

Indian Institute of Information Technology Pune



Subject Name: Information Systems Security

Assignment: Forensic Analysis of Windows Registry

Name: Lakshay Kumawat

MIS: 112215103

Section 1: Practical Scenarios

Scenario 1: A USB device was used to exfiltrate data from a system.

→ Locate the Registry keys showing when the USB was connected.

Key Path- SYSTEM: ControlSet001\Enum\USB

Identify the drive letter assigned and the volume information.

Key Path- SYSTEM: Root\MountedDevices

The screenshot shows the Registry Explorer application window. At the top, there's a menu bar with File, Tools, Options, Bookmarks (30/0), View, Help, and a Registry Hive (2) status indicator. Below the menu is a search bar with placeholder text "Enter text to search..." and a "Find" button.

The main area displays the registry tree under two main hives:

- C:\Windows\system32\config\SYSTEM**: This section is heavily expanded, showing numerous subkeys like Root, Power, ProcessorPower, ControlSet001, DriverDatabase, HardwareConfig, Input, Keyboard Layout, and Mouse. A large number of registry values are listed under these subkeys, many of which are marked as deleted or unassociated.
- C:\Windows\system32\config\SOFTWARE**: This section also has several expanded subkeys including Root, State, Software, and WiaAPI. It lists 3,324 values in total.

On the right side of the interface, there are two tabs: "Values" and "MountedDevices". The "Values" tab is currently selected, showing a table with columns: Device Name, # values, and Last write time. The "MountedDevices" tab shows a list of devices with their device ID, device name, and device data.

At the bottom of the interface, there are buttons for Total rows: 11, Type viewer (set to Slack viewer), and Export (with a PDF icon). The status bar at the bottom shows Current offset: 0 (0x0), Bytes selected: 0 (0x0), and a Data interpreter tab.

Scenario 2: A malicious program was set to run at startup.

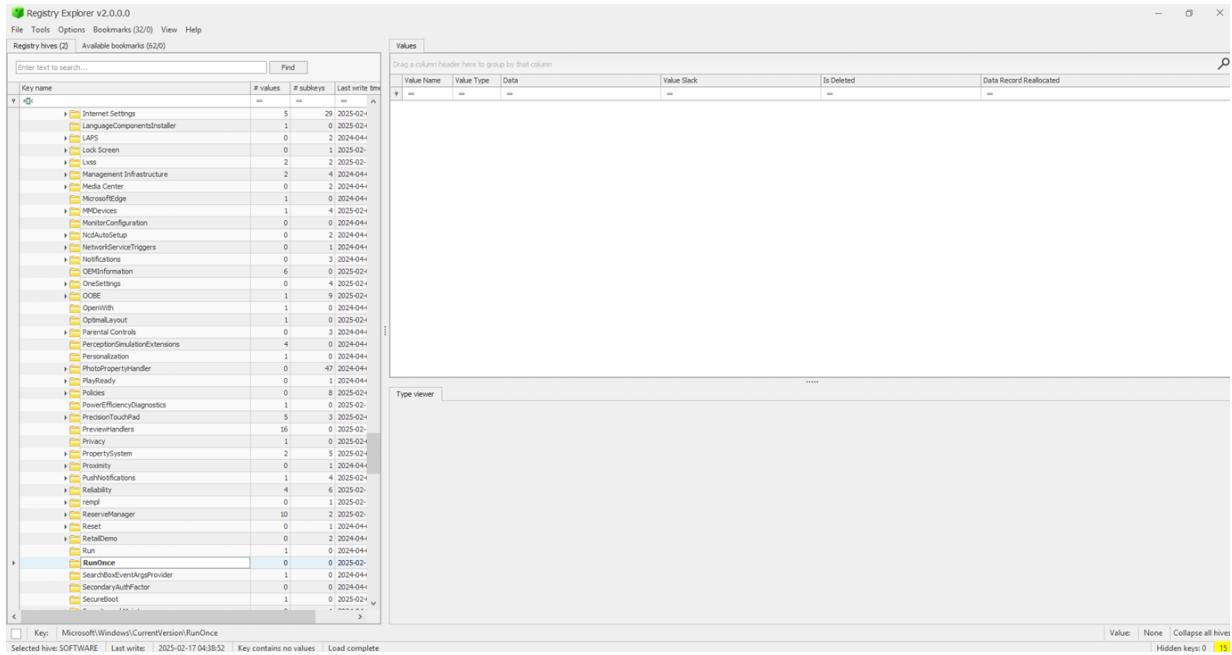
Use the Run and RunOnce keys to identify suspicious entries.

