

Module B10: Windows Registry Forensics Analysis

Pre-requisite Knowledge and Skills:

- 1.

Learning Objectives

1. .

Recommended Running Environment/Tools:

1. Windows OS
2. AccessData FTK Imager
3. Registry Editor

Material:

- 1.

Video Lecture:

1. N/A

Lab Assessment:

Lab Instructions:

Part 1

1. In Windows File Explorer, navigate to the following path:

C:\Windows\System32\config

config

File Home Share View

Clipboard: Pin to Quick access, Copy, Paste, Copy path, Paste shortcut

Organize: Move to, Copy to, Delete, Rename

New: New folder, New item, Easy access

Open: Properties, Edit, History

Select: Select all, Select none, Invert selection, Select

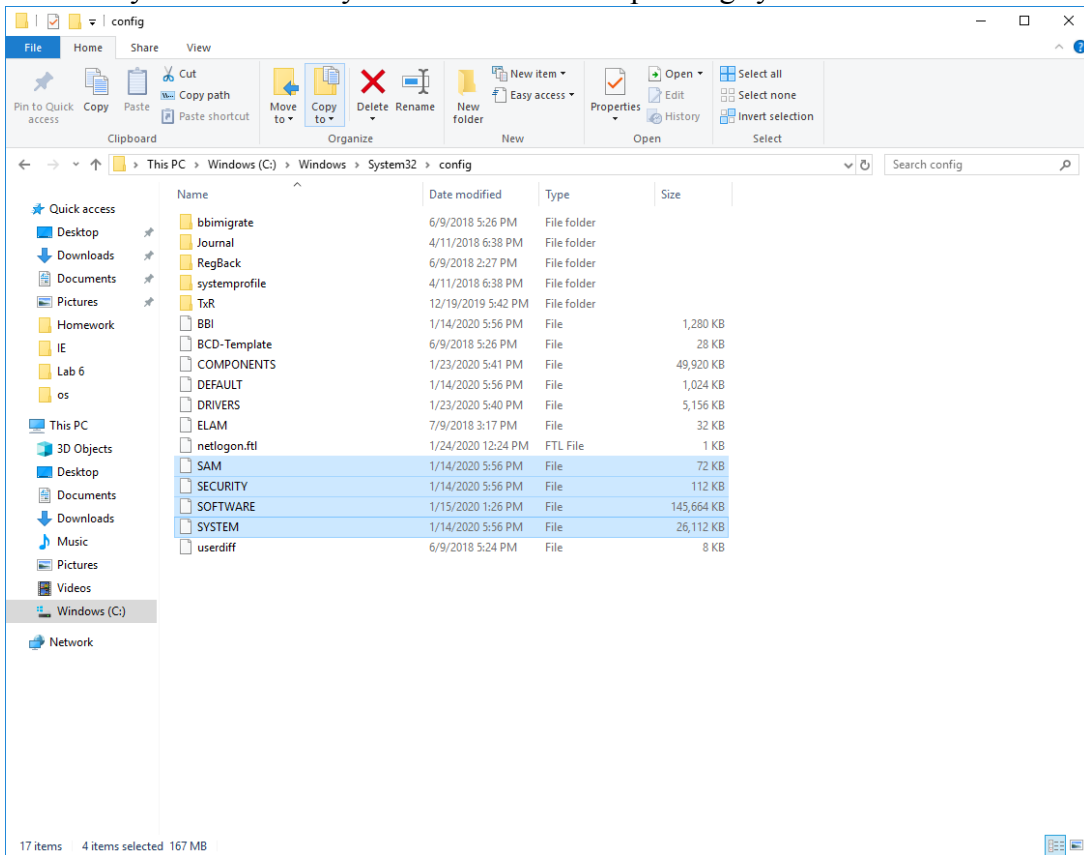
Address bar: < This PC > Windows (C:) > Windows > System32 > config

