Digital Forensics - Lab 12

Class No :	**CH2021221000516**	Slot :	**L49 + L50**
Course Code :	**CSE4004**	Faculty Name :	**Nagaraj SV**

Aadhitya Swarnesh

- 24 November 2021

Question 1 :

Find the list of Wireless Access Points that the computer has been connected.

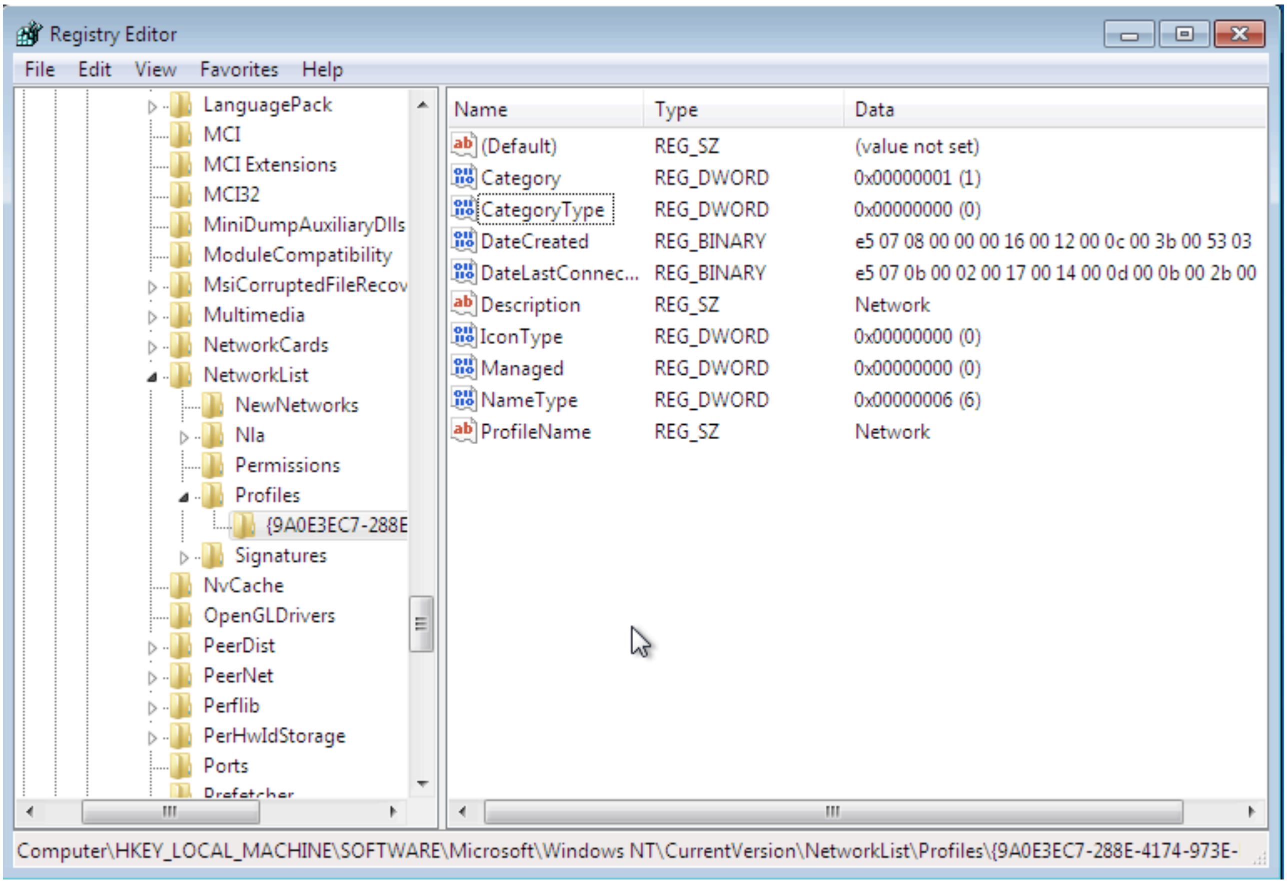
Many hackers crack a local wireless access point and use it for their intrusions. In this way, if the IP address is traced, it will lead back to the neighbor's or other wireless AP and not them. However, evidence about wireless can be got from the registry. A forensic investigator simply has to look in the registry for :

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

There, we will find a list of GUIDs of wireless access points the machine has been connected to. When we click on one, it reveals information including the SSID name and the date last connected in hexadecimal.

We have thereby implemented the same procedure as stated in our computer which is currently running a Windows 7 Professional inside a VirtualBox Environment. I will be using the “regedit” tool available in all windows versions.

The output when we navigate to this location using the regedit is as follows :



Name	Type	Data
(Default)	REG_SZ	(value not set)
Category	REG_DWORD	0x00000001 (1)
CategoryType	REG_DWORD	0x00000000 (0)
DateCreated	REG_BINARY	e5 07 08 00 00 00 16 00 12 00 0c 00 3b 00 53 03
DateLastConnec...	REG_BINARY	e5 07 0b 00 02 00 17 00 14 00 0d 00 0b 00 2b 00
Description	REG_SZ	Network
IconType	REG_DWORD	0x00000000 (0)
Managed	REG_DWORD	0x00000000 (0)
NameType	REG_DWORD	0x00000006 (6)
ProfileName	REG_SZ	Network

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{9A0E3EC7-288E-4174-973E-

Question 2 :

View the most recent documents used or opened on the system.