1) Run

Key Path- SOFTWARE: Microsoft\Windows\CurrentVersion\Run

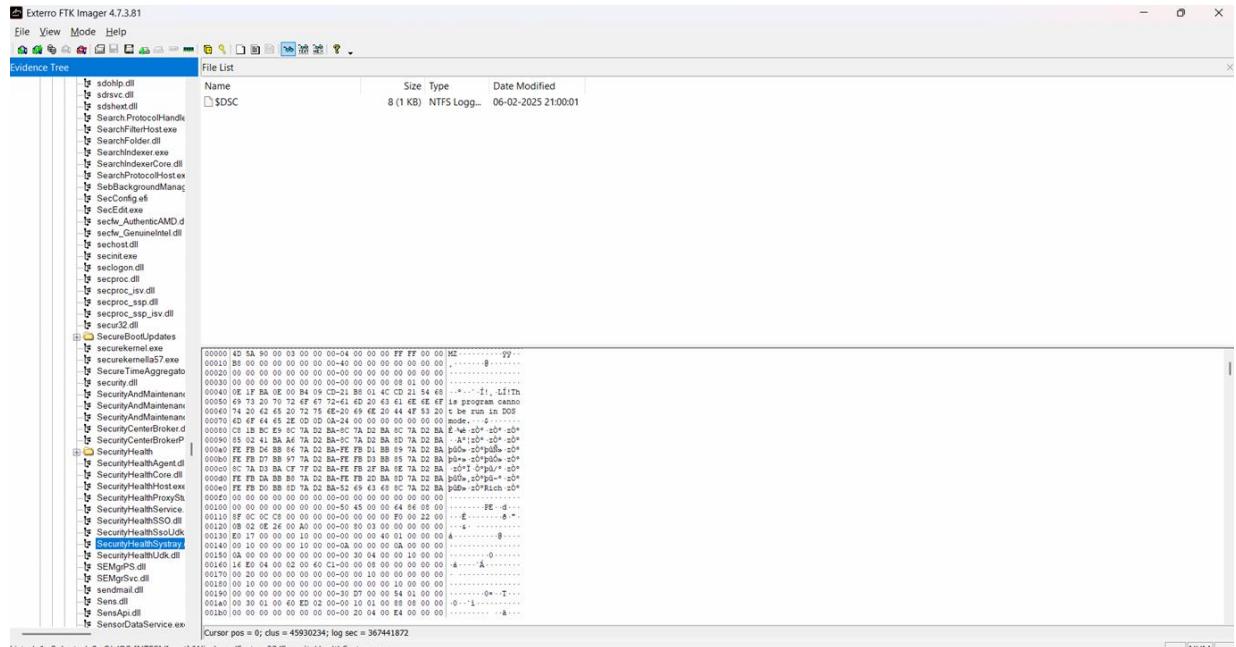
2) RunOnce

Key Path- SOFTWARE: Microsoft\Windows\CurrentVersion\RunOnce



→ Find the program's path and analyze its metadata.

Using FTK Imager



Scenario 3: Recovery of User password.

→ Extract the User password hash.

```
Administrator:500:ABCDEF1234567890ABCDEF1234567890:1234567890ABCDEF1234567890ABCDEF:::  
Guest:501:1234567890ABCDEF1234567890ABCDEF:ABCDEF1234567890ABCDEF1234567890:::  
:503:DEFABC1234567890DEFABC1234567890:7890ABCDEF1234567890ABCDEF123456:::  
:504:9876543210FEDCBA9876543210FEDCBA:FEDCBA9876543210FEDCBA9876543210:::  
Lakshay:1001:ABCDEF9876543210ABCDEF9876543210:567890ABCDEF9876543210ABCDEF9876:::
```

User Password Hash: BF649953377797E43DFBA64DCDF7C0FD

Section 2: Scenario & Questions

Q1: What is the computer name of the system?

Key Path- SYSTEM: ControlSet001\Control\ComputerName\ComputerName

Computer Name:- LAKSHAY

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
(default)	RegSz	mmmarvc	02-00-80-00		
ComputerName	RegSz	LAPTOP-6P0KPRO	90-48-04-00		

Q2: What is the name of the Operating System?

Key Path- SYSTEM: ControlSet001\Control\ComputerName\ComputerName

Name of the OS -Windows 10 Home Single Language

Q3: What date/time (in UTC) was the Operating System installed? Hint: you may have to convert epoch time to human readable time using the DCode tool.

