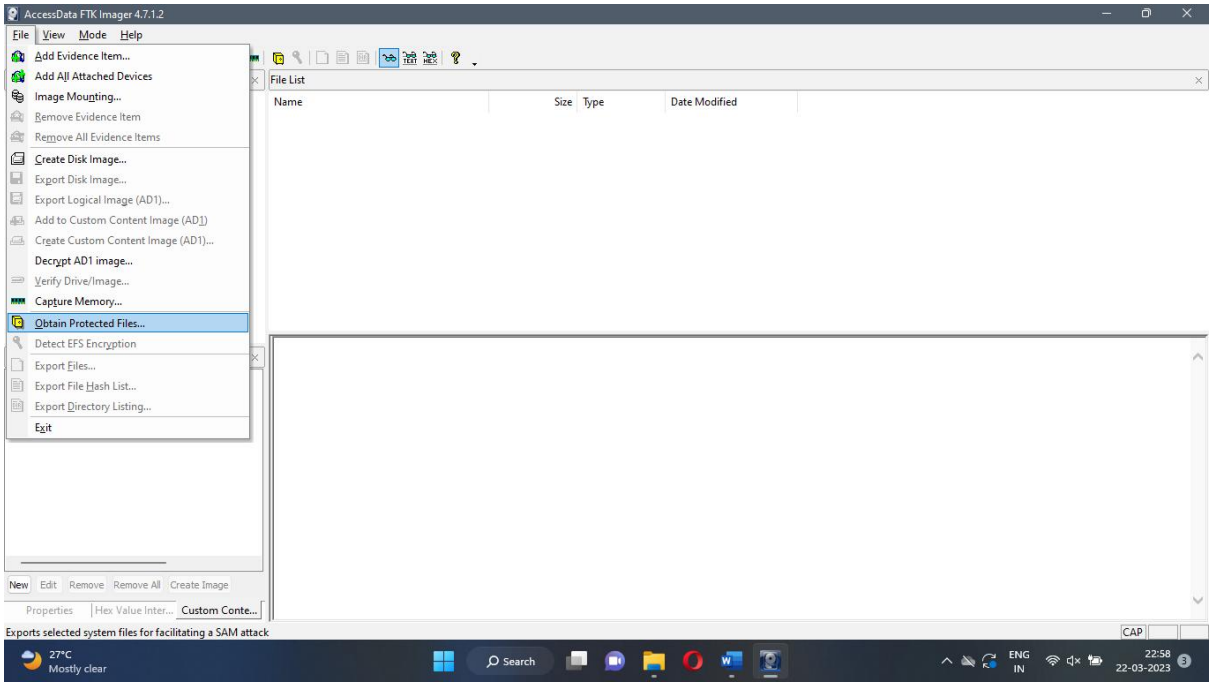
Digital Forensics

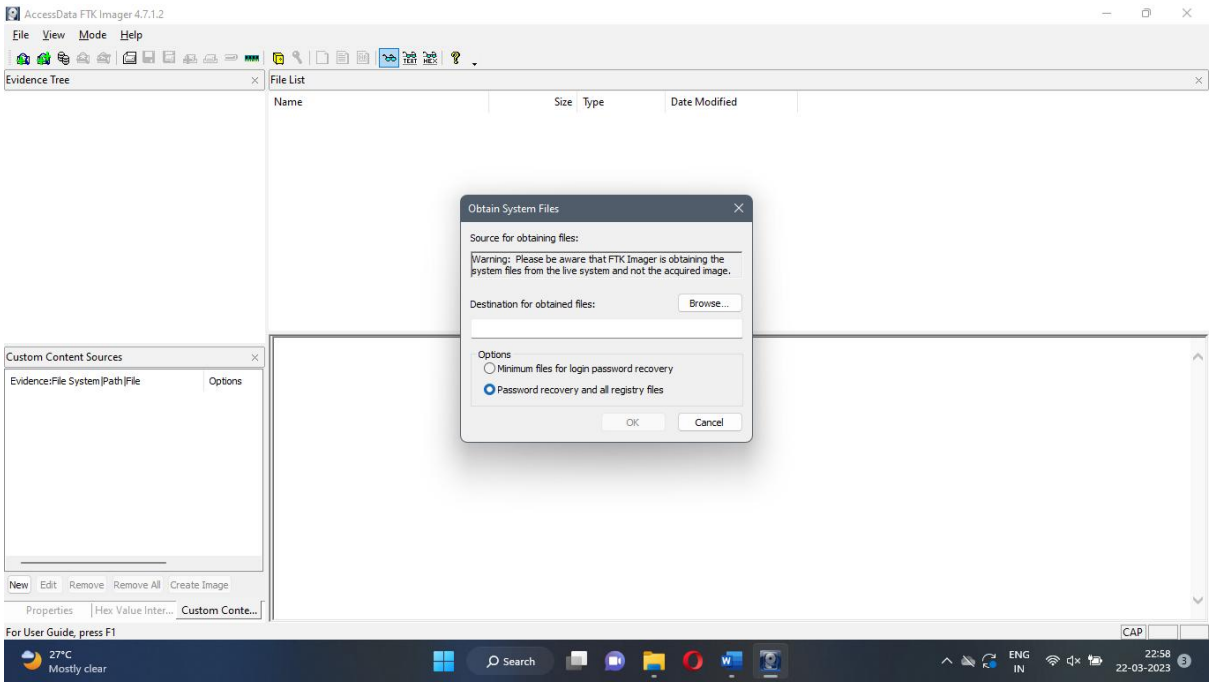
SRN : PES1UG20CS825	NAME : PREM SAGAR J S	SEC : 'H'

Lab Assignment - 8

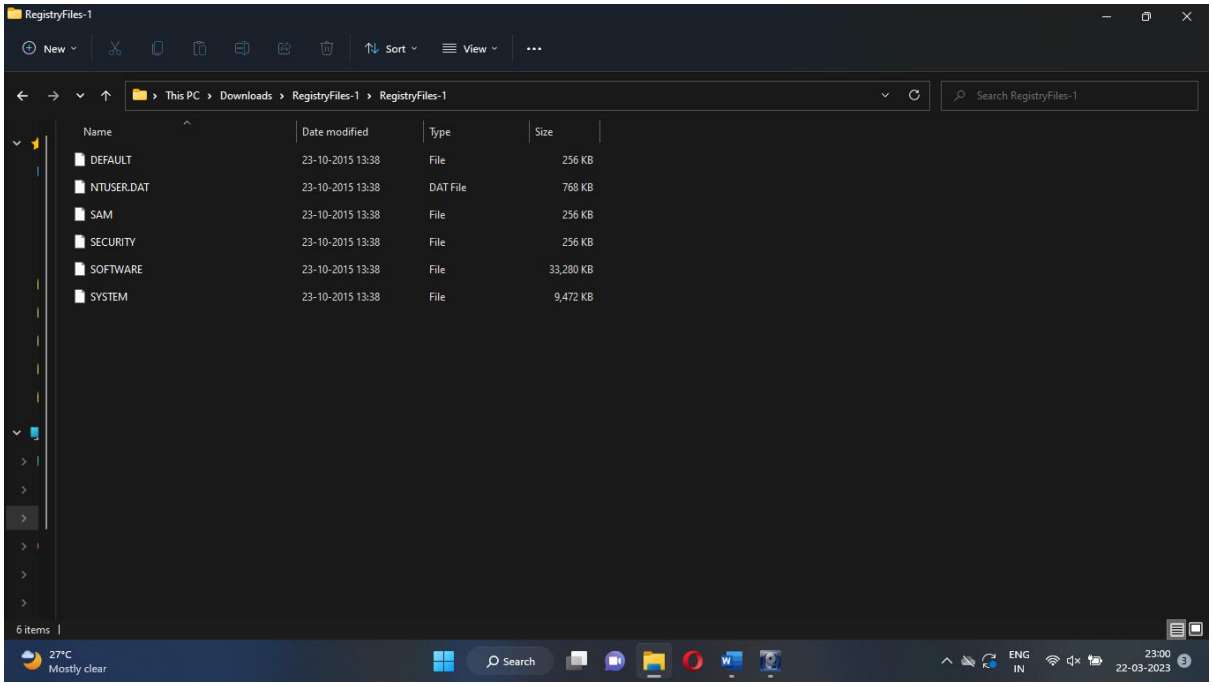
- Open FTK Image, and go to the File menu ➤ Obtain Protected Files…



- A new dialog appears; select where you want to store obtained files, and check the option "Password recovery and all registry files". Finally, click the "OK" button.

