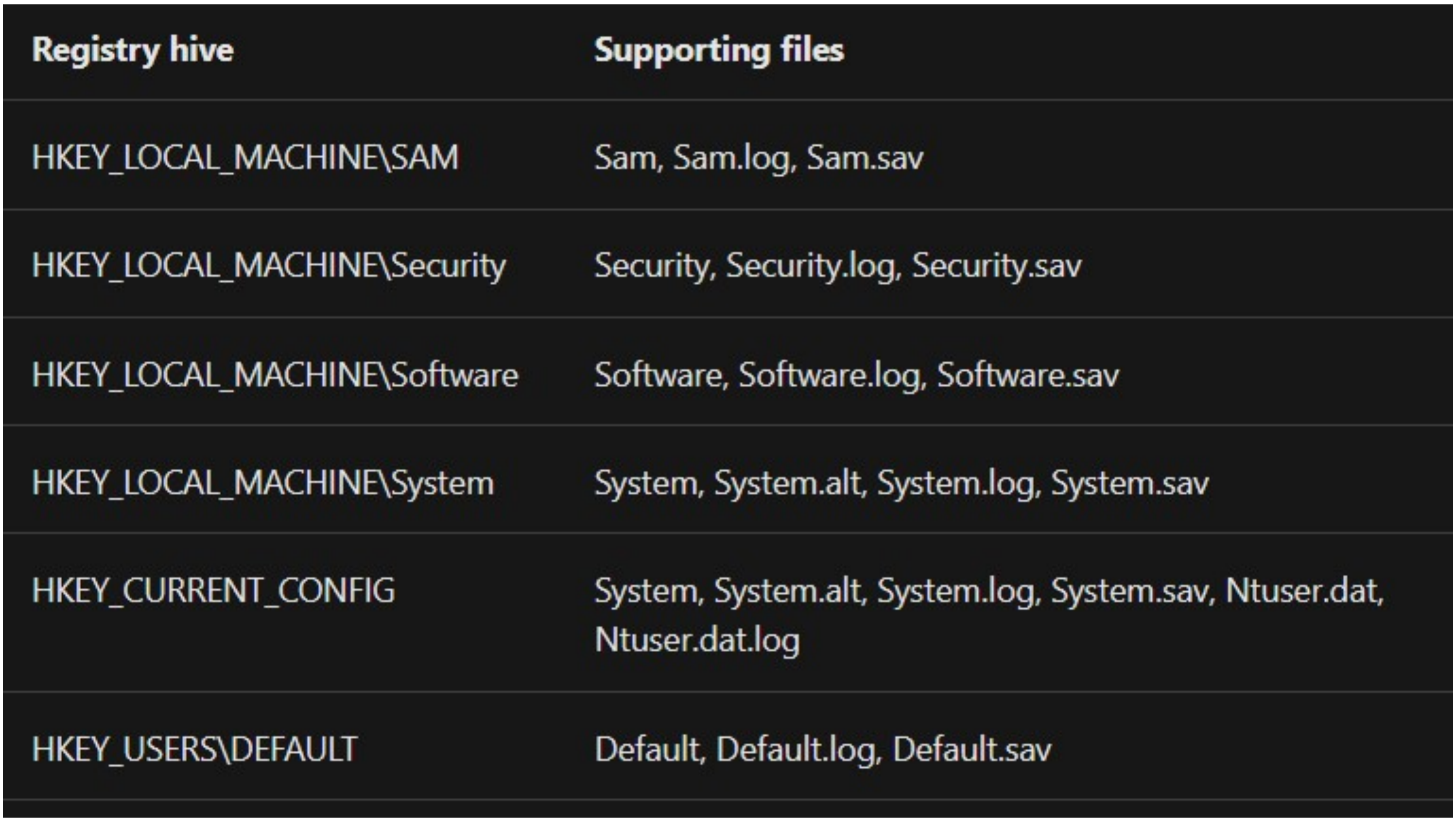
Introduction to Windows Registry Forensics :-

Windows registry, it is a collection of databases which contains informtion such as configuration settings for windows operating systems, profiles for each user, applications installed on the computer, information of hardware which exist on the system, ports being used.