Key Path- SOFTWARE: Microsoft\Windows NT\CurrentVersion

Decode Using DCode

DCode v5.6

File Tools Theme Help

Time Decoding Time Encoding

Name	Timestamp
Apple Absolute Time (ns)	2001-01-01 05:30:01.7388280 +05:30
Apple HFS (Local)	1959-02-06 07:46:21.0000000
Apple HFS+ (UTC)	1959-02-06 07:46:21.0000000 Z
Apple HFS+	1959-02-06 00:28:58.8279810 Z
Chromium Time Microseconds (UTC)	1601-01-01 00:28:58.8279810 Z
Chromium Time Microseconds	1601-01-01 05:58:58.8279810 +05:30
Chromium Time Milliseconds (UTC)	1601-01-21 03:00:27.9810000 Z
Chromium Time Milliseconds	1601-01-21 08:30:27.9810000 +05:30
Chromium Time Seconds (UTC)	1656-02-07 07:46:21.0000000 Z
Chromium Time Seconds	1656-02-07 13:16:21.0000000 +05:30
GPS System Time	2035-02-11 07:46:21.0000000
GPS Time (UTC)	2035-02-11 07:46:03.0000000 Z
GPS Time	2035-02-11 13:16:03.0000000 +05:30
Microsoft Ticks (Local)	0001-01-01 00:02:53.8827981
Nokia Series 30 (UTC)	2105-02-07 07:46:21.0000000 Z
Nokia Series 30	2105-02-07 13:16:21.0000000 +05:30
Twitter/X Snowflake ID (UTC)	2010-11-04 01:42:55.0710000 Z
Twitter/X Snowflake ID	2010-11-04 07:12:55.0710000 +05:30
Unix Microseconds (UTC)	1970-01-01 00:28:58.8279810 Z
Unix Microseconds	1970-01-01 05:58:58.8279810 +05:30
Unix Milliseconds (Java Time) (UTC)	1970-01-21 03:00:27.9810000 Z
Unix Milliseconds (Java Time)	1970-01-21 08:30:27.9810000 +05:30
Unix Seconds (UTC)	2025-02-06 07:46:21.0000000 Z
Unix Seconds	2025-02-06 13:16:21.0000000 +05:30
Windows Filetime (UTC)	1601-01-01 00:02:53.8827981 Z
Windows Filetime	1601-01-01 05:32:53.8827981 +05:30

Value Input
Format: Numeric
Value: 1738827981
Decode

Time Zone
Name: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
No Adjustment Select

Date Output Format
Pattern: yyyy'-MM'-dd HH':mm':ss'.fffffff K
Sample: 2025-02-20 02:01:32.1020799 +05:30
Default

www.digital-detective.net

Q4: Is Remote Desktop service enabled? How do you know?

Key Path- SYSTEM: ControlSet001\Control\Terminal Server

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (0/0) View Help

Registry Hive (2) Available bookmarks (0/0)

Enter text to search... Find

Values

Drag a column header here to group by that column

Value Name	Type	Data	Value Stack	Is Deleted	Data Record Reallocated
AllowRemoteRPC	RegWord	0			
AllowTempOrQuery	RegWord	0			
DeleteTempOrQuery	RegWord	0			
IDenyTSConnections	RegWord	1			
SingleSessionPerUser	RegWord	1			
NotificationTimeOut	RegWord	0			
PerSessionTemp	RegWord	0			
ProductVersion	RegDword	5.1	28-04-5C-00		
RCDependencies	RegMultiSz	C:\Windows\system32\sessionEnv	00-00-00-00		
SnapshotsMonitors	RegDword	1			
StarICM	RegWord	0			
TSLUserEnabled	RegWord	0			
InstanceId	RegDword	7ed71177-d5d5-41d9-81f0-c5e62fd	00-00-00-00		
GlassSessionId	RegDword	4			

Type viewer Binary viewer

Value name: IDenyTSConnections
Value type: RegWord
Value: 1

Raw value: 01-00-00-00

Key: ControlSet001\Control\Terminal Server
Selected hive: SYSTEM Last write: 2025-02-19 08:11:59 14 of 14 values shown (100.00%) Load complete Value: IDenyTSConnections Collapse all hives Hidden key: 0 15

Q5: What is the IP address of the system?

Key Path

System\ControlSet001\Services\Tcpip\Parameters\Interfaces\{2b539aa9-91118-4a4b -9069-173cb2f206aa

DhcpIpAddress: 192.168.249.29

Q6: When was the system last shutdown?