Search: Search config

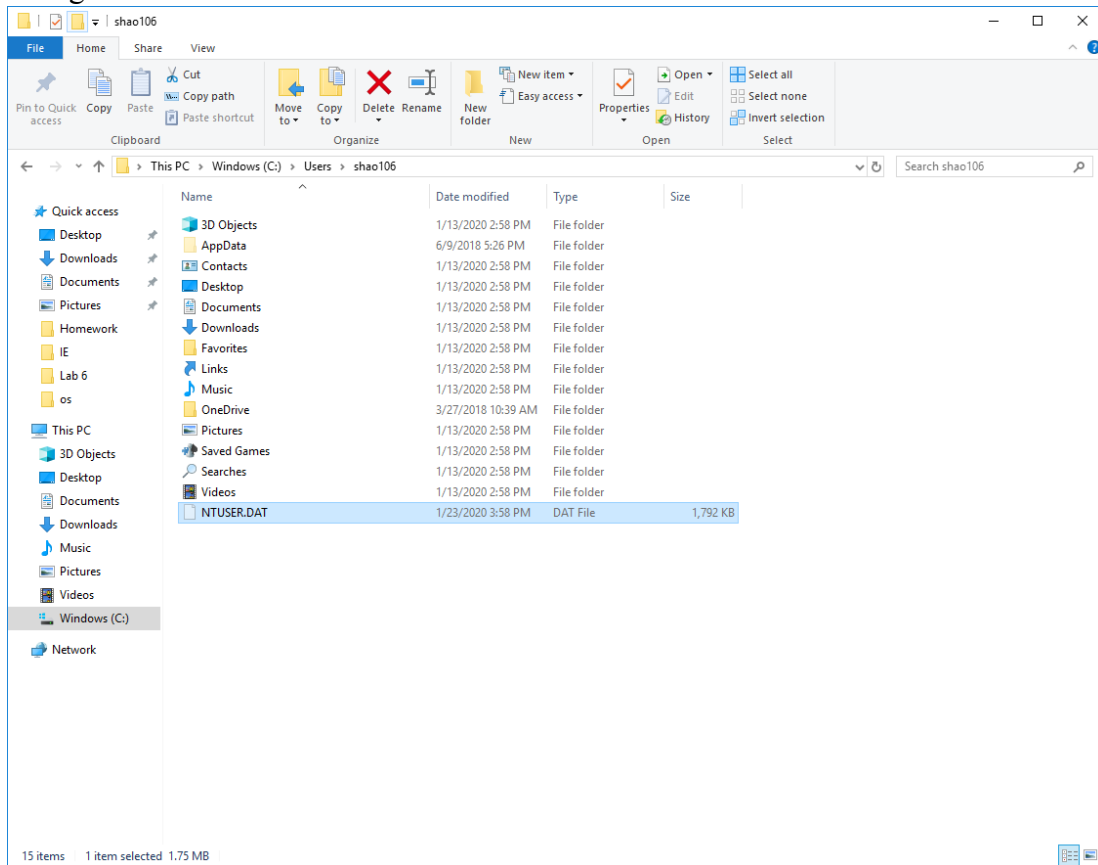
Name	Date modified	Type	Size
bbimigrate	6/9/2018 5:26 PM	File folder	
Journal	4/11/2018 6:38 PM	File folder	
RegBack	6/9/2018 2:27 PM	File folder	
systemprofile	4/11/2018 6:38 PM	File folder	
TxR	12/19/2019 5:42 PM	File folder	
BBI	1/14/2020 5:56 PM	File	1,280 KB
BCD-Template	6/9/2018 5:26 PM	File	28 KB
COMPONENTS	1/23/2020 5:41 PM	File	49,920 KB
DEFAULT	1/14/2020 5:56 PM	File	1,024 KB
DRIVERS	1/23/2020 5:40 PM	File	5,156 KB
ELAM	7/9/2018 3:17 PM	File	32 KB
netlogon.ftl	1/24/2020 12:24 PM	FTL File	1 KB
SAM	1/14/2020 5:56 PM	File	72 KB
SECURITY	1/14/2020 5:56 PM	File	112 KB
SOFTWARE	1/15/2020 1:26 PM	File	145,664 KB
SYSTEM	1/14/2020 5:56 PM	File	26,112 KB
userdiff	6/9/2018 5:24 PM	File	8 KB

17 items

2. View the registry files of **SAM**, **SECURITY**, **SYSTEM**, and **SOFTWARE**. This is where they are traditionally stored in Windows operating systems