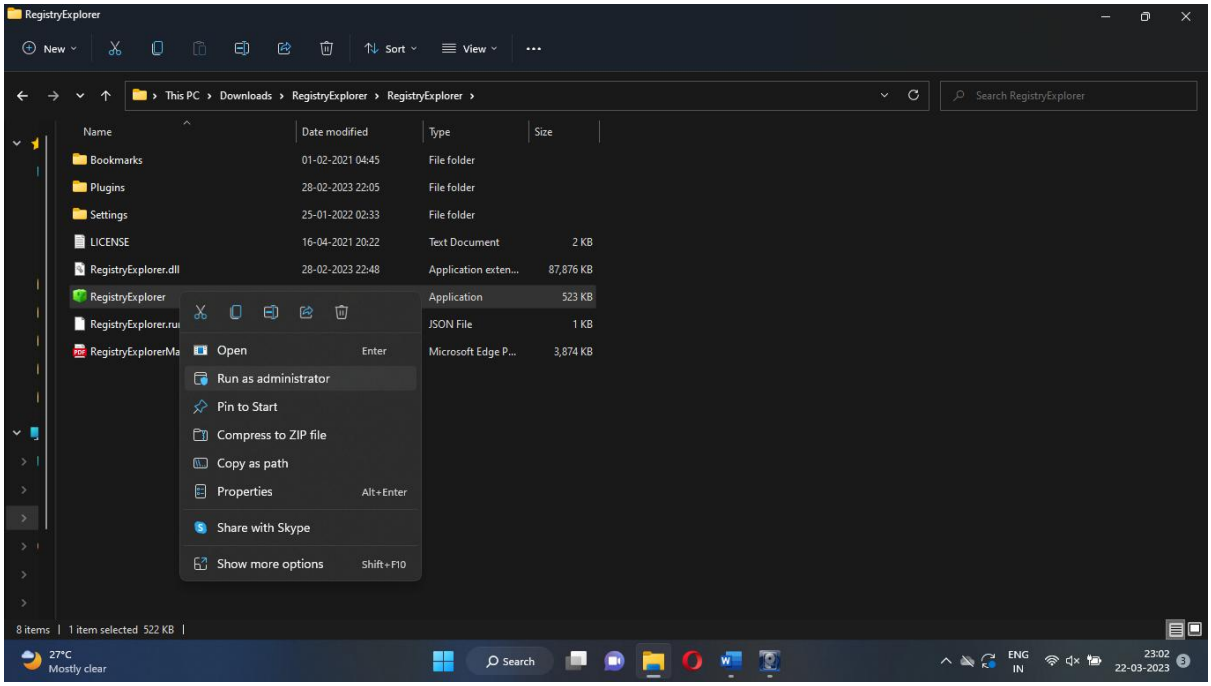


- A progress window will appear showing registry files' export progress; upon finishing, the window will disappear without announcing any success message. Go to the directory where you have saved your registry files to see the resultant files; you should see the five files and one folder.

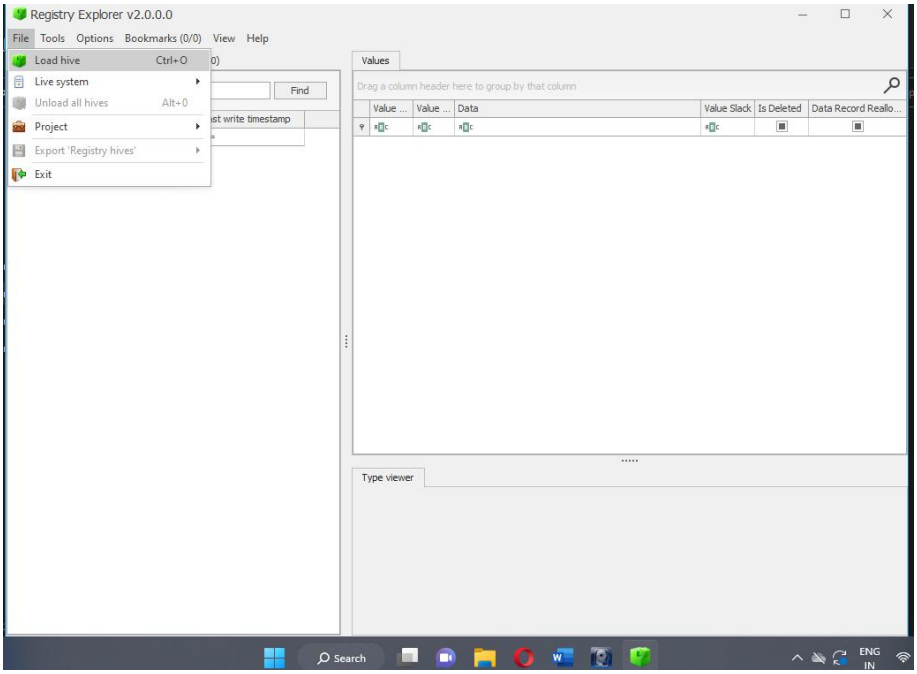


<u>Analyzing extracted registry hives using registry explorer tool</u>

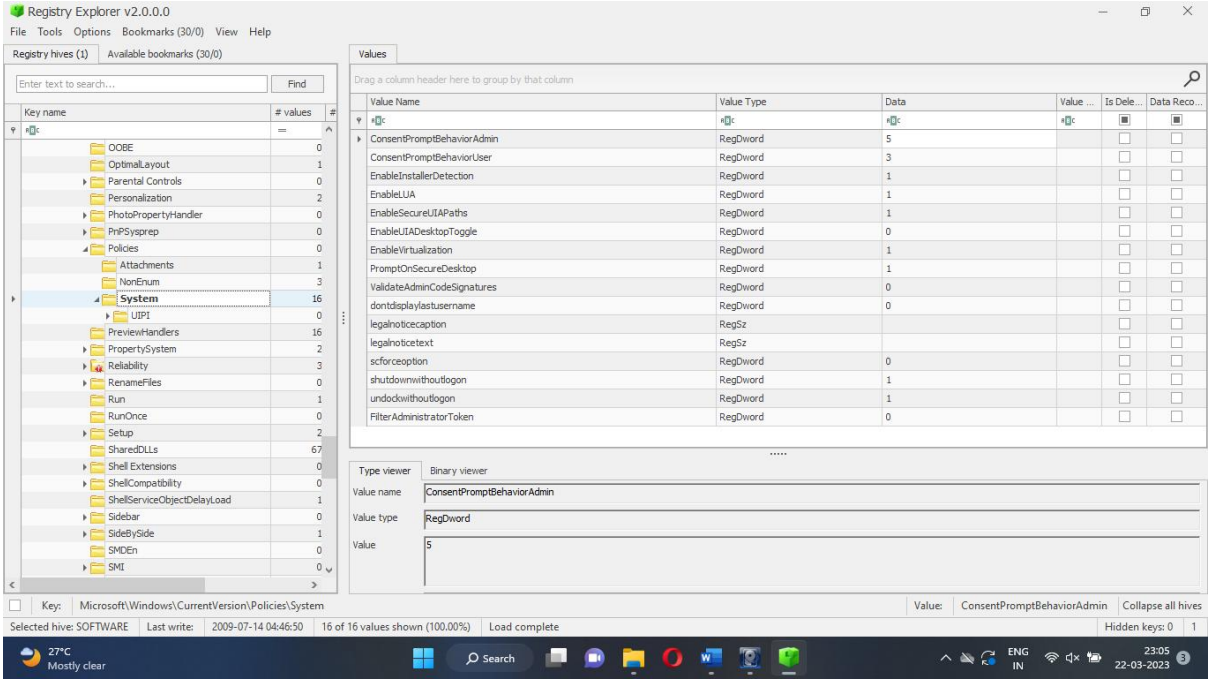
- Download the file called "RegistryFiles-1.zip" and extract the contents of the compressed file to your desktop.
  Right-click the registry explorer tool and select run as administrator.



