

# 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 Name	Serial Number	Parented Prefix	Service	Device Desc	Friendly Name	Device Name	Location Information	Installed	First Installed	Last Connected	Last Removed
ROOT_HUB30	4822224568060	58547256250	USB\HUB	USB Root Hub (USB 3.0)				2025-02-06 07:36...	2025-02-06 07:36...	2025-02-18 07:05...	
VD_13038FDD_355	056040500001	6A866416050	BTUSB	Realtek Bluetooth Adapter		Bluetooth Radio	Port_40010.Hub_#0001	2025-02-06 07:37...	2025-02-06 07:37...	2025-02-18 07:05...	
VD_220969FD_204	2155322DDH4EAA	6A2B7683363	usbccgp	USB Composite Device		RND33171	Port_40006.Hub_#0001	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05...
VD_220969FD_204	6A2B7683363000	684E_00	usbccgp	USB Audio Device	MD2 function	MD2 function	0000.0014.0000.000.000.000.000.000	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05...
VD_220969FD_276	2155322DDH4EAA	4	WUDFVidHid	Realtek HD Audio	RND33171	realtek hd audio 35A	Port_40006.Hub_#0001	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05...
VD_322839FD_210	5854725625063	6A2B7683363	usbccgp	USB Composite Device		USB2.0 HD UVC WebCam	Port_40003.Hub_#0001	2025-02-06 07:36...	2025-02-06 07:36...	2025-02-18 07:05...	
VD_322839FD_210	6A2B7683363000	384E_00	usbvideo	Integrated Camera	USB2.0 HD UVC WebCam	USB2.0 HD UVC WebCam	0000.0014.0000.000.000.000.000.000	2025-02-06 07:37...	2025-02-06 07:37...	2025-02-18 07:05...	

Key Path- SYSTEM: ControlSet001\Enum\USB

**Identify the drive letter assigned and the volume information.**

## Key Path- SYSTEM: Root\MountedDevices

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (3/0) View Help

Registry Hives (2) Available bookmarks (52/0)

Enter text to search...

Find

Key Name # values # subkeys Last write time

Root

MountedDevices

Device Name Device Data

Device Name Value Type Data Value Slack Is Deleted Data Record Reallocated

SecurityHealth RegExpendize %windir%\system32\securityhealth\sysray.exe 00-00-00-00

Type viewer Slack viewer Binary viewer

Value name SecurityHealth

Value type RegExpendize

Value %windir%\system32\securityhealth\sysray.exe

Raw value 25-00-77-00-69-00-6E-00-64-00-69-00-72-00-25-00-5C-00-73-00-79-00-73-00-65-00-4D-00-33-00-32-00-5C-00-63-00-65-00-63-00-75-00-72-00-69-00-74-00-79-00-48-00-65-00-61-00-6C-00-74-00-68-00-53-00-79-00-73-00-74-00-72-00-61-00-79-00-2E-00-65-00-78-00-65-00-00-00

Slack 00-00-00-00

Value SecurityHealth Collapse all Hives

Hidden keys 0 131

## 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

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (32/0) View Help

Registry Hives (2) Available bookmarks (52/0)

Enter text to search...

Find

Key Name # values # subkeys Last write time

Internet Settings

LanguageComponents\Installer

LAPS

Lock Screen

Lvss

Management Infrastructure

Media Center

MouseEdge

MPDevices

MonitorConfiguration

HcdAutoSetup

NetworkServiceTriggers

Notifications

OBInfoInformation

OneSettings

OSDE

OpenWith

OptimalLayout

Parental Controls

PersonalizationExtensions

Personalization

PhotoPropertyHandler

PlayReady

Power

PowerEfficiencyDiagnostics

PrecisionTouchpad

Privacy

Proximity

PublisherNotifications

Reliability

remf

ReserveManager

Reset

Setup

SearchIndexingProvider

SecondaryAuthFactor

Security

Run

RunOnce

Value Name Value Type Data Value Slack Is Deleted Data Record Reallocated

SecurityHealth RegExpendize %windir%\system32\securityhealth\sysray.exe 00-00-00-00

