

Assignment #1: Forensic Analysis of Windows Registry (20th Jan'25)

NAME: Deepesh Patil

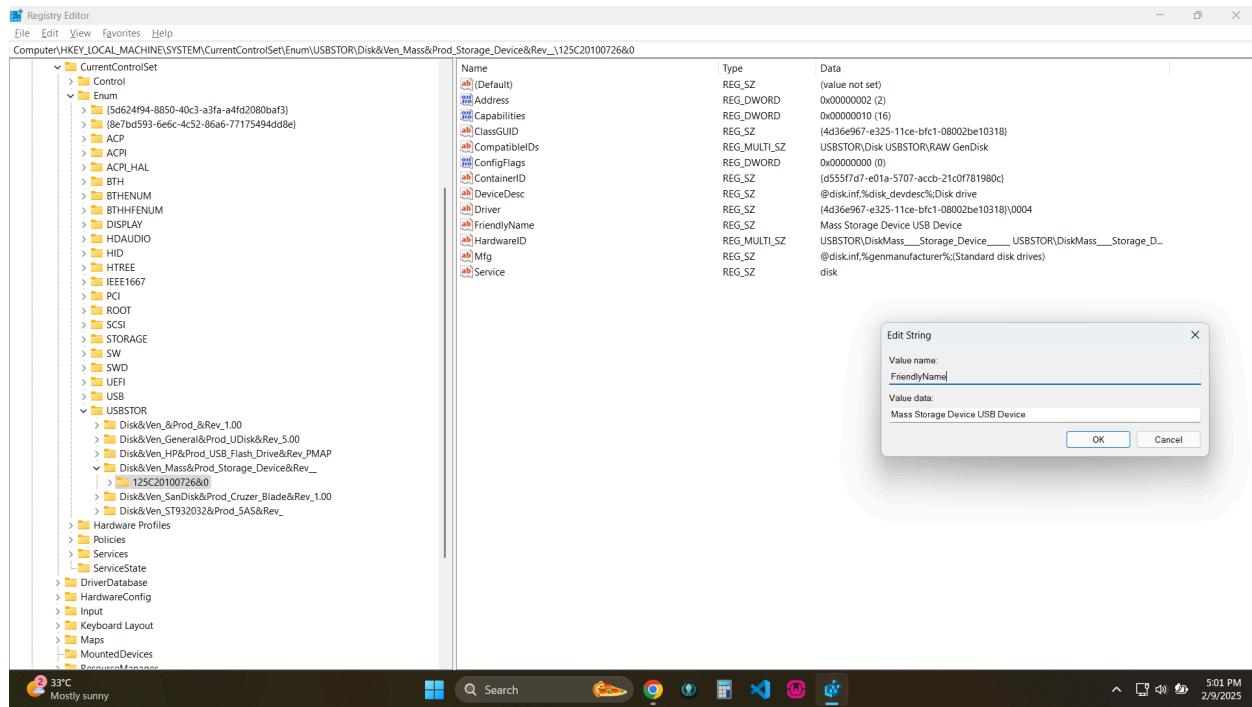
MIS: 112215055

Objective:

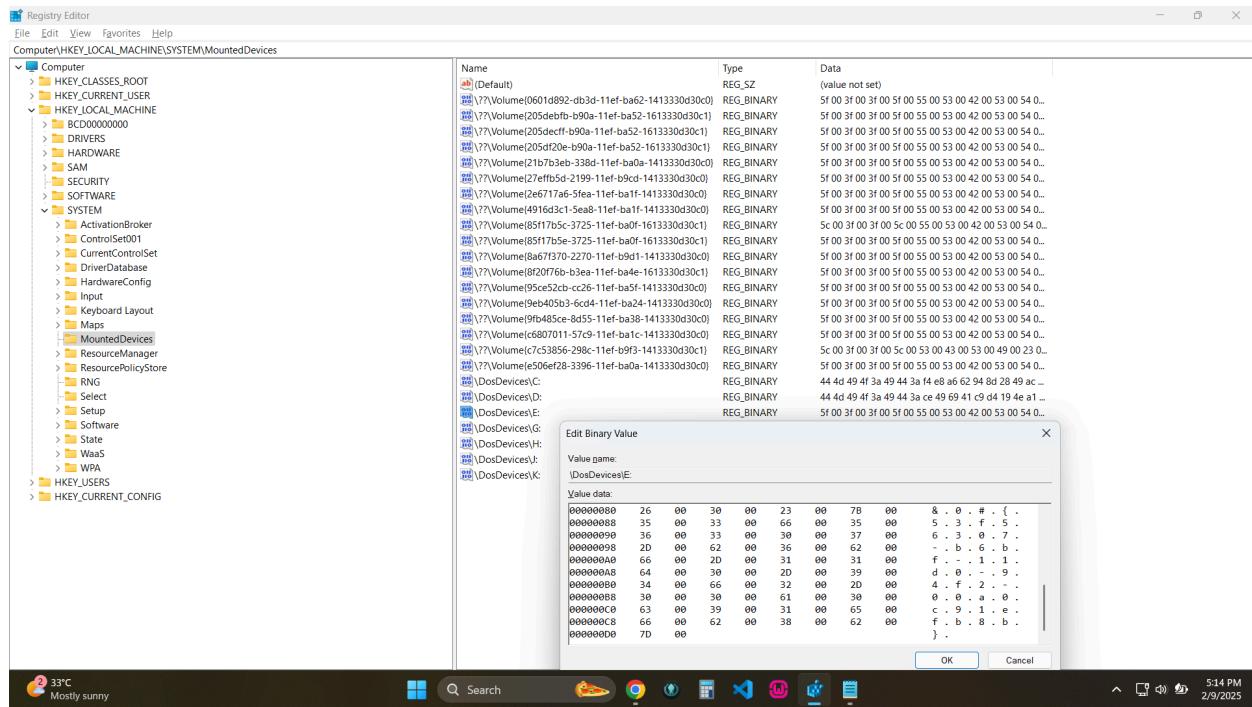
To delve deeper into Windows Registry Forensics, focusing on advanced techniques, artifact recovery, and the application of forensic tools to investigate complex scenarios.

Section 1: Practical Scenarios

1. Scenario 1: A USB device was used to exfiltrate data from a system.
 - Locate the Registry keys showing when the USB was connected.



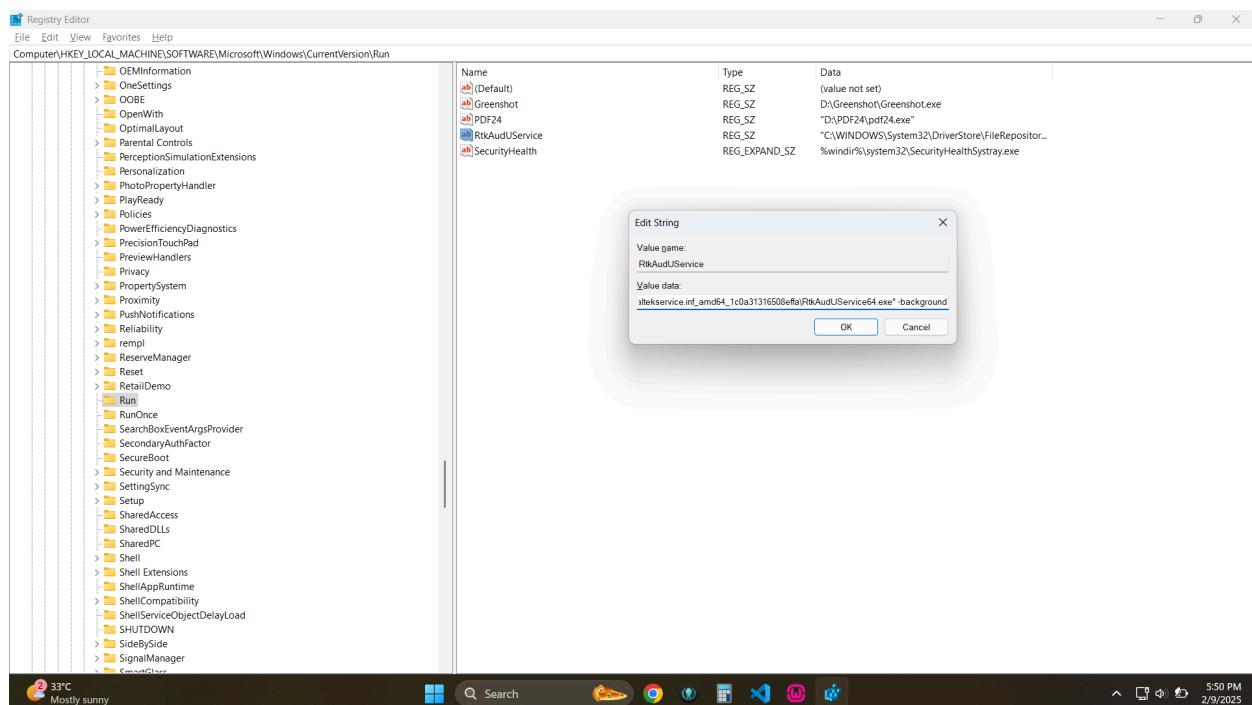
- Identify the drive letter assigned and the volume information.