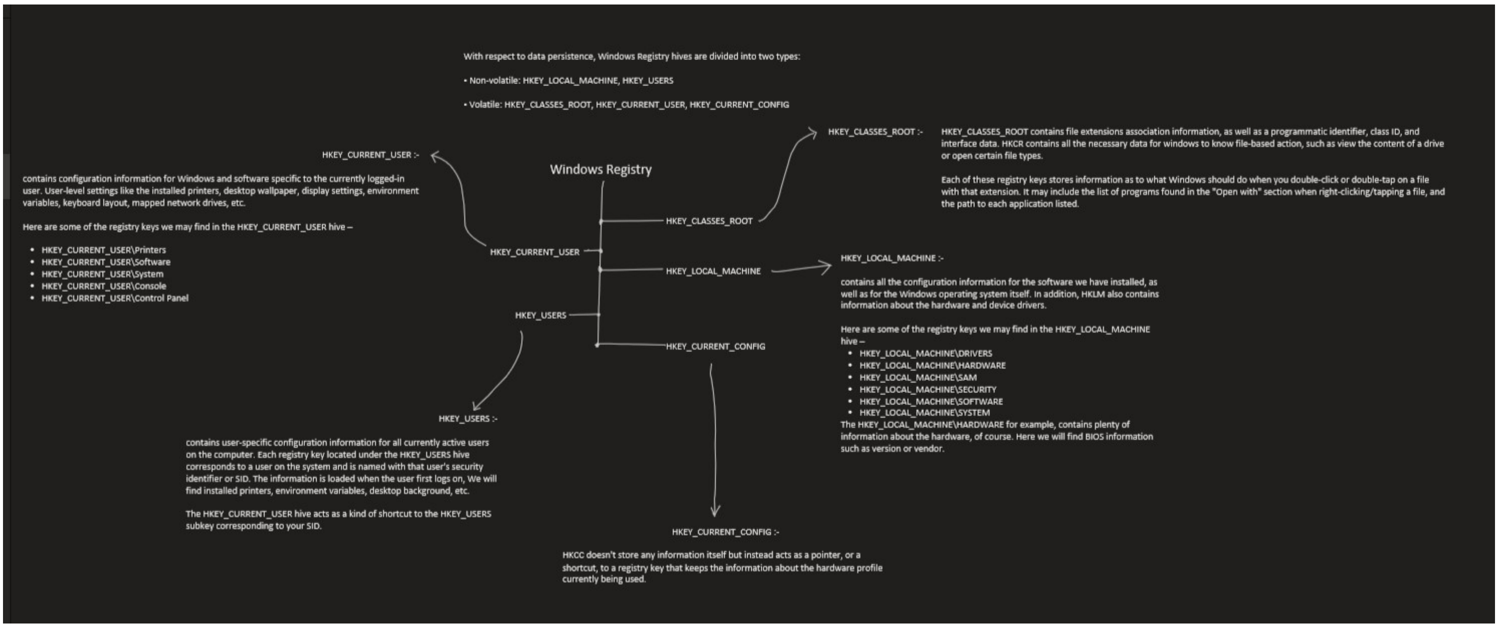


Registry hive	Supporting files
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

For a forensic examiner, a registry hive is a treasure trove of information which he can use to correlate, identify and gather information to prove or disprove a crime. Sometimes, Windows registry can also be used to identify malware infection in the computer.

Windows registry Hierarchy

The following image shows the Hives and their description. These hives contains keys and those keys contain subkeys within them. It is a tree like hierarchical structure.



With respect to data persistence, Windows Registry hives are divided into two types:

- Non-volatile: HKEY_LOCAL_MACHINE, HKEY_USERS
- Volatile: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG

HKEY_CURRENT_USER :-

contains configuration information for Windows and software specific to the currently logged-in user. User-level settings like the installed printers, desktop wallpaper, display settings, environment variables, keyboard layout, mapped network drives, etc.