- To load a hive into registry explorer, select file, Load Hive, and select the path to the “software” hive present in the RegistryFile-1 folder.

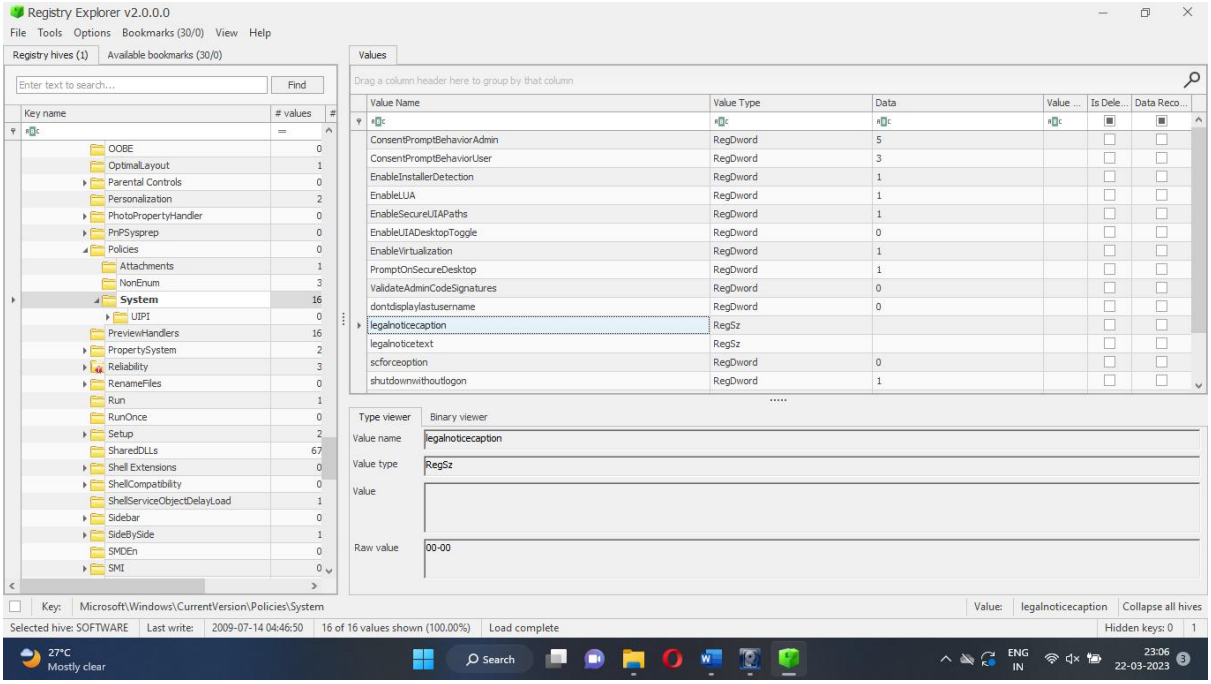


- Confirm the logon banner contained within the Windows Registry of the software hive by navigating down to the following Registry key:
  \Microsoft\Windows\CurrentVersion\Policies\System

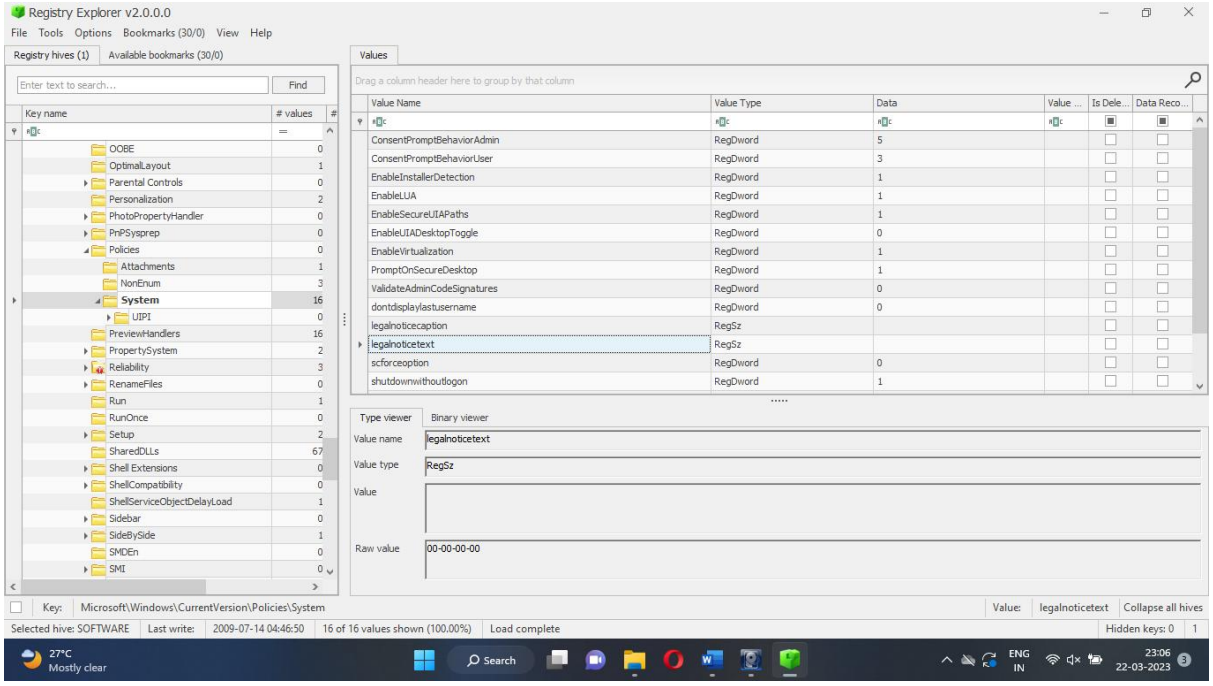


- navigating down to the key, the path will be displayed. Notice two keys: legalnoticecaption and legalnoticetext. The former would contain the text value, which appears in the title bar of the consent banner. The latter is the actual message contained within the body of the consent banner.