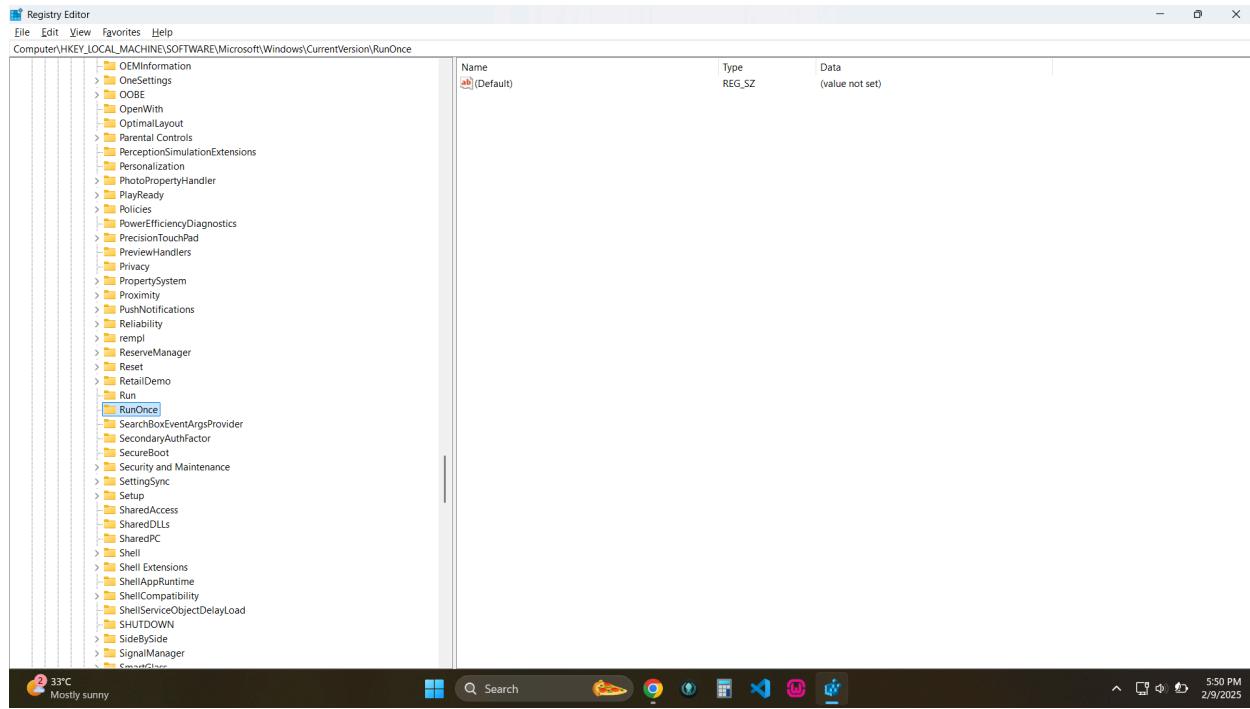


2. Scenario 2: A malicious program was set to run at startup.

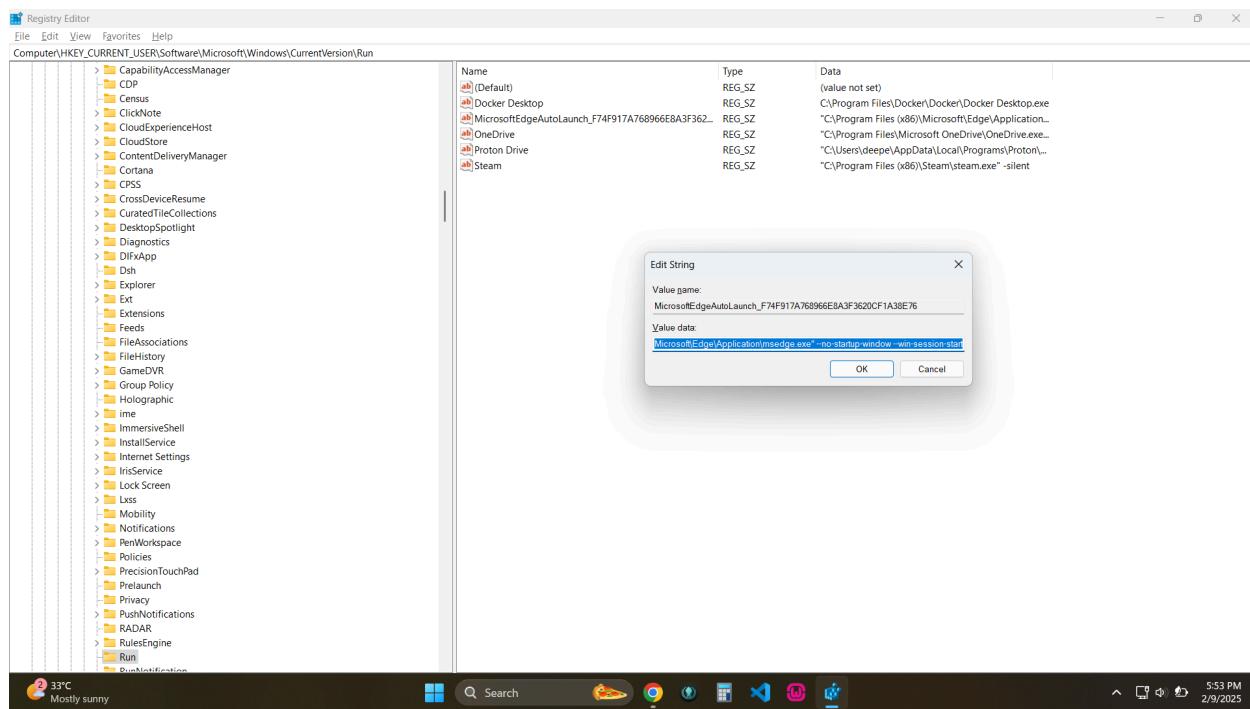
- Use the Run and RunOnce keys to identify suspicious entries.

HKLM :





HKCU :



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

```
>
>
> Get-Item "C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_1c0a31316508effa\RtkAudUService64.exe" | Select-Object Name, CreationTime, LastWriteTime, Length, VersionInfo
Name      : RtkAudUService64.exe
CreationTime : 6/3/2024 12:13:46 AM
LastWriteTime : 9/29/2022 4:49:22 AM
Length     : 1596800
VersionInfo : File:          C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_1c0a31316508effa\RtkAudUService64.exe
              InternalName: RtkAudUService.exe
              OriginalFilename: RtkAudUService.exe
             FileVersion: 1.1.511.1
              FileDescription: Realtek HD Audio Universal Service
              Product: Realtek HD Audio Universal Service
              ProductVersion: 1.1.511.1
              Debug: False
              Patched: False
              PreRelease: False
              PrivateBuild: False
              SpecialBuild: False
              Language: English (United States)

▶ @ pwsh
⌚ 18:06:16 | # 9 Feb, Sunday | ■ in ⌂
└─|
```

```
> Get-Item "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" | Select-Object Name, CreationTime, LastWriteTime, Length, VersionInfo
Name      : msedge.exe
CreationTime : 4/12/2022 12:17:49 AM
LastWriteTime : 1/30/2025 10:16:41 PM
Length     : 3923496
VersionInfo : File:          C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
              InternalName: msedge.exe
              OriginalFilename: msedge.exe
             FileVersion: 132.0.2957.140
              FileDescription: Microsoft Edge
              Product: Microsoft Edge
              ProductVersion: 132.0.2957.140
              Debug: False
              Patched: False
              PreRelease: False
              PrivateBuild: False
              SpecialBuild: False
              Language: English (United States)

▶ @ pwsh
⌚ 18:14:06 | # 9 Feb, Sunday | ■ in ⌂
└─|
```

3. **Scenario 3:** Recovery of User password.