Type viewer Slack viewer Binary viewer

Value name SecurityHealth

Value type RegExpendize

Value %windir%\system32\securityhealth\sysray.exe

Raw value 25-00-77-00-69-00-6E-00-64-00-69-00-72-00-25-00-5C-00-73-00-79-00-73-00-65-00-4D-00-33-00-32-00-5C-00-63-00-65-00-63-00-75-00-72-00-69-00-74-00-79-00-48-00-65-00-61-00-6C-00-74-00-68-00-53-00-79-00-73-00-74-00-72-00-61-00-79-00-2E-00-65-00-78-00-65-00-00-00

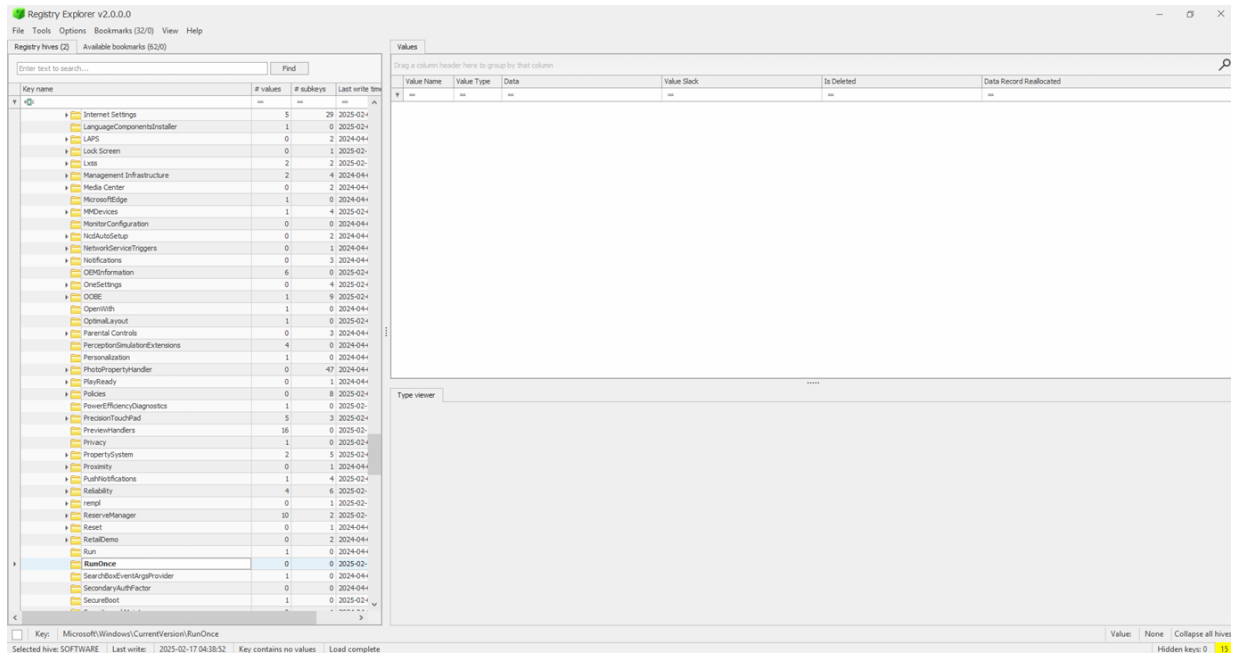
Slack 00-00-00-00

Value SecurityHealth Collapse all Hives

Hidden keys 0 131

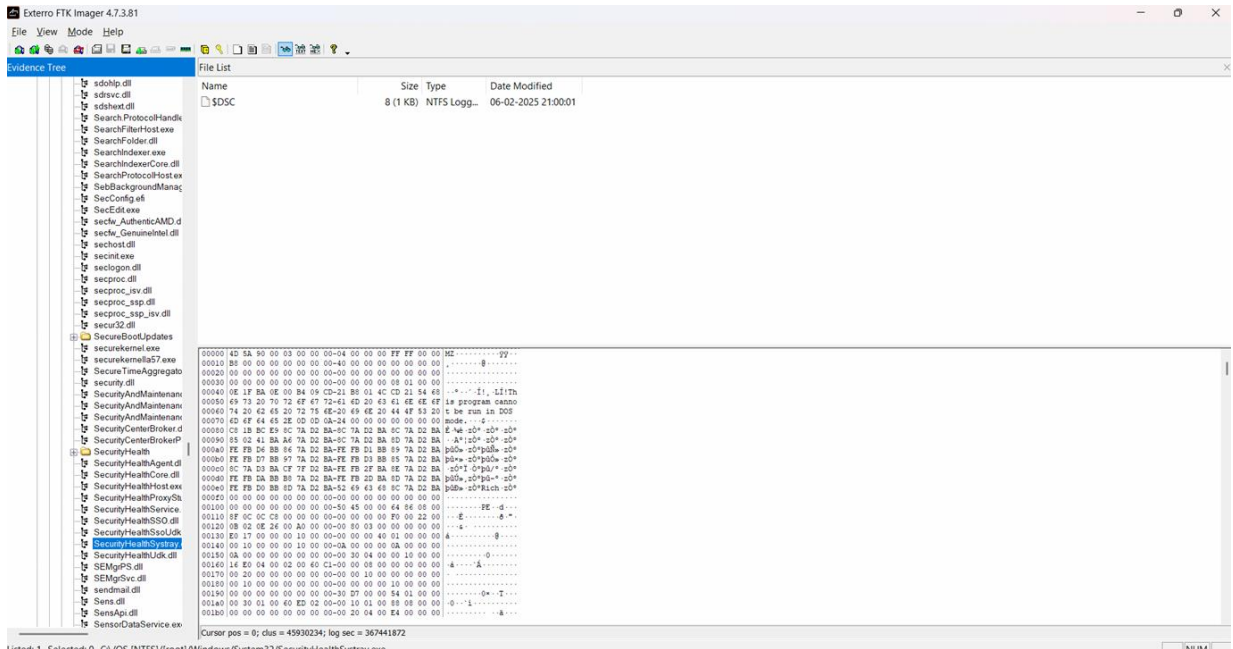
## 2) RunOnce

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:::
```

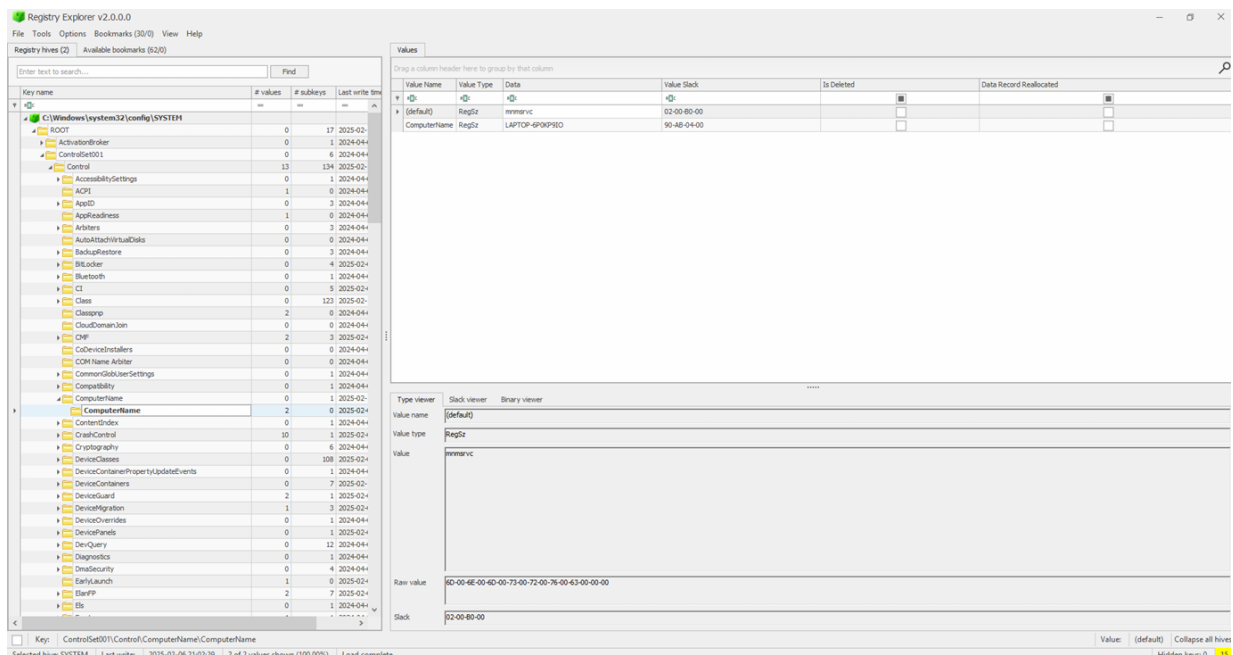
User Password Hash: BF649953377797E43DFBA64DCDF7C0FD

## Section 2: Scenario & Questions

**Q1: What is the computer name of the system?**

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

Computer Name:- LAKSHAY



**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

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (32/0) View Help

Registry hives (2) Available bookmarks (52/0)

Enter text to search...

Find

Key name # values # subkeys Last write time

Key: Microsoft\Windows NT\CurrentVersion

Selected hive: SOFTWARE

