file contains the data to be printed
- In EMF format, the .SPL file contains the name of the file printed, the method and a list of files that contain the data to be printed
- .SHD, .SPL files are deleted after the print job completes

## Linux Forensic

- Linux treats all **devices as a file**. As such, an entry is created in the file system for each hardware device recognized by the operating system.
- For instance, if a standard IDE hard drive is connected to the system, it will be listed under /dev/hdx.

The majority of Linux distributions have a very similar directory structure

#### The Major Linux Directories and Their Functions

| Linux directory path | Description of the Linux directory                                                                                                                                                            |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /                    | The root directory is the lowest level directory in the Linux file system.                                                                                                                    |
| /bin                 | The bin directory contains executable programs which are needed in single user mode. These programs help boot the system or repair it.                                                        |
| /boot                | The boot directory contains a static foals knitted by the boot loader. This directory should hold only files which are needed during the boot process.                                        |
| /dev                 | This directory contains special or device files. These files refer to physical devices.                                                                                                       |
| /etc                 | The etc directory contains consideration files which are local to the machine. Certain larger packages such as X11 have their own subdirectories with consideration files under <i>/etc</i> . |

Linux includes several simple utilities to make imaging and basic analysis of suspect disks and drives simpler. These include:

- `dd` : Command used to copy from an input file or device to an output file or device.
- `dcfldd` : A more advanced variant of `dd` that shows the progress while imaging.
- `sfdisk/fdisk` : Used to determine the structure of a disk.

- md5sum and sha1sum: Create and store an MD5 or SHA hash of a file or list of files (including devices).
- file : Reads file header information in an attempt to ascertain its type, regardless of name or extension.
- xxd : Command line hexdump tool.



**Thank You**