

Digital Forensics

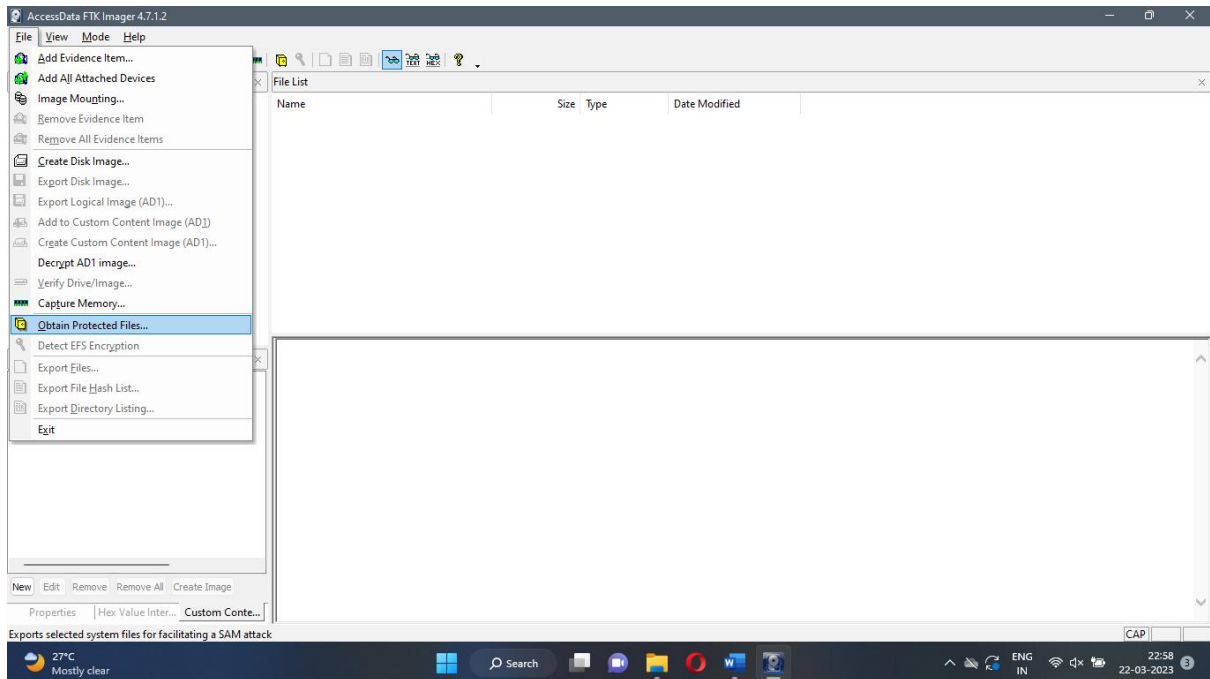
SRN : PES1UG20CS825

NAME : PREM SAGAR J S

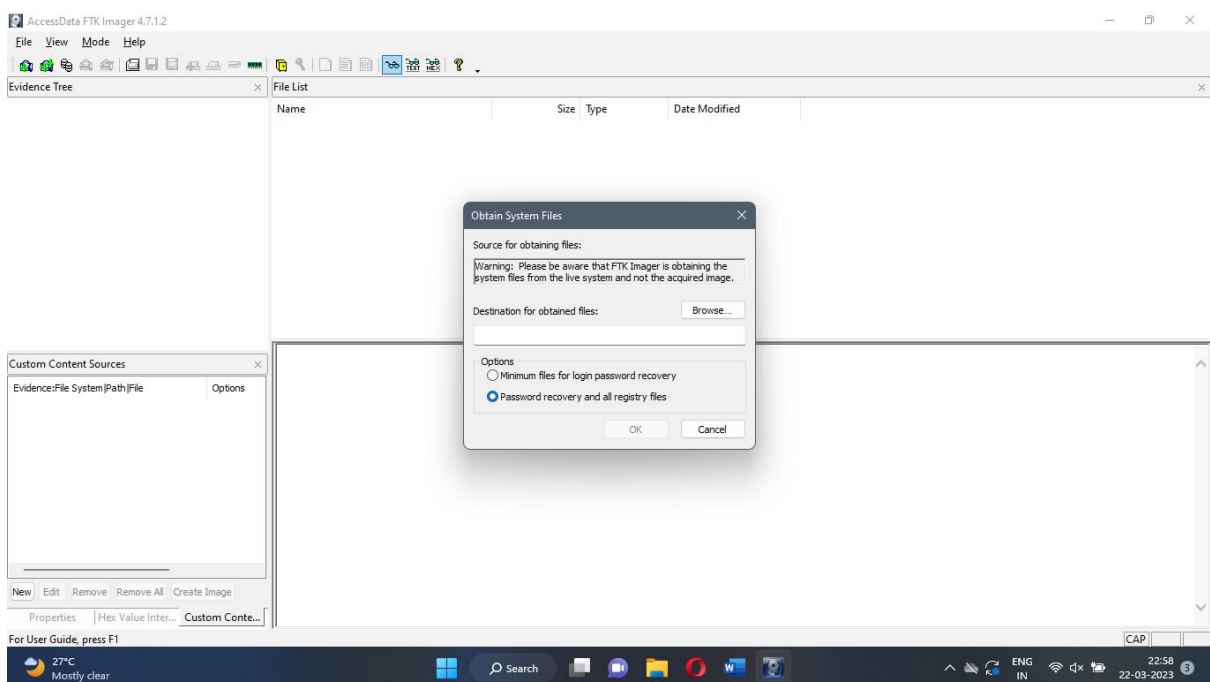
SEC : 'H'

Lab Assignment - 8

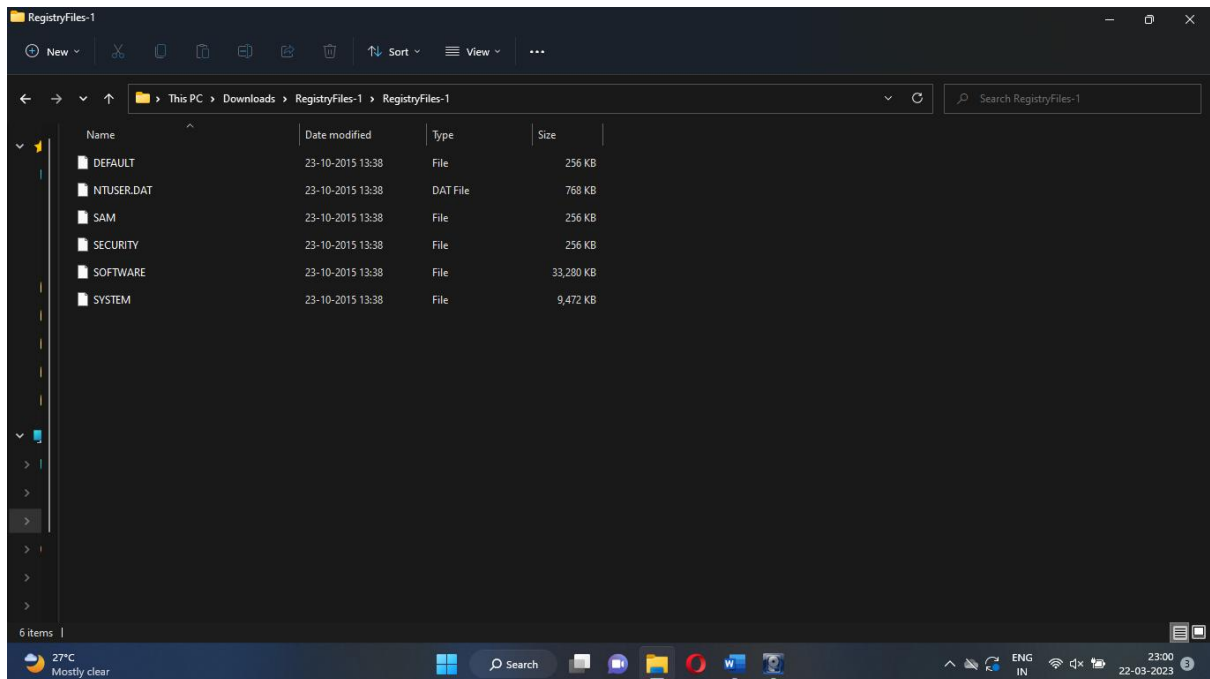
- Open FTK Image, and go to the File menu ➤ Obtain Protected Files...