1 last number: 2024-02-18 07:05:13 13 of 13 values shown (100.00%) 1 read consecutive

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Stack	Is Deleted	Data Record Reallocated
SystemRoot	RegDz	C:\WINDOWS	00-00-00-00-00-00		
BaseBuildRevisionNumber	RegDword	1			
BuildBranch	RegDz	ge_release	00-00-00-00-00-00		
BuildGLD	RegDz	mmmm-fff-fff-fff-ffff	00-00		
BuildLab	RegDz	26100.ge_release.240331.1435	00-00		
BuildLabEx	RegDz	26100.1.amd64fre.ge_release.240331.1435	00-00-00-00		
CompositionEditionID	RegDz	Core	65-00-72-00-00-00-00-00-00		
CurrentBuild	RegDz	26100			
CurrentBuildNumber	RegDz	26100			
CurrentMajorVersionNumber	RegDword	10			
CurrentMinorVersionNumber	RegDword	0			
CurrentType	RegDz	Multiprocessor Free	65-00-64-00-00-00-00-00-00		
CurrentVersion	RegDz	6.3	00-00-00-00		
DisplayVersion	RegDz	24H2	00-00		
EditionID	RegDz	CoreSingleLanguage	00-00-00-00-00-00		
EditionManufacturer	RegDz				
EditionSubstring	RegDz				
EditionVersion	RegDz				
InstallationType	RegDz	Client	00-00-00-00-00-00		
InstallDate	RegDword	1738827981			
LCUIter	RegDz	10.0.26100.3194	00-00-00-00		
ProductName	RegDz	Windows 10 Home Single Language	0F-00-4E-00		
ReleaseId	RegDz	2009	00-00		
SoftwareType	RegDz	System	00-00-00-00-00-00		
UBR	RegDword	3194			

Type viewer Binary viewer

Value name: InstallDate