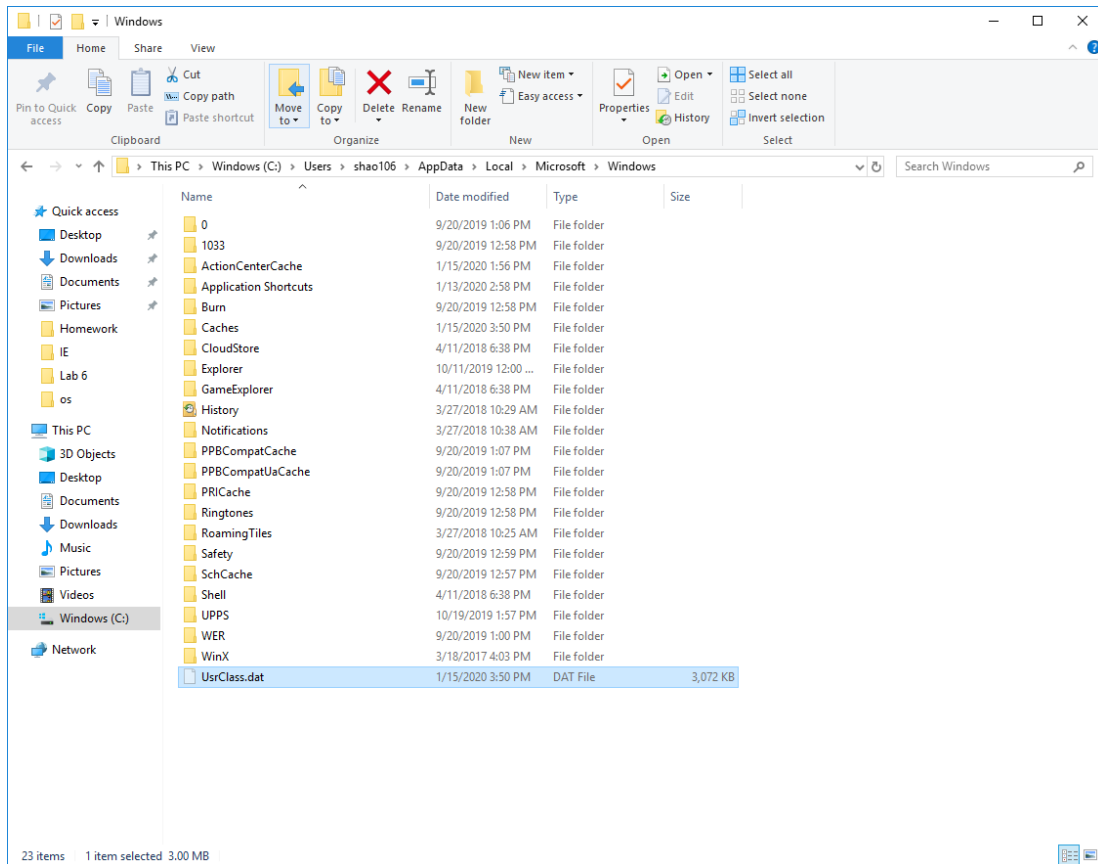


3. Navigate to **C:\Users\username**. View the associated **NTUSER.DAT** file for this user



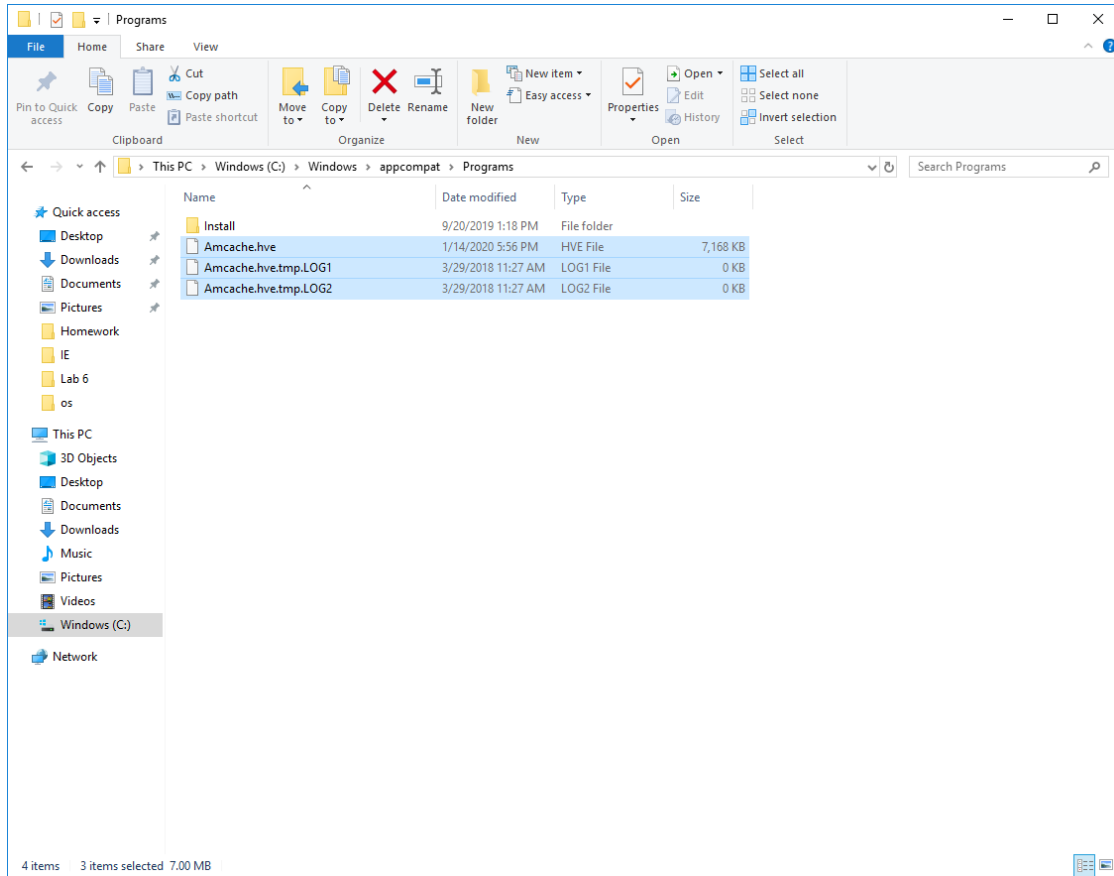
4. Navigate to: **C:\Users\username\AppData\Local\Microsoft\Windows**. View the