- 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.

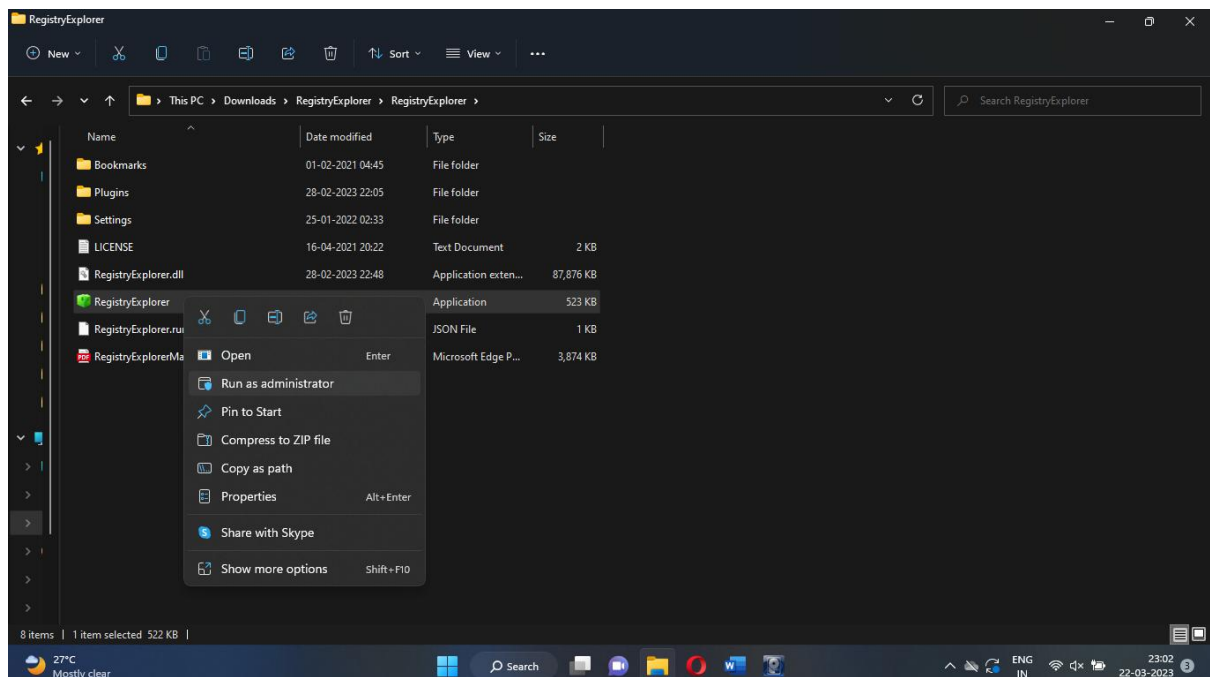


- A progress window will appear showing registry files' export progress; upon finishing, the window will disappear without announcing any success message. Go to the directory where you have saved your registry files to see the resultant files; you should see the five files and one folder.

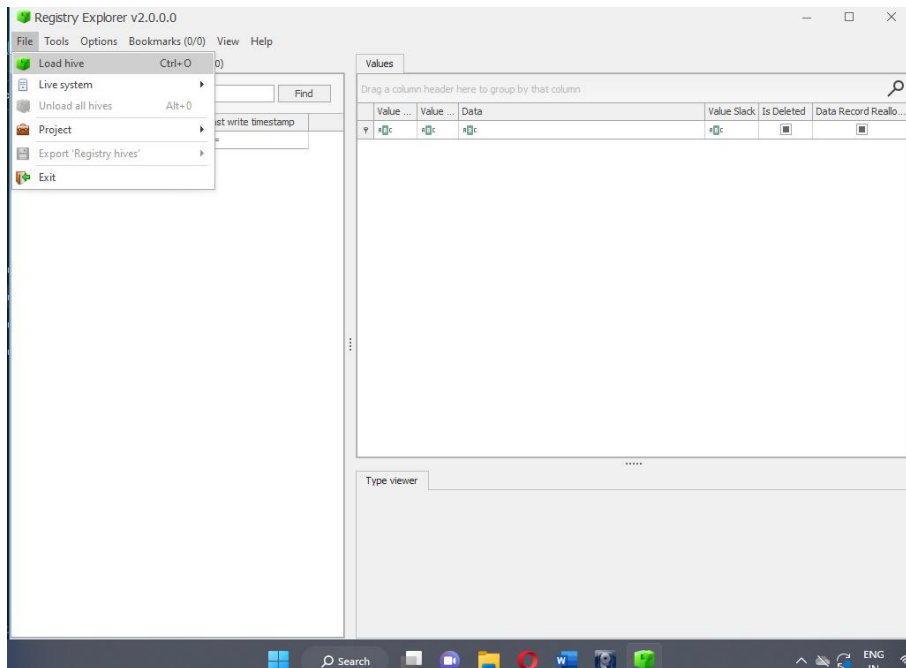


Analyzing extracted registry hives using registry explorer tool

- 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.