- Extract the User password hash.

```
mimikatz # lsadump::sam "D:\mimikatz-2.2.0-20220919\system" D:\mimikatz-2.2.0-20220919\SAM  
Domain : DEEPESH  
SysKey : e70a0d91c32bc842d59ee67ca7eeef30
```

Section 3: Scenario & Questions

Extract the SYSTEM and SOFTWARE hives from your Windows system. (Hint: look in C:\Windows\System32\Config\ using FTK Imager. You can use any Registry parser (E.g. RegRipper/Registry Explorer) and then select the appropriate hive file to answer these questions (put a snapshot for each answer):

1. What is the computer name of the system?

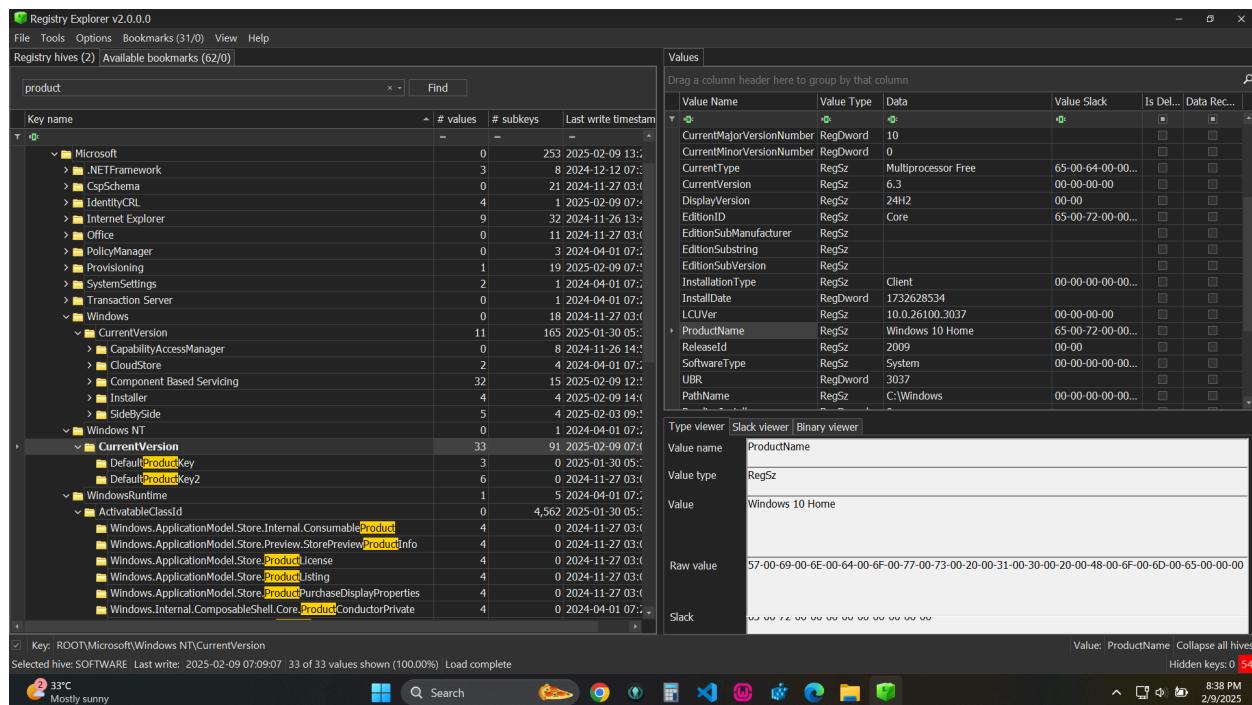
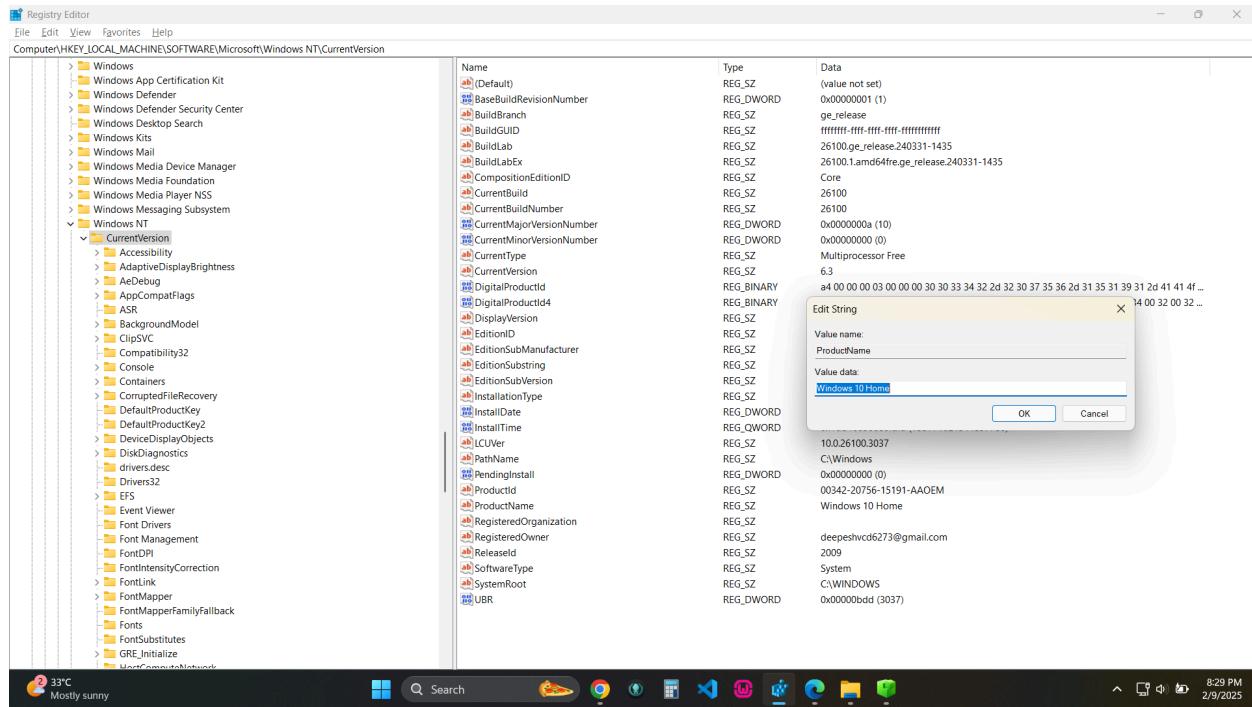
The screenshot shows the Registry Explorer interface with the following details:

- Title Bar:** Registry Explorer v2.0.0.0
- Menu Bar:** File, Tools, Options, Bookmarks (31/0), View, Help
- Toolbar:** Enter text to search..., Find
- Left Panel (Key list):** Shows the registry tree under the SYSTEM key. The ComputerName key is selected.
- Right Panel (Values table):**

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
(default)	RegSz	mmmsrvc	02-00-80-00		
ComputerName	RegSz	DEEPESH	98-A9-03-00		
- Bottom Panel (Details):**

Type viewer	Slack viewer	Binary viewer
Value name	ComputerName	
Value type	RegSz	
Value	DEEPESH	
Raw value	44-00-45-00-45-00-50-00-45-00-53-00-48-00-00-00	
Slack	>> A9-03-00	
- Status Bar:** Key: ROOT\ControlSet001\Control\ComputerName\ComputerName
Selected hive: SYSTEM Last write: 2024-11-27 03:05:57 2 of 2 values shown (100.00%) Load complete
Value: ComputerName Collapse all hives
Hidden keys: 0 54
8:17 PM 2/9/2025

2. What is the name of the Operating System?



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

Value Name	Value Type	Data	Value Slack	Is Del...	Data Rec...
CurrentMajorVersionNumber	RegDword	10			
CurrentMinorVersionNumber	RegDword	0			
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00...		
DisplayVersion	RegSz	24H2	00-00		
EditionID	RegSz	Core	65-00-72-00-00...		
EditionSubManufacturer	RegSz				
EditionSubString	RegSz				
InstallationType	RegSz	Client	00-00-00-00-00...		
InstallDate	RegDword	1732628534			
LCUVer	RegSz	10.0.26100.3037	00-00-00-00		
ProductName	RegSz	Windows 10 Home	65-00-72-00-00...		
ReleaseId	RegSz	2009	00-00		
SoftwareType	RegSz	System	00-00-00-00-00...		
UBR	RegDword	3037			
PathName	RegSz	C:\Windows	00-00-00-00-00...		

Results

1732628534 26/11/2024 13:42:14
(UTC +00:00 heure d'hiver)

Timestamp - dCode
Tag(s) : Date and Time, Informatics

4. Is Remote Desktop service enabled? How do you know?

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

- File Path:** Terminal Server
- Selected Hive:** SYSTEM
- Last Write:** 2025-02-09 07:09:01
- Values Shown:** 14 of 14 values shown (100.00%)
- Key: ROOT\ControlSet001\Control\Terminal Server**
- Value: fDenyTSConnections** (RegDword) - Value is 1, indicating Remote Desktop is disabled.
- Other Values (partial list):**
 - AllowRemoteRPC: 0
 - DelayConMgrTimeout: 0
 - DeleteTempDirsOnExit: 1
 - fSingleSessionPerUser: 1
 - NotificationTimeOut: 0
 - PerSessionTempDir: 0
 - ProductVersion: 5.1
 - RCDependentServices: 0
 - SnapshotMonitors: 1
 - StarRCM: 0
 - TSSUserEnabled: 0
 - InstanceId: 29db55ff-0c91-49... (Raw value: 01-00-00-00)
 - GlassSessionId: 1

If Value = 0, Remote Desktop Service is Enabled.

