Indian Institute of Information Technology Pune

Subject Name: Information Systems Security

Assignment: Forensic Analysis of Windows Registry

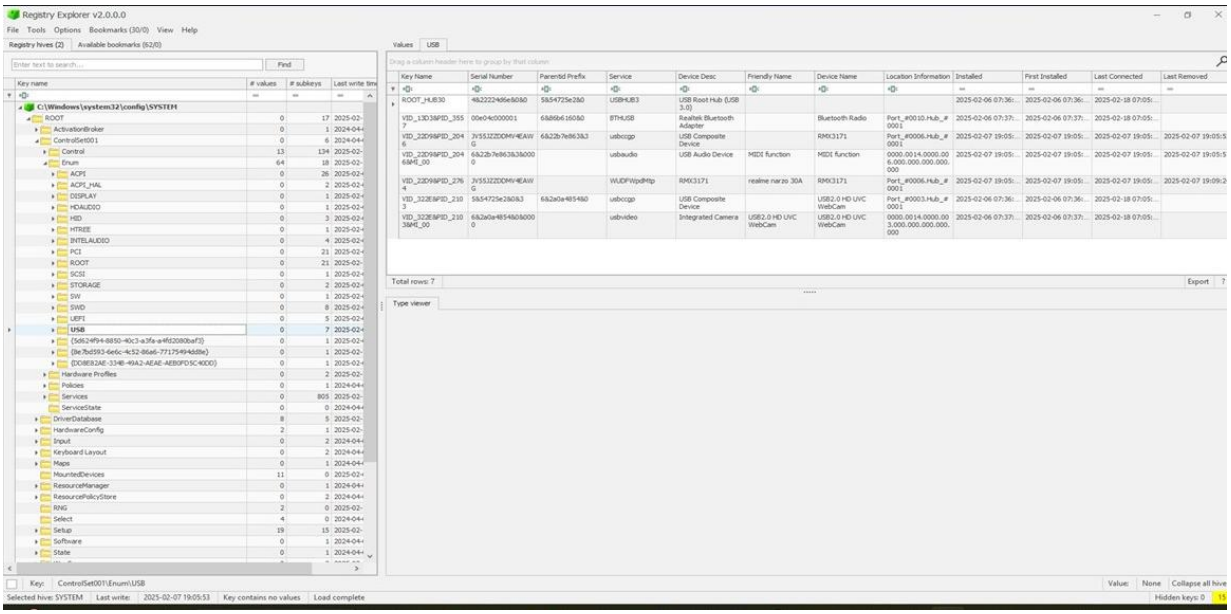
Name: Lakshay Kumawat

MIS: 112215103

Section 1: Practical Scenarios

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

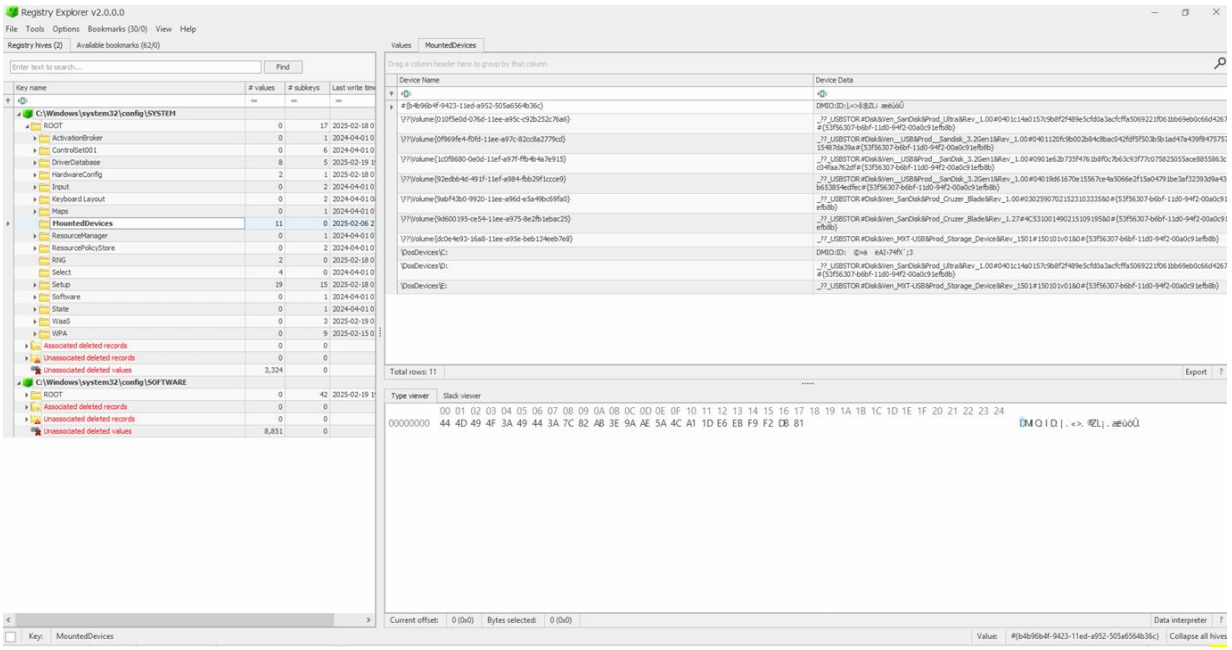
→ Locate the Registry keys showing when the USB was connected.



Key Path- SYSTEM: ControlSet001\Enum\USB

Identify the drive letter assigned and the volume information.

Key Path- SYSTEM: Root\MountedDevices

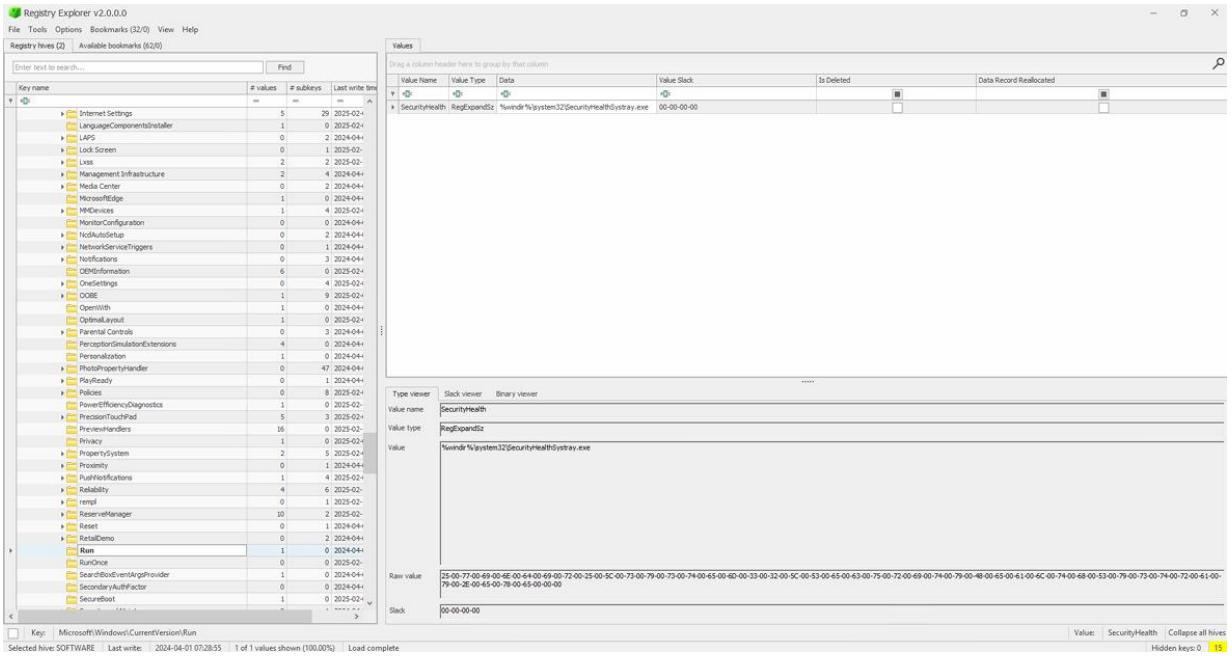


Scenario 2: A malicious program was set to run at startup.

Use the Run and RunOnce keys to identify suspicious entries.

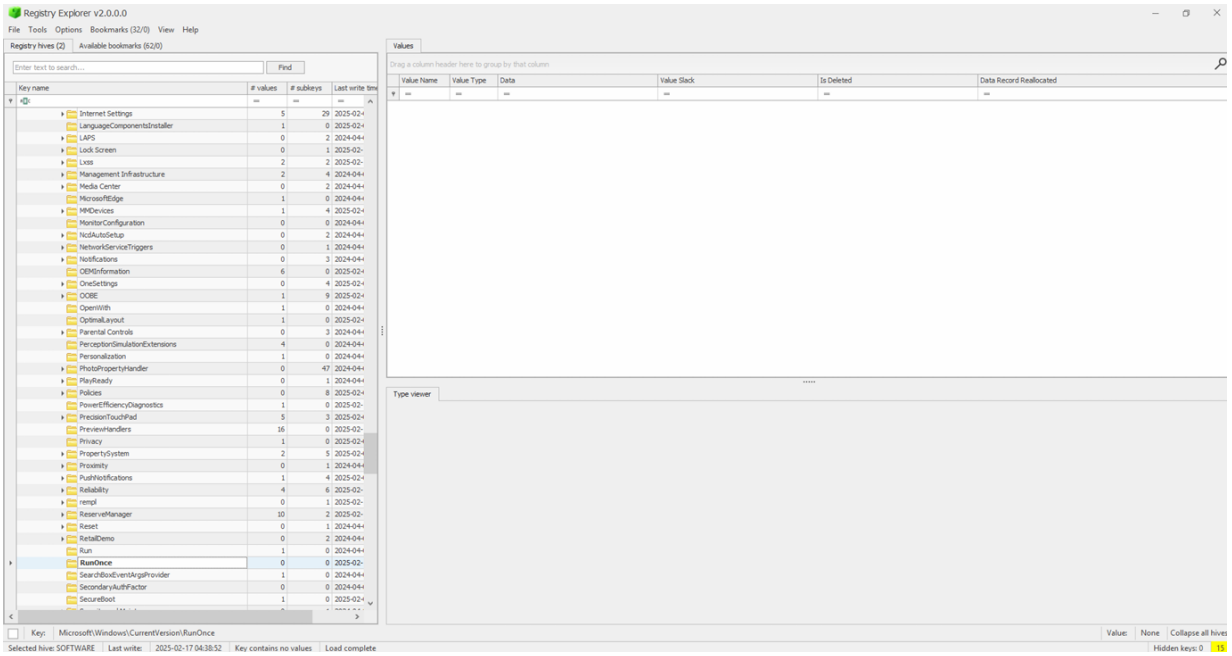
1) **Run**

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



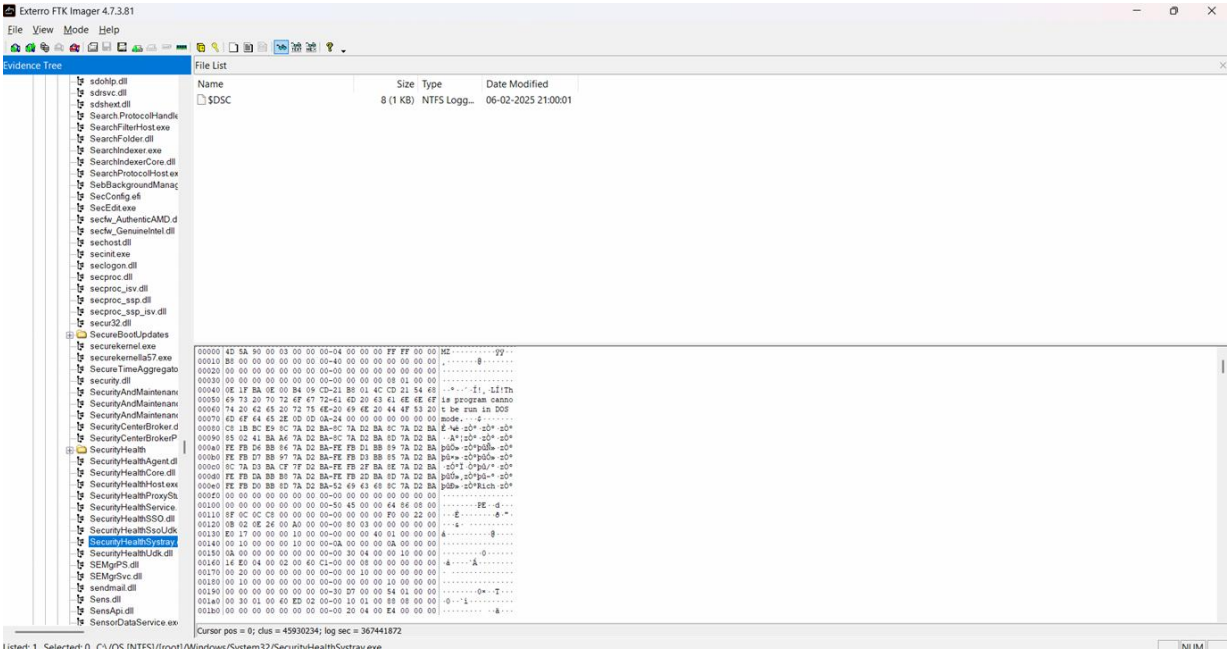
2) RunOnce

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:::
```

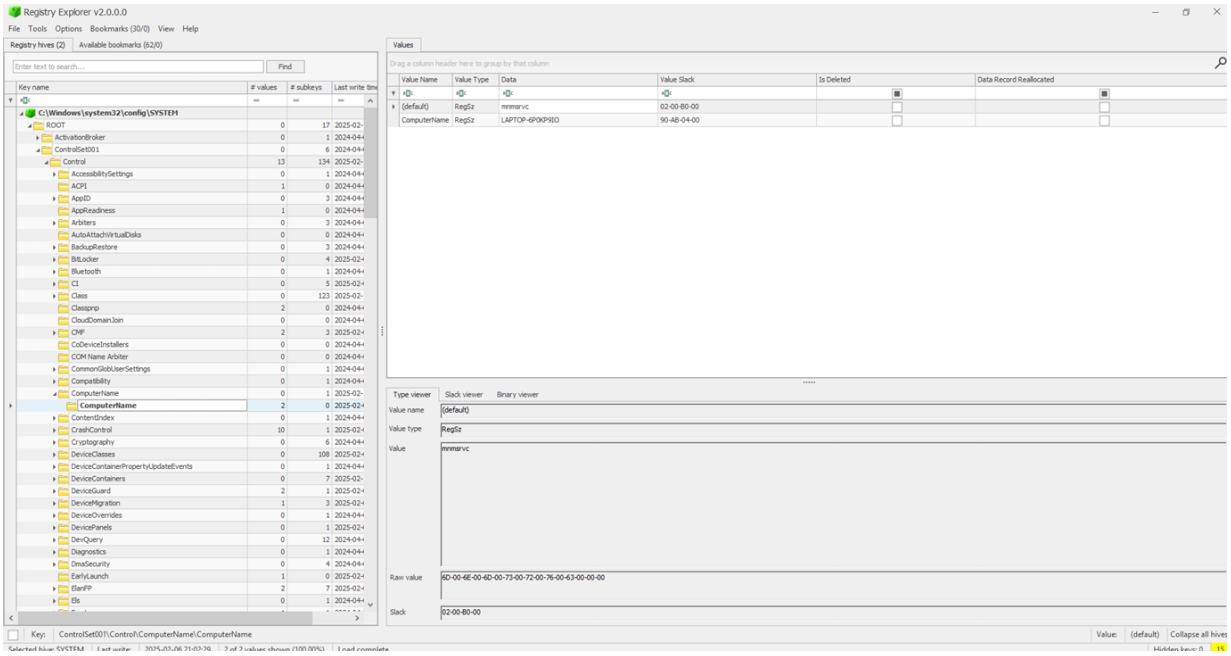
User Password Hash: BF649953377797E43DFBA64DCDF7C0FD

Section 2: Scenario & Questions

Q1: What is the computer name of the system?

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

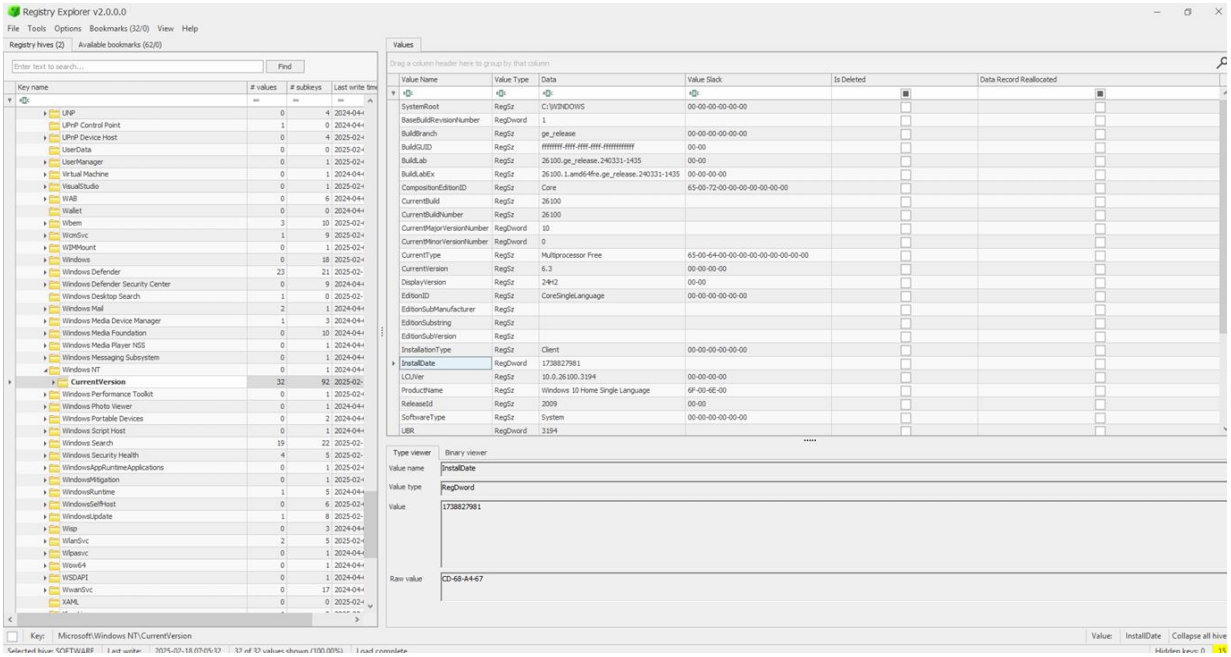
Computer Name:- LAKSHAY



Q2: What is the name of the Operating System?

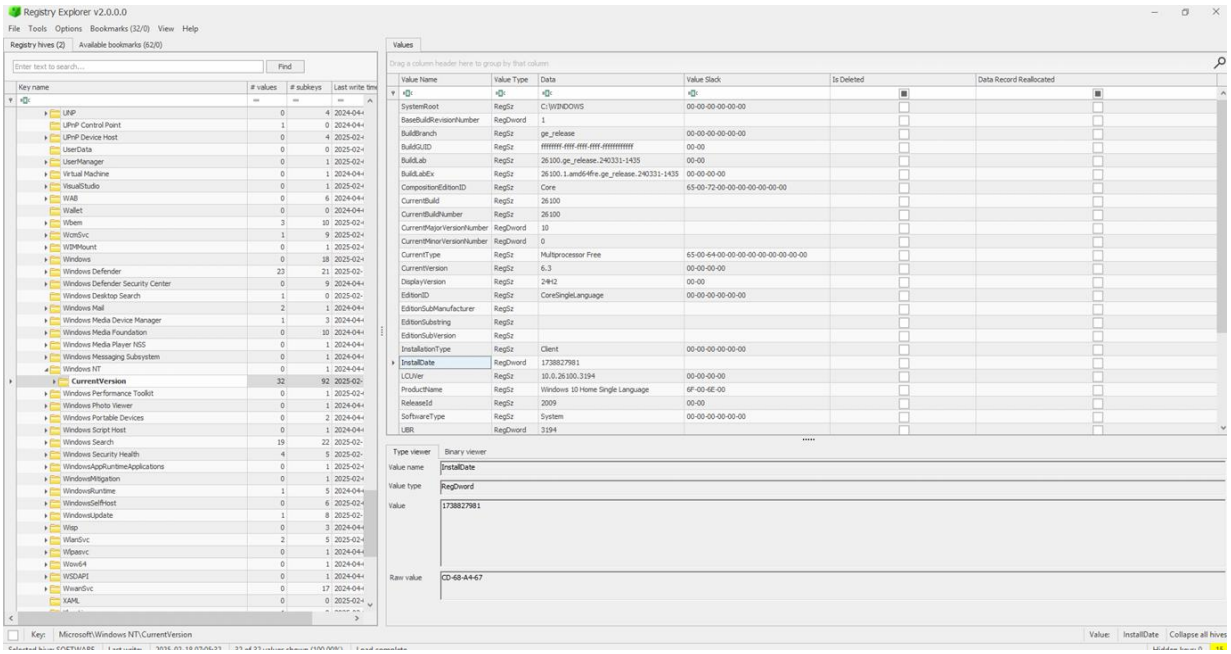
Key Path- SYSTEM: ControlSet001\Control\ComputerName\ComputerName

Name of the OS -Windows 10 Home Single Language

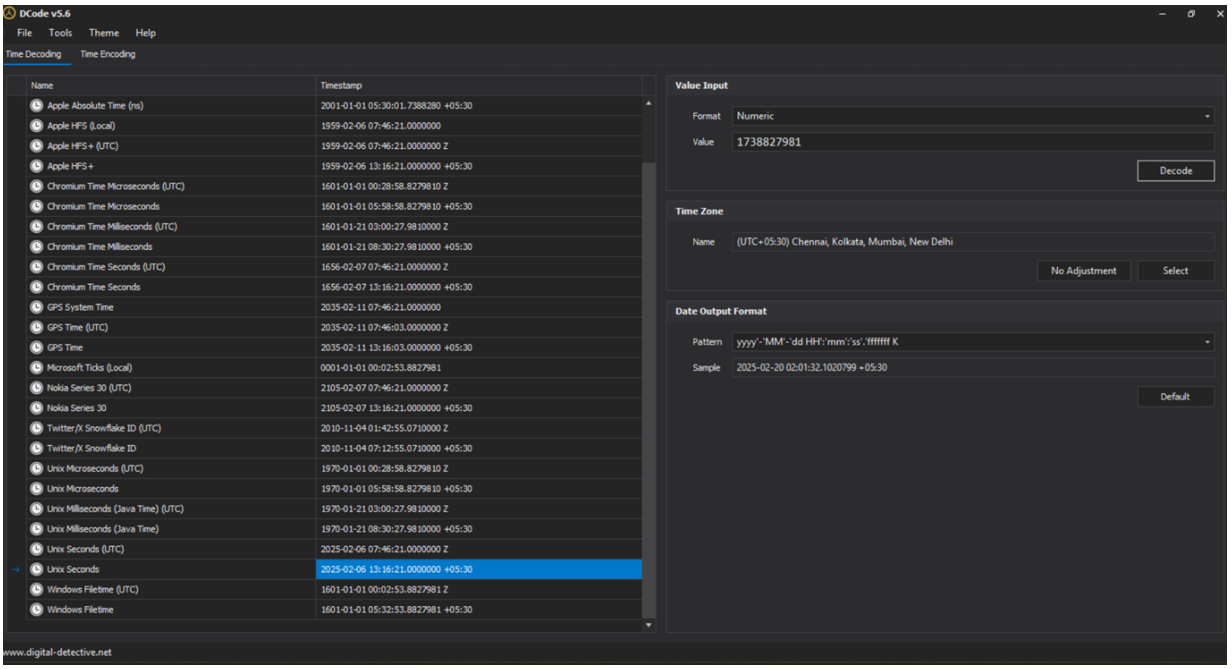


Q3: What date/time (in UTC) was the Operating System installed? Hint: you may have to convert epoch time to human readable time using the DCode tool.

Key Path- SOFTWARE: Microsoft\Windows NT\CurrentVersion

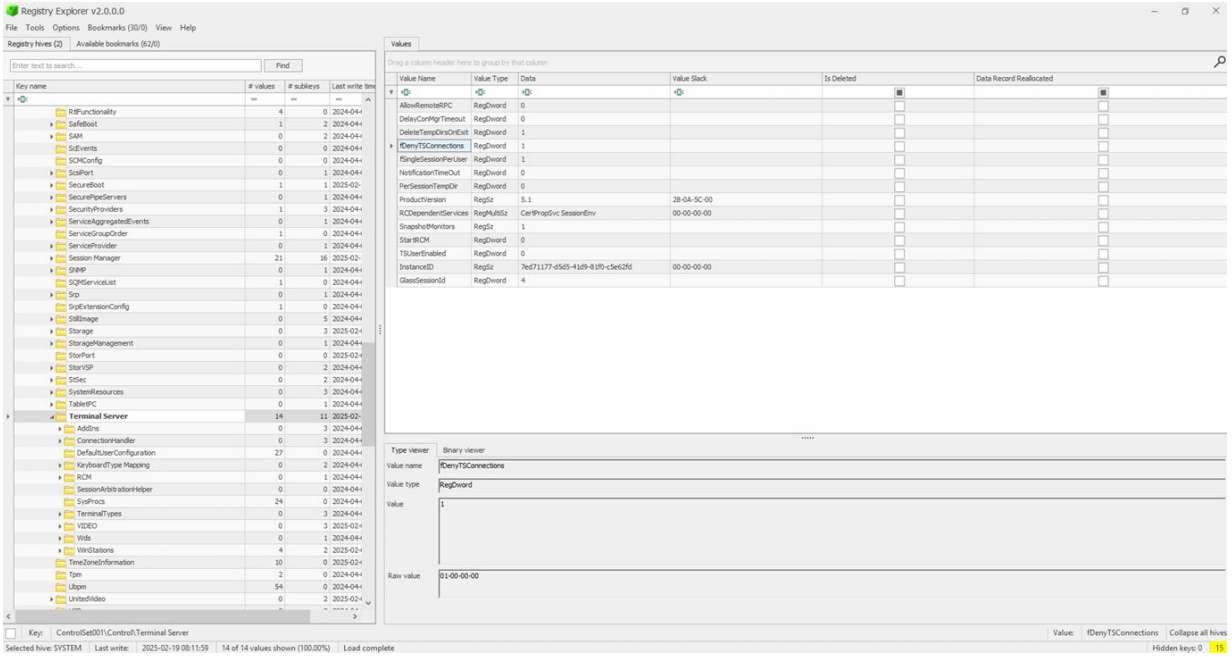


Decode Using DCode



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

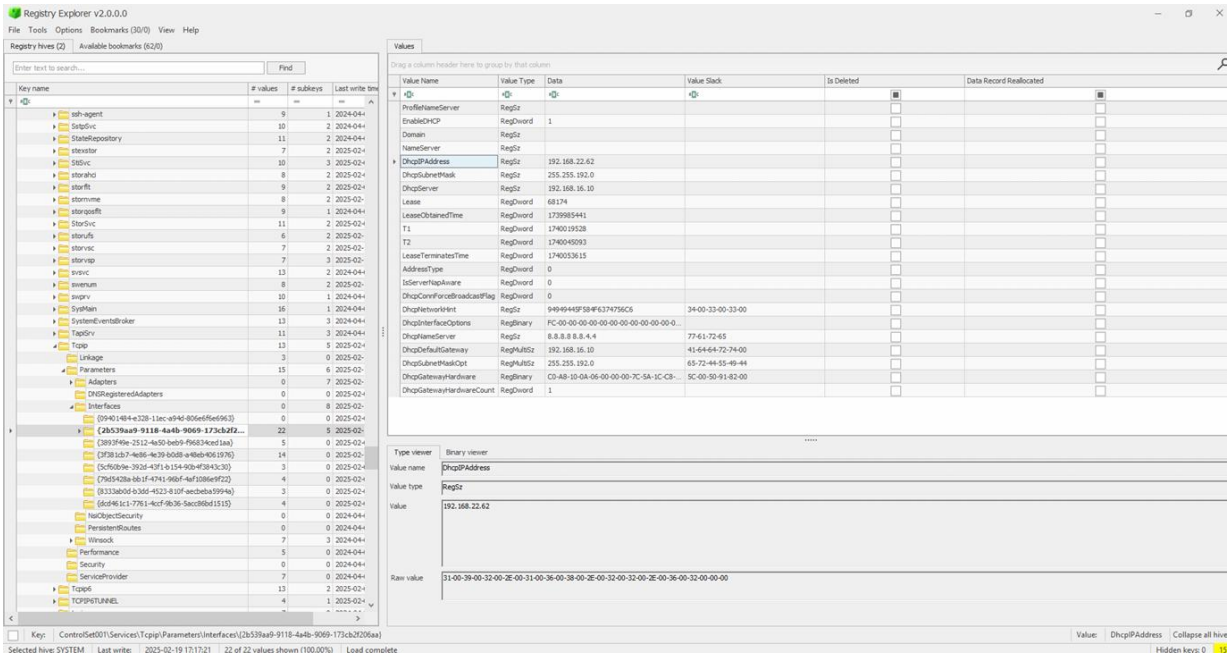
Key Path- SYSTEM: ControlSet001\Control\Terminal Server



Q5: What is the IP address of the system?

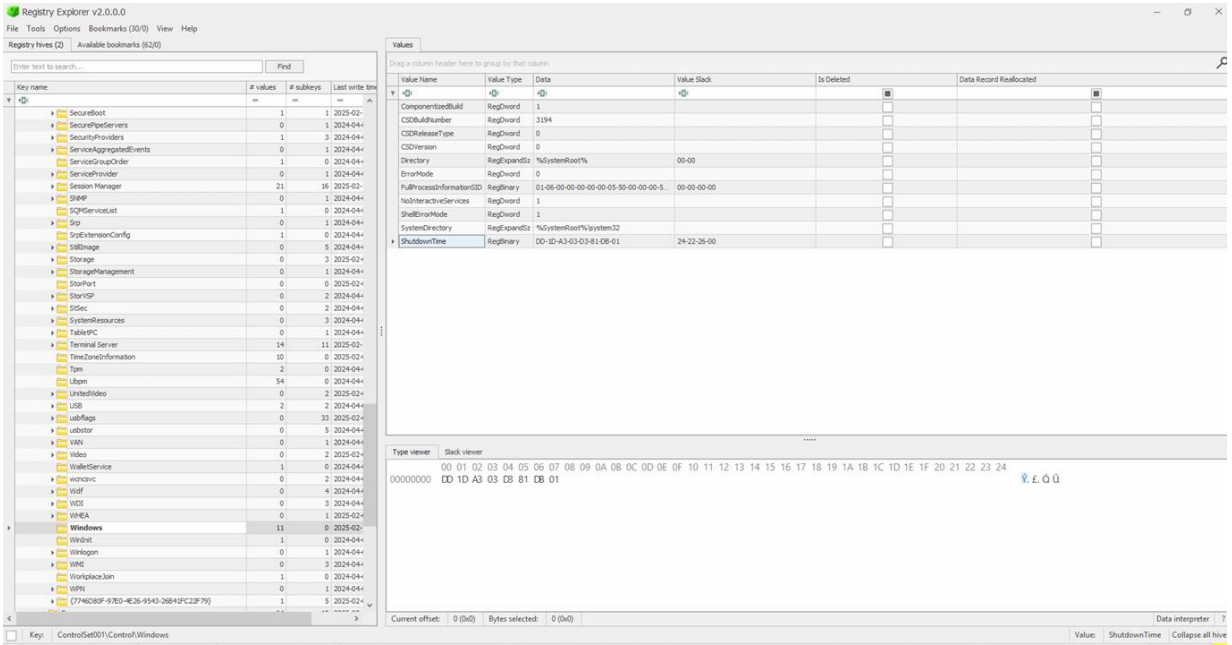
Key Path
System\ControlSet001\Services\Tcpip\Parameters\Interfaces\{2b539aa9-91118-4a4b -9069-173cb2f206aa

DhcpIpAddress: 192.168.249.29

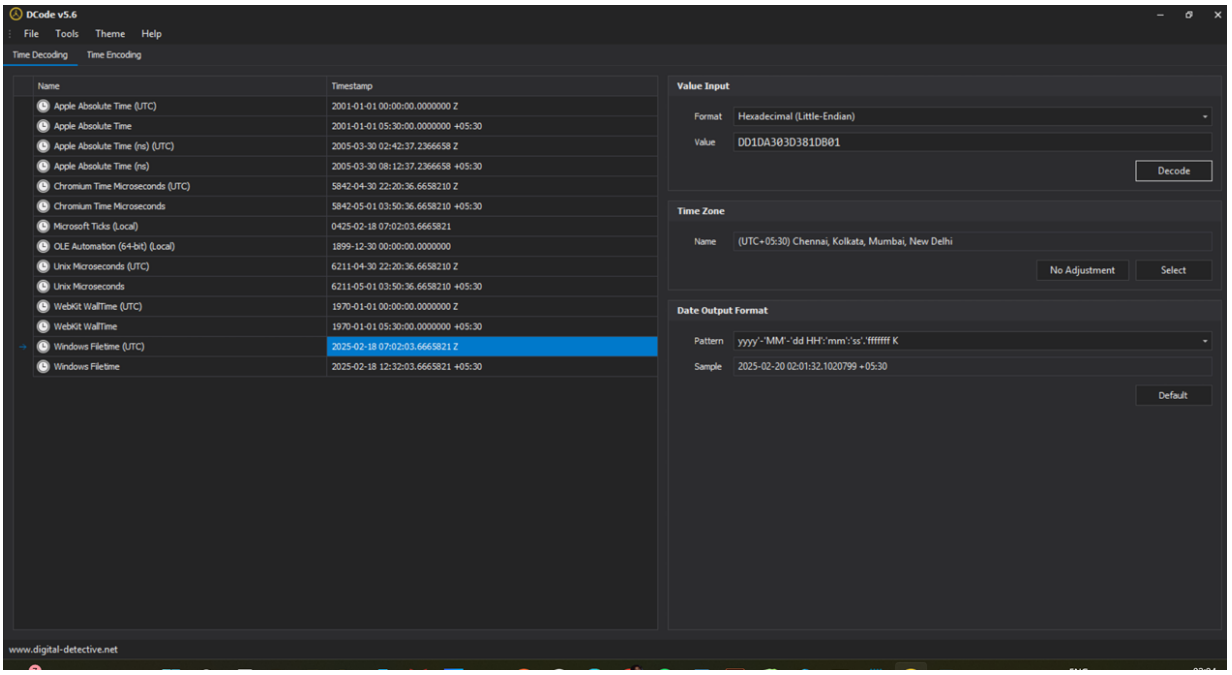


Q6: When was the system last shutdown?

Key Path- SYSTEM: ControlSet001\Control\Windows

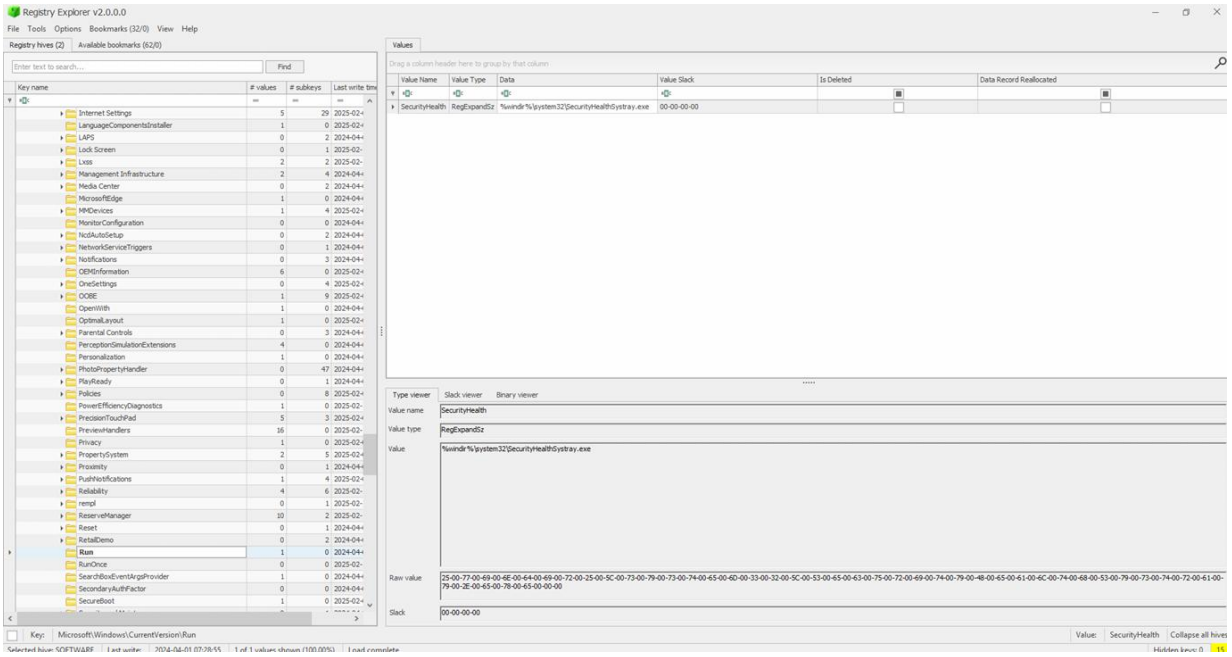


Decode using DCode



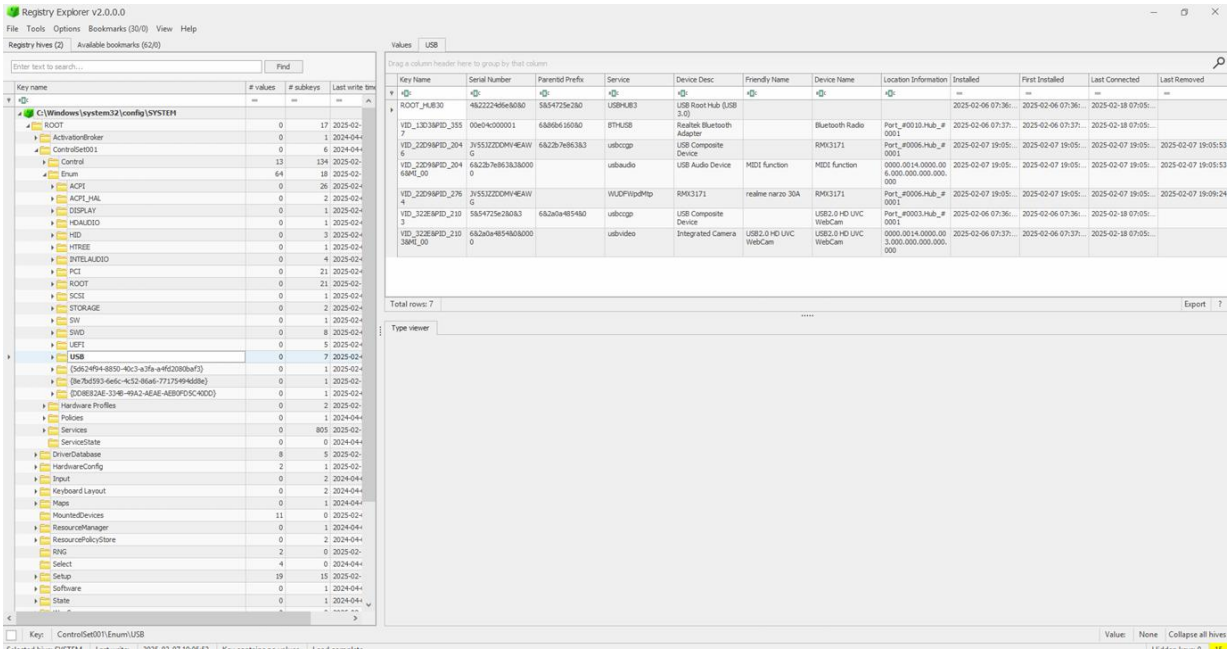
Q7:List out program names launching at startup.

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

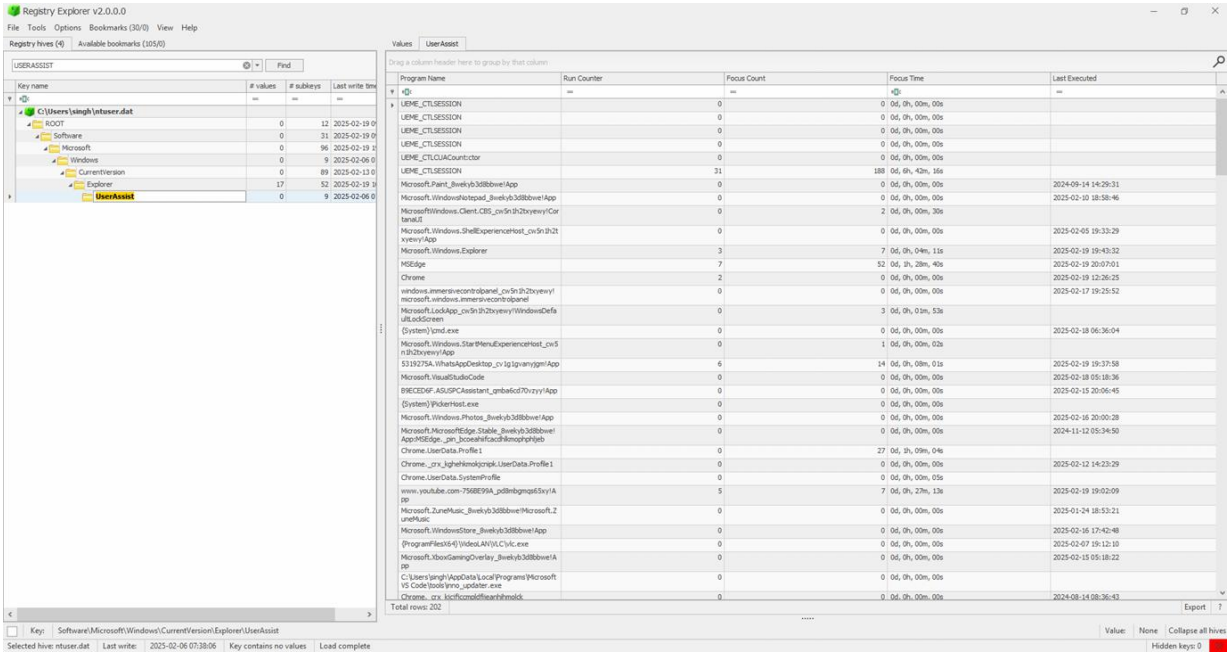


Q8: What are the name of USB drives (drive letter & volume information) you have plugged in to your system?

Key Path- SYSTEM: ControlSet001\Enum\USB



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.



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**