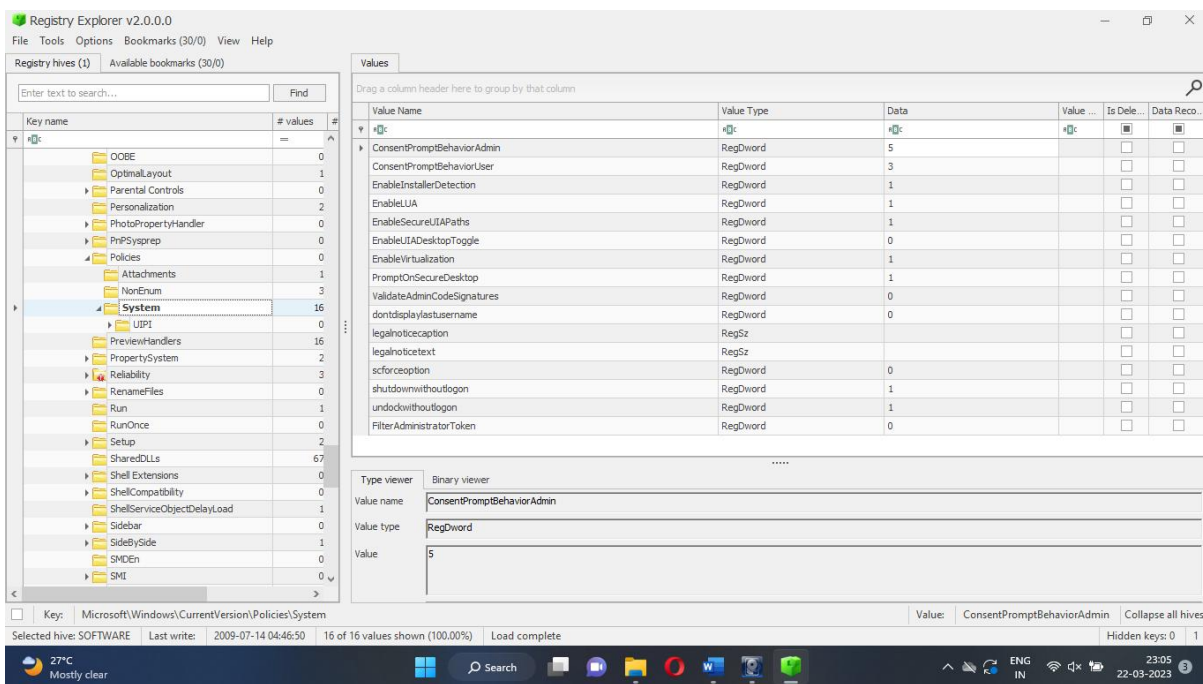


- To load a hive into registry explorer, select file, Load Hive, and select the path to the “software” hive present in the RegistryFile-1 folder.



- 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 :

The screenshot shows the Registry Explorer v2.0.0.0 interface. The left pane displays the tree structure of the registry, with the path `Microsoft\Windows\CurrentVersion\Policies\System` selected. The right pane shows the values for this key. The `legalnoticecaption` value is highlighted, and its details are shown in the bottom pane. The value is a `RegSz` type with a raw value of `00-00`.

Value Name	Value Type	Data	Value ...	Is Dele...	Data Reco...
ConsentPromptBehaviorAdmin	RegDword	5		<input type="checkbox"/>	<input type="checkbox"/>
ConsentPromptBehaviorUser	RegDword	3		<input type="checkbox"/>	<input type="checkbox"/>
EnableInstallerDetection	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
EnableLUA	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
EnableSecureUIAPaths	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
EnableUIADesktopToggle	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
EnableVirtualization	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
PromptOnSecureDesktop	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
ValidateAdminCodeSignatures	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
dontdisplaylastusername	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
legalnoticecaption	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
legalnoticetext	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
scforcecaption	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
shutdownwithoutlogon	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>

Key: Microsoft\Windows\CurrentVersion\Policies\System
Selected hive: SOFTWARE Last write: 2009-07-14 04:46:50 16 of 16 values shown (100.00%) Load complete
Value: legalnoticecaption Collapse all hives
Hidden keys: 0 1

Legalnoticetext:

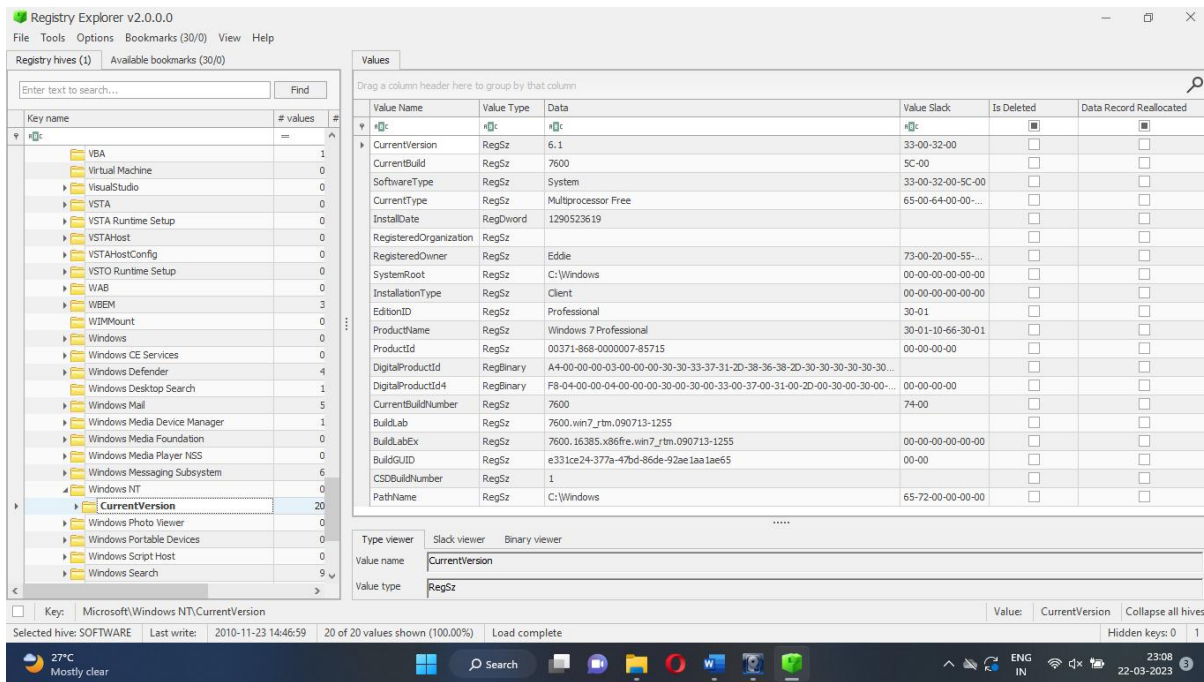
The screenshot shows the Registry Explorer v2.0.0.0 interface. The left pane displays the tree structure of the registry, with the path `Microsoft\Windows\CurrentVersion\Policies\System` selected. The right pane shows the values for this key. The `legalnoticetext` value is highlighted, and its details are shown in the bottom pane. The value is a `RegSz` type with a raw value of `00-00-00-00`.

Value Name	Value Type	Data	Value ...	Is Dele...	Data Reco...
ConsentPromptBehaviorAdmin	RegDword	5		<input type="checkbox"/>	<input type="checkbox"/>
ConsentPromptBehaviorUser	RegDword	3		<input type="checkbox"/>	<input type="checkbox"/>
EnableInstallerDetection	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
EnableLUA	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
EnableSecureUIAPaths	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
EnableUIADesktopToggle	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
EnableVirtualization	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
PromptOnSecureDesktop	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
ValidateAdminCodeSignatures	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
dontdisplaylastusername	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
legalnoticecaption	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
legalnoticetext	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
scforcecaption	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
shutdownwithoutlogon	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>

Key: Microsoft\Windows\CurrentVersion\Policies\System
Selected hive: SOFTWARE Last write: 2009-07-14 04:46:50 16 of 16 values shown (100.00%) Load complete
Value: legalnoticetext Collapse all hives
Hidden keys: 0 1