If Value = 1, remote Desktop Service is Disabled.

5. What is the IP address of the system?

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (31/0) View Help

Registry hives (2) Available bookmarks (62/0)

networklist

Find

Key name	# values	# subkeys
ROOT	0	47
Microsoft	0	253
PolicyManager	0	3
default	0	267
NetworkListManager	0	8
Windows	0	18
CurrentVersion	11	165
SideBySide	5	4
Winners	0	17,541
Windows NT	0	1
CurrentVersion	33	91
NetworkList	3	7
WindowsRuntime	1	5
ActivatableClassId	0	4,562
NetworkUX.View.NetworkListViewItemContainerStyleSelector	4	0
WOW6432Node	0	24
Microsoft	0	146
Windows NT	0	1
CurrentVersion	26	44
NetworkList	1	1

Values Known networks

Drag a column header here to group by that column

First Network	Network Na...	Name Type	First Connec...	Last Connect...	Managed	DNS Suffix	Gateway Ma...	Profile GUID
Krish 3	Krish 3	Wireless	2024-08-15 ...	2024-08-15 ...	■	<none>	66-7C-ED-7-	{0080943F-CD
IITP_WIFI_14	IITP_WIFI_14	Wireless	2024-10-01 ...	2024-10-01 ...	■	<none>	C5-92	-EF-4898-A587
								-F5412C880B
								7}
Twingate 2	Twingate 2		2024-12-18 ...	2024-12-18 ...	■	<none>	3A-1A-DA-E4-	{00C4D691-9B
								53-10
Realme 9 Pro+ 22	Realme 9 Pro+ 22	Wireless	2024-07-28 ...	2024-07-28 ...	■	<none>	AE-DD-A8-04-	{030985D1-76
Realme 9 Pro+ 50	Realme 9 Pro+ 50	Wireless	2024-08-06 ...	2024-08-06 ...	■	<none>	C5-D3	-BC-4EAE-9924
								-C558CDDA5
								99}

Total rows: 324

Type viewer Slack viewer Binary viewer

Value name (default)

Value type RegSz

Value 192.228.79.201

Raw value 31-00-39-00-32-00-2E-00-32-00-38-00-2E-00-37-00-39-00-2E-00-32-00-30-00-31-00-00-00

Slack 00 00 00 00 00 00

Value: (default) Collapse all hives

Hidden keys: 0 54

Selected hive: SOFTWARE Last write: 2025-02-09 07:09:01 3 of 3 values shown (100.00%) Load complete

23°C Mostly sunny 901 PM 2/9/2025

6. When was the system last shutdown?

133,830,437,306,107,729

HEX 1DB 7612 DBC4 0751

DEC 133,830,437,306,107,729

Enter number in full or in scientific/exponential notation:

Milliseconds are discarded (last 7 digits of the LDAP timestamp)