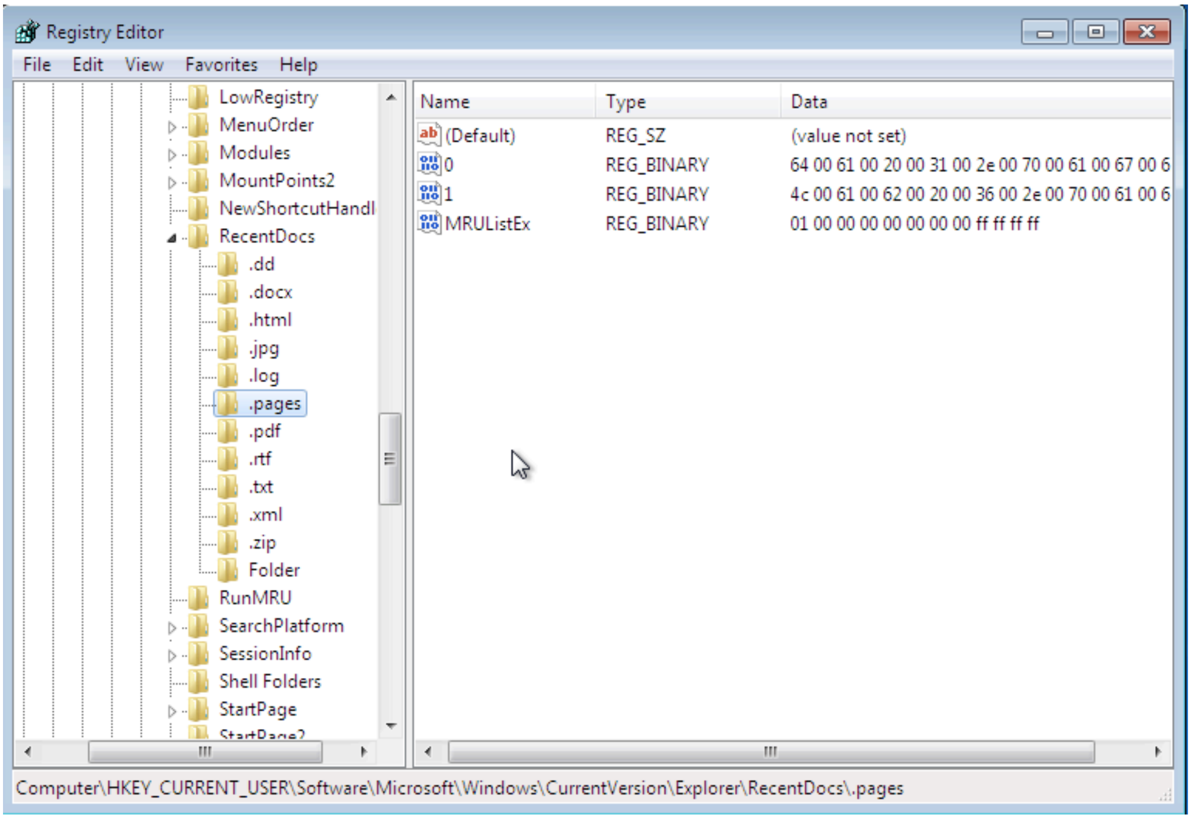
The "RecentDocs" key tracks the most recent documents used or opened on the system by file extension. It can be found at:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

We will now follow this path using the same regedit tool to figure out the documents opened recently. You can see that there are a few different types of file types inside, this shows that the files have been categorized by their file types. On opening these folders, the individual files can be seen as listed.

Let us open a few of these data types and view the underlying data below :

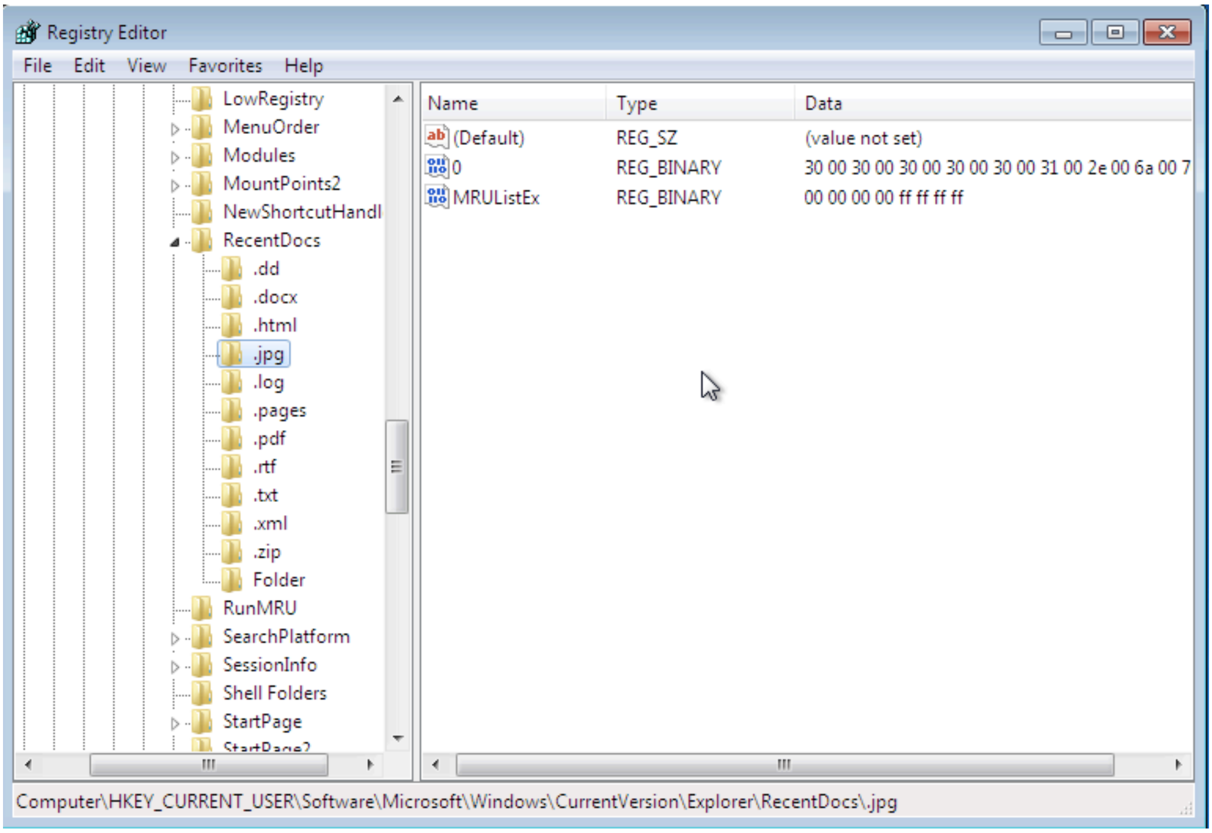
The following image shows the files of type “pages” :



Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	64 00 61 00 20 00 31 00 2e 00 70 00 61 00 67 00 6
1	REG_BINARY	4c 00 61 00 62 00 20 00 36 00 2e 00 70 00 61 00 6
MRUListEx	REG_BINARY	01 00 00 00 00 00 00 00 ff ff ff ff

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pages

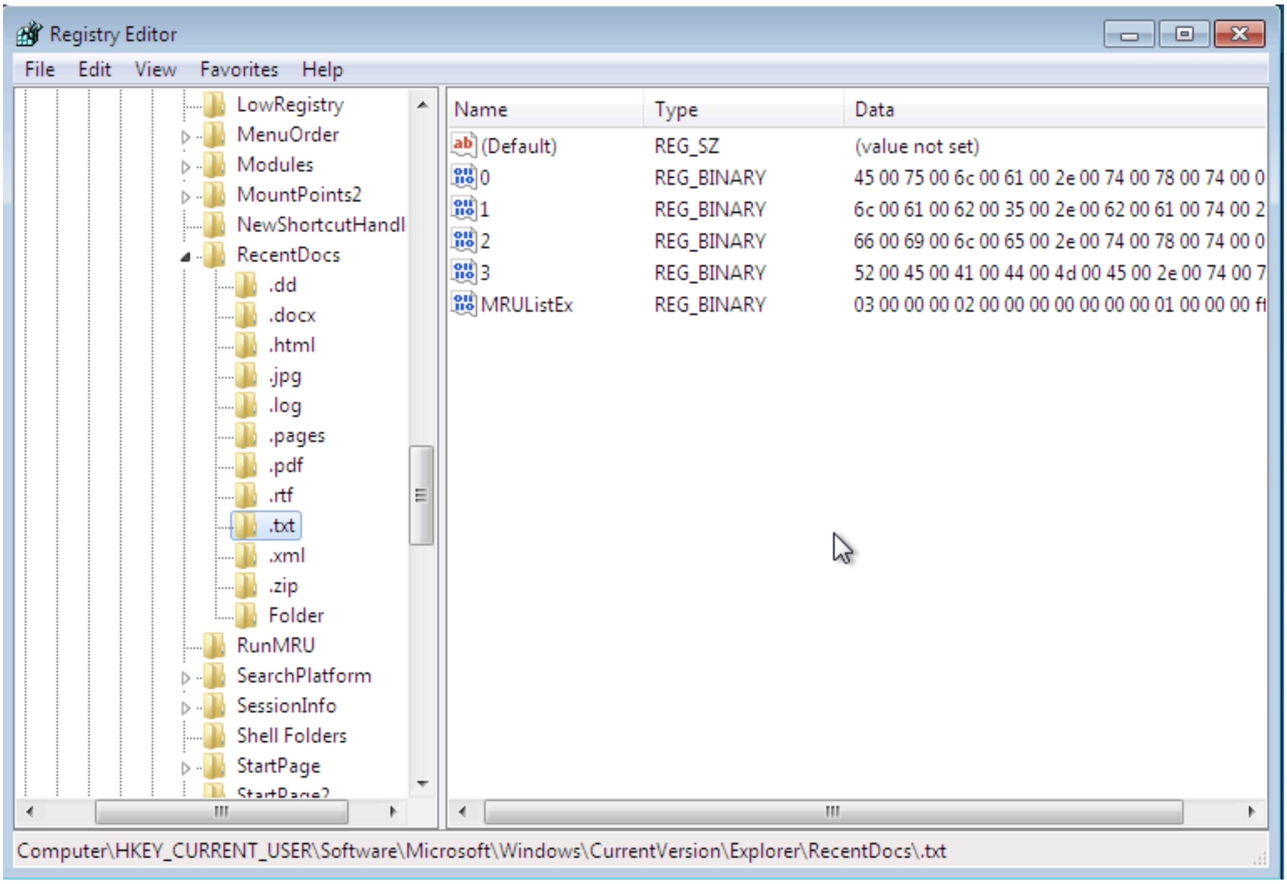
The following image shows the files of type “jpg” :



Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	30 00 30 00 30 00 30 00 30 00 31 00 2e 00 6a 00 7
MRUListEx	REG_BINARY	00 00 00 00 ff ff ff ff

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg

The following image shows the files of type “txt” :



Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	45 00 75 00 6c 00 61 00 2e 00 74 00 78 00 74 00 0
1	REG_BINARY	6c 00 61 00 62 00 35 00 2e 00 62 00 61 00 74 00 2
2	REG_BINARY	66 00 69 00 6c 00 65 00 2e 00 74 00 78 00 74 00 0
3	REG_BINARY	52 00 45 00 41 00 44 00 4d 00 45 00 2e 00 74 00 7
MRUListEx	REG_BINARY	03 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 ff

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt

Question 3 :

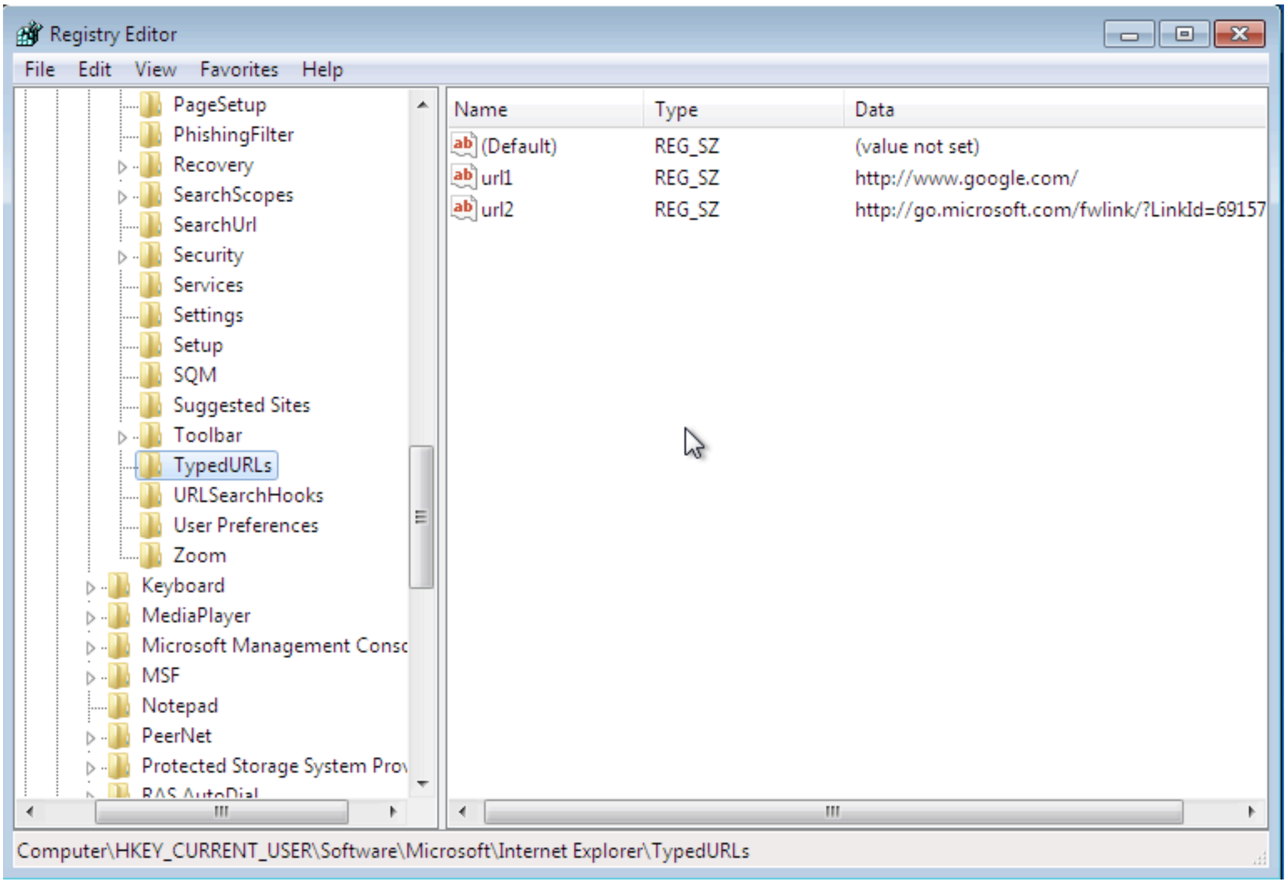
List the last URLs that the user visited with Internet Explorer.

When the user types a URL in Internet Explorer, this value is stored in the registry at:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

When we open that key in the registry, it lists the last URLs that the user visited with Internet Explorer. This could reveal the source of malicious malware that was used in the breach, or in civil or policy violation types of investigations, may reveal what the user was looking for.

In the following image, we see the list of URL's that I have visited recently using the Internet Explorer.



Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	http://www.google.com/
url2	REG_SZ	http://go.microsoft.com/fwlink/?LinkId=69157

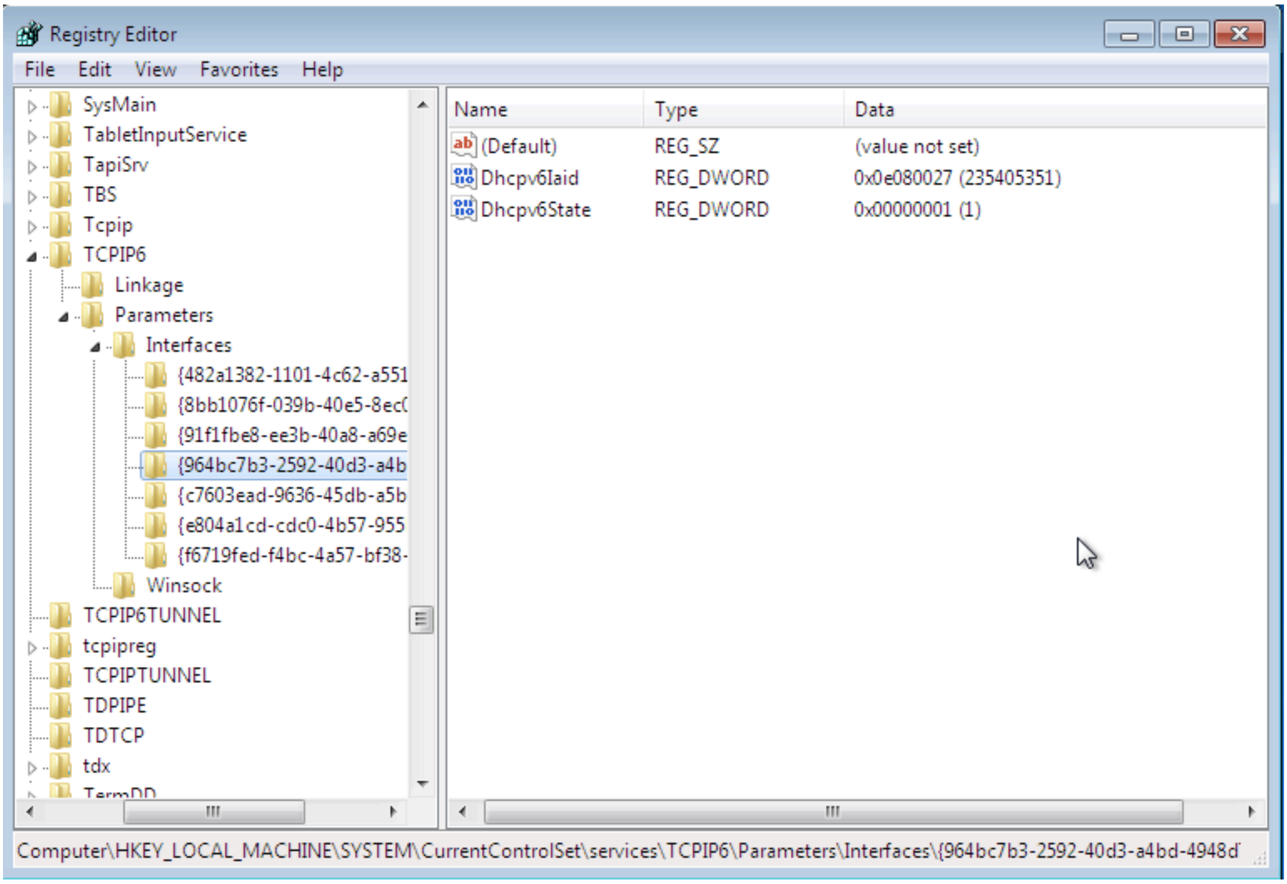
Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

The registry also tracks the IP addresses of the user interfaces. Note that there may be numerous interfaces and this registry key tracks each interface's IP address and related information. This can be viewed in the location :

HKEY_LOCAL_MACHINE\System\Services\CurrentControlSet\services\Tcpip\Parameters\Interfaces

We can find the IP address assigned to the interface, the subnet mask, and the time when the DHCP server leased the IP. In this way, we can tell whether the suspect was using that particular IP at the time of the intrusion or crime.

If we navigate to this location, we can see the IP addresses assigned to the system currently in use :



Name	Type	Data
(Default)	REG_SZ	(value not set)
Dhcpv6Iaid	REG_DWORD	0x0e080027 (235405351)
Dhcpv6State	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters\Interfaces\{964bc7b3-2592-40d3-a4bd-4948d