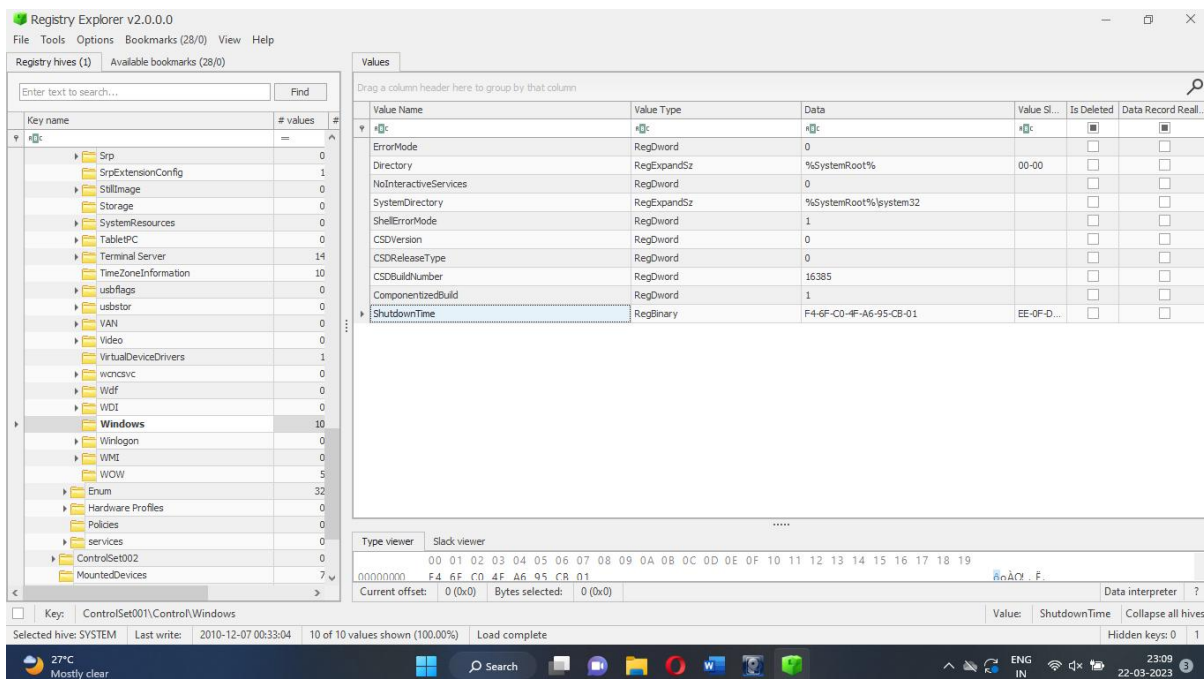
- Navigate to the following key to identify the installation information for the versions of Windows:

Microsoft\Windows NT\CurrentVersion



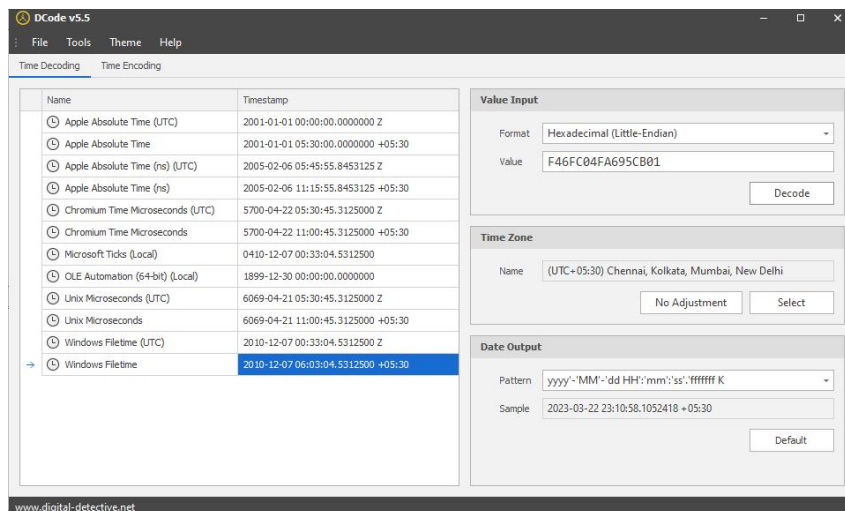
- Open the “SYSTEM” hive using registry explorer and find the “CurrentControlSet”. Navigate to the following subkey:

CurrentControlSet001\Control\Windows



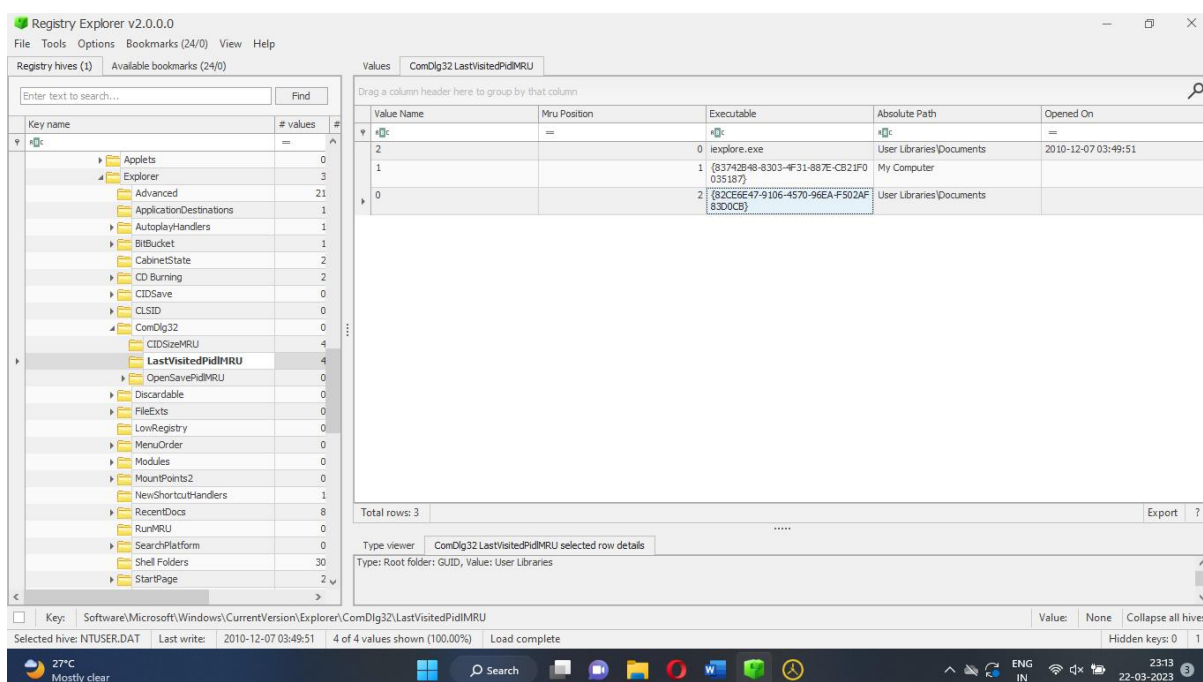
- Using the Dcode tool, convert the hexadecimal time to IST. You can download the tool from the following link – Dcode v5.5 (<https://www.digital-detective.net/dcode/>).