133830437306107729

Convert 18-digit LDAP to human date/epoch

Epoch/Unix time: 1738570130

GMT: Monday, February 3, 2025 8:08:50 AM

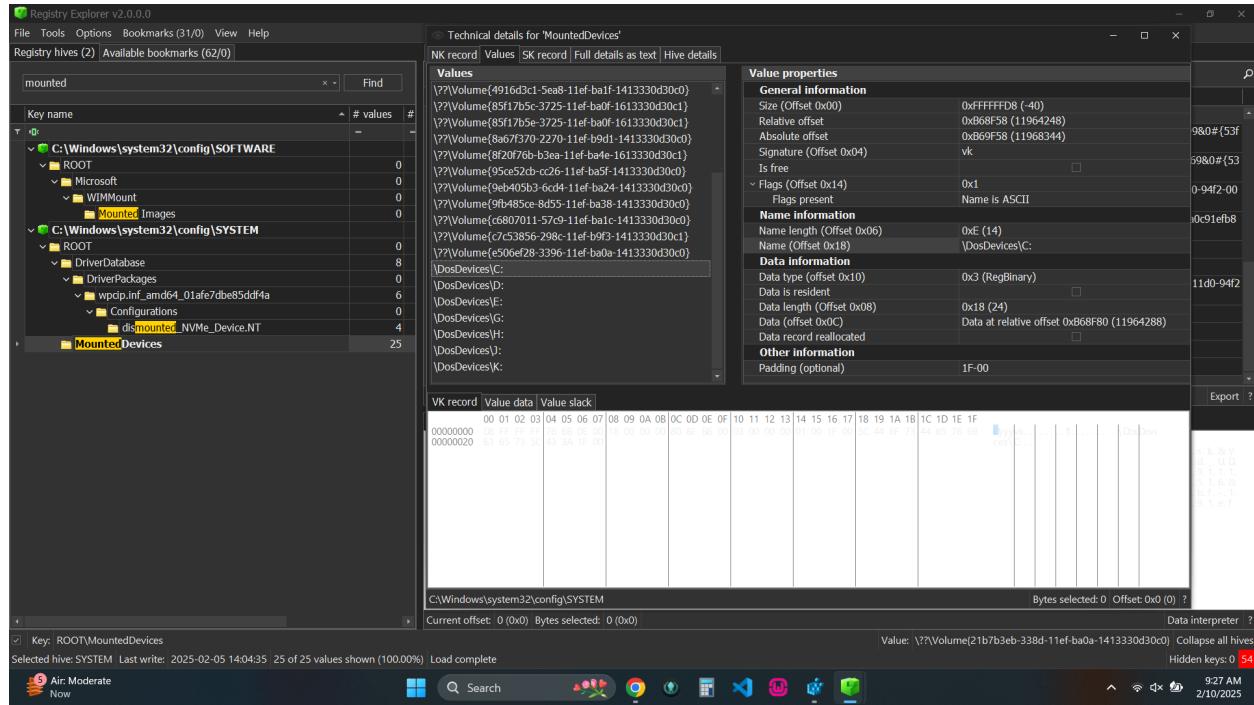
Your time zone: Monday, February 3, 2025 1:38:50 PM GMT+05:30

7. List out program names launching at startup.

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

- File Path:** C:\Windows\system32\config\Software\Microsoft\Windows\CurrentVersion\Run
- Key Name:** Runonce
- Subkeys:** CurrentVersion, RunOnce, SideBySide, Windows, Wow6432Node
- Values:**
 - PDF24
 - RtkAudUService
 - SecurityHealth
 - Greenshot
 - Parental Controls
 - PerceptionSimulationExtensions
 - Personalization
 - PhotoPropertyHandler
 - PlayReady
 - Policies
 - PowerEfficiencyDiagnostics
 - PrecisionTouchPad
 - PreviewHandlers
 - Privacy
 - PropertySystem
 - Proximity
 - PushNotifications
 - Reliability
 - repl
 - ReserveManager
 - Reset
 - RetailDemo
 - Run
 - RunOnce
 - SearchBoxEventArgsProvider
 - SecondaryAuthFactor
 - SecureBoot
 - Security and Maintenance
 - SettingSync
 - Setup
 - SharedAccess
- Value Properties (for PDF24):**
 - General information:** Size (Offset 0x00) 0xFFFFFFF (-32), Relative offset 0x3599A40 (56203940), Absolute offset 0x359AA40 (56207936), Signature (Offset 0x04) VK
 - Flags:** Is free 0x1, Flags present Name is ASCII
 - Name information:** Name length (Offset 0x06) 0x5 (5), Name (Offset 0x18) PDF24
 - Data information:** Data type (offset 0x10) 0x1 (RegSz), Data is resident, Data length (Offset 0x08) 0x2A (42), Data (Offset 0x0C) Data at relative offset 0x3599A40
 - Other information:** Padding (optional) 35-25-00
- Value Data:** A hex dump of the value data, showing bytes 00 through FF.
- Bottom Status Bar:** Key: ROOT\Microsoft\Windows\CurrentVersion\Run, Selected hive: SOFTWARE, Last write: 2025-01-30 05:34:51, 11 of 11 values shown (100.00%), Load complete, Value: ProgramFilesRun, Collected all hives, Hidden keys: 0, 54, 2/10/2025, 9:00 AM.

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



9. 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.

Program Name	Execution Path	Last Execution TimeStamp
UEME_CTLSESSION		1/25/2025 10:08:39 AM +00:00

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