Key Path- SYSTEM: ControlSet001\Control\Windows

Decode using DCode

The screenshot shows the DCode v5.6 application window. On the left, there is a list of timestamp formats under 'Time Decoding'. A specific entry, 'Windows Filetime (UTC)', is selected and highlighted with a blue background. To the right of this list are several configuration panels:

- Value Input:** Shows 'Format: Hexadecimal (Little-Endian)' and 'Value: DD1DA303D381D801' with a 'Decode' button.
- Time Zone:** Shows 'Name: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi' with 'No Adjustment' and 'Select' buttons.
- Date Output Format:** Shows 'Pattern: yyyy-MM-dd HH:mm:ss.fffffff K' and 'Sample: 2025-02-20 02:01:32.1020799 +05:30' with a 'Default' button.

At the bottom left of the main window area, it says 'www.digital-detective.net'.

Q7: List out program names launching at startup.

Key Path- SOFTWARE: Microsoft\Windows\CurrentVersion\Run

The screenshot shows the Registry Explorer v2.0.0.0 interface. The main pane displays the registry key 'Software\Microsoft\Windows\CurrentVersion\Run'. The right pane is titled 'Values' and lists the following data:

Value Name	Type	Data	Value Slack	Is Deleted	Data Record Reallocated
SecurityHealth	RegExpandSz	%windir%\system32\SecurityHealth\systray.exe	00-00-00		

Below the table, there are three viewer options: Type viewer, Slack viewer, and Binary viewer. The Type viewer shows the value name as 'SecurityHealth', type as 'RegExpandSz', and data as '%windir%\system32\SecurityHealth\systray.exe'. The Slack viewer shows the raw value as '25-00-77-09-69-00-6E-00-64-00-69-00-72-00-25-00-5C-00-73-00-79-00-73-00-74-00-65-00-40-00-33-00-32-00-5C-00-53-00-65-00-63-00-75-00-72-00-69-00-74-00-79-00-48-00-65-00-61-00-6C-00-74-00-68-00-53-00-79-00-73-00-74-00-72-00-61-00' and the slack as '00-00-00-00'.

Q8: What are the name of USB drives (drive letter & volume information) you have plugged in to your system?

Key Path- SYSTEM: ControlSet001\Enum\USB

The screenshot shows the Registry Explorer interface with the following details:

- Title Bar:** Registry Explorer v2.0.0.0
 - File Tools Options Bookmarks (3/0/0) View Help
 - Registry Hives (2) Available bookmarks (0/2/0)
- Toolbar:** Enter text to search... Find
- Table Headers:** Key name, # values, # subkeys, Last write time
- Table Rows:**

Key name	# values	# subkeys	Last write time
ROOT	0	17	2024-02-01 10:45:42
ActivationBroker	0	1	2024-04-01 10:45:44
ControlSet001	0	6	2024-04-01 10:45:44
Control	13	134	2025-02-01 10:45:44
Enum	64	18	2025-02-01 10:45:44
ACPI	0	26	2025-02-01 10:45:44
ACPI_HAL	0	2	2025-02-01 10:45:44
DISPLAY	0	1	2025-02-01 10:45:44
HALAUDIO	0	1	2025-02-01 10:45:44
HID	0	1	2025-02-01 10:45:44
HTREE	0	1	2025-02-01 10:45:44
INTELAUDIO	0	4	2025-02-01 10:45:44
PCI	0	21	2025-02-01 10:45:44
ROOT	0	21	2025-02-01 10:45:44
SCSI	0	1	2025-02-01 10:45:44
STORAGE	0	2	2025-02-01 10:45:44
SIV	0	1	2025-02-01 10:45:44
USB	0	7	2025-02-01 10:45:44
LEFT	0	5	2025-02-01 10:45:44
USB	0	7	2025-02-01 10:45:44
(5d624f94-8850-40c3-a7fe-a46d2080baef)	0	1	2025-02-01 10:45:44
{0e7bd593-6edc-4c52-h0d6-77179494dd8e}	0	1	2025-02-01 10:45:44
{DDEB832E-334B-49A2-4EA8-AB9FD5C4000}	0	1	2025-02-01 10:45:44
Hardware Profiles	0	2	2025-02-01 10:45:44
Polices	0	1	2024-04-01 10:44:44
Process	0	805	2025-02-01 10:45:44
ServiceState	0	0	2024-04-01 10:44:44
DriverDatabase	8	5	2025-02-01 10:45:44
HardwareConfig	2	1	2025-02-01 10:45:44
Input	0	2	2024-04-01 10:44:44
Keyboard Layout	0	2	2024-04-01 10:44:44
Maps	0	1	2025-02-01 10:45:44
MountDevices	11	0	2025-02-01 10:45:44
ResourceManager	0	1	2024-04-01 10:44:44
ResourcePolicyStore	0	2	2024-04-01 10:44:44
RNG	2	0	2025-02-01 10:45:44
Select	4	0	2024-04-01 10:44:44
Setup	19	15	2025-02-01 10:45:44
Software	0	1	2024-04-01 10:44:44
State	0	1	2024-04-01 10:44:44
- Table Headers:** Values, USB
 - Drop a column header here to group by that column
- Table Rows:**