Here are some of the registry keys we may find in the HKEY_CURRENT_USER hive –

- HKEY_CURRENT_USER\Printers
- HKEY_CURRENT_USER\Software
- HKEY_CURRENT_USER\System
- HKEY_CURRENT_USER\Console
- HKEY_CURRENT_USER\Control Panel

HKEY_CLASSES_ROOT :-

HKEY_CLASSES_ROOT contains file extensions association information, as well as a programmatic identifier, class ID, and interface data. HKCR contains all the necessary data for windows to know file-based action, such as view the content of a drive or open certain file types.

Each of these registry keys stores information as to what Windows should do when you double-click or double-tap on a file with that extension. It may include the list of programs found in the "Open with" section when right-clicking/tapping a file, and the path to each application listed.

HKEY_LOCAL_MACHINE :-

contains all the configuration information for the software we have installed, as well as for the Windows operating system itself. In addition, HKLM also contains information about the hardware and device drivers.

Here are some of the registry keys we may find in the HKEY_LOCAL_MACHINE hive –

- HKEY_LOCAL_MACHINE\DRIVERS
- HKEY_LOCAL_MACHINE\HARDWARE
- HKEY_LOCAL_MACHINE\SAM
- HKEY_LOCAL_MACHINE\SECURITY
- HKEY_LOCAL_MACHINE\SOFTWARE
- HKEY_LOCAL_MACHINE\SYSTEM

The HKEY_LOCAL_MACHINE\HARDWARE for example, contains plenty of information about the hardware, of course. Here we will find BIOS information such as version or vendor.

HKEY_USERS :-

contains user-specific configuration information for all currently active users on the computer. Each registry key located under the HKEY_USERS hive corresponds to a user on the system and is named with that user's security identifier or SID. The information is loaded when the user first logs on, We will find installed printers, environment variables, desktop background, etc.

The HKEY_CURRENT_USER hive acts as a kind of shortcut to the HKEY_USERS subkey corresponding to your SID.

HKEY_CURRENT_CONFIG :-

HKCC doesn't store any information itself but instead acts as a pointer, or a shortcut, to a registry key that keeps the information about the hardware profile currently being used.

Tools and Procedure :-

Useful Tools for Windows Registry Forensics :-

- Regedit - Windows registry explorer

- Regripper

- Accessdata FTK Imager

Procedure :-

1. First get hold of registry hive by either exporting from registry editor

   - Open Registry Editor
   - Choose a hive you'd like to export
   - Click on File menu and select export.

   or using reg command in command prompt.

   ex: reg export <hive/key/subkey> <path to save> or reg save <hive/key/subkey> <path to save>

