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

NAME: Deepesh Patil

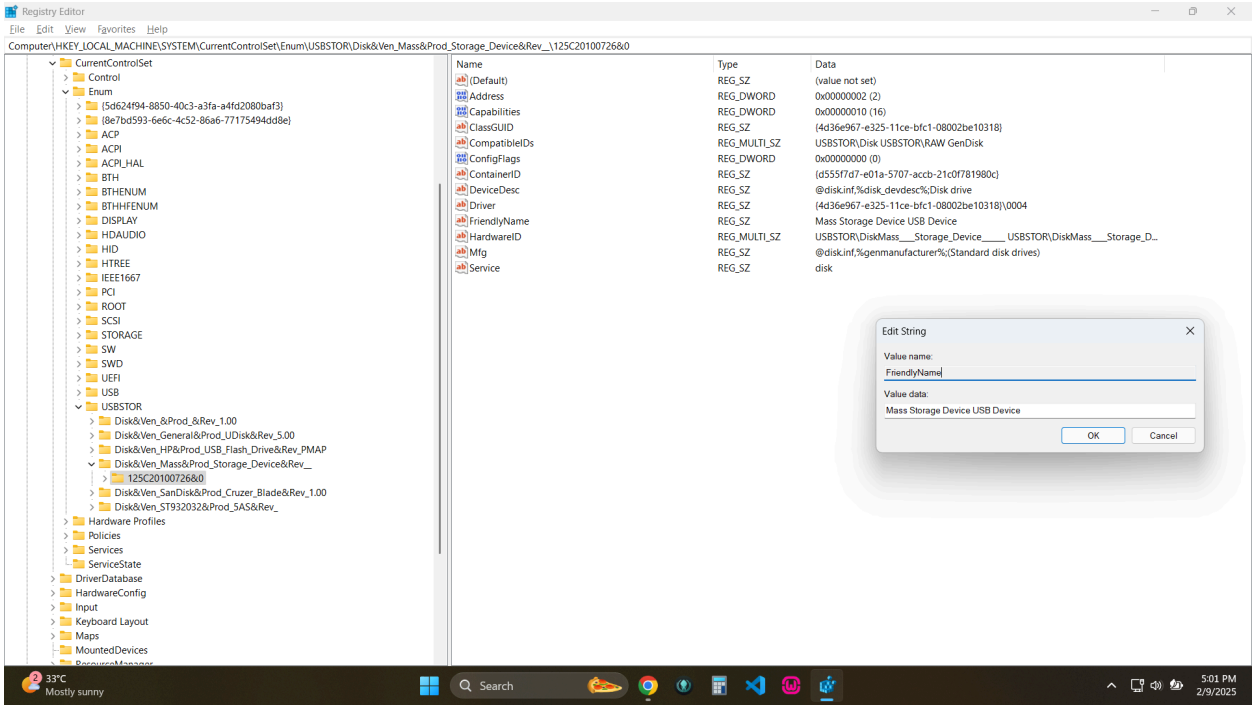
MIS: 112215055

Objective:

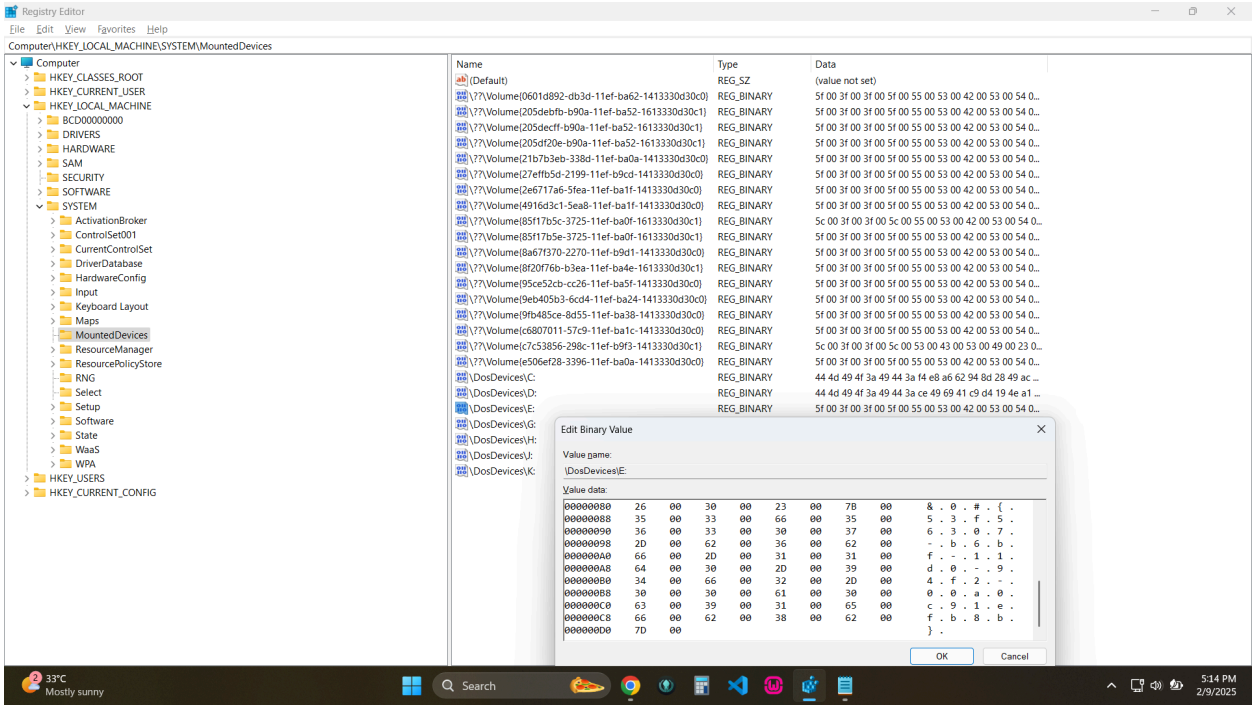
To delve deeper into Windows Registry Forensics, focusing on advanced techniques, artifact recovery, and the application of forensic tools to investigate complex scenarios.

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.

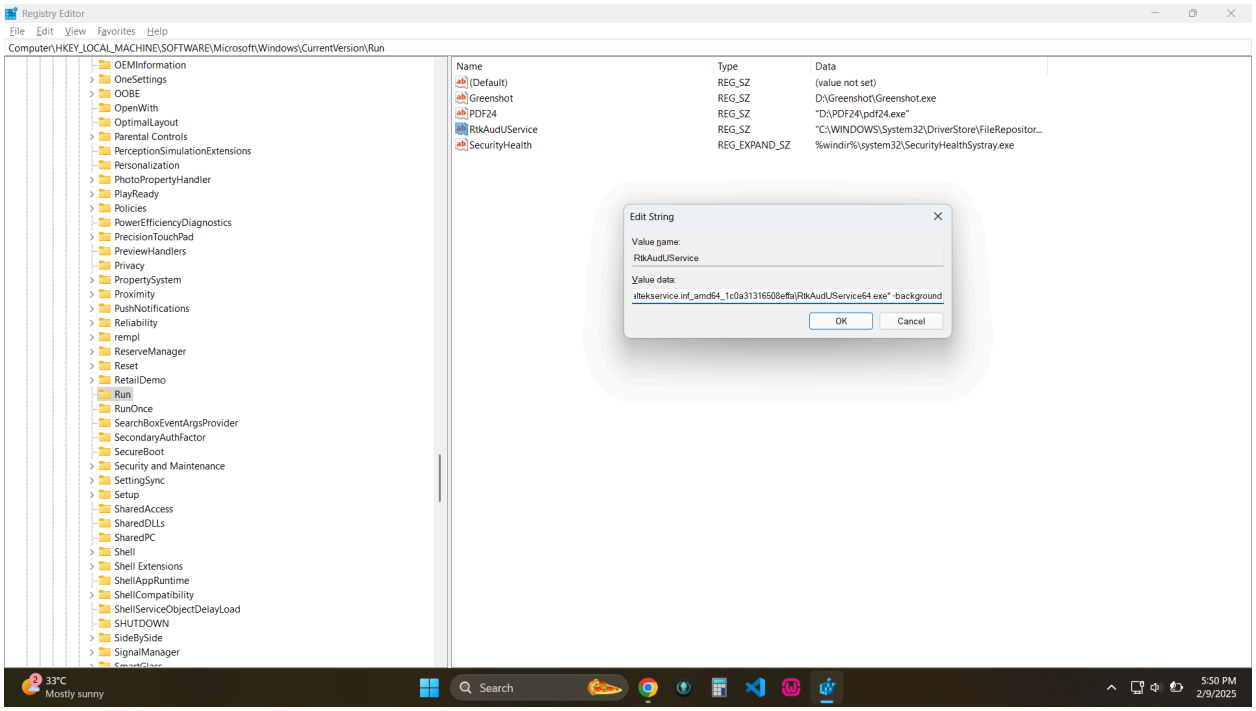


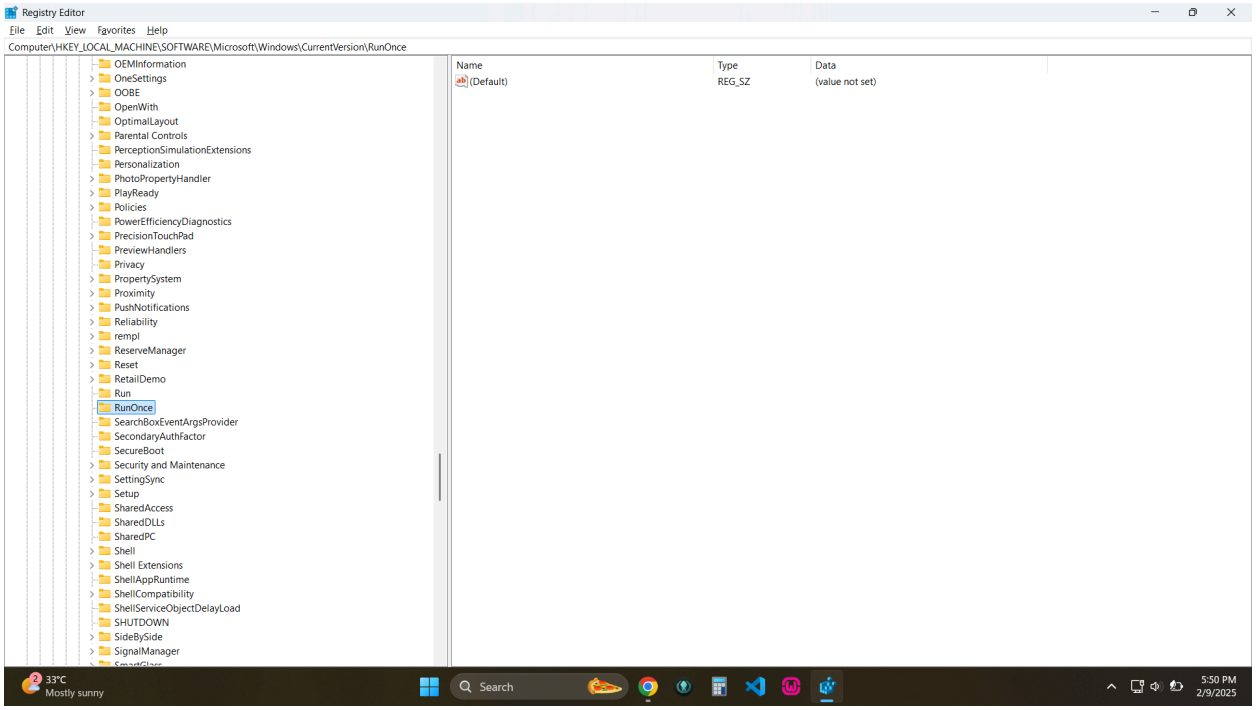
- Identify the drive letter assigned and the volume information.



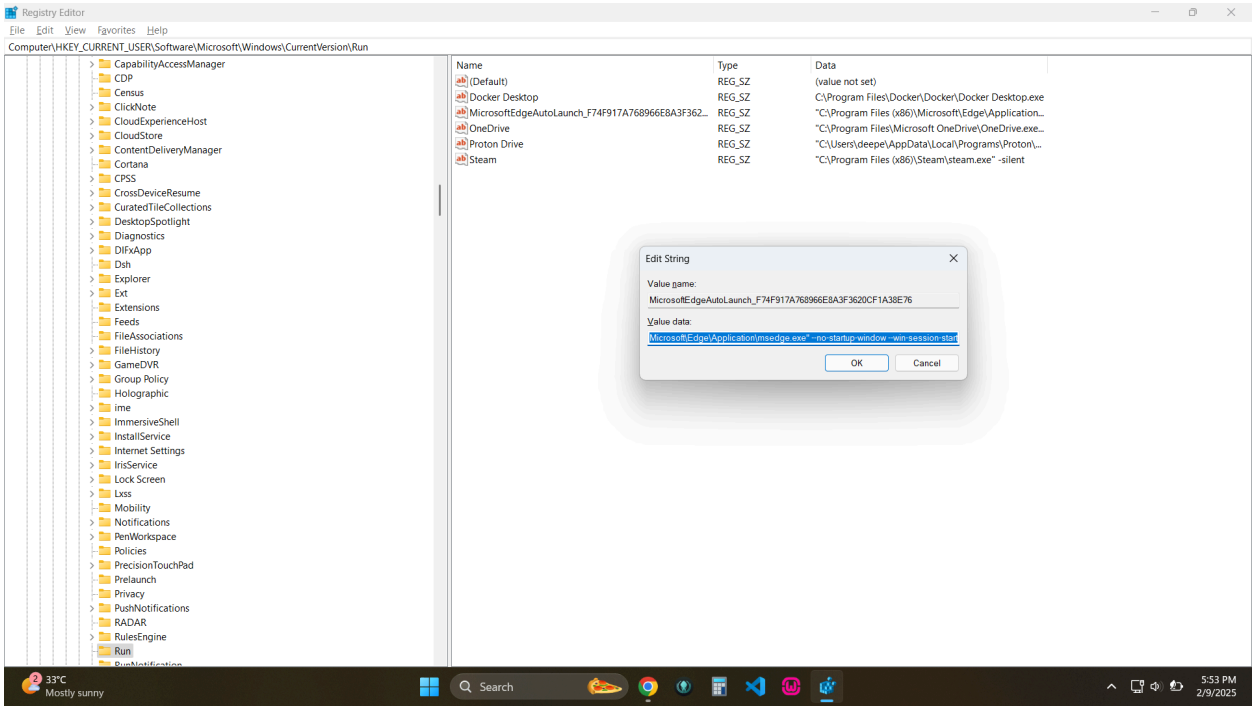
2. **Scenario 2:** A malicious program was set to run at startup.
   - Use the Run and RunOnce keys to identify suspicious entries.

HKLM :

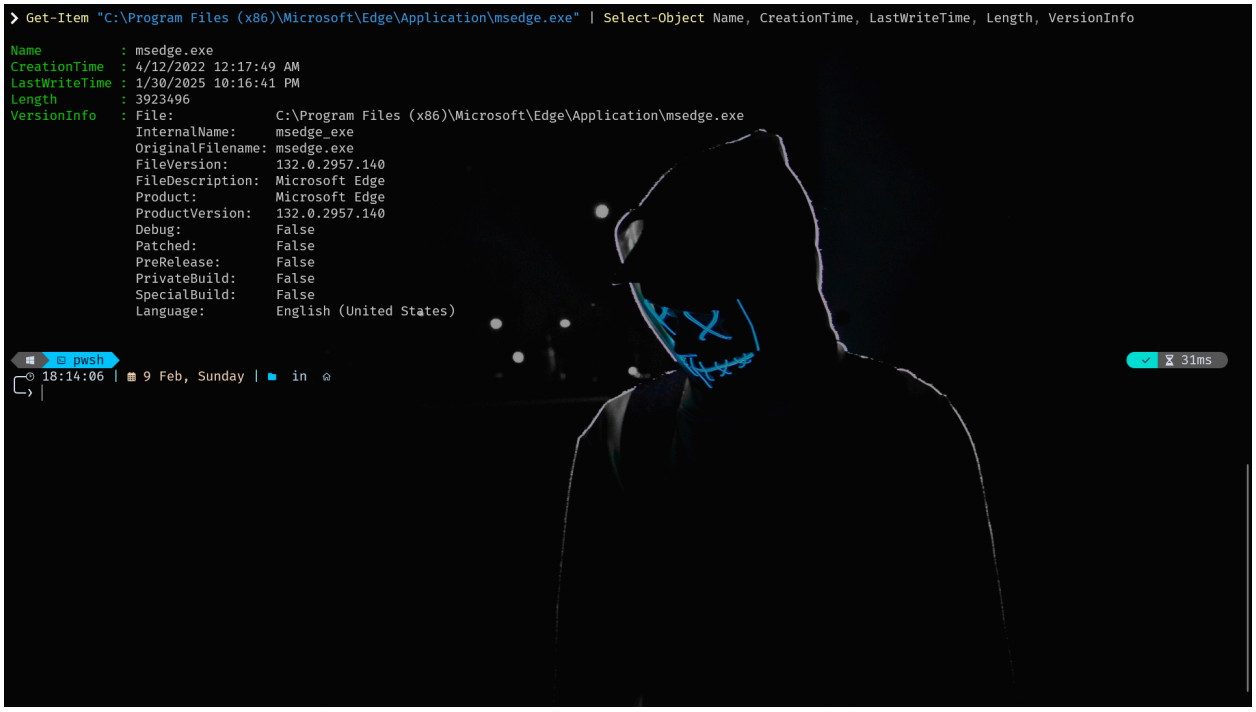



Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
OEMInformation
OneSettings
OOBE
OpenWith
OptimalLayout
Parental Controls
PerceptionSimulationExtensions
Personalization
PhotoPropertyHandler
PlayReady
Policies
PowerEfficiencyDiagnostics
PrecisionTouchPad
PreviewHandlers
Privacy
PropertySystem
Proximity
PushNotifications
Reliability
rempl
ReserveManager
Reset
RetailDemo
Run
RunOnce
SearchBoxEventArgsProvider
SecondaryAuthFactor
SecureBoot
Security and Maintenance
SettingSync
Setup
SharedAccess
SharedDLLs
SharedPC
Shell
Shell Extensions
ShellAppRuntime
ShellCompatibility
ShellServiceObjectDelayLoad
SHUTDOWN
SideBySide
SignalManager
Name
Type
Data
(Default)
REG_SZ
(value not set)
33°C
Mostly sunny
Search
5:50 PM
2/9/2025

HKCU :


Registry Editor
File Edit View Favorites Help
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
CapabilityAccessManager
CDP
Census
ClickNote
CloudExperienceHost
CloudStore
ContentDeliveryManager
Cortana
CPSS
CrossDeviceResume
CuratedTileCollections
DesktopSpotlight
Diagnostics
DIFxApp
Dsh
Explorer
Ext
Extensions
Feeds
FileAssociations
FileHistory
GameDVR
Group Policy
Holographic
ime
ImmersiveShell
InstallService
Internet Settings
IrisService
Lock Screen
Lxss
Mobility
Notifications
PenWorkspace
Policies
PrecisionTouchPad
Prelaunch
Privacy
PushNotifications
RADAR
RulesEngine
Run
Name
Type
Data
(Default)
REG_SZ
(value not set)
Docker Desktop
REG_SZ
C:\Program Files\Docker\Docker\Docker Desktop.exe
MicrosoftEdgeAutoLaunch_F74F917A768966E8A3F362...
REG_SZ
"C:\Program Files (x86)\Microsoft\Edge\Application...
OneDrive
REG_SZ
"C:\Program Files\Microsoft OneDrive\OneDrive.exe...
Proton Drive
REG_SZ
"C:\Users\deepe\AppData\Local\Programs\Proton\...
Steam
REG_SZ
"C:\Program Files (x86)\Steam\steam.exe" -silent
Edit String
Value name:
MicrosoftEdgeAutoLaunch_F74F917A768966E8A3F3620CF1A38E76
Value data:
Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-star
OK
Cancel
33°C
Mostly sunny
Search
5:53 PM
2/9/2025

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



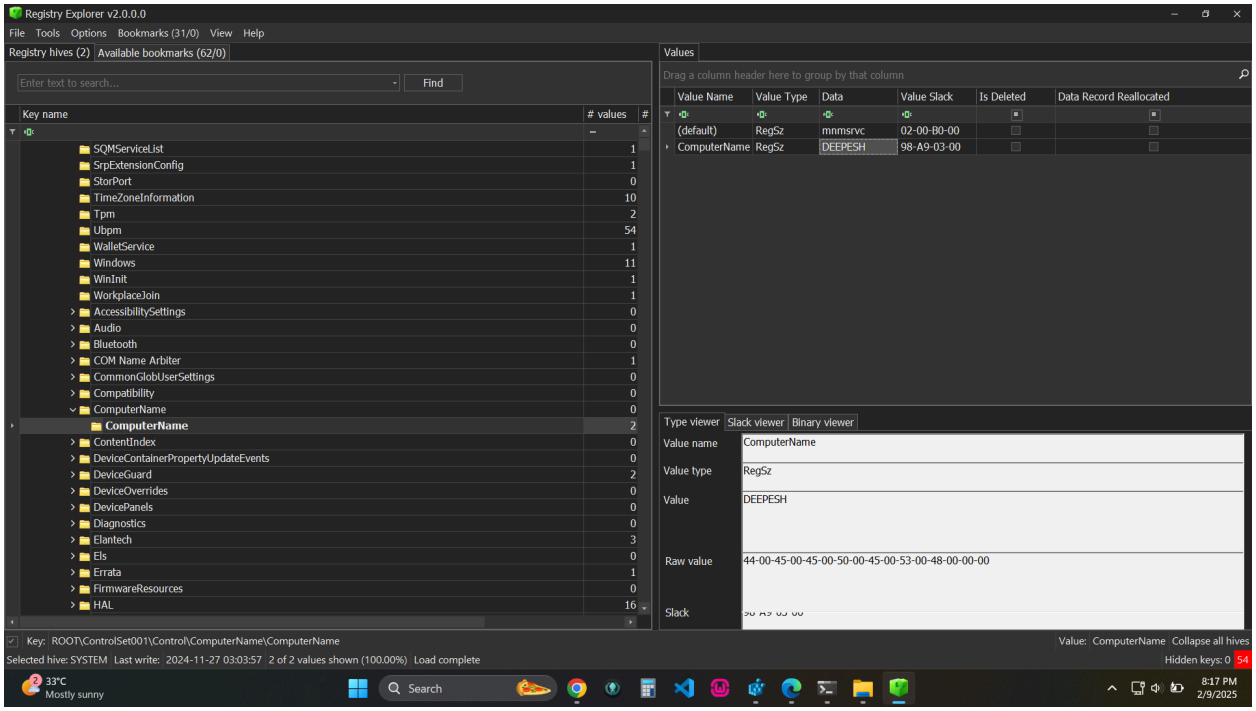
3. **Scenario 3:** Recovery of User password.
   - Extract the User password hash.

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

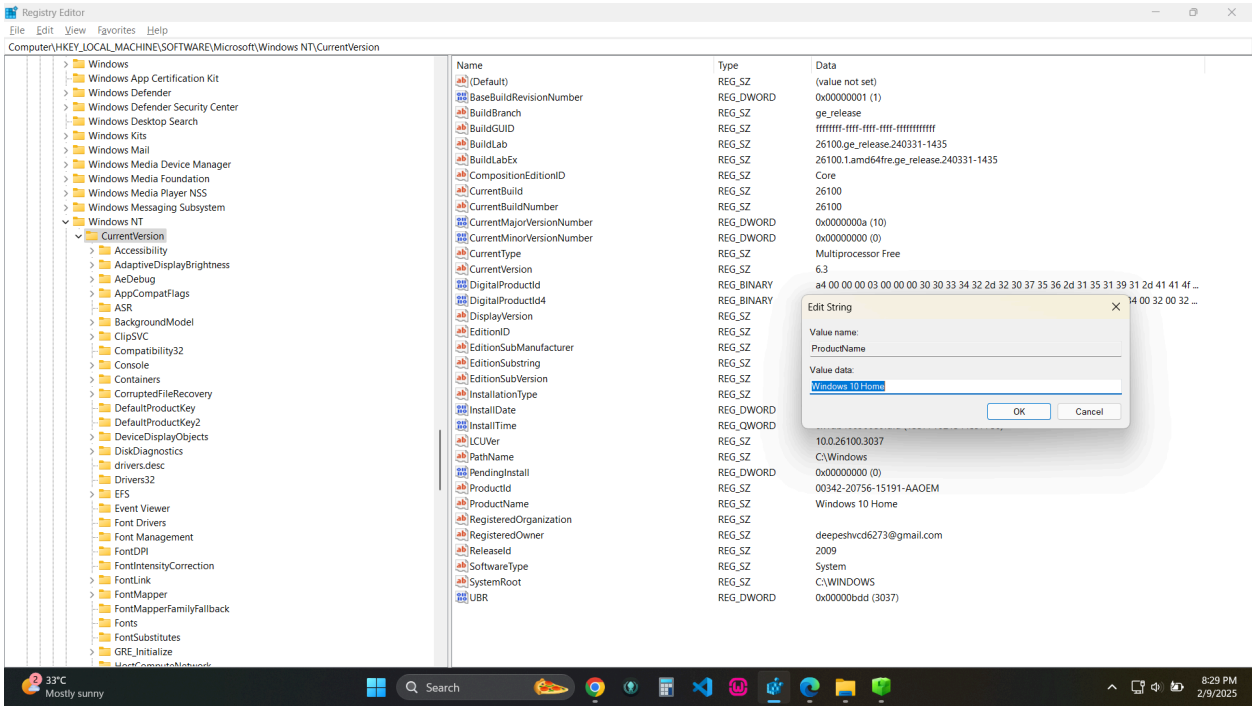
Section 3: Scenario & Questions

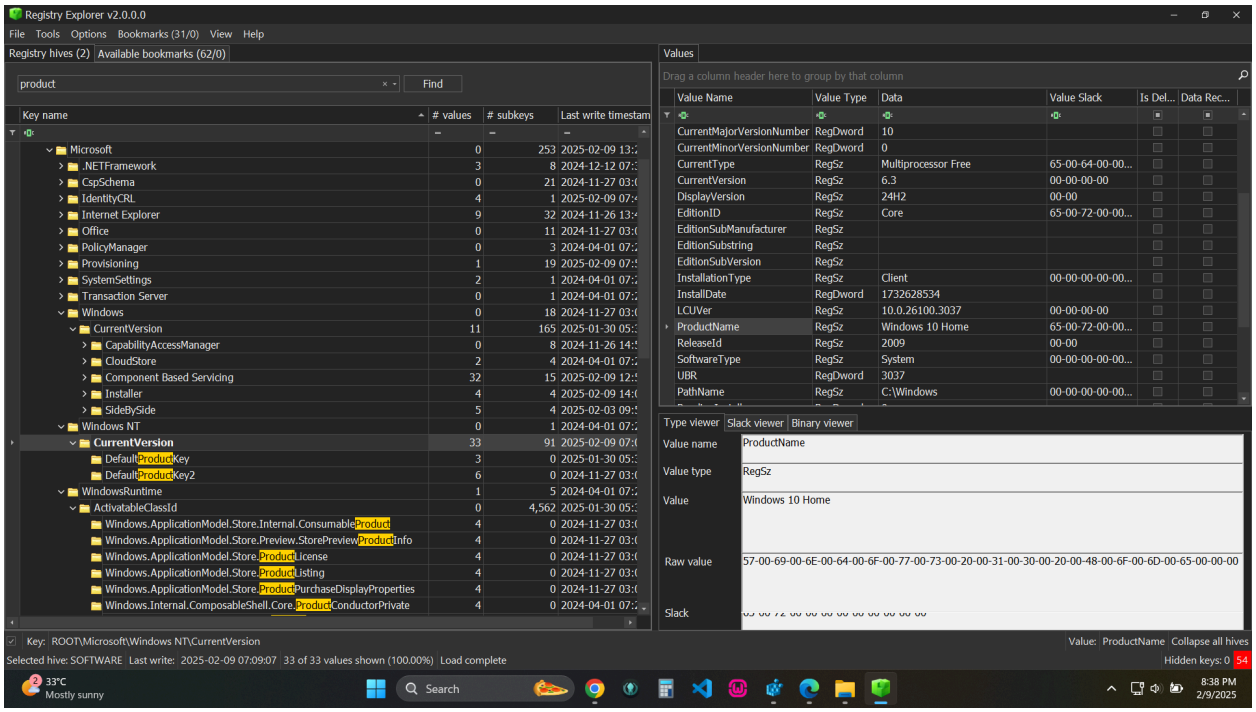
Extract the SYSTEM and SOFTWARE hives from your Windows system. (Hint: look in C:\Windows\System32\Config\) using FTK Imager. You can use any Registry parser (E.g. RegRipper/Registry Explorer) and then select the appropriate hive file to answer these questions (put a snapshot for each answer):

1. What is the computer name of the system?

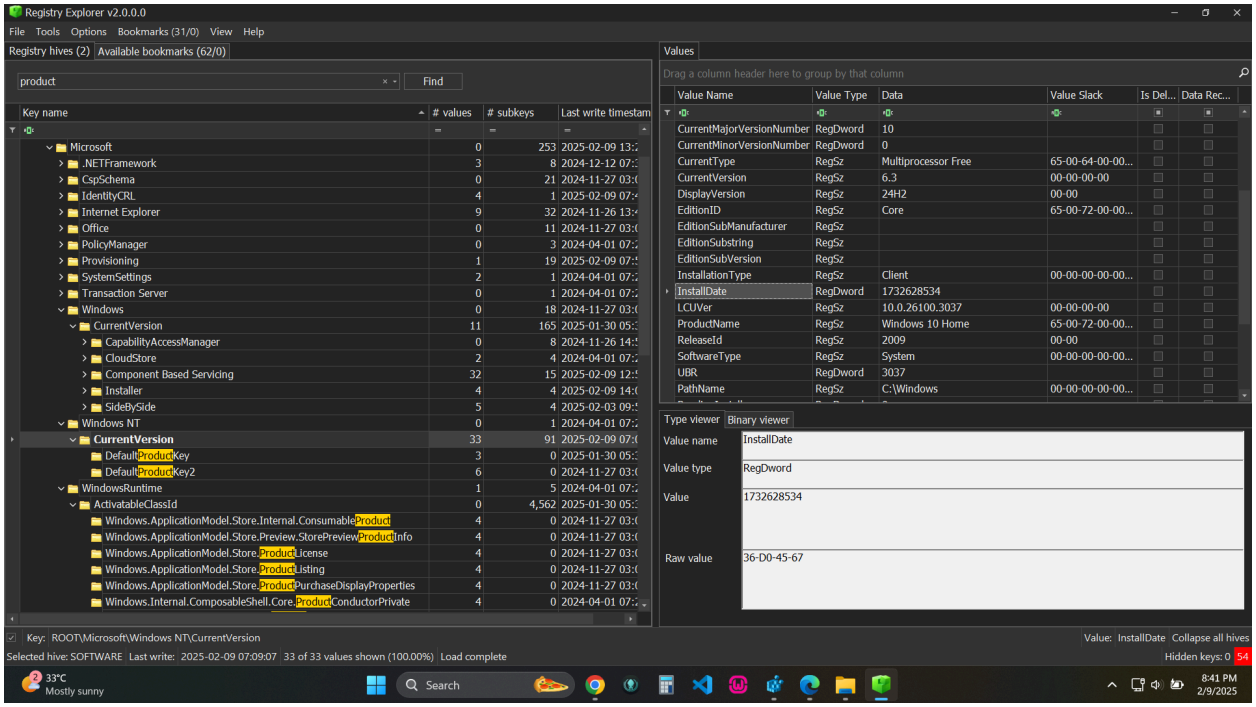


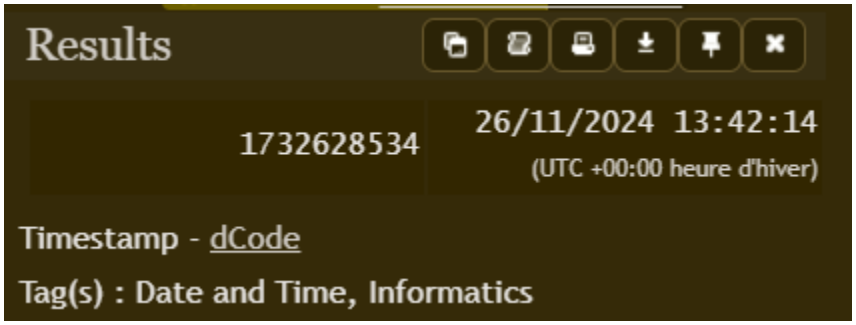
2. What is the name of the Operating System?



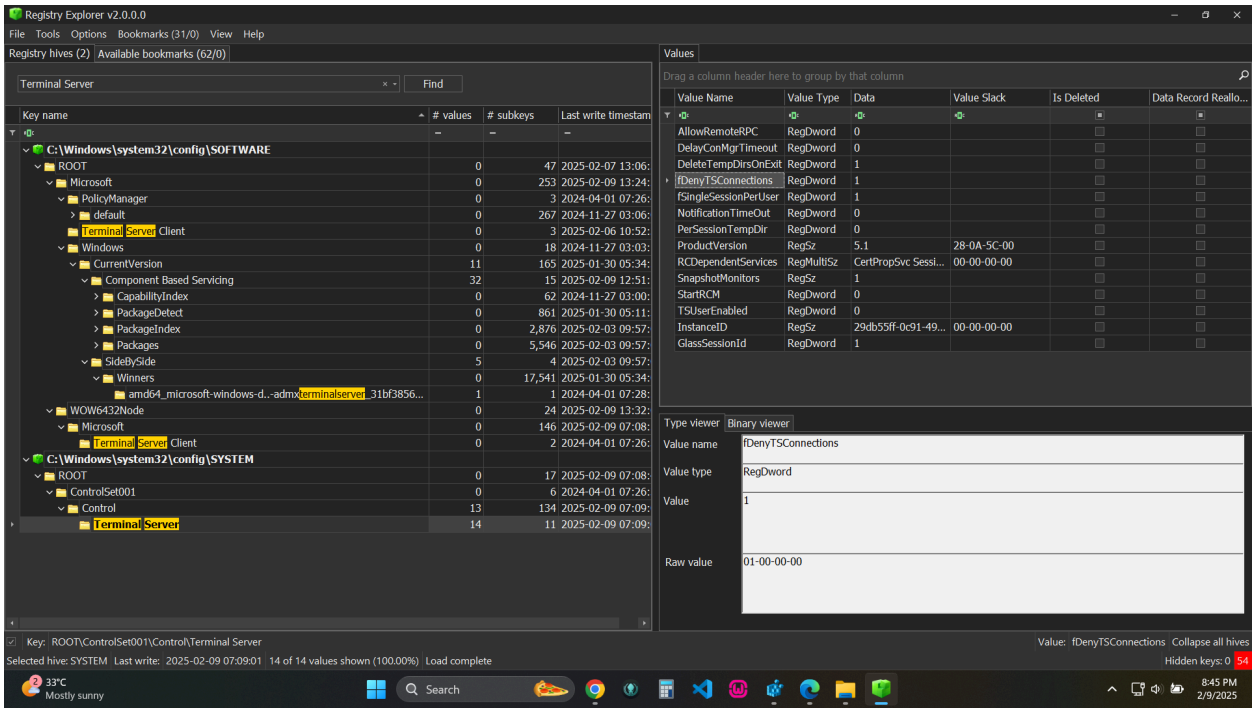


3. What date/time (in UTC) was the Operating System installed? Hint: you may have to convert epoch time to human readable time using DCode tool.



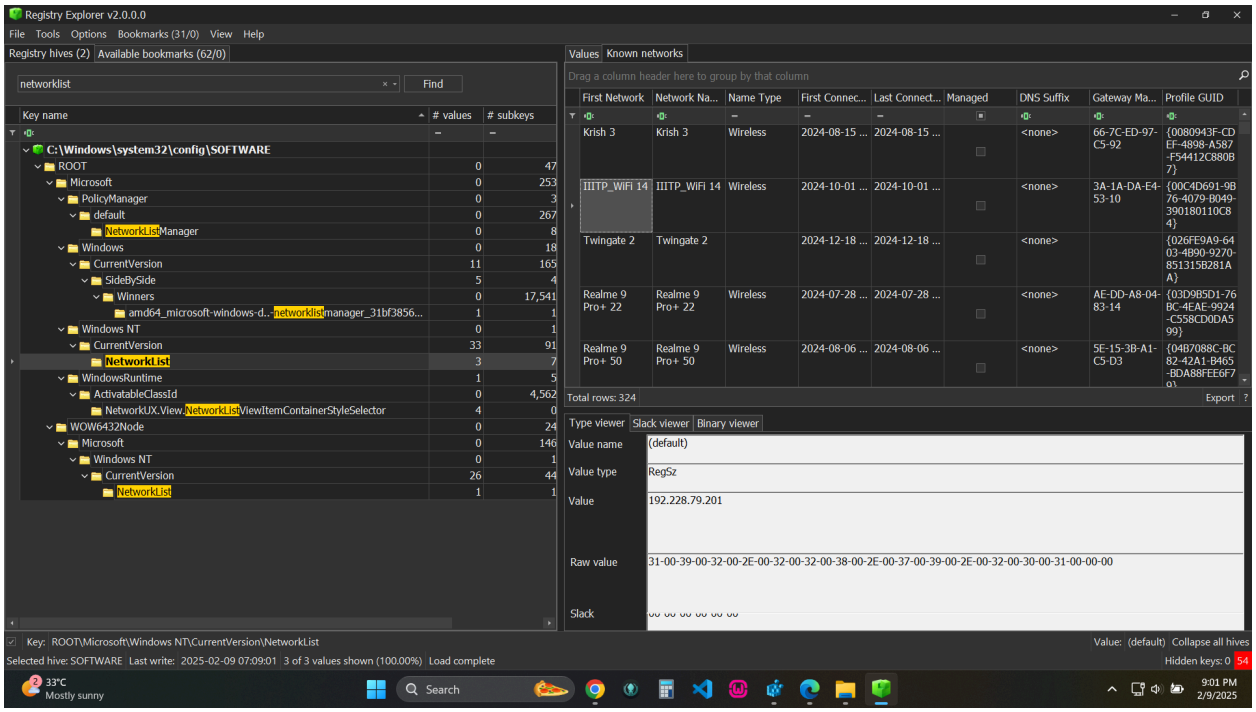


4. Is Remote Desktop service enabled? How do you know?

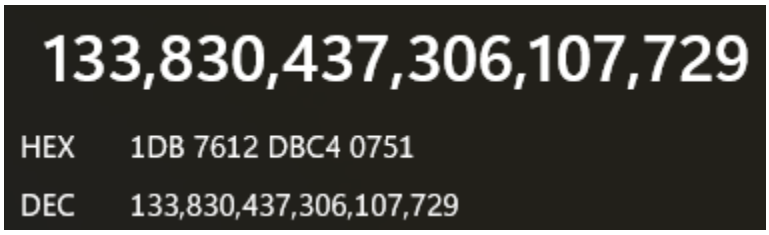


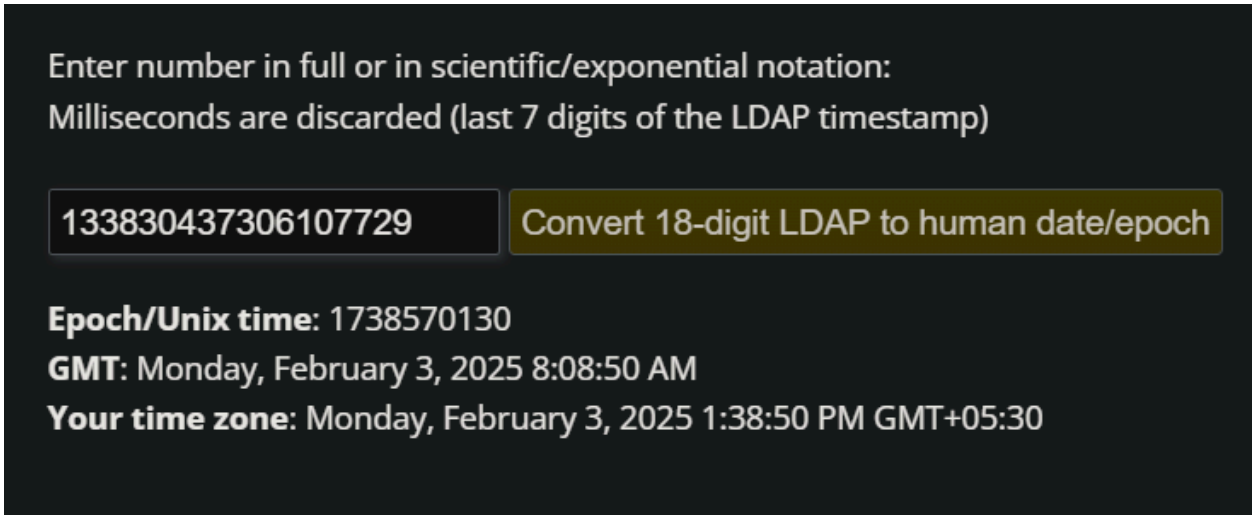
If Value = 0, Remote Desktop Service is Enabled.
If Value = 1, remote Desktop Service is Disabled.

5. What is the IP address of the system?

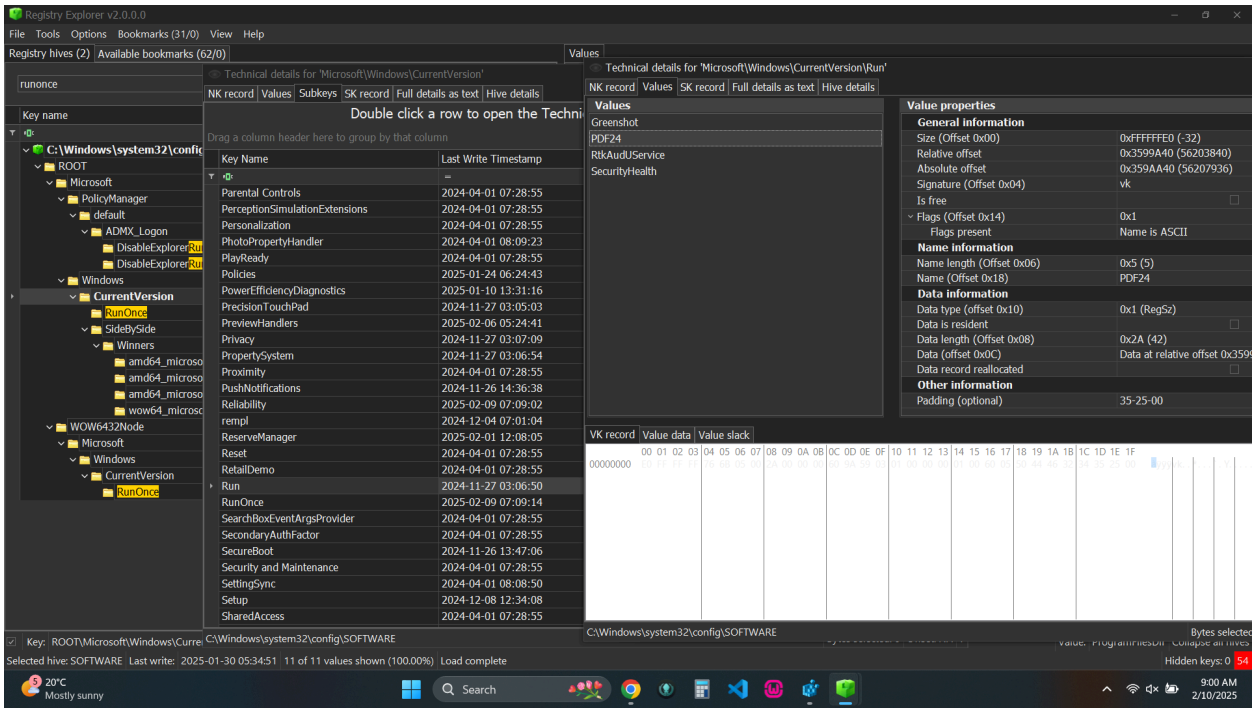


6. When was the system last shutdown?

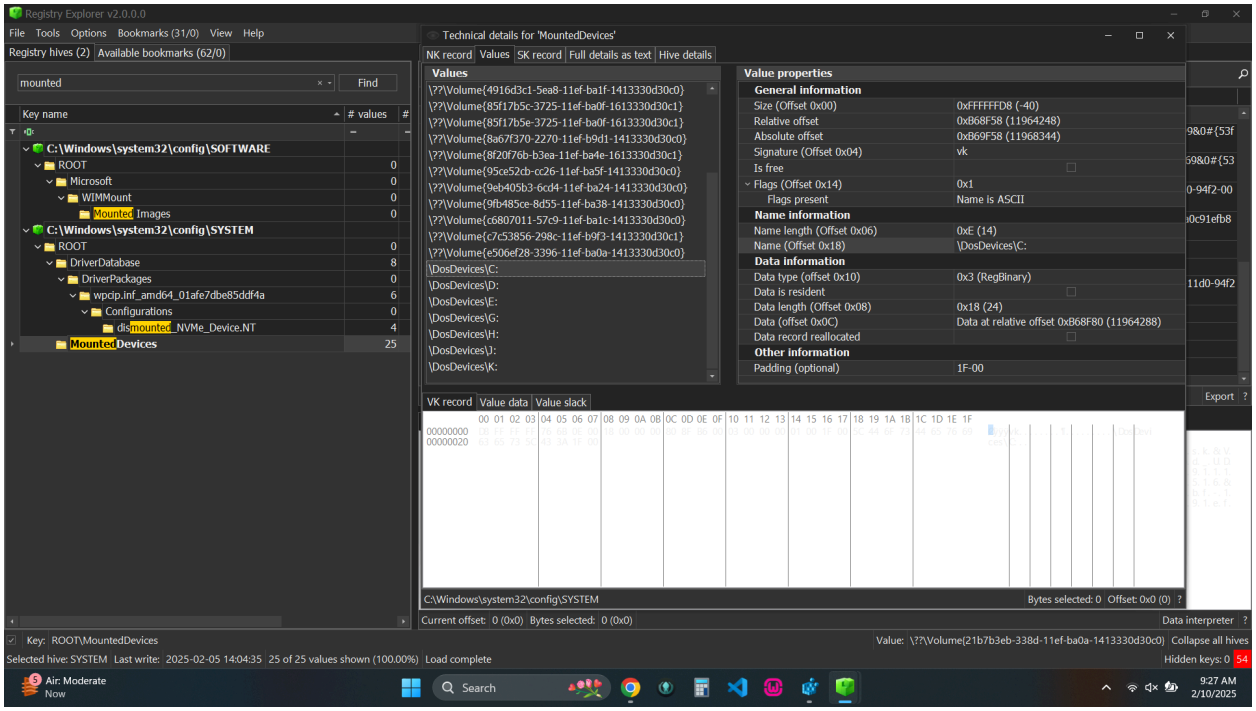




7. List out program names launching at startup.



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.