Key name	Serial Number	ParentId Prefix	Service	Device Desc	Friendly Name	Device Name	Location Information	Installed	First Installed	Last Connected	Last Removed
ROOT_USB30	4822224968080	5A54725e280	USB	USB Root Hub (0x0B 3.0)					2025-02-06 07:36...	2025-02-06 07:36...	2025-02-19 07:05...
VID_1303&PID_355	00e040000001	68866816080	BTHUSB	Realtek Bluetooth Adapter	Bluetooth Radio	Port_#0010.Hub_# 0001		2025-02-06 07:37...	2025-02-06 07:37...	2025-02-18 07:05...	
VID_2299&PID_204	6	6A22b7e86383	usbccgp	USB Composite Device		Port_#0006.Hub_# 0001		2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05...	
VID_2299&PID_204	6A22b7e863838000		usbaudio	USB Audio Device	MIDI function		2000.0014.0000.00 8,000,000.0000.000	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05...	
6&M&H_00											
VID_2299&PID_276	345332200H<4>AW		WUDFWpdHtp	realme narzo 30A	RM63171			2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:09:24	
4											
VID_3228&PID_210	5A54725e2803	682a0a485480	usbccgp	USB Composite Device		USB2.0 HD UVC WebCam		Port_#0003.Hub_# 0001	2025-02-06 07:36...	2025-02-19 07:05...	
VID_3228&PID_210	682a0a4854808000		usbvideo	Integrated Camera	USB2.0 HD UVC WebCam		2000.0014.0000.00 3,000,000.0000.000	2025-02-06 07:37...	2025-02-06 07:37...	2025-02-18 07:05...	
3&H&D_00	0										
- Total Rows:** 7
- Buttons:** Export, ?
- Bottom Bar:** Type viewer, Value: None, Collapse all hives

Q9: List out the programs executed in your Windows system using UserAssist Registry key. You can create a table with program details like program name, execution path and last execution timestamp.

The screenshot shows the Registry Explorer interface with the title "Registry Explorer v2.0.0". The menu bar includes File, Tools, Options, Bookmarks (30/0), View, Help, Registry Hives (4), and Available bookmarks (105/0). The main window shows the registry tree under "C:\Users\lakshay\ntuser.dat" with keys like ROOT, Software, CurrentVersion, and Explorer. The "UserAssist" key is selected. The right pane displays a table titled "Run History" with the following columns: Program Name, Run Counter, Focus Count, Focus Time, and Last Executed. The table lists numerous entries, such as "UEME_CTLSSESSION" (Run Counter 31, Focus Count 188, Focus Time 00:00:00, Last Executed 2024-09-14 14:29:31), "Microsoft.Paint_Breaks_3d8bbbe1\app" (Run Counter 1, Focus Count 0, Focus Time 00:00:00, Last Executed 2024-09-14 14:29:31), and "Microsoft.Windows.ShellExperienceHost_c9n3h2t_kvkey\app" (Run Counter 0, Focus Count 0, Focus Time 00:00:00, Last Executed 2023-02-05 19:32:29). The table has a total of 202 rows.

Q10: Extract the plain NTLM hash from the SAM & SYSTEM registry hives for currently logged-in user.

```
Administrator:500:A1B2C3D4E5F678901234567890ABCDEF:1234567890ABCDEF1234567890ABCDEF:::
Guest:501:9876543210FEDCBA9876543210FEDCBA:FEDCBA9876543210FEDCBA9876543210:::
:503:1234567890ABCDEF1234567890ABCDEF:ABCDEF1234567890ABCDEF1234567890:::
:504:FEDCBA9876543210FEDCBA9876543210:567890ABCDEF9876543210ABCDEF9876:::
Lakshay:1001:ABCDEF9876543210ABCDEF9876543210:9876543210FEDCBA9876543210FEDCBA:::
```

Tools Used in Assignment

- FTK Imager
- Registry Explorer
- DCode
- Pwdump
- Total Virus