Legalnoticecaption :

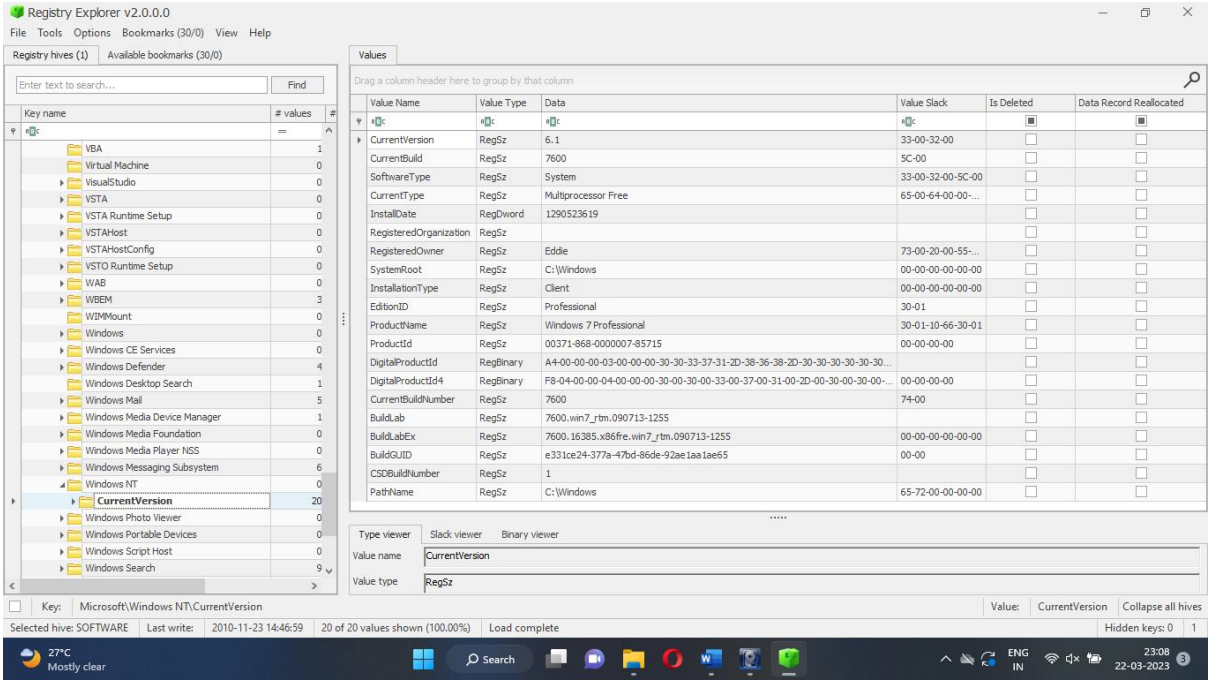


Legalnoticetext:



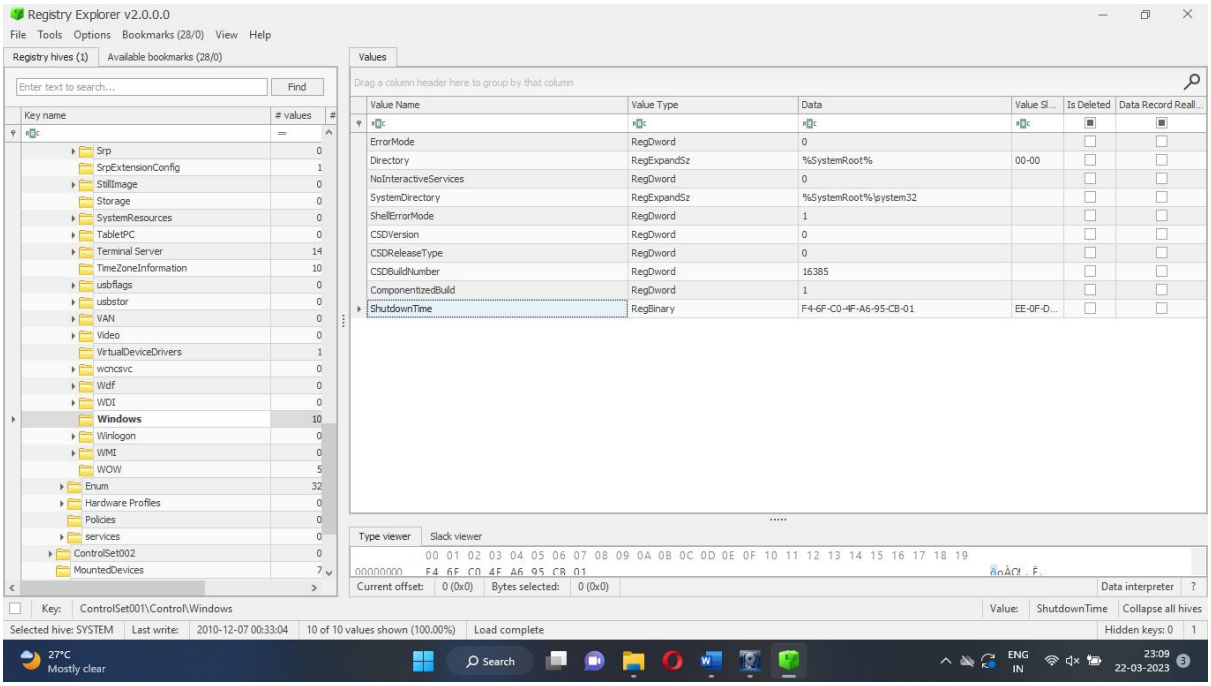
- Navigate to the following key to identify the installation information for the versions of Windows:

  Microsoft\Windows NT\CurrentVersion



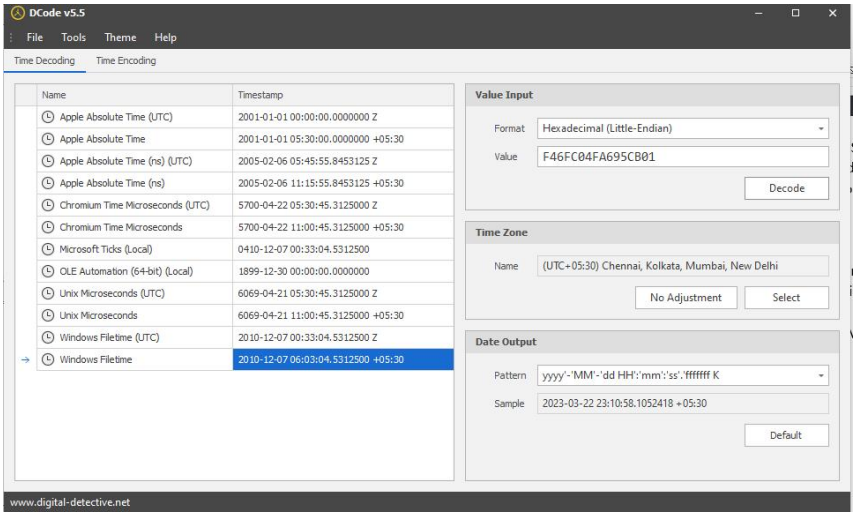
- Open the "SYSTEM" hive using registry explorer and find the "CurrentControlSet". Navigate to the following subkey:

  CurrentControlSet001\Control\Windows



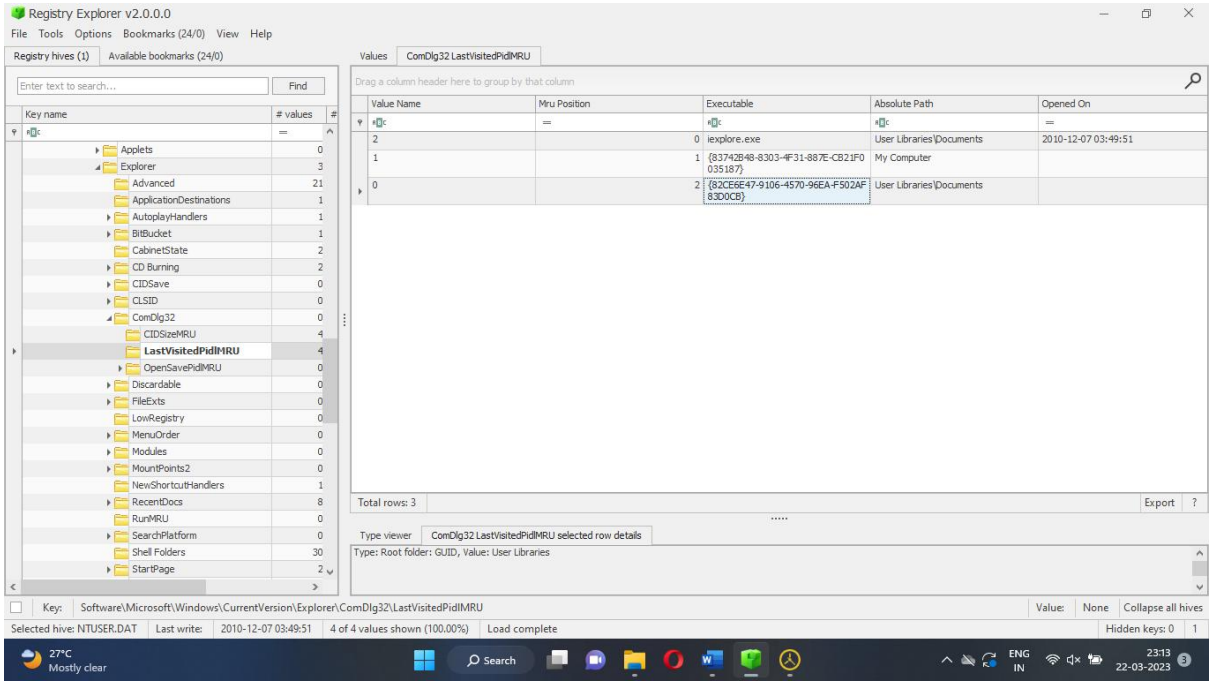
- Using the Dcode tool, convert the hexadecimal time to IST. You can download the tool from the following link - Dcode v5.5 (https://www.digital-detective.net/dcode/).

  The input format is Hexadecimal (Little Endian), Time Zone as New Delhi and click decode.



- Identify the executable files that have been executed sometime back in the target system. Open the "NTUSER.DAT" found on the user profile and navigate to the given subkey:

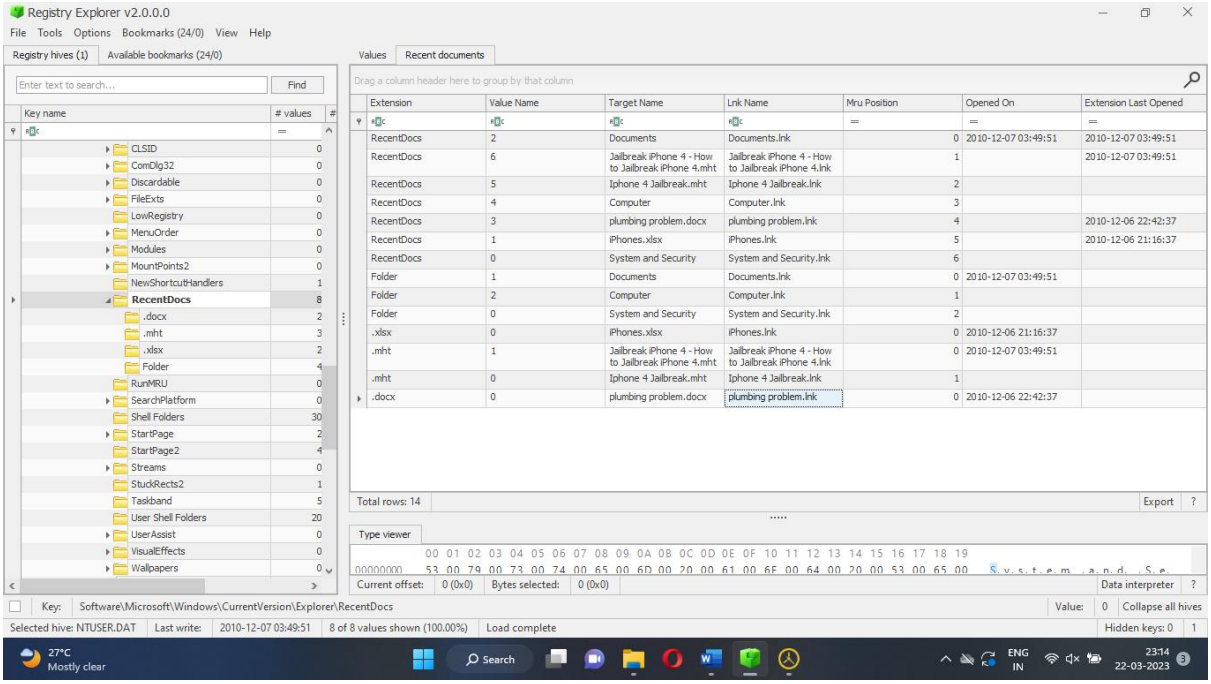
  Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPIDlMRU



- Identifying the files that have been recently accessed.

  Open the "NTUSER.DAT" found on the user profile and navigate to this subkey:

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

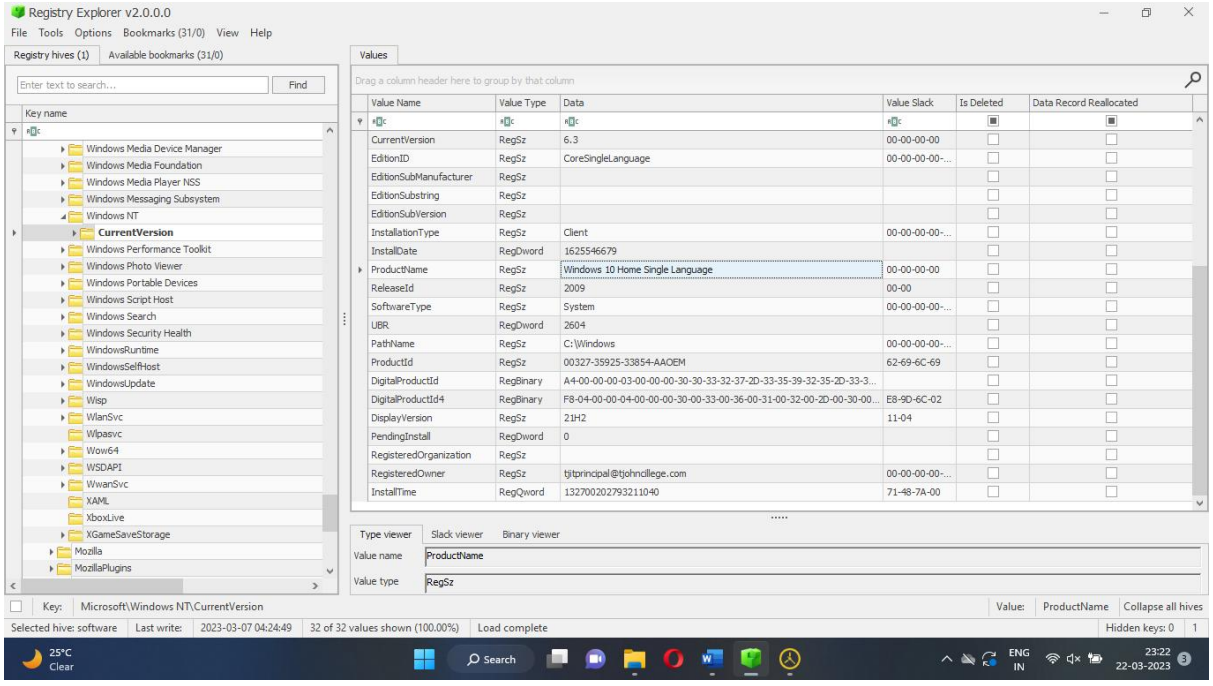


Hands-On Project

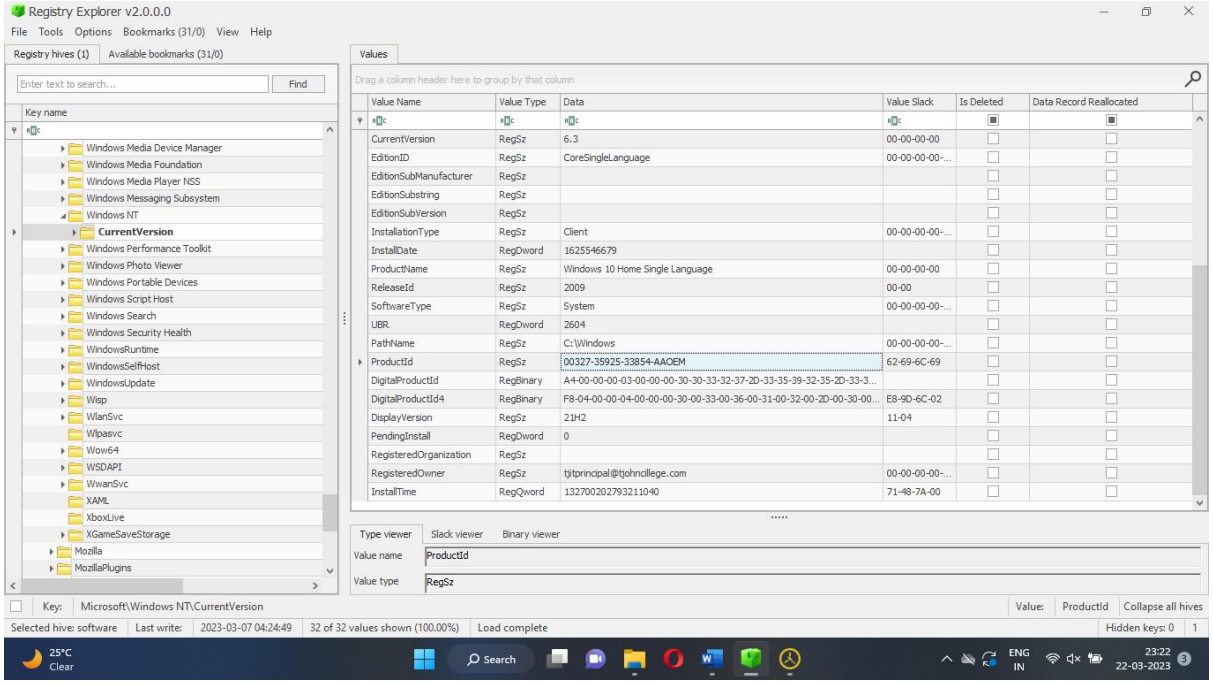
Analyze the given image and answer the following questions:

- What is the name of the Windows product?

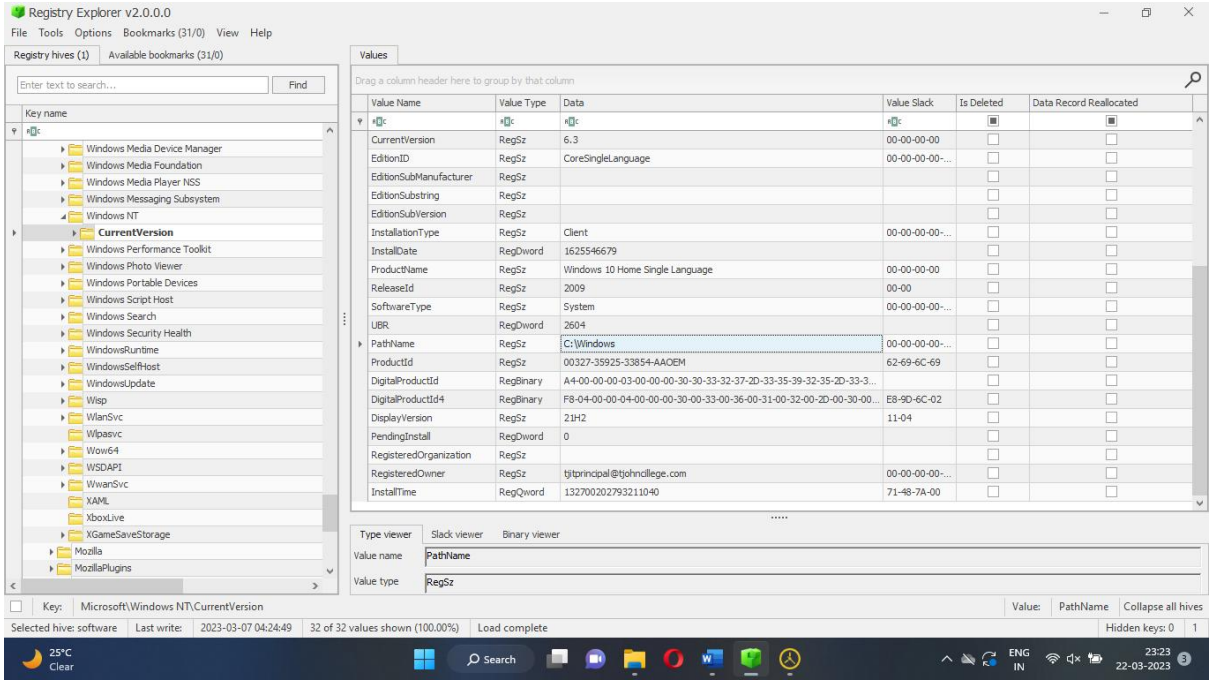
  => Windows 10 Home Single Language



- What is the product ID number?
  =>00327-35925-33854-AAOEM

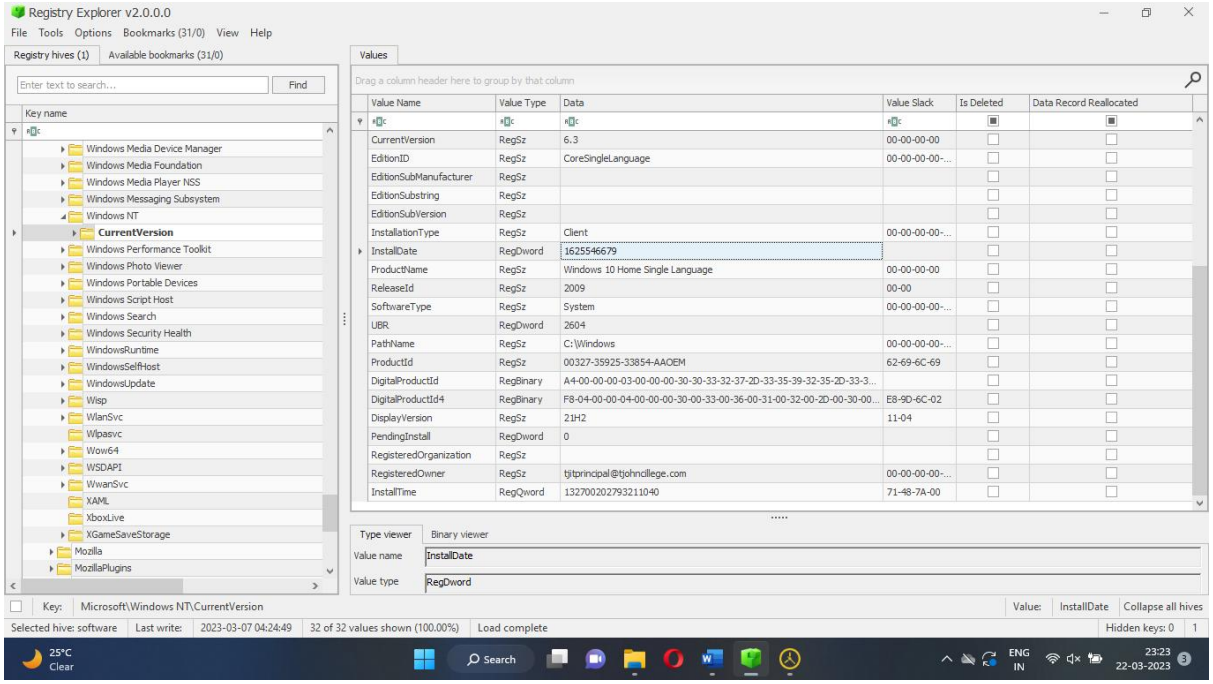


- In what directory on the system is the operating system running?
  =>C:\Windows