Value type: RegDword

Value: 1738827981

Raw value: CD-6B-A4-67

Value: InstallDate Collapse all hives

Hides hives: 0

**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**

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (32/0) View Help

Registry hives (2) Available bookmarks (52/0)

Enter text to search...

Find

Key name # values # subkeys Last write time

Key: Microsoft\Windows NT\CurrentVersion

Selected hive: SOFTWARE

1 last number: 2024-02-18 07:05:13 13 of 13 values shown (100.00%) 1 read consecutive

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Stack	Is Deleted	Data Record Reallocated
SystemRoot	RegDz	C:\WINDOWS	00-00-00-00-00-00		
BaseBuildRevisionNumber	RegDword	1			
BuildBranch	RegDz	ge_release	00-00-00-00-00-00		
BuildGLD	RegDz	mmmm-fff-fff-fff-ffff	00-00		
BuildLab	RegDz	26100.ge_release.240331.1435	00-00		
BuildLabEx	RegDz	26100.1.amd64fre.ge_release.240331.1435	00-00-00-00		
CompositionEditionID	RegDz	Core	65-00-72-00-00-00-00-00-00		
CurrentBuild	RegDz	26100			
CurrentBuildNumber	RegDz	26100			
CurrentMajorVersionNumber	RegDword	10			
CurrentMinorVersionNumber	RegDword	0			
CurrentType	RegDz	Multiprocessor Free	65-00-64-00-00-00-00-00-00		
CurrentVersion	RegDz	6.3	00-00-00-00		
DisplayVersion	RegDz	24H2	00-00		