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:

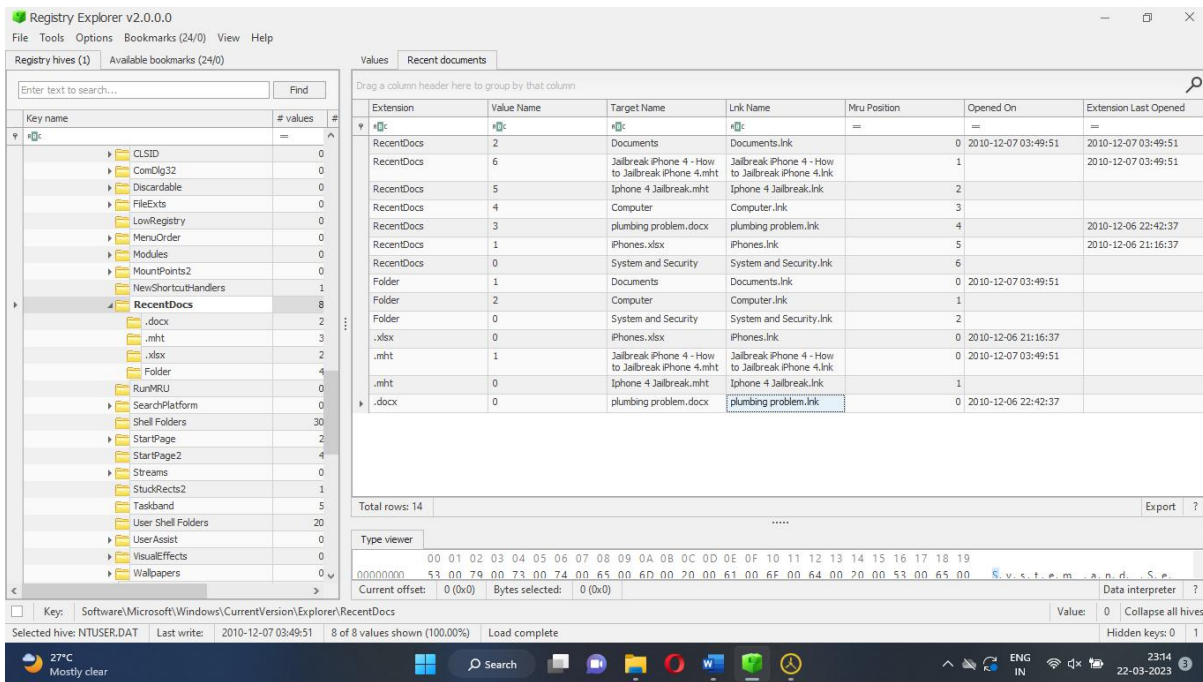
Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Last VisitedPIDMRU



➤ 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

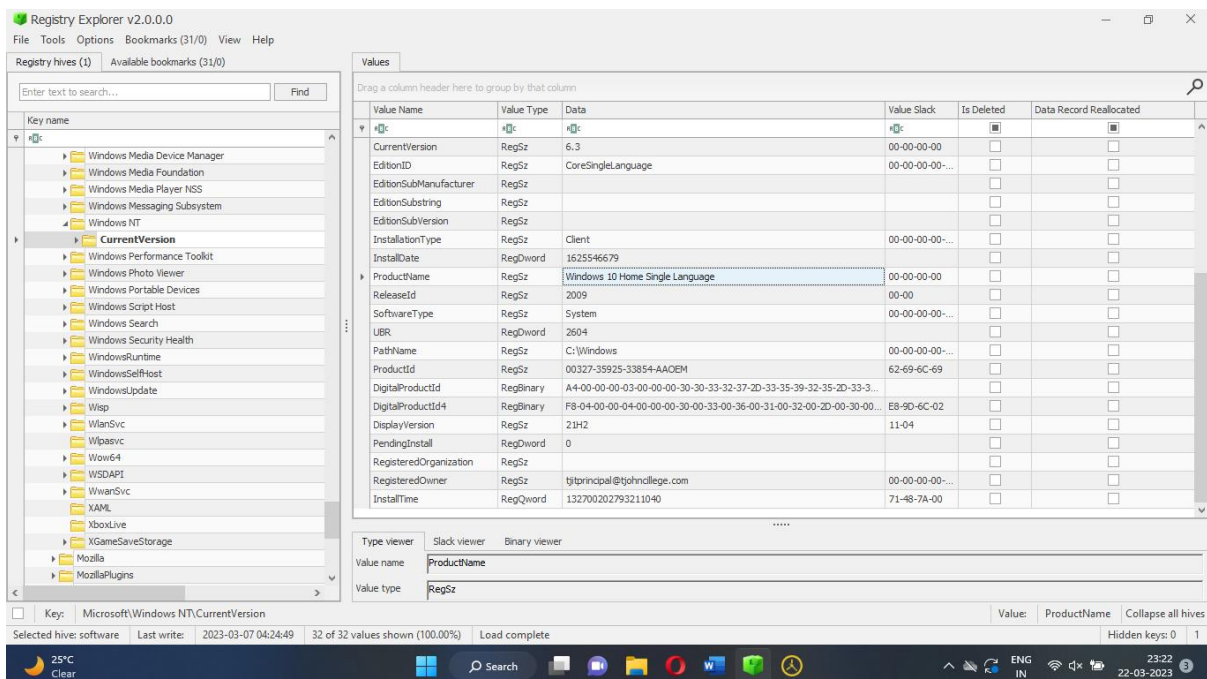


Hands-On Project

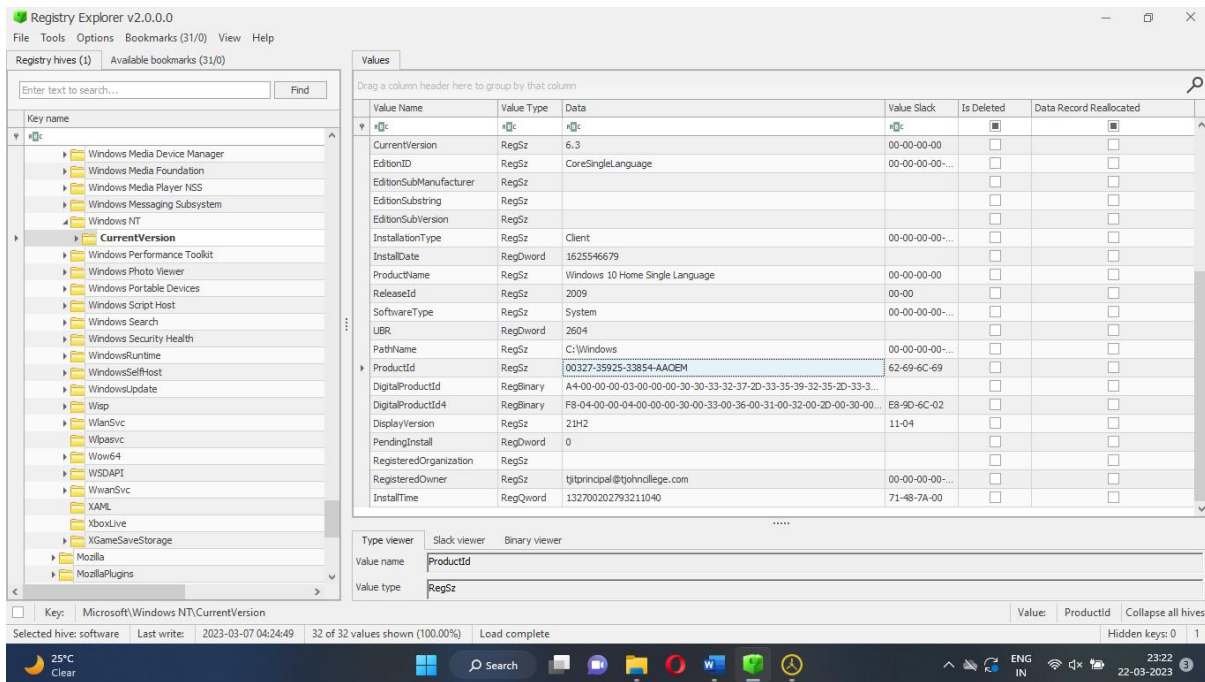
Analyze the given image and answer the following questions:

➤ What is the name of the Windows product?