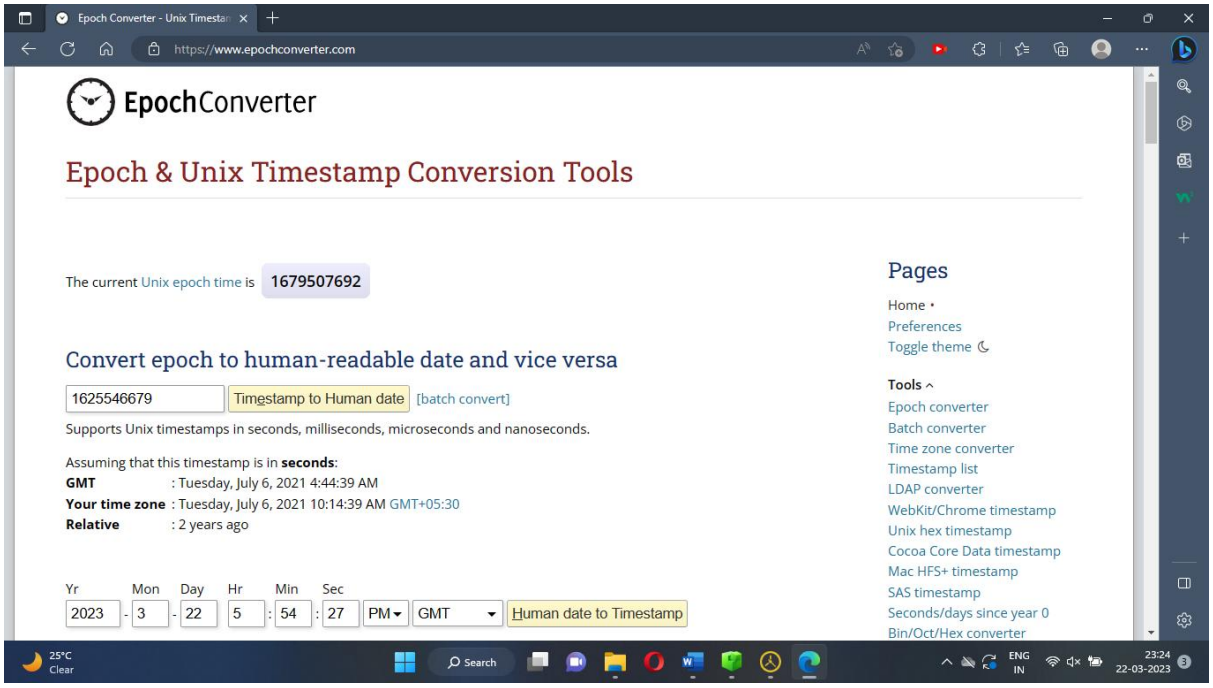


➢ When was the operating system installed?

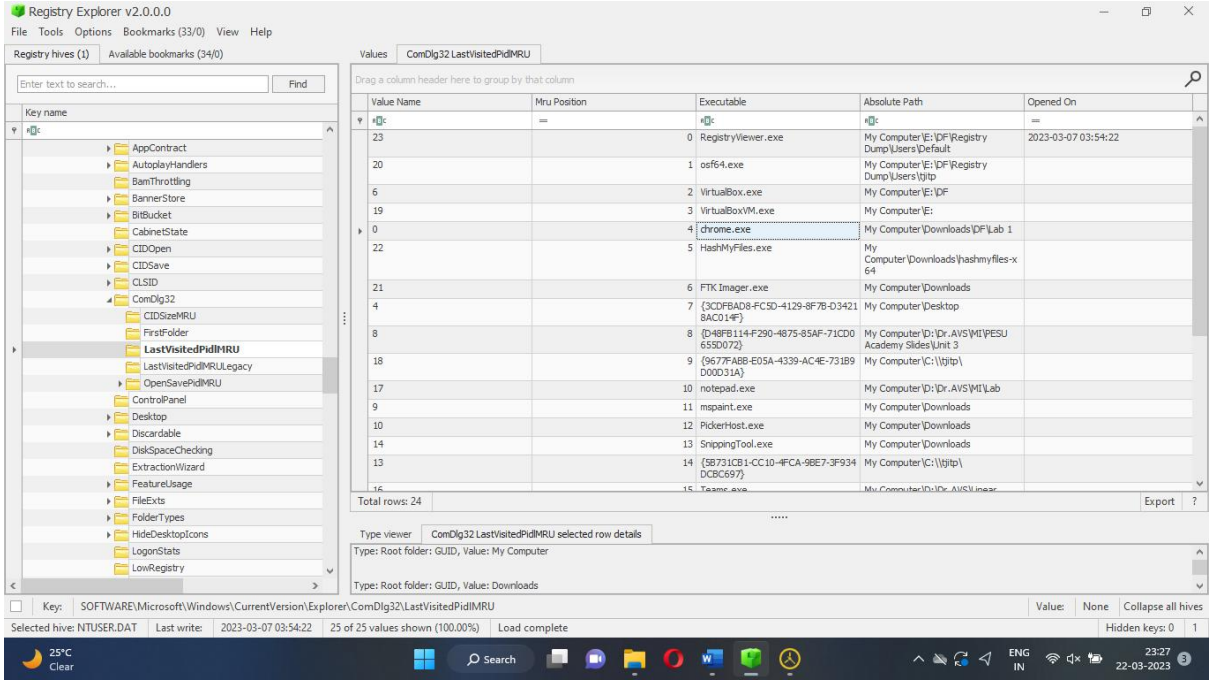
Based on the Registry, the installation date is listed as 1625546679 (, which is a timestamp recorded in Epoch time. Using a resource, such as www.epochconverter.com, converts the value to March 22, 2023 at 16:56:17 GMT.)