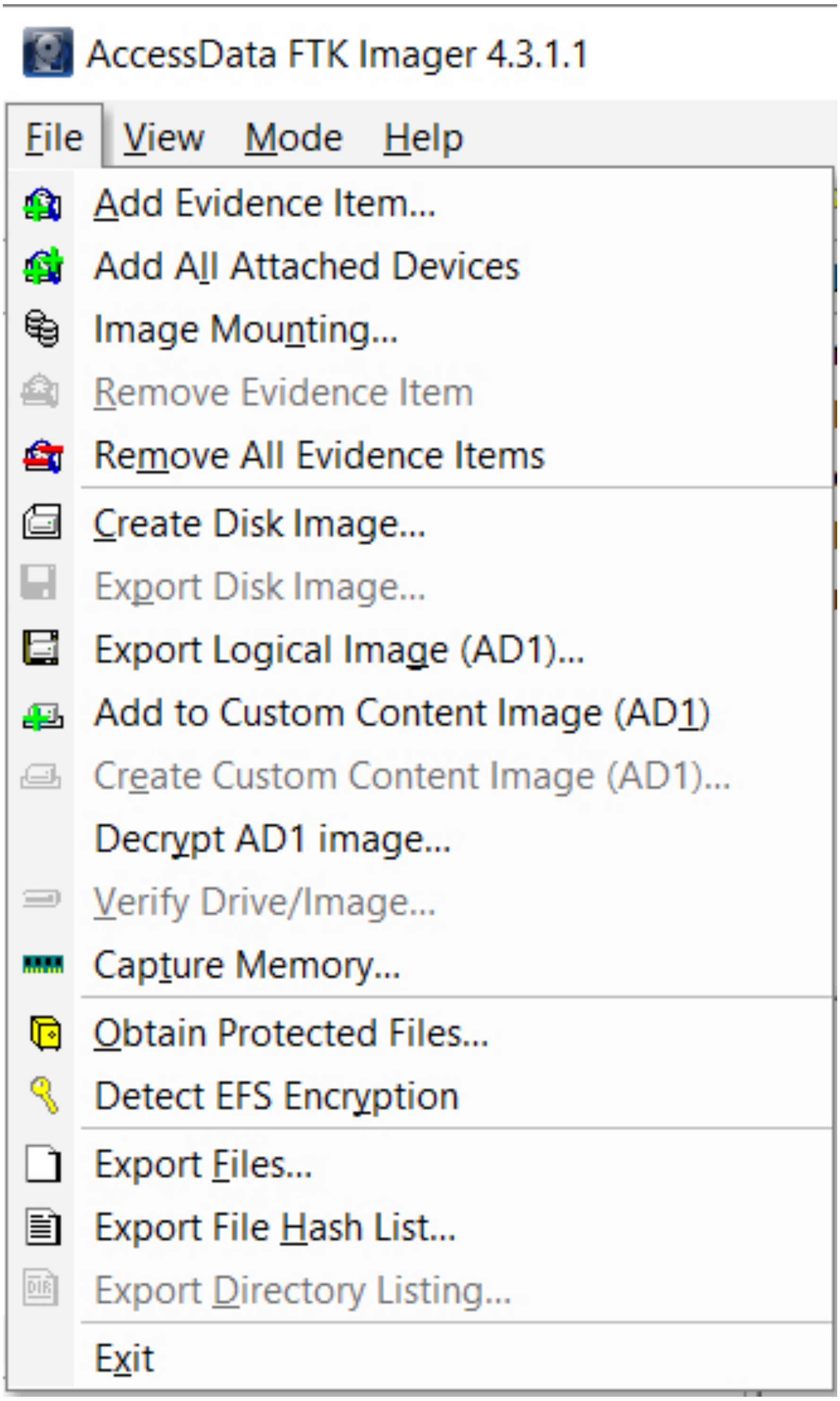
2. Then open regripper tool, load the hive file and choose a report file to save the output to.