=> Windows 10 Home Single Language



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



Registry Explorer v2.0.0.0

File Tools Options Bookmarks (31/0) View Help

Registry hives (1) Available bookmarks (31/0)

Enter text to search... Find

Key name

- Windows Media Device Manager
- Windows Media Foundation
- Windows Media Player NSS
- Windows Messaging Subsystem
- Windows NT
- CurrentVersion**
- Windows Performance Toolkit
- Windows Photo Viewer
- Windows Portable Devices
- Windows Script Host
- Windows Search
- Windows Security Health
- WindowsRuntime
- WindowsSelfHost
- WindowsUpdate
- Wsp
- WlanSvc
- WpaSvc
- Wow64
- WSDAPI
- WwanSvc
- XAML
- XboxLive
- XGameSaveStorage
- Mozilla
- MozillaPlugins

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
CurrentVersion	RegSz	6.3	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
EditionID	RegSz	CoreSingleLanguage	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
EditionSubManufacturer	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
EditionSubstring	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
EditionSubVersion	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
InstallationType	RegSz	Client	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
InstallDate	RegDword	1625546679		<input type="checkbox"/>	<input type="checkbox"/>
ProductName	RegSz	Windows 10 Home Single Language	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
ReleaseId	RegSz	2009	00-00...	<input type="checkbox"/>	<input type="checkbox"/>
SoftwareType	RegSz	System	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
UBR	RegDword	2604		<input type="checkbox"/>	<input type="checkbox"/>
PathName	RegSz	C:\Windows	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
ProductId	RegSz	00327-35925-33854-AAOEM	62-69-6C-69	<input type="checkbox"/>	<input type="checkbox"/>
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-33-32-37-2D-33-35-39-32-35-2D-33-3...		<input type="checkbox"/>	<input type="checkbox"/>
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-30-00-33-00-36-00-31-00-32-00-2D-00-30-00...	E8-90-6C-02	<input type="checkbox"/>	<input type="checkbox"/>
DisplayVersion	RegSz	21H2	11-04	<input type="checkbox"/>	<input type="checkbox"/>
PendingInstall	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
RegisteredOrganization	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
RegisteredOwner	RegSz	tjprincipal@tjohndcollege.com	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
InstallTime	RegQword	132700202793211040	71-48-7A-00	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer Binary viewer

Value name ProductId

Value type RegSz

Key: Microsoft\Windows NT\CurrentVersion

Selected hive: software Last write: 2023-03-07 04:24:49 32 of 32 values shown (100.00%) Load complete

Value: ProductId Collapse all hives

Hidden keys: 0 1

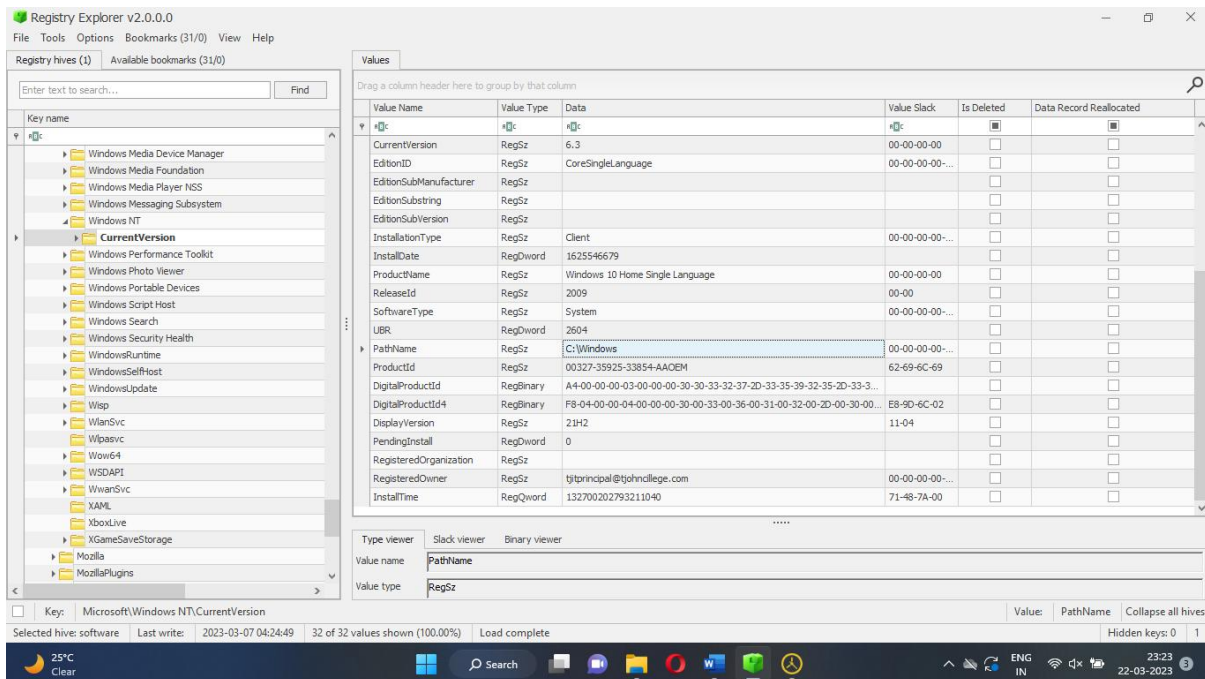
25°C Clear

Search

ENG IN

23:22 22-03-2023

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



Registry Explorer v2.0.0.0

File Tools Options Bookmarks (31/0) View Help

Registry hives (1) Available bookmarks (31/0)

Enter text to search... Find

Key name

- Windows Media Device Manager
- Windows Media Foundation
- Windows Media Player NSS
- Windows Messaging Subsystem
- Windows NT
- CurrentVersion**
- Windows Performance Toolkit
- Windows Photo Viewer
- Windows Portable Devices
- Windows Script Host
- Windows Search
- Windows Security Health
- WindowsRuntime
- WindowsSelfHost
- WindowsUpdate
- Wsp
- WlanSvc
- WpaSvc
- Wow64
- WSDAPI
- WwanSvc
- XAML
- XboxLive
- XGameSaveStorage
- Mozilla
- MozillaPlugins

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
CurrentVersion	RegSz	6.3	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
EditionID	RegSz	CoreSingleLanguage	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
EditionSubManufacturer	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
EditionSubstring	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
EditionSubVersion	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
InstallationType	RegSz	Client	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
InstallDate	RegDword	1625546679		<input type="checkbox"/>	<input type="checkbox"/>
ProductName	RegSz	Windows 10 Home Single Language	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
ReleaseId	RegSz	2009	00-00...	<input type="checkbox"/>	<input type="checkbox"/>
SoftwareType	RegSz	System	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
UBR	RegDword	2604		<input type="checkbox"/>	<input type="checkbox"/>
PathName	RegSz	C:\Windows	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
ProductId	RegSz	00327-35925-33854-AAOEM	62-69-6C-69	<input type="checkbox"/>	<input type="checkbox"/>
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-33-32-37-2D-33-35-39-32-35-2D-33-3...		<input type="checkbox"/>	<input type="checkbox"/>
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-30-00-33-00-36-00-31-00-32-00-2D-00-30-00...	E8-90-6C-02	<input type="checkbox"/>	<input type="checkbox"/>
DisplayVersion	RegSz	21H2	11-04	<input type="checkbox"/>	<input type="checkbox"/>
PendingInstall	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
RegisteredOrganization	RegSz			<input type="checkbox"/>	<input type="checkbox"/>
RegisteredOwner	RegSz	tjprincipal@tjohndcollege.com	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
InstallTime	RegQword	132700202793211040	71-48-7A-00	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer Binary viewer