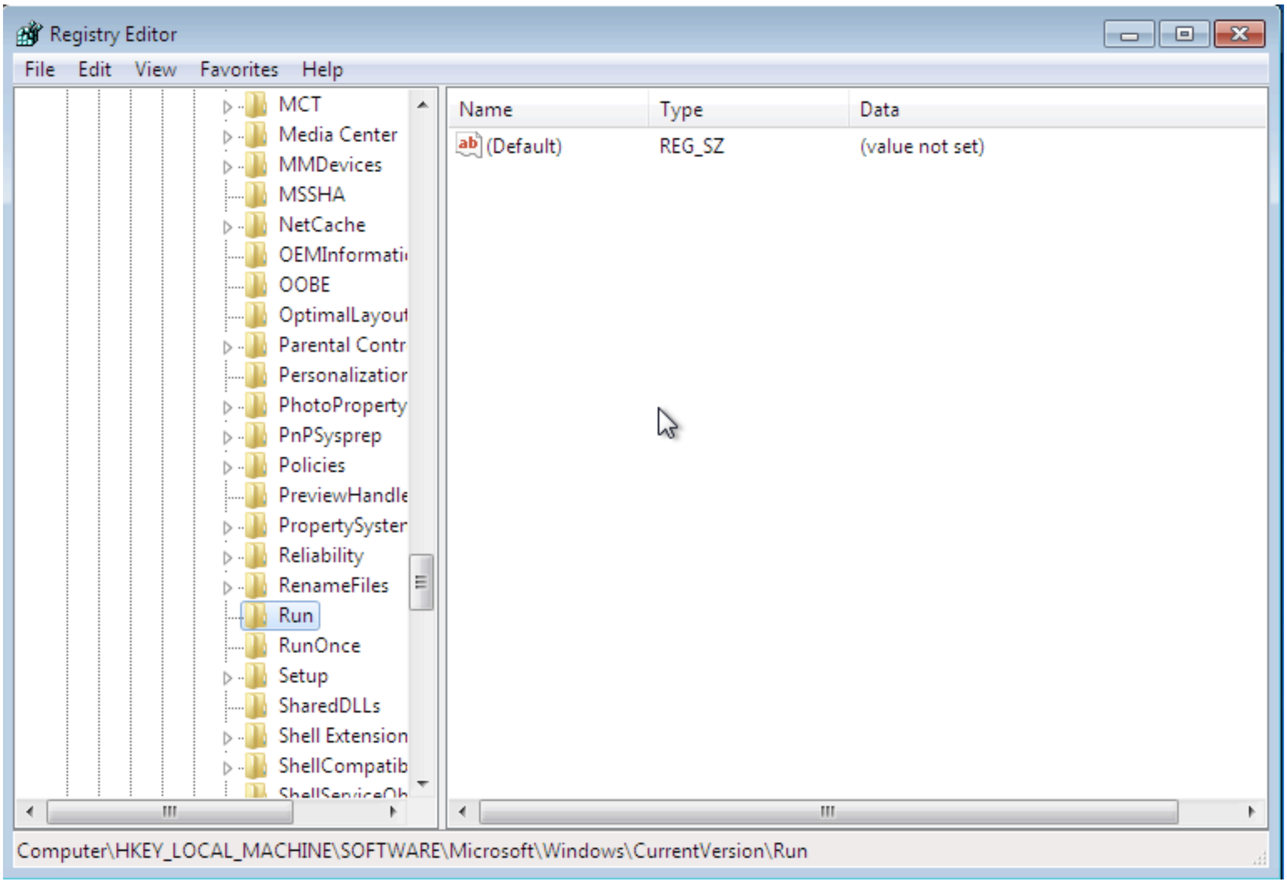
Question 4 :

Find what applications or services set to start when the system starts, in other words — Startup Applications.

As a forensic investigator, we often need to find what applications or services were set to start when the system starts. Malware is often set to start each time the system restarts to keep the attacker connected. This information can be located in the registry in literally tens of locations. Probably the most used location is:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

In our current system, this looks as follows, and it shows the applications or services in my system which are slated to start once the system starts.



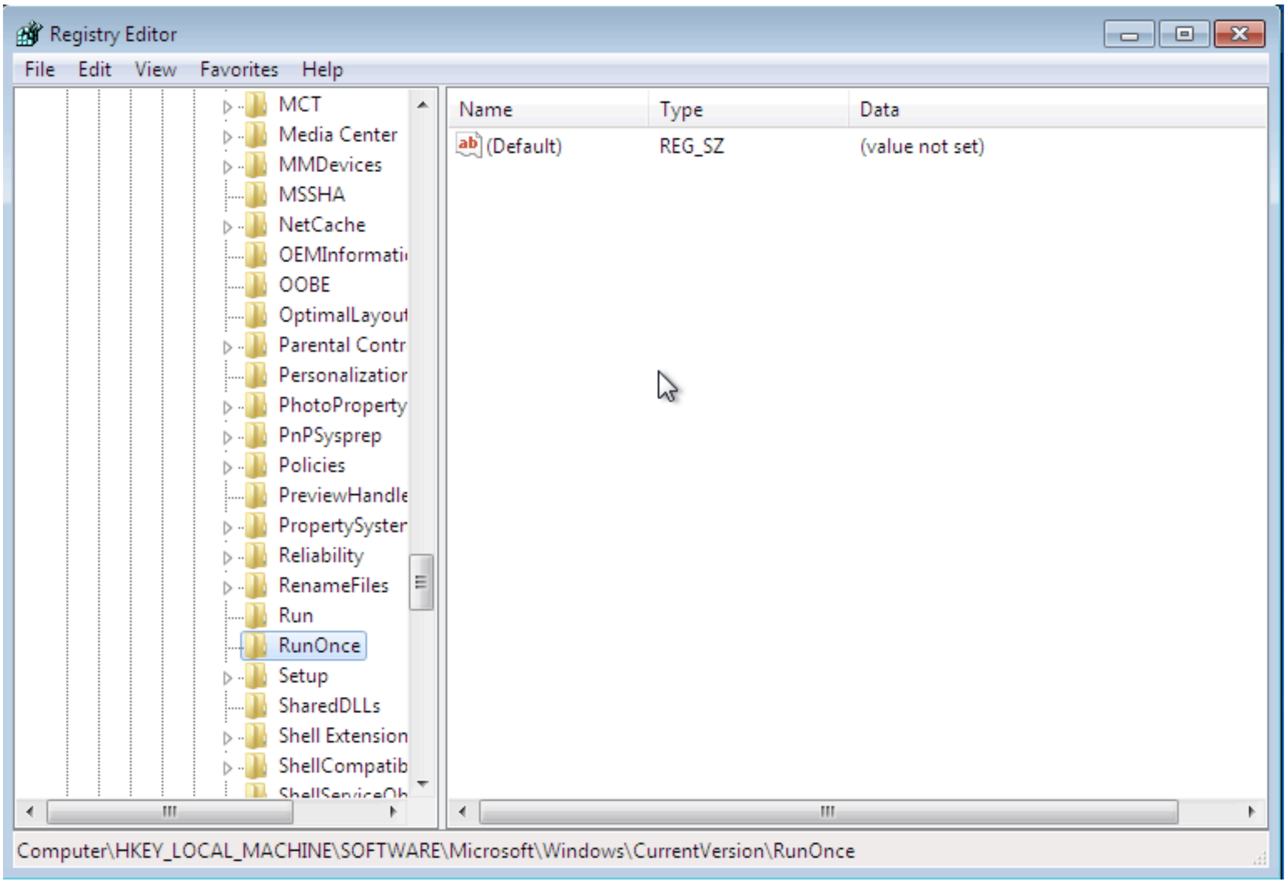
Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Any software/locations designated in these subkeys will start every time the system starts. Rootkits and other malicious software can often be found here and they will start each time the system starts. If the hacker just wanted the software to run once at start up, the subkey may be set here.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

In my current system, it can be set here as shown, and here we can see the single service which has been registered for running just once during the startup process of the system.



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

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Question 5 :

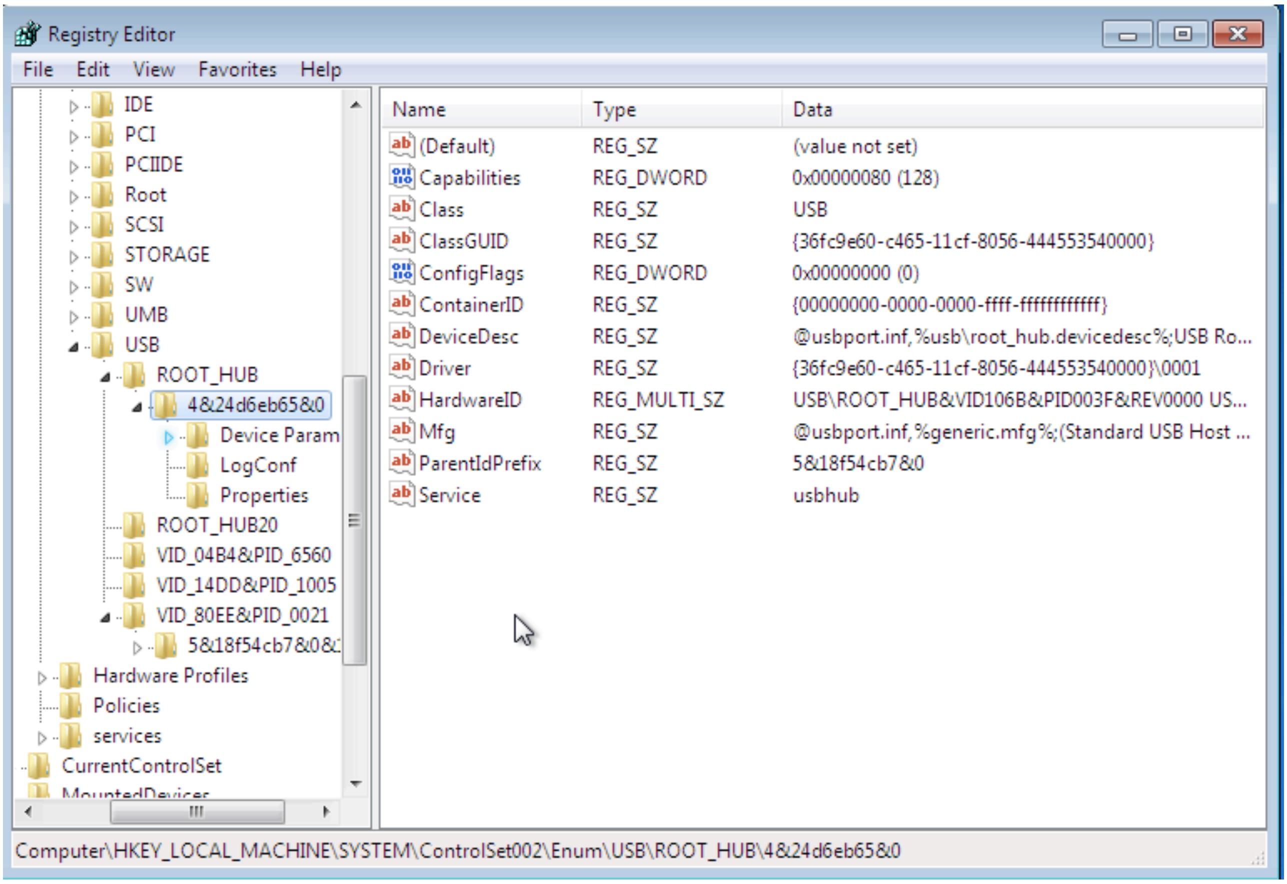
Find a list of all USB devices connected to the system.

Often, the suspect will use a Flash drive or hard drive for their malicious activities and then remove them so as not to leave any evidence. A skilled forensic investigator, though, can still find traces of evidence of those storage devices within the registry, if they know where to look.

To find evidence of USB storage devices, we would want to look at the following key :

HKEY_Local_Machine\System\ControlSet00x\Enum\USBSTOR

In this key, we will find evidence of any USB storage device that has ever been connected to this system. Expand USBSTOR to see a listing of every USB storage device ever connected to this system.



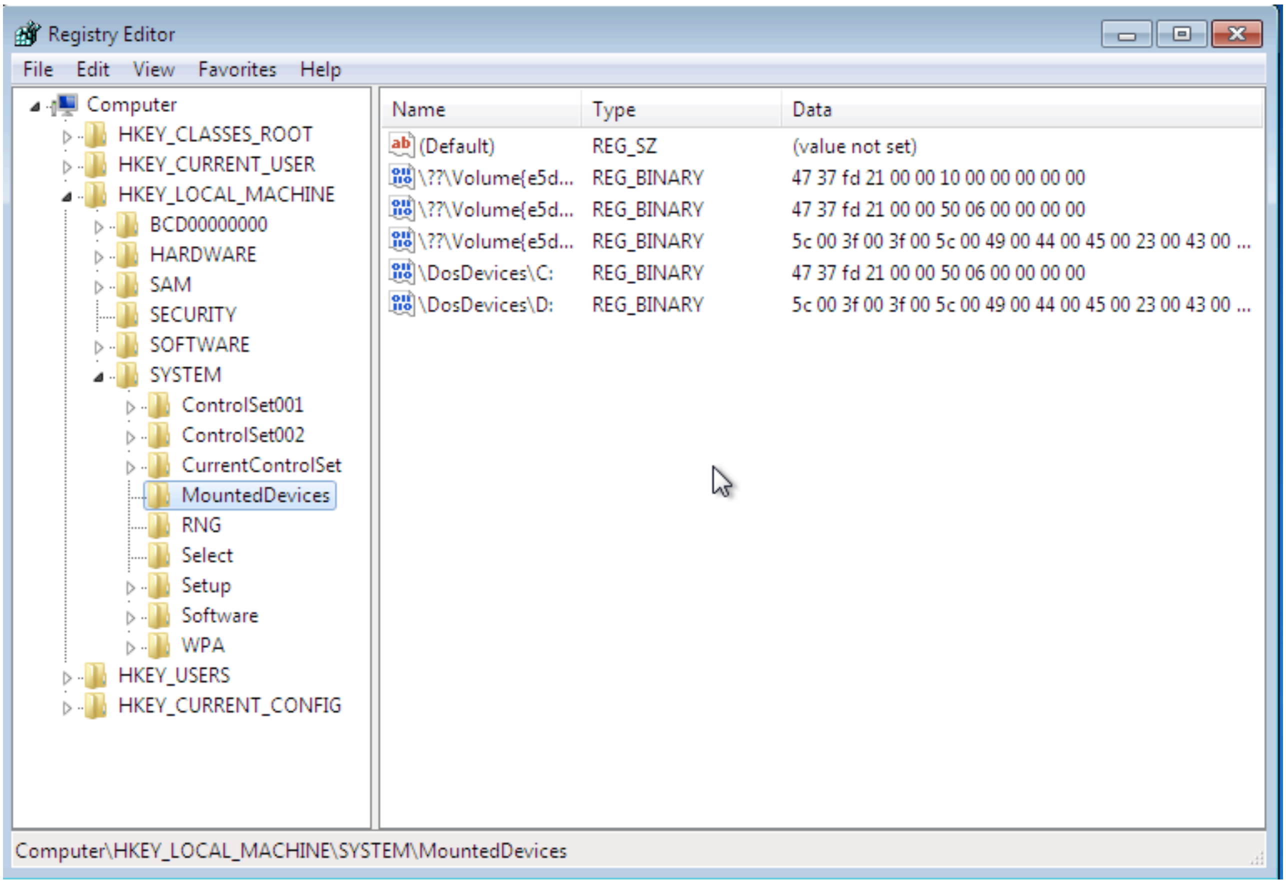
Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000080 (128)
Class	REG_SZ	USB
ClassGUID	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{00000000-0000-0000-ffff-ffffffffffff}
DeviceDesc	REG_SZ	@usbport.inf,%usb\root_hub.devicedesc%;USB Ro...
Driver	REG_SZ	{36fc9e60-c465-11cf-8056-444553540000}\0001
HardwareID	REG_MULTI_SZ	USB\ROOT_HUB&VID106B&PID003F&REV0000 US...
Mfg	REG_SZ	@usbport.inf,%generic.mfg%;(Standard USB Host ...
ParentIdPrefix	REG_SZ	5&18f54cb7&0
Service	REG_SZ	usbhub

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Enum\USB\ROOT_HUB\4&24d6eb65&0

If the suspect used any hardware device that must be mounted to either read or write data (CD-ROM, DVD, hard drive, flash drive, etc.), the registry will record the mounted device. This information is stored at:

HKEY_LOCAL_MACHINE\System\MountedDevices

Let us now use this key in order to get this information on the mounted devices so as to have a practice of gaining more forensic knowledge.



Name	Type	Data
(Default)	REG_SZ	(value not set)
\??\Volume{e5d...	REG_BINARY	47 37 fd 21 00 00 10 00 00 00 00 00
\??\Volume{e5d...	REG_BINARY	47 37 fd 21 00 00 50 06 00 00 00 00
\??\Volume{e5d...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ...
\DosDevices\C:	REG_BINARY	47 37 fd 21 00 00 50 06 00 00 00 00
\DosDevices\D:	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ...

Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

CONCLUSION

In this lab experiments, we have dealt with and seen the various keys associated with the Windows operating system, namely how we can use this internal data tool to explore the various scenarios which is done during a forensic investigation. Though this is not a standard forensic tool, this can thus be a strong backup tool in cases where we do not have any tool ready. Thus the **regedit** tool has been proved to be a tool which provides useful functionalities for ease of forensic analysis.