3. Then, rip it. Regripper will dump all the parsed data from the input hive file.

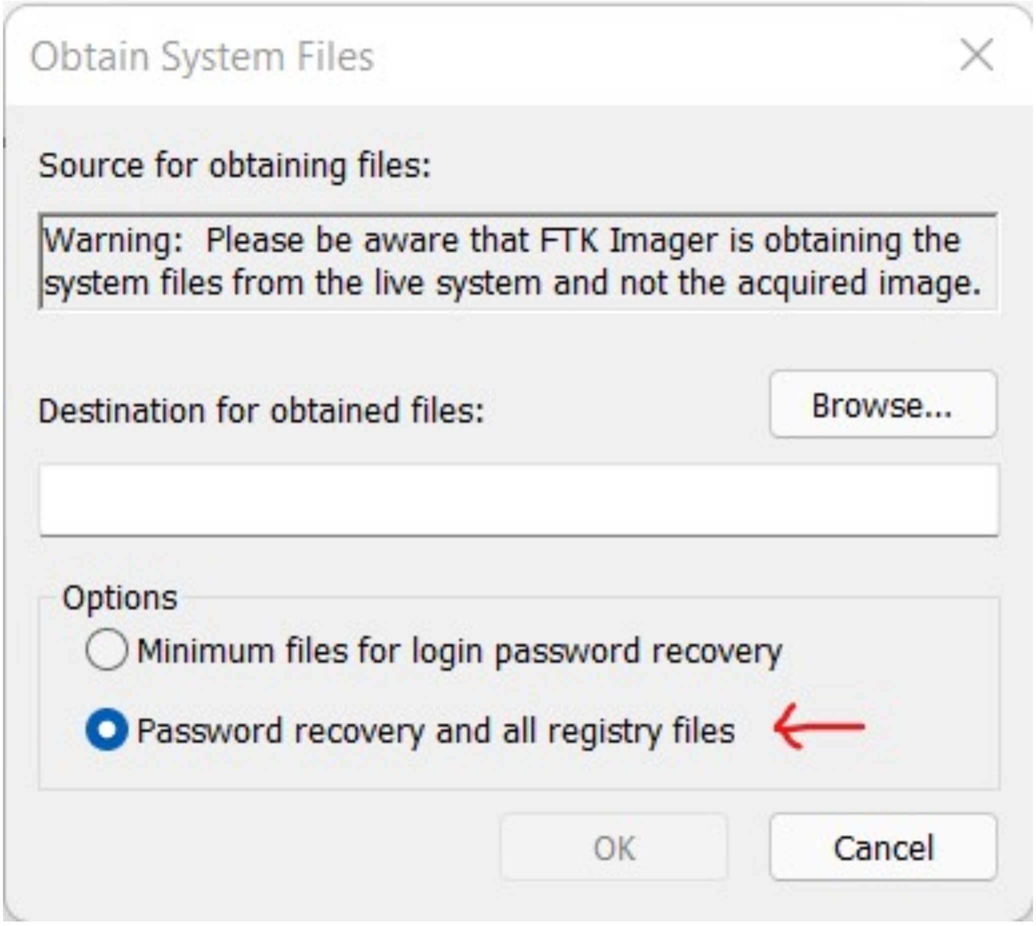
We can also acquire using FTK imager,

1. Click on File.

2. Choose “Obtain Protected Files”.



3. Choose Password recovery and all registry files.



Obtain System Files

Source for obtaining files:

Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image.

Destination for obtained files:

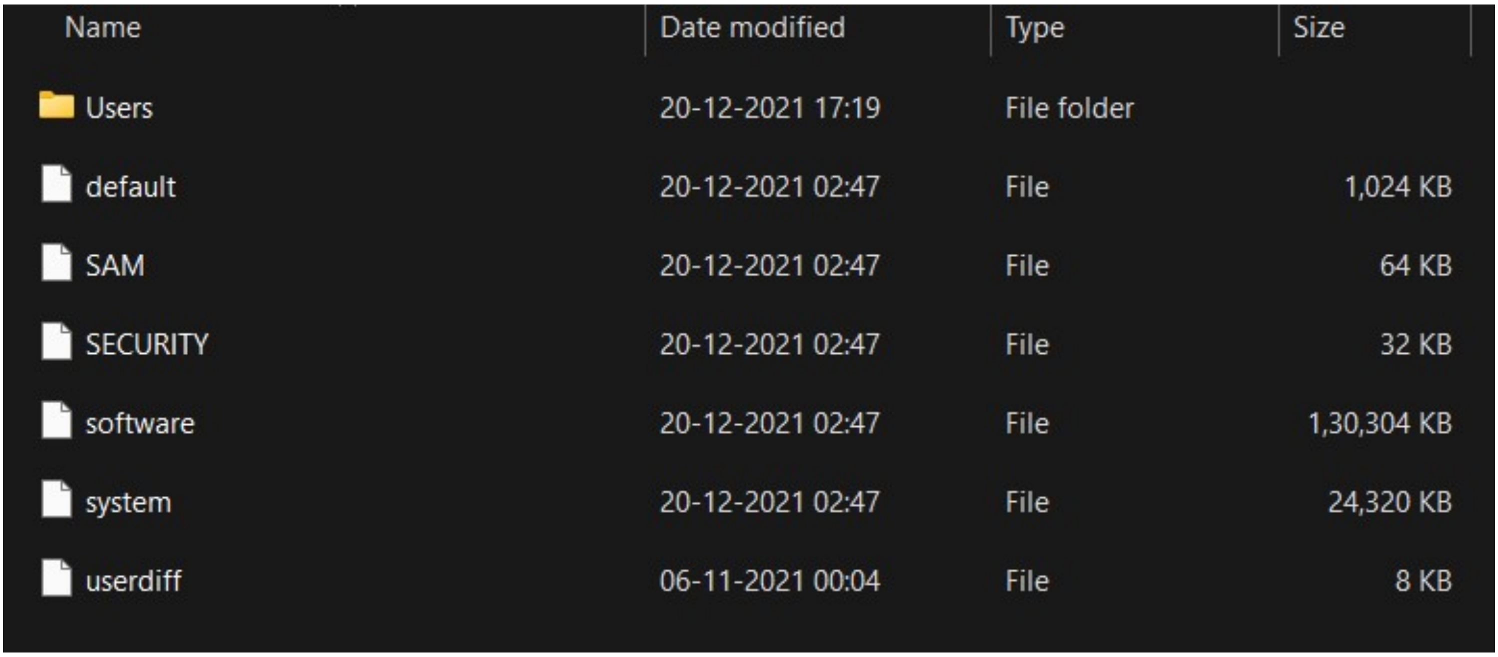
Options

○ Minimum files for login password recovery

● Password recovery and all registry files

4. Choose a destination folder to save the files to.

5. You'll find 6 new files in the destination directory.



Name	Date modified	Type	Size
Users	20-12-2021 17:19	File folder	
default	20-12-2021 02:47	File	1,024 KB
SAM	20-12-2021 02:47	File	64 KB
SECURITY	20-12-2021 02:47	File	32 KB
software	20-12-2021 02:47	File	1,30,304 KB
system	20-12-2021 02:47	File	24,320 KB
userdiff	06-11-2021 00:04	File	8 KB

6. Then, Using RegRipper, we can perform registry analysis on these files.

Interesting Keys to Look at :-

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU - contains a list of recently opened or saved files.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs - recent files which we can find in explorer

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU - recent commands used in run dialog box

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist - contains two GUID subkeys, and each subkey maintains a list of system objects such as program and control panel applets that a user has accessed

HKCU\Software\Microsoft\Internet Explorer\TypedURLs - Recent URL's opened in Internet Explorer (upto 25 url's)

HKLM\SYSTEM\MountedDevices - lists any volume that is mounted and assigned a drive letter.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPCVolume - the key records shares on remote systems such as C$, Temp$, etc.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run - contains programs or components paths that are automatically run during system startup without requiring user interaction.

HKLM\SOFTWARE\Microsoft\Command Processor - contains a command that is automatically executed each time cmd.exe is running.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon - contains windows logon activities often used by attackers to create persistence on the Operating system.

HKEY_CURRENT_USER\software\microsoft\windows\currentversion\Explorer\RunMRU - Contains recent apps opened by the user

HKEY_LOCAL_MACHINE\SYSTEM\controlset001\Enum\USBSTOR - Contains USB related information

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB - Lists all the USB devices previously connected to the machine (**C:>\Windows\inf\setupapi.dev.log** also contains USB related information)

HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices - It shows associated drive letter, GUID, name, vendor ID, product ID and serial number of the USB mass storage device.

HKEY_CURRENT_USER\Software - shows the software being used

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Currentversion\Search\RecentApps - Recent apps searched

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\<id> - go through the subkeys to find network related information like IP address , DHCP server address etc.

Usually, Persistent payloads add themselves in registry. Check the following keys in registry for persistent backdoors.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

If the backdoor is installed with elevated privileges, then look in the following keys, It'll be executed with admin privileges after next reboot,

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx\0001
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend (usually an arbitrary dll file will be placed in this key.)
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce