Artifacts

Dr. Darryl J D’Souza
Mob No: 9986382162

WHAT IS "OPEN SOURCE?"

Generically, "open source" means just that: the source code is open and available for review. However, just because you can view the source code doesn't mean you have license to do anything else with it.

The Open Source Initiative has created a formal definition that lays out the requirements for a software license to be truly open source. In a nutshell, to be considered open source, a piece of software must be freely redistributable, must provide access to the source code, must allow the end user to modify the source code at will, and must not restrict the end use of the software.

"Free" vs "Open"

Due to the overloading of the word "free" in the English language, confusion about what "free" software is can arise. Software available free of charge (gratis) is not necessarily free from restriction (libre). In the open source community, "free software" generally means software considered "open source" and without restriction, in addition to usually being available at no cost. This is in contrast to various "freeware" applications generally found on Windows system available solely in binary, executable format but at no cost.

Open Source Licenses

There are 58 licenses recognized as “Open Source” by the Open Source Initiative.

The two most commonly used licenses are :

- GNU Public License (GPL)
- Berkeley Software Distribution License (BSD).

To grossly simplify, the core difference between these two licenses is that the GPL requires that any modifications made to GPL code that is then incorporated into distributed compiled software be made available in source form as well.

The BSD license does not have this requirement, instead only asking for acknowledgment that the distributed software contains code from a BSD-licensed project.

Open Source Licenses

This means that a widget vendor using GPL-licensed code in their widget controller code must provide customers that purchase their widgets the source code upon request.

If the widget was driven using BSD license software, this would not be necessary. In other words, the GPL favors the rights of the original producer of the code, while the BSD license favors the rights of the user or consumer of the code.

Because of this requirement, the GPL is known as a copyleft license (a play on "copyright"). The BSD license is what is known as a permissive license. Most permissive licenses are considered GPL compatible because they give the end user authority over what he or she does with the code, including using it in derivative works that are GPL licensed.

Additional popular GPL-compatible licenses include the Apache Public License (used by Apache Foundation projects) and the X11/MIT License.

What are artifacts?

Artifacts are the objects or areas within a computer system that have important information related to the activities performed by the computer user. The type and location of this information depends upon the operating system. During forensic analysis, these artifacts play a very important role in approving or disapproving the investigator’s observation.

What are Forensic Artifacts?

Forensic artifacts are the forensic objects that have some forensic value. Any object that contains some data or evidence of something that has occurred like logs, register, hives, and many more. In this section, we will be going through some of the forensic artifacts that a forensic investigator look for while performing a Forensic analysis in Windows.

Task 1 -Introduction to Windows Forensics

Task 1 - Introduction to Windows Forensics

Microsoft Windows is by large the most used Desktop Operating System right now. Private users and Enterprises prefer it, and it currently holds roughly 80% of the Desktop market share.

This means that it is important to know how to perform forensic analysis on Microsoft Windows for someone interested in Digital Forensics. In this module, we will learn about the different ways we can gather forensic data from the Windows Registry and make conclusions about the activity performed on a Windows system based on this data.

So is my computer spying on me? What do you think?

Windows saves these preferences to make your computer more personalized. However, forensic investigators use these preferences as artifacts to identify the activity performed on a system.

So while your computer might be spying on you, it is not for the explicit reason of spying, instead to make it more pleasant to use the computer according to your taste. But that same information is used by forensic investigators to perform forensic analysis. As we move through this room, we'll see that Windows stores these artifacts in different locations throughout the file system such as in the registry, a user's profile directory, in application-specific files, etc.

Importance of Windows Artifacts for Forensics

Windows artifacts assume significance due to the following reasons −

- Around 90% of the traffic in world comes from the computers using Windows as their operating system. That is why for digital forensics examiners Windows artifacts are very essentials.
- The Windows operating system stores different types of evidences related to the user activity on computer system. This is another reason which shows the importance of Windows artifacts for digital forensics.
- Many times the investigator revolves the investigation around old and traditional areas like user crated data. Windows artifacts can lead the investigation towards non-traditional areas like system created data or the artifacts.
- Great abundance of artifacts is provided by Windows which are helpful for investigators as well as for companies and individuals performing informal investigations.
- Increase in cyber-crime in recent years is another reason that Windows artifacts are important.

Task 2 -Windows Registry and Forensics

Common Windows Artifacts

Windows Registry

What is the Windows registry?

The Windows Registry is a collection of databases that contains the system's configuration data. This configuration data can be about the hardware, the software, or the user's information. It also includes data about the recently used files, programs used, or devices connected to the system. As you can understand, this data is beneficial from a forensics standpoint. Throughout this room, we will learn ways to read this data to identify the required information about the system. You can view the registry using regedit.exe, a built-in Windows utility to view and edit the registry. We'll explore other tools to learn about the registry in the upcoming tasks.

The Windows registry consists of Keys and Values. When you open the regedit.exe utility to view the registry, the folders you see are Registry Keys. Registry Values are the data stored in these Registry Keys. A Registry Hive is a group of Keys, subkeys, and values stored in a single file on the disk.

The Windows Registry is a hierarchical database that stores configurations for users, applications, and hardware devices. Here's how Microsoft describes it:

The Registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system, and the ports that are being used.

Windows Registry

The Windows registry is an invaluable source of forensic artifacts for all examiners and analysts. The registry holds configurations for Windows and is a substitute for the .INI files in Windows 3.1.

It is a binary, hierarchical database and some of its contents include configuration settings and data for the OS and for the different applications relying on it.

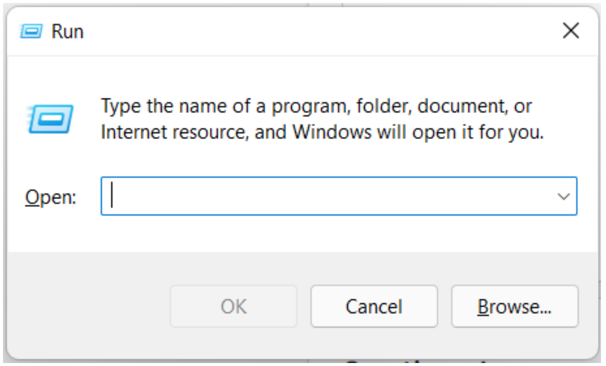
The registry not only keeps records of OS and application settings but it also monitors and records user-specific data in order to structure and enhance the user's experience during interactions with the system.

Most of the time users do not interact with the registry in a straightforward manner, but they interact indirectly with it via installation routines, applications, and programs, such as Microsoft Installer files.

Nonetheless, system admins have the capability of interacting directly with the registry via regedit.exe (the registry editor) that comes with all varieties of Windows.

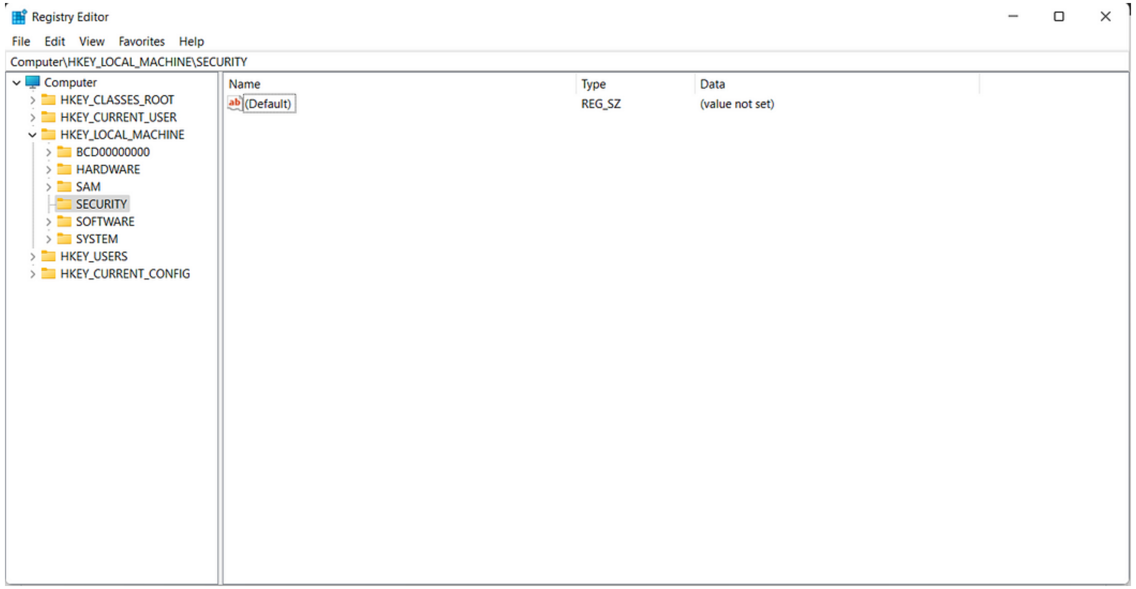
Windows Registry

You can view these keys when you open the regedit.exe utility. To open the registry editor, press the Windows key and the R key simultaneously. It will open a run prompt that looks like this:



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

In this prompt, type regedit.exe, and you will be greeted with the registry editor window. It will look something like this:



Computer\HKEY_LOCAL_MACHINE\SECURITY

Name	Type	Data
(Default)	REG_SZ	(value not set)

Windows Registry

The Windows registry consists of Keys and Values. When you open the regedit.exe utility to view the registry, the folders you see are Registry Keys. Registry Values are the data stored in these Registry Keys. A Registry Hive is a group of Keys, subkeys, and values stored in a single file on the disk.

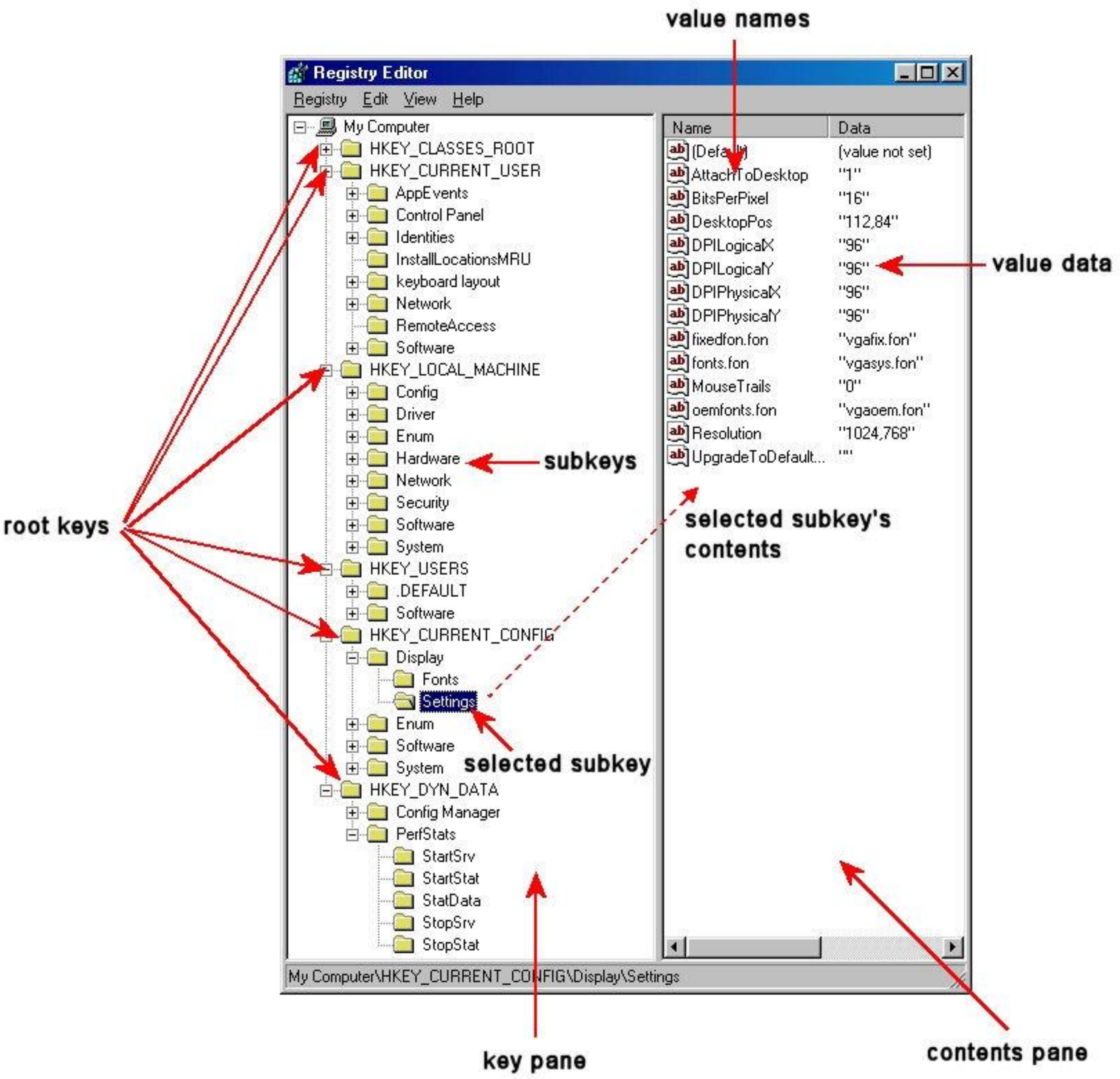
Hives

The Windows Registry is composed of five main root keys, also known as hives, under the root key Computer, these are:

HKEY_CLASSES_ROOT (HKCR) — contains information about file types and their associated programs.
HKEY_CURRENT_USER (HKCU) — contains information about the logged in user, including screen colors, and control panel settings.
HKEY_LOCAL_MACHINE (HKLM) — contains information about the system configuration (for any user).
HKEY_USERS (HKU) — contains information about actively loaded user profiles on the system, including profiles and settings.
HKEY_CURRENT_CONFIG (HKCC) — contains information about the hardware profile of the system.

Registry Structure

The registry is structured very similarly to the Windows directory/subdirectory structure. You have the five root keys or hives and then subkeys. In some cases, you have sub-subkeys. These subkeys then have descriptions and values that are displayed in the contents pane. Very often, the values are simply 0 or 1, meaning on or off, but also can contain more complex information usually displayed in hexadecimal.



- My Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
    - AppEvents
    - Control Panel
    - Identities
    - InstallLocationsMRU
    - keyboard layout
    - Network
    - RemoteAccess
    - Software
  - HKEY_LOCAL_MACHINE
    - Config
    - Driver
    - Enum
    - Hardware
    - Network
    - Security
    - Software
    - System
  - HKEY_USERS
    - .DEFAULT
    - Software
  - HKEY_CURRENT_CONFIG
    - Display
      - Fonts
      - Settings
    - Enum
    - Software
    - System
  - HKEY_DYN_DATA
    - Config Manager
    - PerfStats
      - StartSrv
      - StartStat
      - StatData
      - StopSrv
      - StopStat

Name	Data
(Default)	(value not set)
AttachToDesktop	"1"
BitsPerPixel	"16"
DesktopPos	"112,84"
DPILogicalX	"96"
DPILogicalY	"96"
DPIPhysicalX	"96"
DPIPhysicalY	"96"
fixedfon.fon	"vgafix.fon"
fonts.fon	"vgasys.fon"
MouseTrails	"0"
oemfonts.fon	"vgaoem.fon"
Resolution	"1024,768"
UpgradeToDefault...	""

My Computer\HKEY_CURRENT_CONFIG\Display\Settings

value names

value data

root keys

subkeys

selected subkey's contents

selected subkey

key pane

contents pane

Windows Registry

Here you can see the root keys in the left pane in a tree view that shows the included registry keys, and the values in the selected key are shown in the right pane.

You can right-click on the value shown in the right pane and select properties to view the properties of this value.

Here is how Microsoft defines each of these root keys. For more detail and information about the following Windows registry keys, please visit Microsoft’s documentation.

Windows Registry

Each of these keys contains a hierarchy of subkeys and values that store specific information about the system and its configuration. For example, the configuration for the mouse, such as sensitivity, and double click speed are stored in Computer\HKEY_CURRENT_USER\Control Panel\Mouse. We can also visualize it as a tree where each branch represents a subkey:

```
Computer
|__ HKEY_CURRENT_USER
        |__ Control Panel
                |__ Mouse
```

Registry keys can be viewed and modified by using the built-in Registry Editor. Following are two ways to open it, through the Search bar or by using the Run command (Win + R).

An alternative approach is to do it the other way around by first modifying the registry keys, and then seeing the changes after rebooting the computer or signing out and signing back in.

Information in the Registry with Forensic Value

As a forensic investigator, the registry can prove to be a treasure trove of information on who, what, where, and when something took place on a system that can directly link the perpetrator to the actions being called into question.

Information that can be found in the registry includes:

- Users and the time they last used the system
- Most recently used software
- Any devices mounted to the system including unique identifiers of flash drives, hard drives, phones, tablets, etc.
- When the system connected to a specific wireless access point
- What and when files were accessed
- A list any searches done on the system

And much, much more

Task 3 -Accessing registry hives offline

Task 3 - Accessing registry hives offline

If you are accessing a live system, you will be able to access the registry using regedit.exe, and you will be greeted with all of the standard root keys we learned about in the previous task. However, if you only have access to a disk image, you must know where the registry hives are located on the disk. The majority of these hives are located in the C:\Windows\System32\Config directory and are:

DEFAULT (mounted on HKEY_USERS\DEFAULT)

SAM (mounted on HKEY_LOCAL_MACHINE\SAM)

SECURITY (mounted on HKEY_LOCAL_MACHINE\Security)

SOFTWARE (mounted on HKEY_LOCAL_MACHINE\Software)

SYSTEM (mounted on HKEY_LOCAL_MACHINE\System)

Hives containing user information:

Apart from these hives, two other hives containing user information can be found in the User profile directory. For Windows 7 and above, a user’s profile directory is located in C:\Users\<username>\ where the hives are:

NTUSER.DAT (mounted on HKEY_CURRENT_USER when a user logs in)

USRCLASS.DAT (mounted on HKEY_CURRENT_USER\Software\CLASSES)

The NTUSER.DAT hive is located in the directory C:\Users\<username>\.

The USRCLASS.DAT hive is located in the directory C:\Users\<username>\AppData\Local\Microsoft\Windows.

Remember that NTUSER.DAT and USRCLASS.DAT are hidden files.

Malware

Malware often adds registry values in specific locations to achieve persistence. Common keys to check include:

- **HKCU\Software\Microsoft\Windows\CurrentVersion\Run**
  Malware may add an entry here to execute at user login.
- **HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce**
- **HKCU\Environment**
  Some malware modifies environment variables.
- **HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon**
- **HKCU\Software\Classes\exefile\shell\open\command** (used for file association hijacking).

Hives containing user information:

The Amcache Hive:

Apart from these files, there is another very important hive called the AmCache hive. This hive is located in C:\Windows\AppCompat\Programs\Amcache.hve. Windows creates this hive to save information on programs that were recently run on the system.

Transaction Logs and Backups:

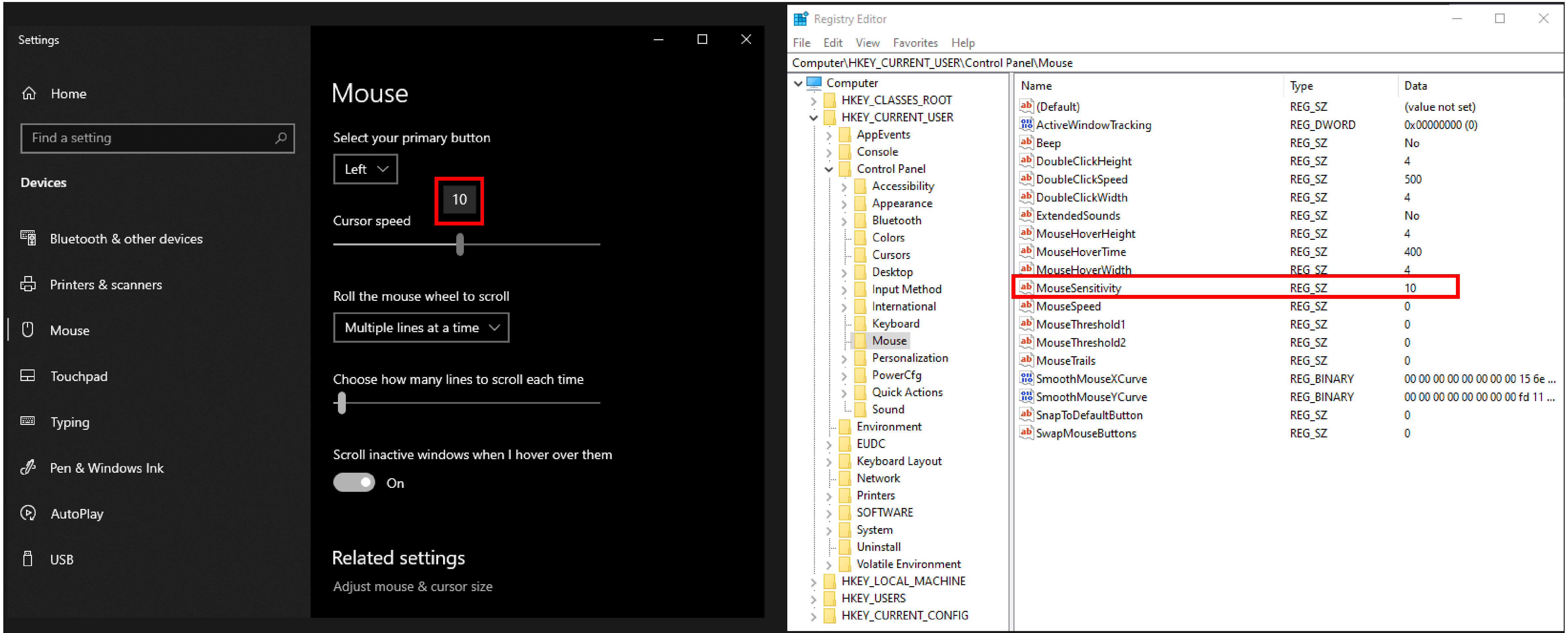
Some other very vital sources of forensic data are the registry transaction logs and backups. The transaction logs can be considered as the journal of the changelog of the registry hive. Windows often uses transaction logs when writing data to registry hives. This means that the transaction logs can often have the latest changes in the registry that haven’t made their way to the registry hives themselves. The transaction log for each hive is stored as a .LOG file in the same directory as the hive itself. It has the same name as the registry hive, but the extension is .LOG. For example, the transaction log for the SAM hive will be located in C:\Windows\System32\Config in the filename SAM.LOG. Sometimes there can be multiple transaction logs as well. In that case, they will have .LOG1, .LOG2 etc., as their extension. It is prudent to look at the transaction logs as well when performing registry forensics.

For you to try

Registry backups are the opposite of Transaction logs. These are the backups of the registry hives located in the C:\Windows\System32\Config directory. These hives are copied to the C:\Windows\System32\Config\RegBack directory every ten days. It might be an excellent place to look if you suspect that some registry keys might have been deleted/modified recently.

Windows Registry

To test it out, we can modify the mouse sensitivity in settings and see the changes reflected in registry keys. An alternative approach is to do it the other way around by first modifying the registry keys, and then seeing the changes after rebooting the computer or signing out and signing back in.



Mouse

Select your primary button: Left

Cursor speed: 10

Roll the mouse wheel to scroll: Multiple lines at a time

Choose how many lines to scroll each time

Scroll inactive windows when I hover over them: On

Computer\HKEY_CURRENT_USER\Control Panel\Mouse

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveWindowTracking	REG_DWORD	0x00000000 (0)
Beep	REG_SZ	No
DoubleClickHeight	REG_SZ	4
DoubleClickSpeed	REG_SZ	500
DoubleClickWidth	REG_SZ	4
ExtendedSounds	REG_SZ	No
MouseHoverHeight	REG_SZ	4
MouseHoverTime	REG_SZ	400
MouseHoverWidth	REG_SZ	4
MouseSensitivity	REG_SZ	10
MouseSpeed	REG_SZ	0
MouseThreshold1	REG_SZ	0
MouseThreshold2	REG_SZ	0
MouseTrails	REG_SZ	0
SmoothMouseXCurve	REG_BINARY	00 00 00 00 00 00 00 00 15 6e ...
SmoothMouseYCurve	REG_BINARY	00 00 00 00 00 00 00 00 fd 11 ...
SnapToDefaultButton	REG_SZ	0
SwapMouseButtons	REG_SZ	0

Wireless Evidence in the Registry

Many hackers crack a local wireless access point and use it for their intrusions. In this way, if the IP address is traced, it will lead back to the neighbor's or other wireless AP and not them.

Case Example - January 2012, an Anonymous member, John Borrell III, hacked into the computer systems of the Salt Lake City police department and the Utah Chiefs of Police. The FBI was called in to investigate and they traced the hacker back to the IP address of Blessed Sacrament Church's Wi-Fi AP in Toledo, Ohio. The hacker had apparently cracked the password of the church's wireless AP and was using it to hack "anonymously" on the Internet.

Eventually, the FBI was able to find the suspect through various investigation techniques, mostly low-tech, exhaustive, detective work. It helped that John Borrell had bragged on Twitter of his success as a hacker. Eventually, Mr. Borrell was convicted and sentenced to two years in Federal prison.
When the FBI tracked down Mr. Borrell and seized his computer, they were able to prove he had been connected to the church AP by examining his registry. The forensic investigator simply had to look in the registry at this location:

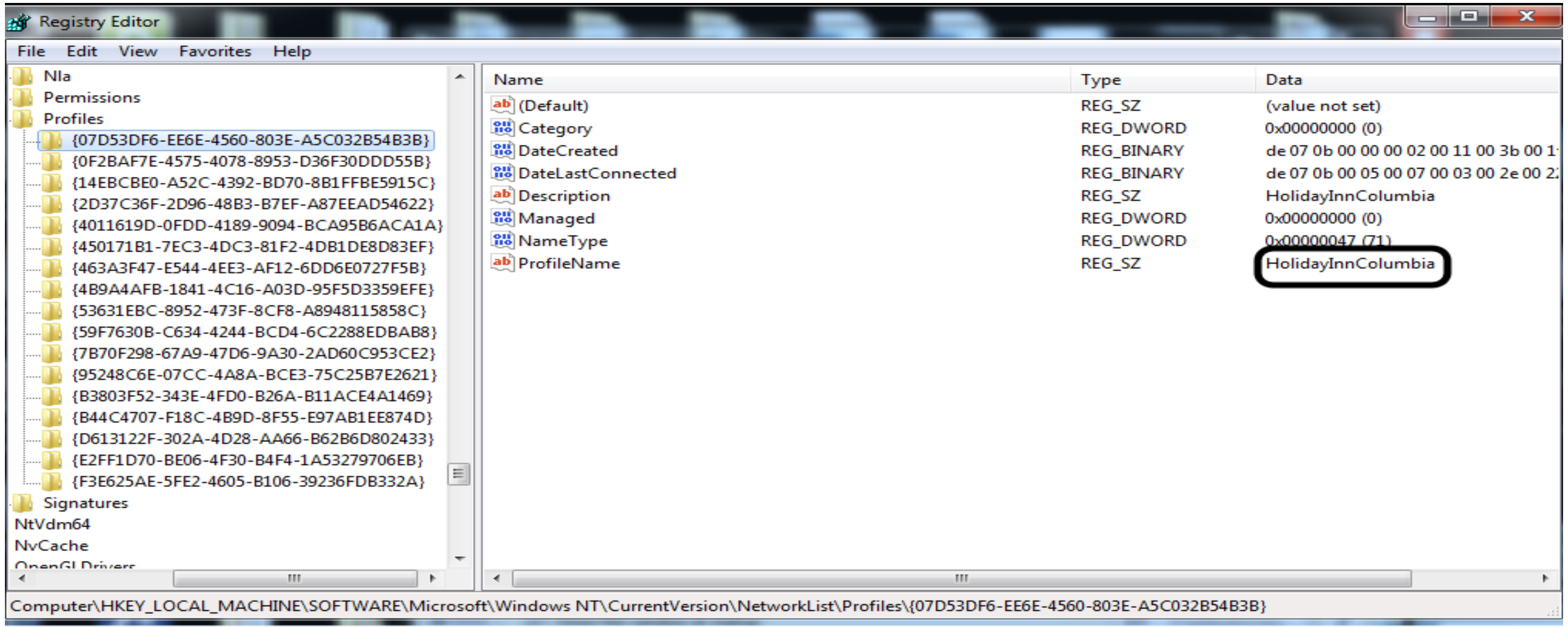
For You to try:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

Wireless Evidence in the Registry

There, you will find a list of GUIDs of wireless access points the machine has been connected to. When you click on one, it reveals information including the SSID name and the date last connected in hexadecimal. So, although Mr. Borrell initially denied his involvement with this hack, this evidence was conclusive and he eventually plead guilty.

You can see in this screenshot below showing the perpetrator had connected to the "HolidayInnColumbia" SSID in November 2014.



```
Nla
Permissions
Profiles
    {07D53DF6-EE6E-4560-803E-A5C032B54B3B}
    {0F2BAF7E-4575-4078-8953-D36F30DDD55B}
    {14EBCBE0-A52C-4392-BD70-8B1FFBE5915C}
    {2D37C36F-2D96-48B3-B7EF-A87EEAD54622}
    {4011619D-0FDD-4189-9094-BCA95B6ACA1A}
    {450171B1-7EC3-4DC3-81F2-4DB1DE8D83EF}
    {463A3F47-E544-4EE3-AF12-6DD6E0727F5B}
    {4B9A4AFB-1841-4C16-A03D-95F5D3359EFE}
    {53631EBC-8952-473F-8CF8-A8948115858C}
    {59F7630B-C634-4244-BCD4-6C2288EDBAB8}
    {7B70F298-67A9-47D6-9A30-2AD60C953CE2}
    {95248C6E-07CC-4A8A-BCE3-75C25B7E2621}
    {B3803F52-343E-4FD0-B26A-B11ACE4A1469}
    {B44C4707-F18C-4B9D-8F55-E97AB1EE874D}
    {D613122F-302A-4D28-AA66-B62B6D802433}
    {E2FF1D70-BE06-4F30-B4F4-1A53279706EB}
    {F3E625AE-5FE2-4605-B106-39236FDB332A}
Signatures
NtVdm64
NvCache
OpenGLDrivers
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Category	REG_DWORD	0x00000000 (0)
DateCreated	REG_BINARY	de 07 0b 00 00 00 02 00 11 00 3b 00 1
DateLastConnected	REG_BINARY	de 07 0b 00 05 00 07 00 03 00 2e 00 2
Description	REG_SZ	HolidayInnColumbia
Managed	REG_DWORD	0x00000000 (0)
NameType	REG_DWORD	0x00000047 (71)
ProfileName	REG_SZ	HolidayInnColumbia

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{07D53DF6-EE6E-4560-803E-A5C032B54B3B}

Task 4 -Exploring Windows Registry

Task 5 - Exploring Windows Registry

Once we have extracted the registry hives, we need a tool to view these files as we would in the registry editor. Since the registry editor only works with live systems and can't load exported hives, we can use the following tools:

1. *AccessData's Registry Viewer :* has a similar user interface to the Windows Registry Editor. There are a couple of limitations, though. It only loads one hive at a time, and it can't take the transaction logs into account.
2. *Zimmerman's Registry Explorer:* Eric Zimmerman has developed a handful of tools that are very useful for performing Digital Forensics and Incident Response.
3. *RegRipper*: RegRipper is a utility that takes a registry hive as input and outputs a report that extracts data from some of the forensically important keys and values in that hive. The output report is in a text file and shows all the results in sequential order.

Eric Zimmerman Tools

Eric Zimmerman is a senior director in Kroll's Cyber Risk practice, based in the New York Office. Eric has a tremendous depth and breadth of expertise in the cyber realm, spanning complex law enforcement investigations, computer forensics, expert witness testimony, computer systems design, and application architecture.

Eric Zimmerman is a well-known digital forensics and incident response (DFIR) professional who has developed several open-source and free tools that are widely used in the digital forensics community. These tools cover various aspects of digital investigations and forensic analysis.

Eric Zimmerman tools:

Registry Explorer (RECmd):

1. A command-line tool to parse and export data from Windows registry hives.

ShellBags Explorer (SBECmd):

1. A command-line tool to parse and display information from Windows ShellBags artifacts.

RECmd (Rapid Environment for Cyber Incident Response):

1. A collection of tools that automate various digital forensics and incident response tasks.

JLECmd (Jump List Explorer):

1. A command-line tool for parsing and displaying information from Windows Jump Lists.

Eric Zimmerman Tools

Eric Zimmerman tools:

LNKParse:

A command-line tool for parsing Windows shortcut files (LNK files).

AmcacheParser:

A tool for parsing the Amcache.hve registry hive, which contains information about executed applications on Windows systems.

Registry Decoder:

A tool for decoding various Windows registry artifacts.

AppCompatCacheParser:

A tool for parsing the ShimCache registry key and the Amcache.hve file.

USB WriteBlocker:

A tool that helps prevent writing to USB devices, useful for preserving evidence during forensic analysis.

EvtxECmd:

A command-line tool for parsing Windows Event Log files (evtx).

SuperTimeline:

A tool for creating SuperTimeline charts from various forensic artifacts.

LNK Files

LNK files are the shortcut files that serve as a quick access to frequently used files, folders, or programs on the system. These files typically have a .lnk file extension and can be found in locations such as the desktop, start menu, and recent documents folder.

Whenever a file is accessed for the first time, a .lnk file gets created in the Recents folder. This information is particularly useful in identifying when a file was first accessed.

These files are usually found in:

C:\Users\%USERNAME%\Recent

C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent

C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Office\Recent

C:\Users\%USERNAME%\Desktop

One way to explore LNK files and extract useful information from them is by using a tool called LECmd. We can use it to extract original full path of the file, the date and time the file was created, last modified, last accessed, the desktop name, and the MAC address of the system where the file was created.

More info at - https://github.com/EricZimmerman/LECmd

Task 5 -System Information and System Accounts

Let’s find out where to look in the registry to perform our forensic analysis.

When we start performing forensic analysis, the first step is to find out about the system information. This task will cover gathering information related to a machine’s System and Account information.

Current control set:

The hives containing the machine's configuration data used for controlling system startup are called Control Sets. Commonly, we will see two Control Sets, ControlSet001 and ControlSet002, in the SYSTEM hive on a machine. In most cases, ControlSet001 will point to the Control Set that the machine booted with, and ControlSet002 will be the last known good configuration. Their locations will be:

SYSTEM\ControlSet001

SYSTEM\ControlSet002

Windows creates a volatile Control Set when the machine is live, called the CurrentControlSet (HKLM\SYSTEM\CurrentControlSet). For getting the most accurate system information, this is the hive that we will refer to. We can find out which Control Set is being used as the CurrentControlSet by looking at the following registry value:

SYSTEM\Select\Current

Similarly, the last known good configuration can be found using the following registry value:

SYSTEM\Select\LastKnownGood

Computer Name:

It is crucial to establish the Computer Name while performing forensic analysis to ensure that we are working on the machine we are supposed to work on. We can find the Computer Name from the following location:

SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

Time Zone Information:

For accuracy, it is important to establish what time zone the computer is located in. This will help us understand the chronology of the events as they happened. For finding the Time Zone Information, we can look at the following location:

SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Time Zone Information is important because some data in the computer will have their timestamps in UTC/GMT and others in the local time zone. Knowledge of the local time zone helps in establishing a timeline when merging data from all the sources.

OS Version:

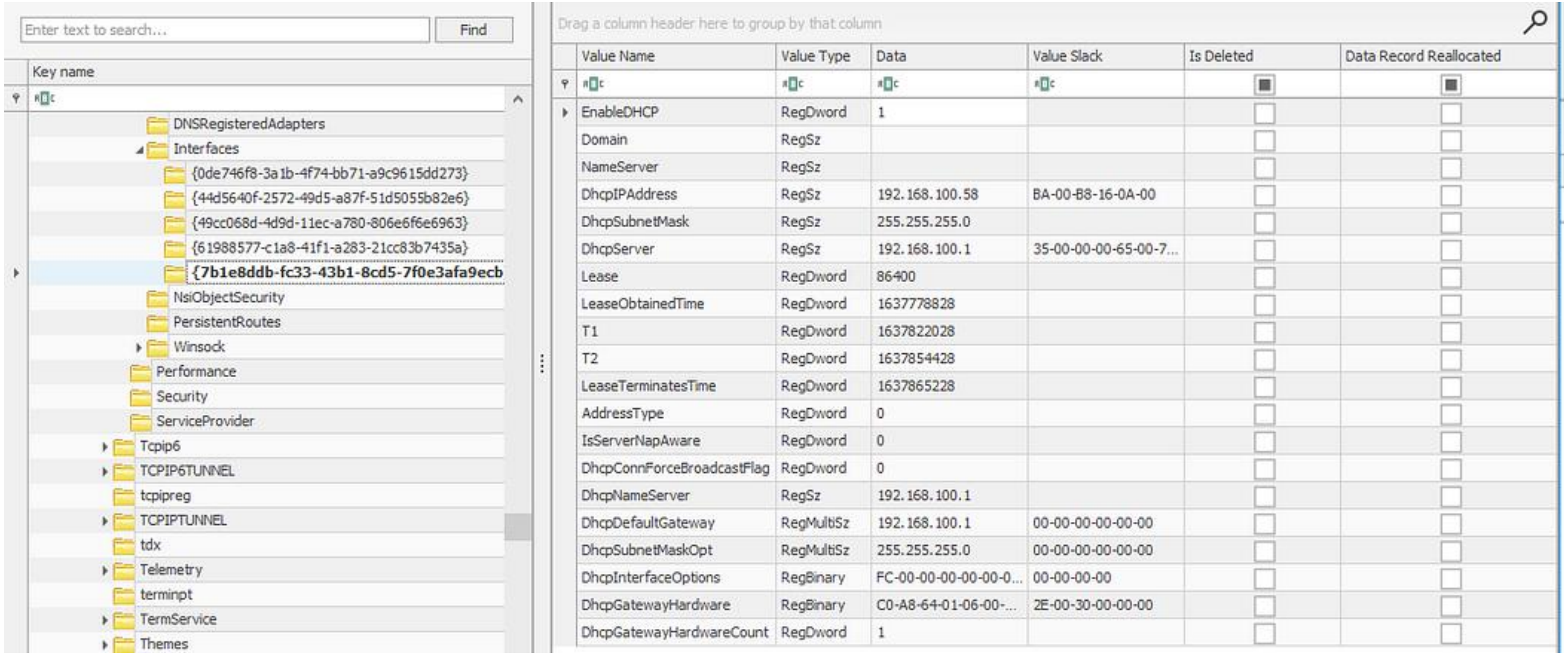
If we only have triage data to perform forensics, we can determine the OS version from which this data was pulled through the registry. To find the OS version, we can use the following registry key:

SOFTWARE\Microsoft\Windows NT\CurrentVersion

Network Interfaces and Past Networks:

The following registry key will give a list of network interfaces on the machine we are investigating:

SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces



Key name

- DNSRegisteredAdapters
- Interfaces
  - {0de746f8-3a1b-4f74-bb71-a9c9615dd273}
  - {44d5640f-2572-49d5-a87f-51d5055b82e6}
  - {49cc068d-4d9d-11ec-a780-806e6f6e6963}
  - {61988577-c1a8-41f1-a283-21cc83b7435a}
  - **{7b1e8ddb-fc33-43b1-8cd5-7f0e3afa9ecb**
- NsiObjectSecurity
- PersistentRoutes
- Winsock
- Performance
- Security
- ServiceProvider
- Tcpip6
- TCPIP6TUNNEL
- tcpipreg
- TCPIPTUNNEL
- tdx
- Telemetry
- terminpt
- TermService
- Themes

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
EnableDHCP	RegDword	1		□	□
Domain	RegSz			□	□
NameServer	RegSz			□	□
DhcpIPAddress	RegSz	192.168.100.58	BA-00-B8-16-0A-00	□	□
DhcpSubnetMask	RegSz	255.255.255.0		□	□
DhcpServer	RegSz	192.168.100.1	35-00-00-00-65-00-7...	□	□
Lease	RegDword	86400		□	□
LeaseObtainedTime	RegDword	1637778828		□	□
T1	RegDword	1637822028		□	□
T2	RegDword	1637854428		□	□
LeaseTerminatesTime	RegDword	1637865228		□	□
AddressType	RegDword	0		□	□
IsServerNapAware	RegDword	0		□	□
DhcpConnForceBroadcastFlag	RegDword	0		□	□
DhcpNameServer	RegSz	192.168.100.1		□	□
DhcpDefaultGateway	RegMultiSz	192.168.100.1	00-00-00-00-00-00	□	□
DhcpSubnetMaskOpt	RegMultiSz	255.255.255.0	00-00-00-00-00-00	□	□
DhcpInterfaceOptions	RegBinary	FC-00-00-00-00-00-0...	00-00-00-00	□	□
DhcpGatewayHardware	RegBinary	C0-A8-64-01-06-00-...	2E-00-30-00-00-00	□	□
DhcpGatewayHardwareCount	RegDword	1		□	□

Network Interfaces and Past Networks:

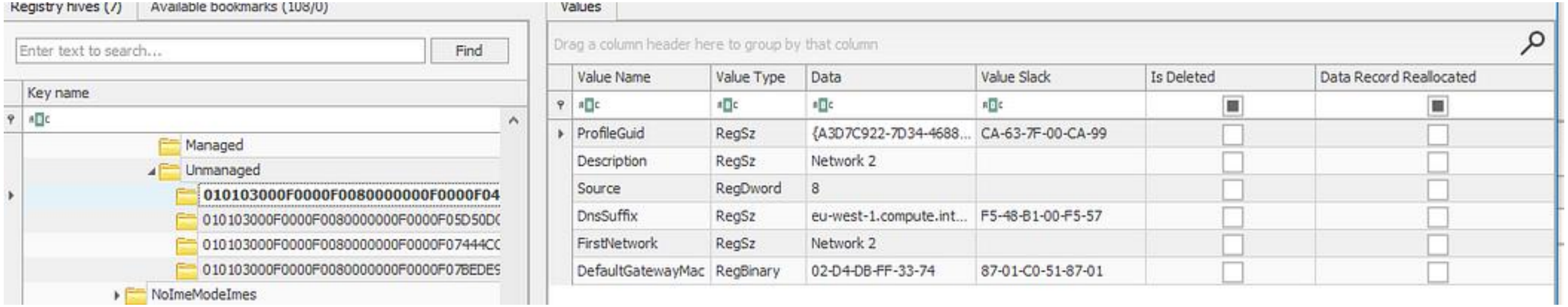
Each Interface is represented with a unique identifier (GUID) subkey, which contains values relating to the interface’s TCP/IP configuration. This key will provide us with information like IP addresses, DHCP IP address and Subnet Mask, DNS Servers, and more. This information is significant because it helps you make sure that you are performing forensics on the machine that you are supposed to perform it on.

The past networks a given machine was connected to can be found in the following locations:

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed

These registry keys contain past networks as well as the last time they were connected. The last write time of the registry key points to the last time these networks were connected.


Registry hives (7)
Available bookmarks (108/0)
Enter text to search...
Find
Values
Drag a column header here to group by that column

Key name

- Managed
- Unmanaged
  - 010103000F0000F0080000000F0000F04
  - 010103000F0000F0080000000F0000F05D50D(
  - 010103000F0000F0080000000F0000F07444CC
  - 010103000F0000F0080000000F0000F07BEDES
- NoImeModeImes

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
ProfileGuid	RegSz	{A3D7C922-7D34-4688...	CA-63-7F-00-CA-99	□	□
Description	RegSz	Network 2		□	□
Source	RegDword	8		□	□
DnsSuffix	RegSz	eu-west-1.compute.int...	F5-48-B1-00-F5-57	□	□
FirstNetwork	RegSz	Network 2		□	□
DefaultGatewayMac	RegBinary	02-D4-DB-FF-33-74	87-01-C0-51-87-01	□	□

Dr. Darryl J D’Souza

Autostart Programs (Autoruns):

The following registry keys include information about programs or commands that run when a user logs on.

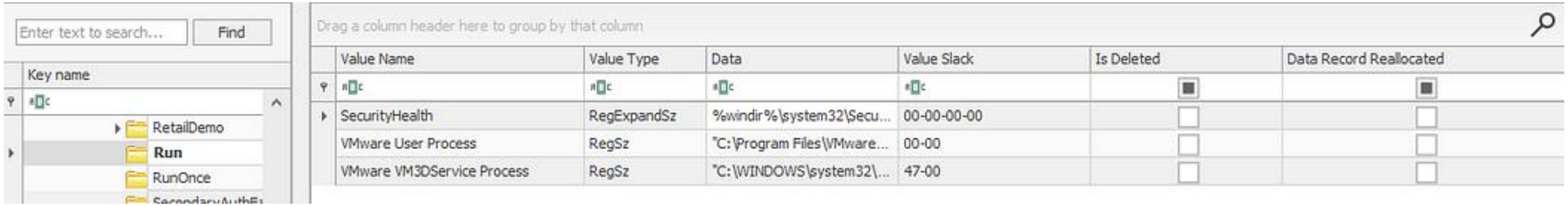
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce

SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

SOFTWARE\Microsoft\Windows\CurrentVersion\Run



Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
SecurityHealth	RegExpandSz	%windir%\system32\Secu...	00-00-00-00	□	□
VMware User Process	RegSz	"C:\Program Files\VMware...	00-00	□	□
VMware VM3DService Process	RegSz	"C:\WINDOWS\system32\...	47-00	□	□

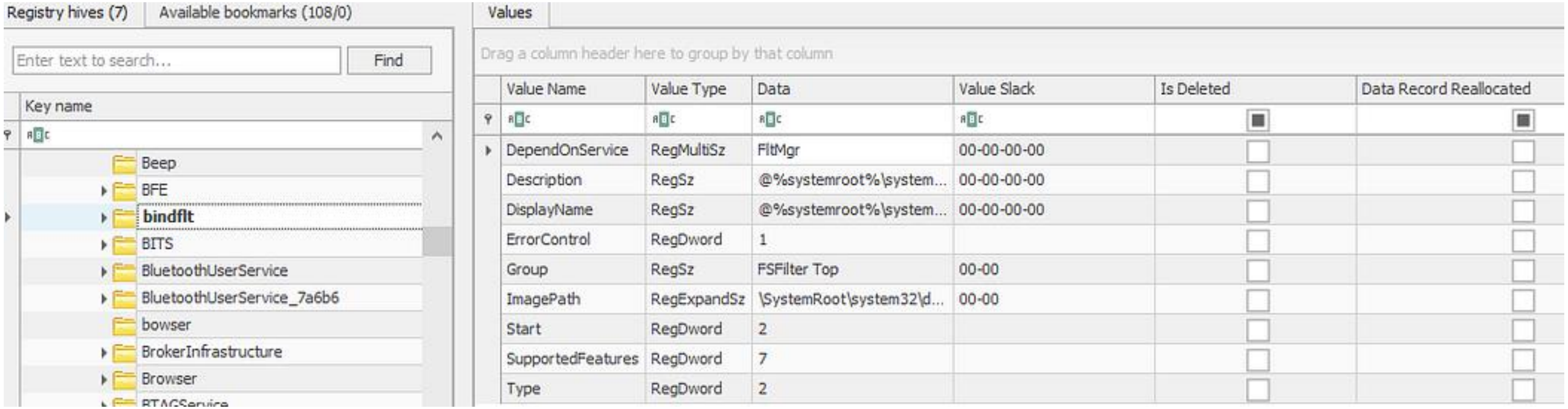
Autostart Programs (Autoruns):

The following registry key contains information about services:

SYSTEM\CurrentControlSet\Services

Notice the Value of the Start key in the screenshot below.

In this registry key, if the start key is set to 0x02, this means that this service will start at boot.



Registry hives (7)
Available bookmarks (108/0)
Enter text to search...
Find
Key name
Values
Drag a column header here to group by that column

- Beep
- BFE
- **bindflt**
- BITS
- BluetoothUserService
- BluetoothUserService_7a6b6
- bowser
- BrokerInfrastructure
- Browser
- BTAGService

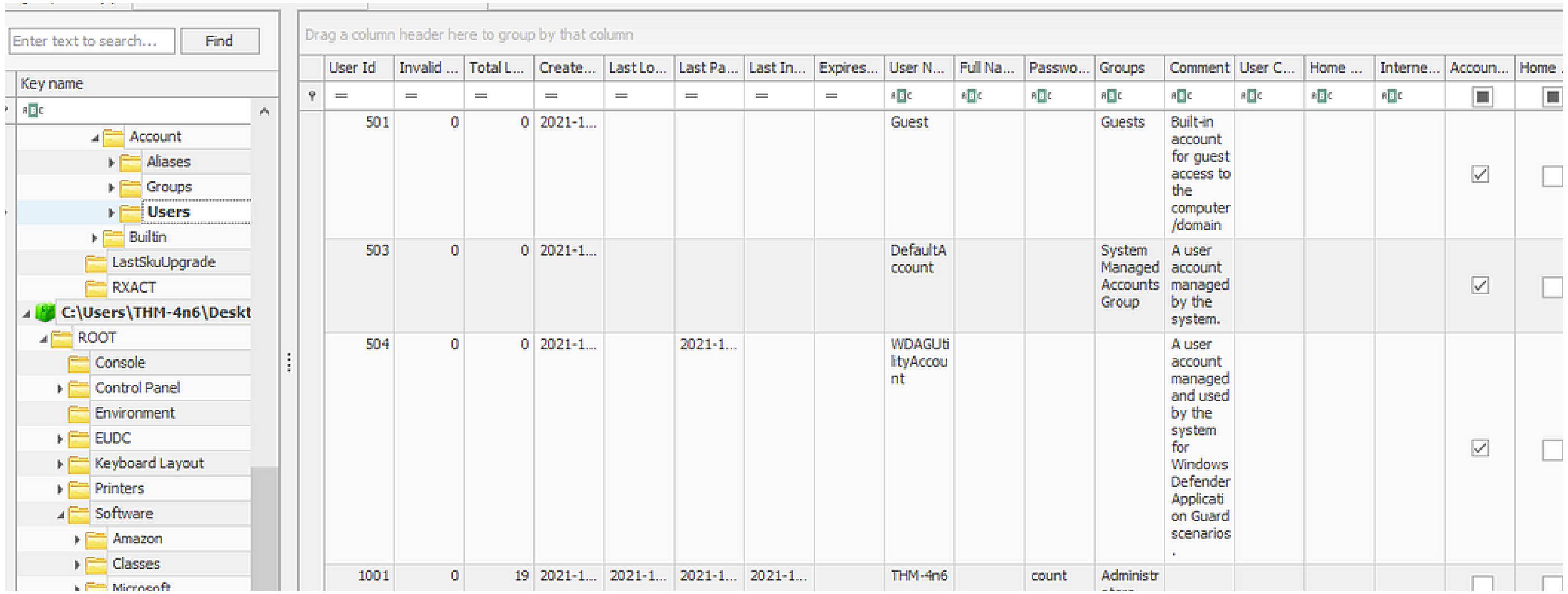
Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
DependOnService	RegMultiSz	FltMgr	00-00-00-00	☐	☐
Description	RegSz	@%systemroot%\system...	00-00-00-00	☐	☐
DisplayName	RegSz	@%systemroot%\system...	00-00-00-00	☐	☐
ErrorControl	RegDword	1		☐	☐
Group	RegSz	FSFilter Top	00-00	☐	☐
ImagePath	RegExpandSz	\SystemRoot\system32\d...	00-00	☐	☐
Start	RegDword	2		☐	☐
SupportedFeatures	RegDword	7		☐	☐
Type	RegDword	2		☐	☐

SAM hive and user information:

The SAM hive contains user account information, login information, and group information. This information is mainly located in the following location:

SAM\Domains\Account\Users

The information contained here includes the relative identifier (RID) of the user, number of times the user logged in, last login time, last failed login, last password change, password expiry, password policy and password hint, and any groups that the user is a part of.



User Id	Invalid ...	Total L...	Create...	Last Lo...	Last Pa...	Last In...	Expires...	User N...	Full Na...	Passwo...	Groups	Comment	User C...	Home ...	Interne...	Accoun...	Home ..
501	0	0	2021-1...					Guest			Guests	Built-in account for guest access to the computer /domain				☑	□
503	0	0	2021-1...					DefaultAccount			System Managed Accounts Group	A user account managed by the system.				☑	□
504	0	0	2021-1...		2021-1...			WDAGUtilityAccount				A user account managed and used by the system for Windows Defender Application Guard scenarios .				☑	□
1001	0	19	2021-1...	2021-1...	2021-1...	2021-1...		THM-4n6		count	Administr					□	□

Questions

1. What is the most used Desktop Operating System right now?
2. What is the short form for HKEY_LOCAL_MACHINE?
3. What is the path for the five main registry hives, DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM?
4. What is the path for the AmCache hive?

5. What is the Current Build Number of the Target machine whose data is being investigated?
    1. Which ControlSet contains the last known good configuration?
    2. What is the Computer Name of the computer?
    3. What is the value of the TimeZoneKeyName?
    4. What is the DHCP IP address
    5. What is the RID of the Guest User account?

Lab Questions

1. Given the registry file of a system that was compromised, answer the following:

I. What’s the mouse double-click speed?

II. What’s the most recent typed path accessed as recorded in the registry?

III. What’s the new value added to the registry by the malware in order to establish persistence over the system?