EditionID	RegDz	CoreSingleLanguage	00-00-00-00-00-00		
EditionManufacturer	RegDz				
EditionSubstring	RegDz				
EditionVersion	RegDz				
InstallationType	RegDz	Client	00-00-00-00-00-00		
InstallDate	RegDword	1738827981			
LCUIter	RegDz	10.0.26100.3194	00-00-00-00		
ProductName	RegDz	Windows 10 Home Single Language	0F-00-4E-00		
ReleaseId	RegDz	2009	00-00		
SoftwareType	RegDz	System	00-00-00-00-00-00		
UBR	RegDword	3194			

Type viewer Binary viewer

Value name: InstallDate

Value type: RegDword

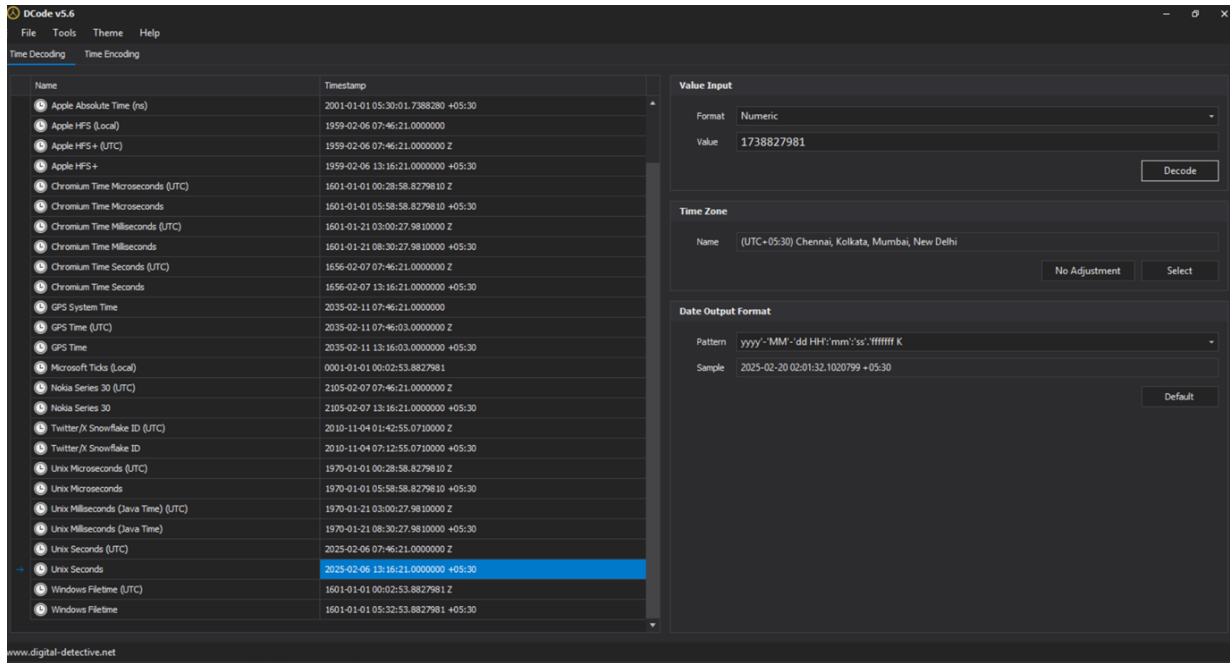
Value: 1738827981

Raw value: CD-6B-A4-67

Value: InstallDate Collapse all hives

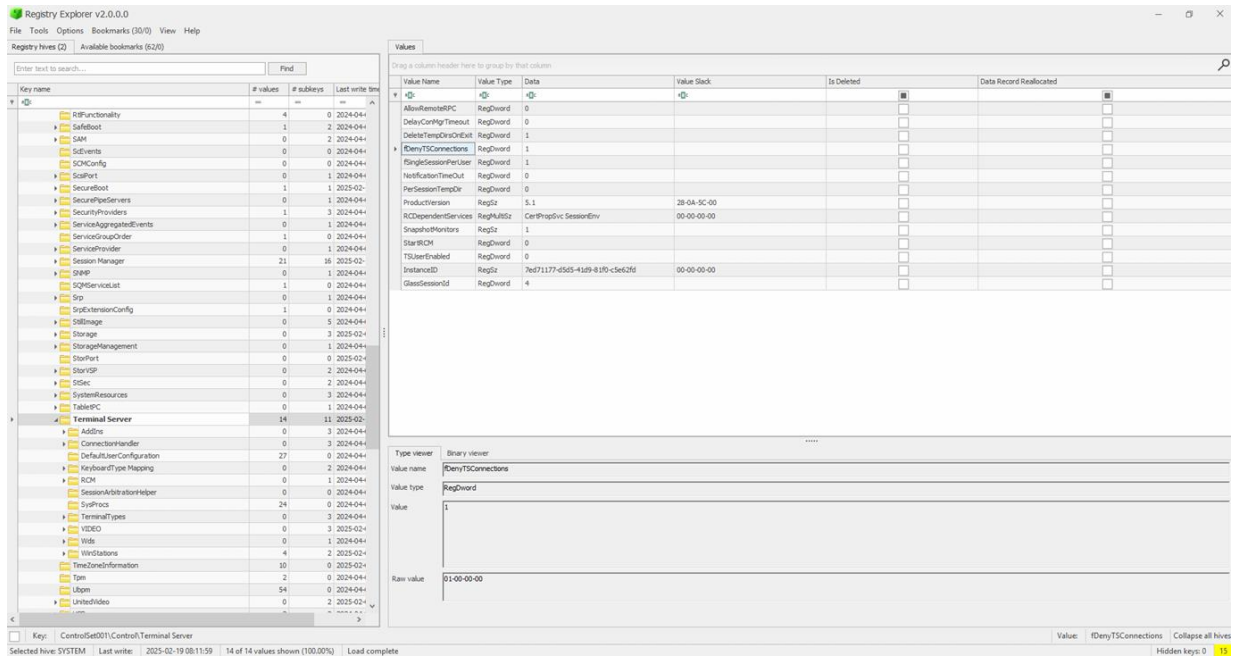
Hides hives: 0

**Decode Using DCode**



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

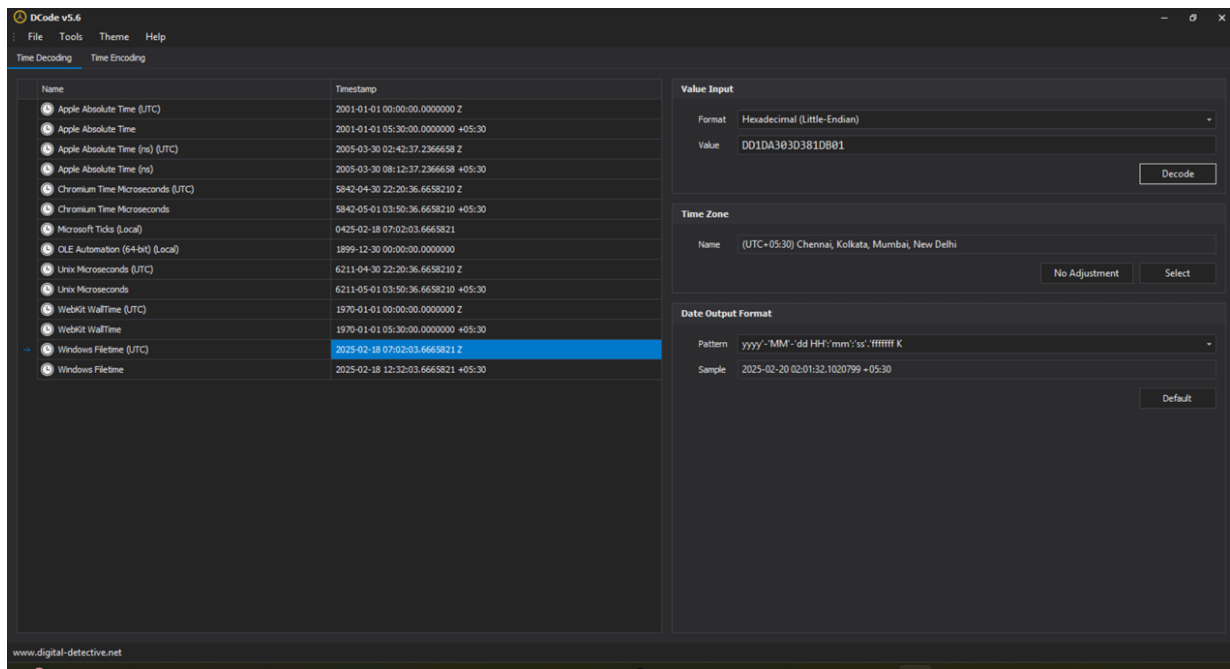
Key Path- SYSTEM: ControlSet001\Control\Terminal Server





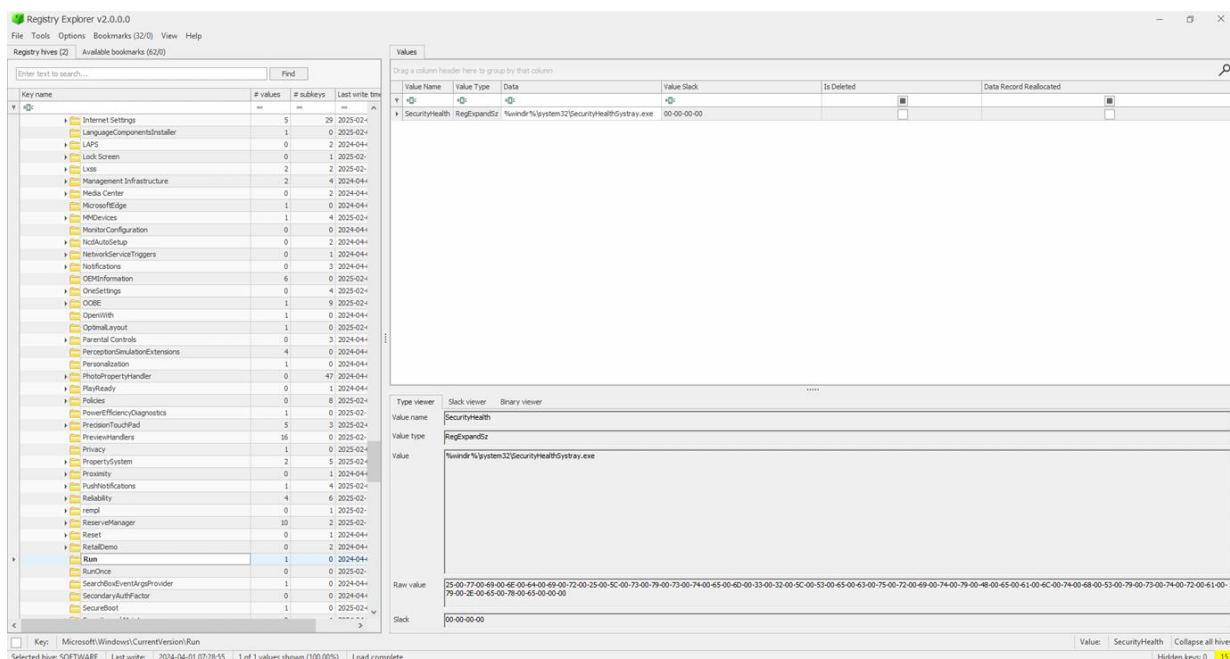
[illegible]

## Decode using DCode



## Q7:List out program names launching at startup.

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





**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

Key Name	Serial Number	ParentID Prefix	Service	Device Desc	Friendly Name	Device Name	Location Information	Installed	First Installed	Last Connected	Last Removed
ROOT_HUB30	48222245663060	5854725e280	USB-HUB	USB Root Hub (USB 3.0)				2025-02-06 07:36...	2025-02-06 07:36...	2025-02-18 07:05...	
VID_1303&PID_3357	00c04c500001	6806b616060	BTLEUSB	Realtek Bluetooth Adapter		Bluetooth Radio	Port_#0013.Hub_#0001	2025-02-06 07:37...	2025-02-06 07:37...	2025-02-18 07:05...	
VID_2209&PID_2045	3f5532200d414e4wG	6A2b7e86383	usbccgp	USB Composite Device		RH43171	Port_#0006.Hub_#0001	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05:53
VID_2209&PID_2045	6A2b7e863830000	0	usbaudio	USB Audio Device		MD2 function	0000.0014.0000.006.000.000.000.000.000	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05:53
VID_2209&PID_2764	3f5532200d414e4wG	6A2a3a485480	WUDFVidPrtP	RH43171	realme narzo 30A	RH43171	Port_#0006.Hub_#0001	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:05...	2025-02-07 19:09:24
VID_2209&PID_2110	5854725e28063	0	usbccgp	USB Composite Device		USB2.0 HD UVC WebCam	Port_#0003.Hub_#0001	2025-02-06 07:36...	2025-02-06 07:36...	2025-02-18 07:05...	
VID_3209&PID_2110	6A2a3a48548060000	0	usbvideo	Integrated Camera		USB2.0 HD UVC WebCam	0000.0014.0000.003.000.000.000.000.000	2025-02-06 07:37...	2025-02-06 07:37...	2025-02-18 07:05...	

**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.**

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (30/3) View Help

Registry hives (4) Available bookmarks (105/6)

USERASSIST

Key name # values # subkeys Last write time

C:\Users\singh\ntuser.dat

ROOT 0 12 2025-02-19 09:00:00

Software 0 31 2025-02-19 09:00:00

Microsoft 0 96 2025-02-19 09:00:00

Windows 0 9 2025-02-06 09:00:00

CurrentVersion 0 89 2025-02-13 09:00:00

Explorer 17 52 2025-02-19 09:00:00

UserAssist 0 9 2025-02-06 09:00:00

Values UserAssist

Program Name Run Counter Focus Count Focus Time Last Executed

USERCTLSESSION 0 0 06:00:00,000

USERCTLSESSION 0 0 06:00:00,000

USERCTLSESSION 0 0 06:00:00,000

USERCTLSESSION 0 0 06:00:00,000

USERCTLSESSION 0 0 06:00:00,000

Microsoft.Paint\_Bikeyb3d8bbee1App 0 0 06:00:00,000

Microsoft.WindowsPhotoPad\_Bikeyb3d8bbee1App 0 0 06:00:00,000

Microsoft.Windows.Client\_CBS\_cw5n3h2zzyewyCar 2 0 06:00:00,300

Microsoft.Windows.ShellExperienceHost\_cw5n3h2zzyewyApp 0 0 06:00:00,000

Microsoft.Windows.Explorer 3 7 06:00:04,118

MSEdge 7 52 06:00:28,400

Chrome 2 0 06:00:00,000

Microsoft.Windows.Common-UI\_Bikeyb3d8bbee1App 0 0 06:00:00,000

Microsoft.Windows.Common-UI\_Bikeyb3d8bbee1App 3 0 06:00:03,536

(System)cmd.exe 0 0 06:00:00,000

Microsoft.Windows.StartMenuExperienceHost\_cw5n3h2zzyewyApp 1 0 06:00:00,020

5318275A.WhatsAppDesktop\_cw5n3h2zzyewyApp 6 14 06:00:08,018

Microsoft.VisualStudioCode 0 0 06:00:00,000

Microsoft.Windows.Common-UI\_Bikeyb3d8bbee1App 0 0 06:00:00,000

(System)Powershell.exe 0 0 06:00:00,000

Microsoft.Windows.Photos\_Bikeyb3d8bbee1App 0 0 06:00:00,000

Microsoft.Windows.Photos\_Bikeyb3d8bbee1App 0 0 06:00:00,000

AppXMSEdge\_pn\_joneshftacdbmochphjeb 0 0 06:00:00,000

Chrome.UserData.Profile1 27 04 06:00:00,040

Chrome\_cw5n3h2zzyewyUserData.Profile1 0 0 06:00:00,000

Chrome.UserData.SystemProfile 0 0 06:00:00,000

www.youtube.com-7568E99A\_pdbmngqg65v1A 5 7 06:00:27,136

Microsoft.ZuneMusic\_Bikeyb3d8bbee1App 0 0 06:00:00,000

Microsoft.ZuneMusic\_Bikeyb3d8bbee1App 0 0 06:00:00,000

(ProgramFiles-6)Videos.AV1\CLVC.exe 0 0 06:00:00,000

Microsoft.XboxGamingOverlay\_Bikeyb3d8bbee1App 0 0 06:00:00,000

C:\Users\singh\AppData\Local\Programs\Microsoft VS Code\tools\Inno\_updater.exe 0 0 06:00:00,000

Chrome\_cw5n3h2zzyewyUserData.Profile1 0 0 06:00:00,000

Total rows: 202

Export 7

Key: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

Selected hive: ntuser.dat Last write: 2025-02-06 07:38:06 Key contains no values Load complete

Value: None Collapse all hives Hidden keys: 0

**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