Value name PathName

Value type RegSz

Key: Microsoft\Windows NT\CurrentVersion

Selected hive: software Last write: 2023-03-07 04:24:49 32 of 32 values shown (100.00%) Load complete

Value: PathName Collapse all hives

Hidden keys: 0 1

25°C Clear

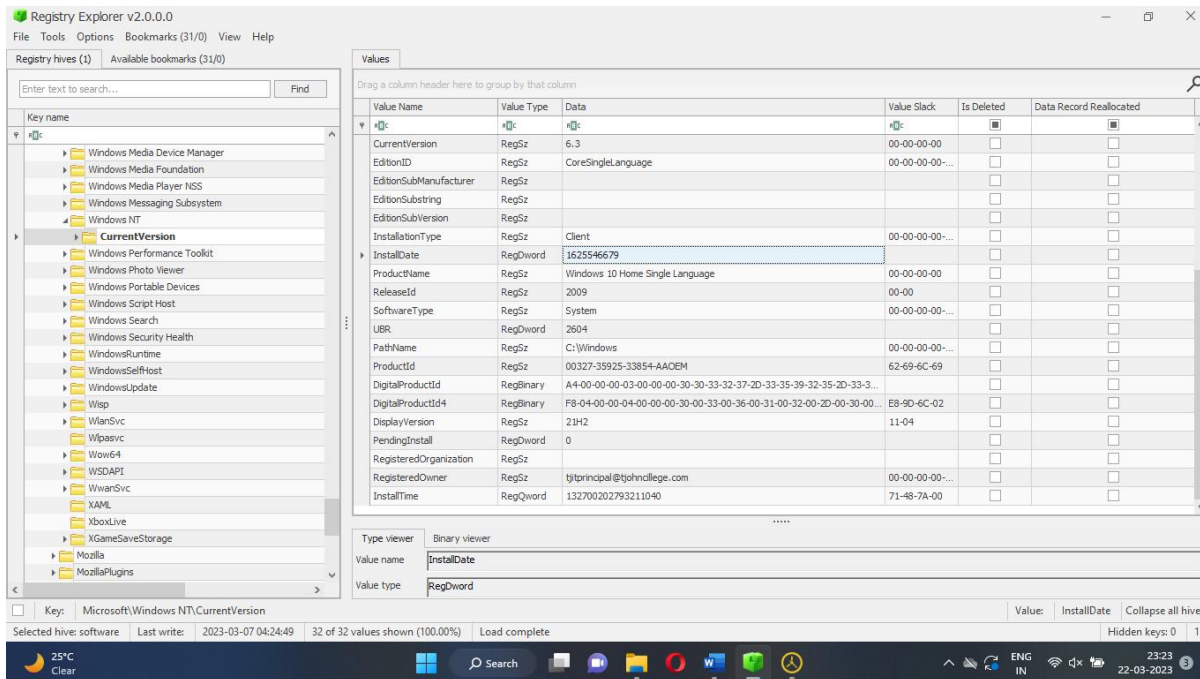
Search

ENG IN

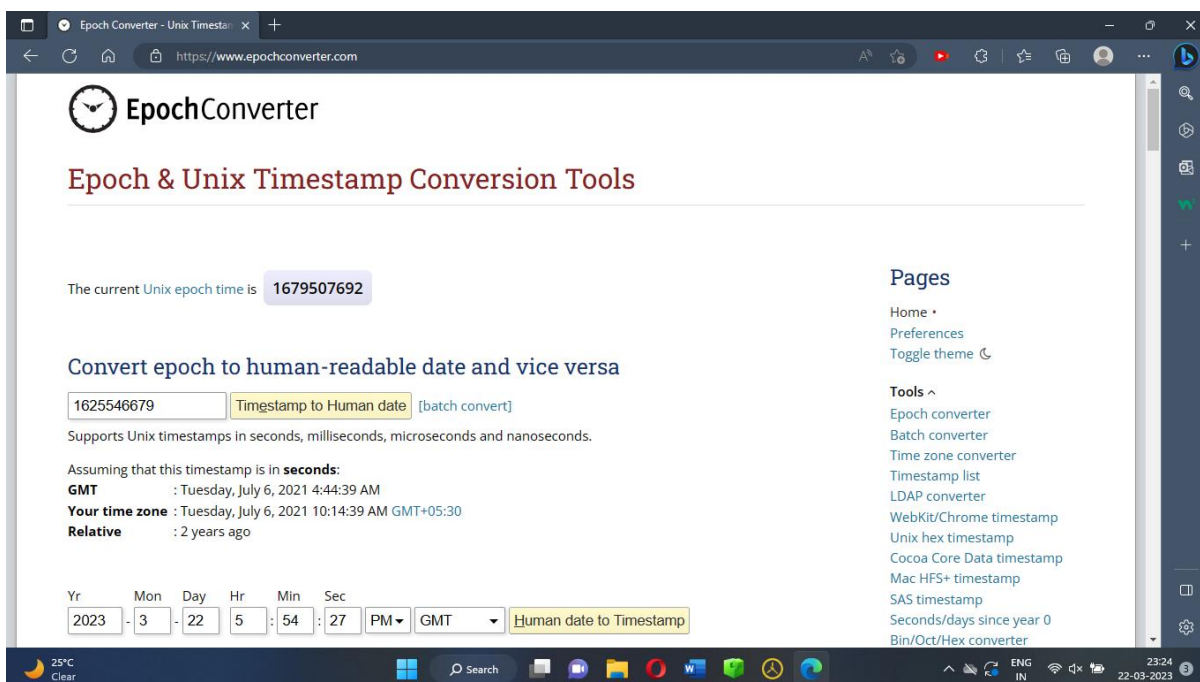
23:23 22-03-2023

➤ When was the operating system installed?

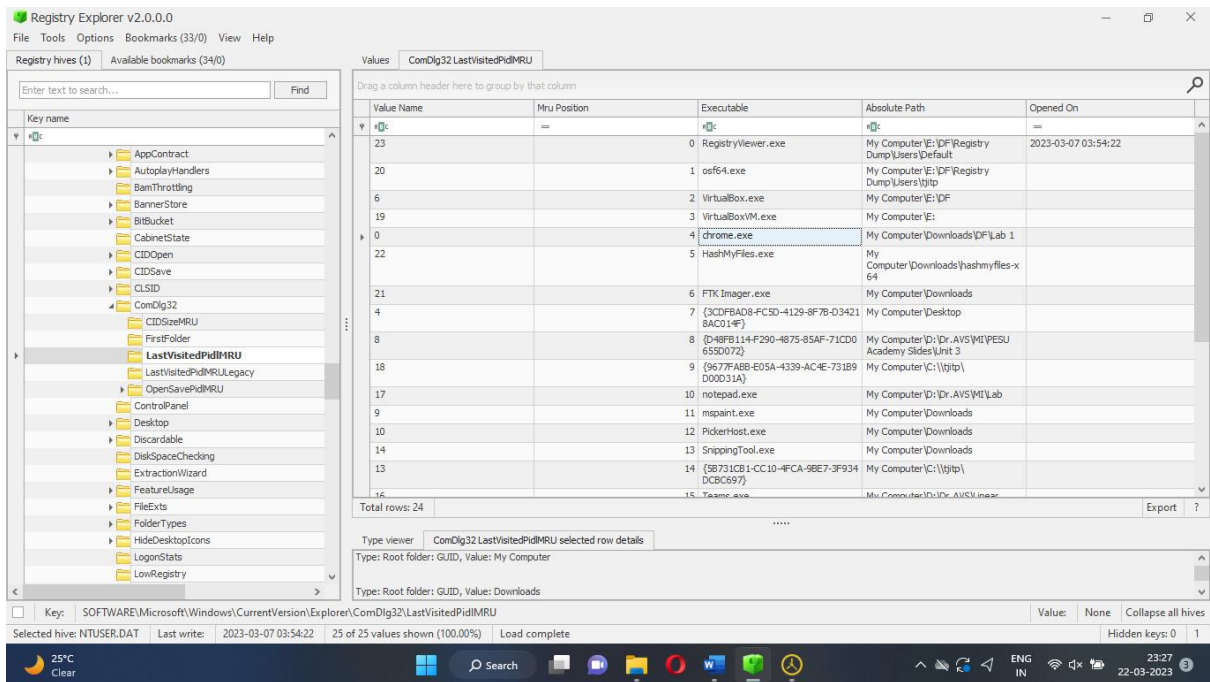
Based on the Registry, the installation date is listed as 1625546679 (, which is a timestamp recorded in Epoch time. Using a resource, such as www.epochconverter.com, converts the value to March 22, 2023 at 16:56:17 GMT.)



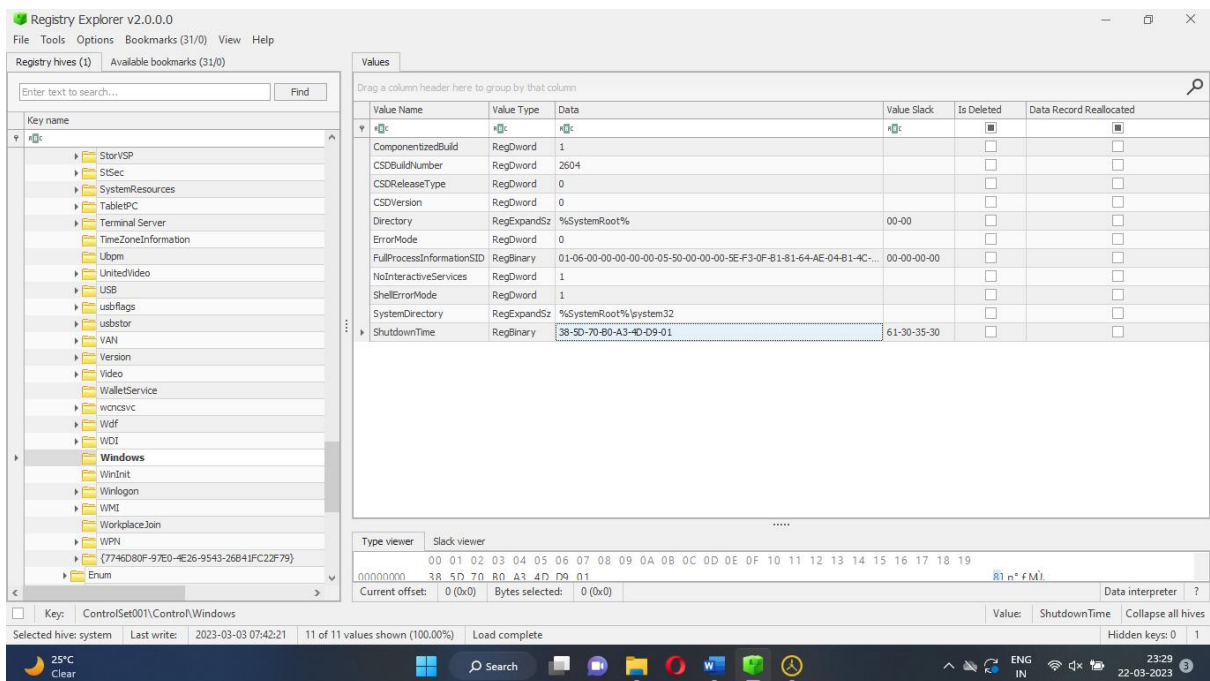
Decoding the TimeStamp



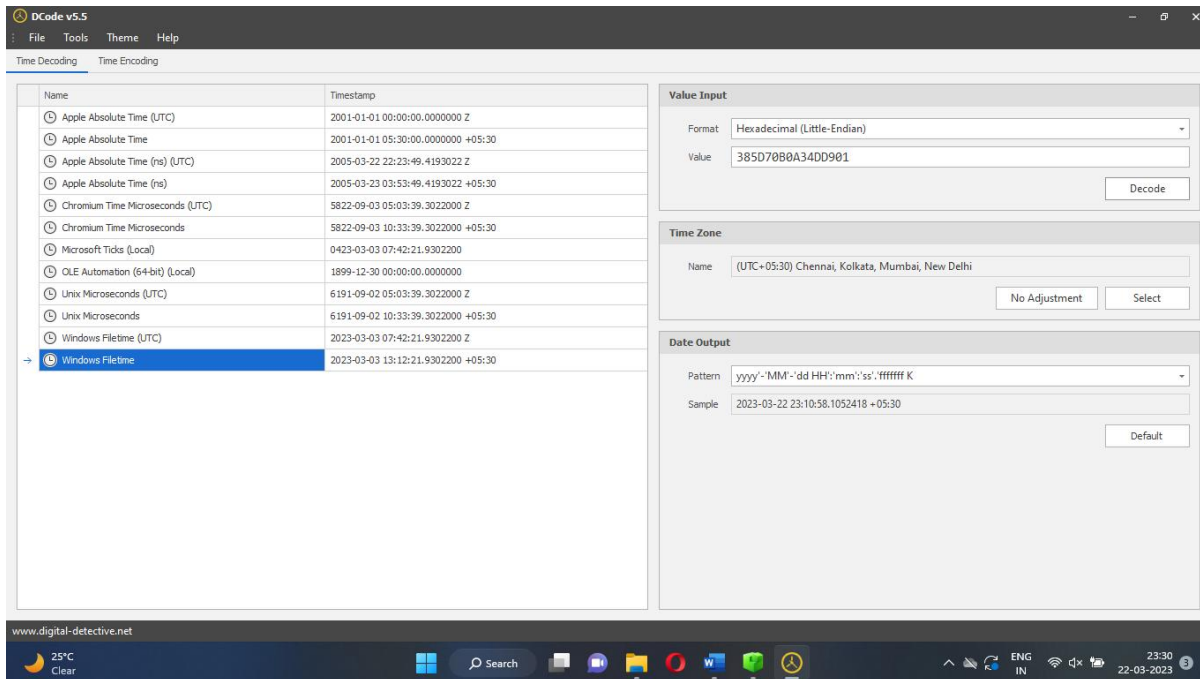
- Identify the executable files that have been executed in the target system.



- 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?