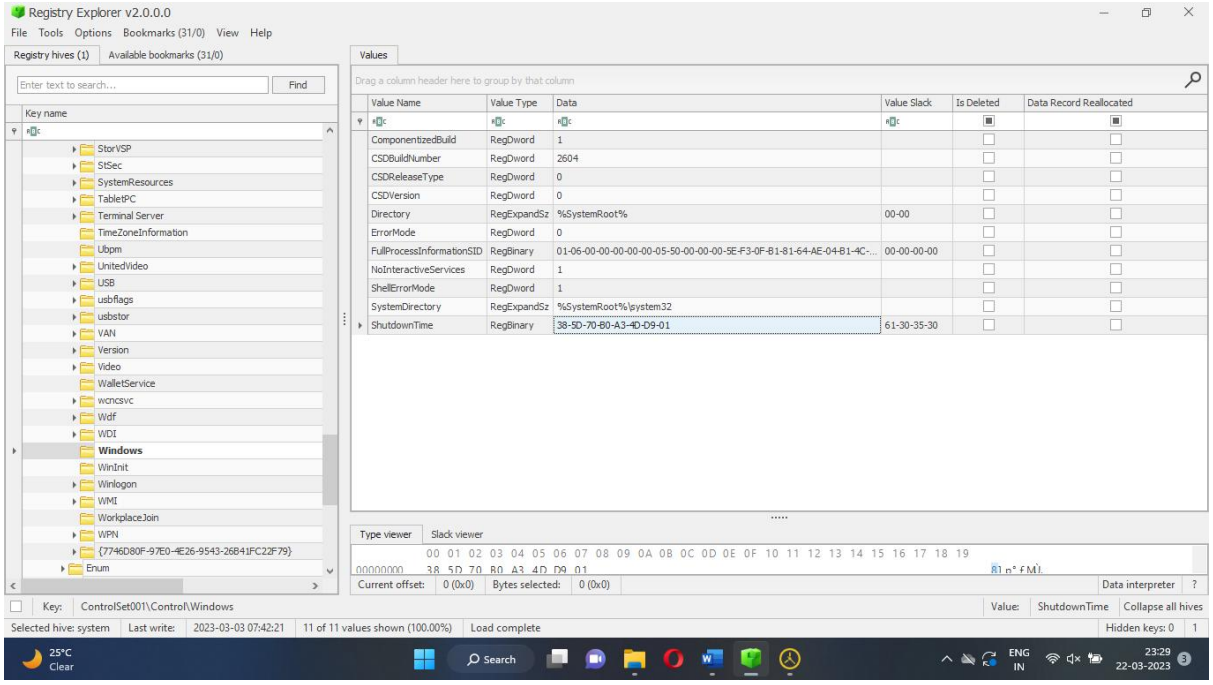
Decoding the TimeStamp



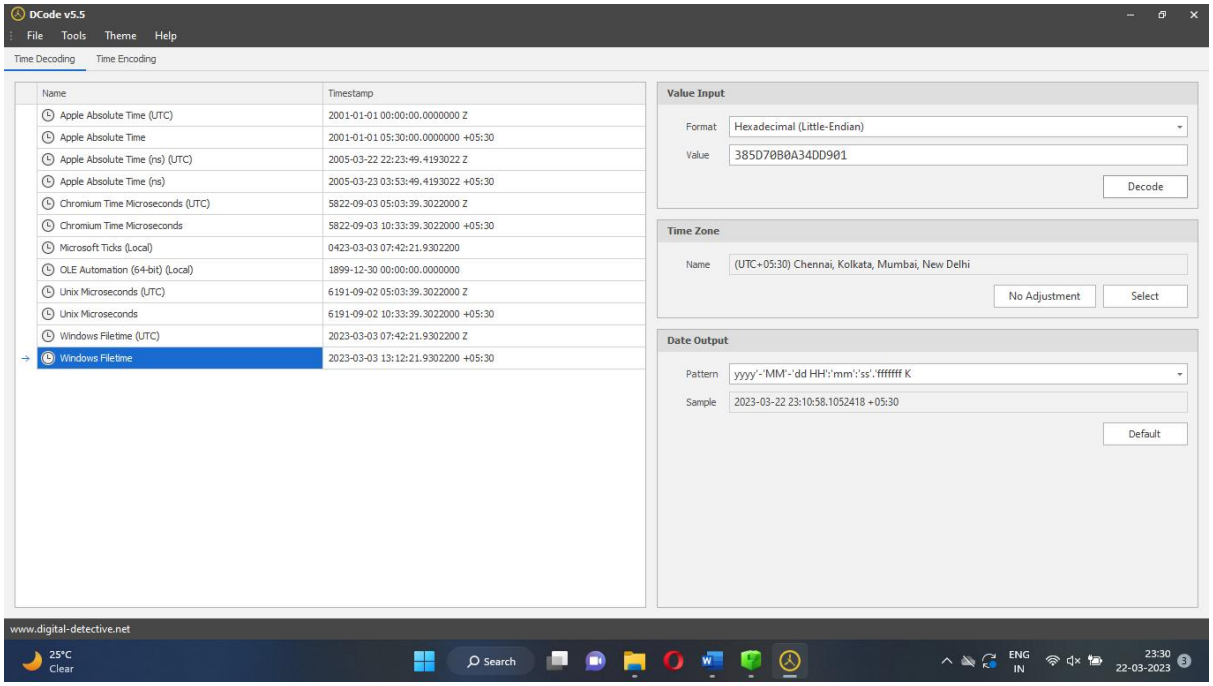
➢ Identify the executable files that have been executed in the target system.



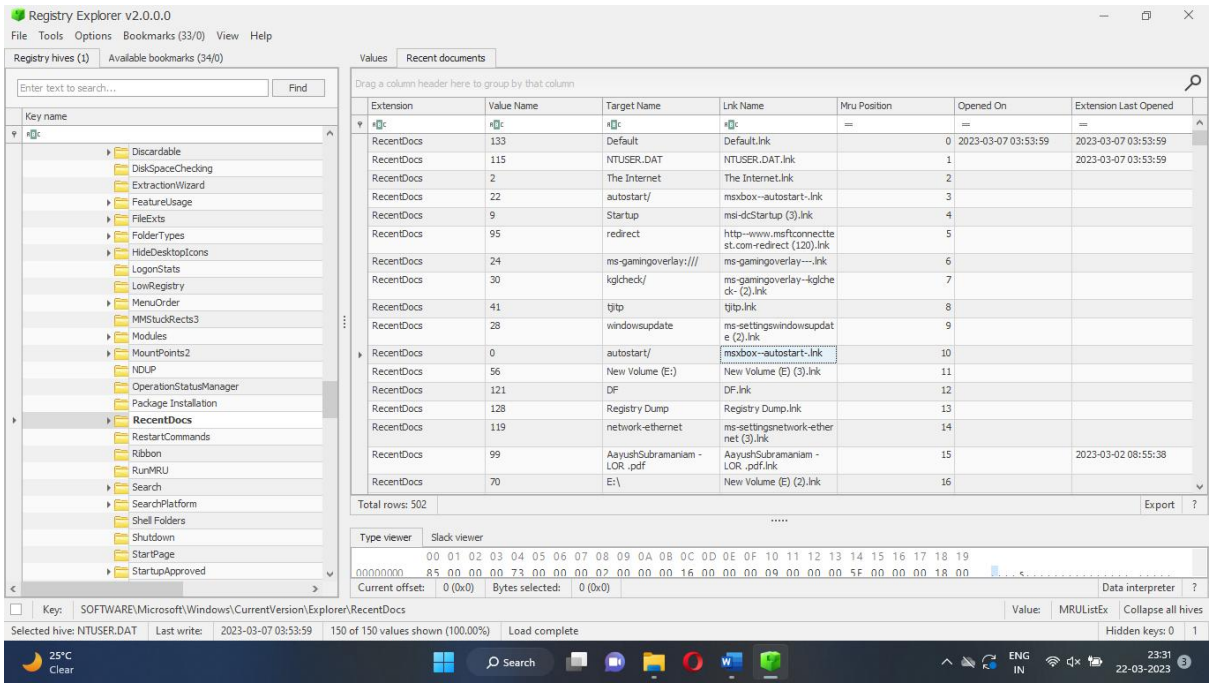
➢ What was the last shutdown time of the target system?



Using the Dcode Software to Decode the Shutdown Time



➢ What files have been recently accessed?



==========**********==========