associated UsrClass.dat file for this user



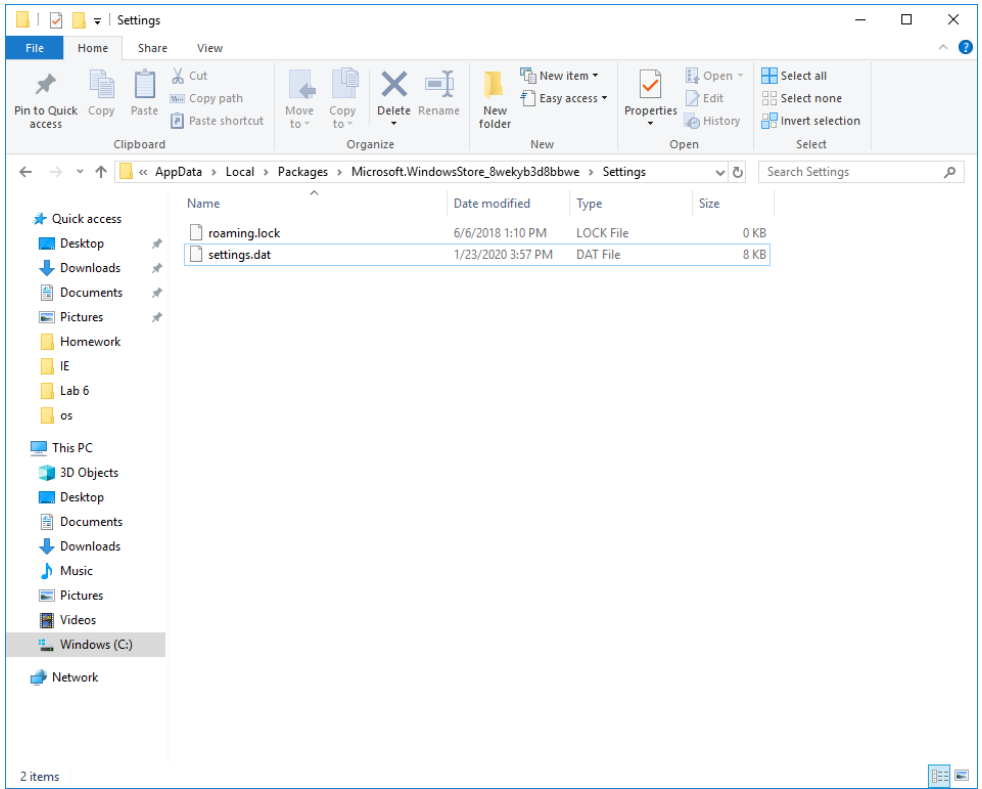
5. Navigate to: **C:\Windows\appcompat\Programs**. View the Amcache.hve file for this operating system. This is not an official registry file, but is created using the registry

format to track data.



6. Navigate to:
C:\Users\username\AppData\Local\Packages\Microsoft.WindowsStore_8wekyb3d8bbw

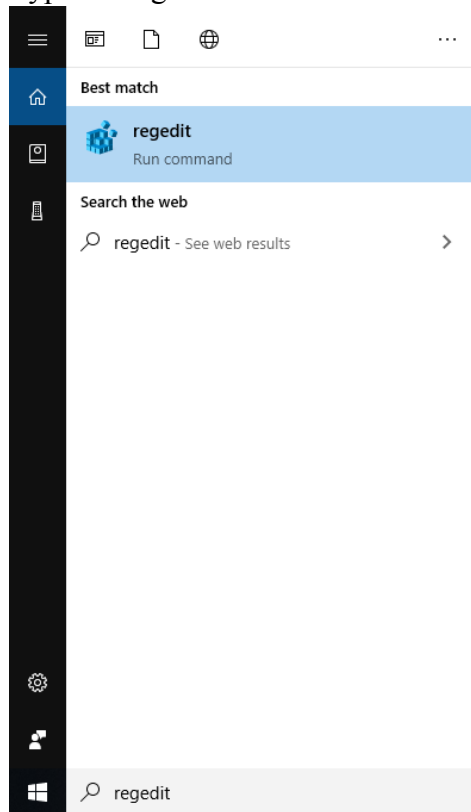
eSettings. View the associated settings.dat for this application. This is not a registry file



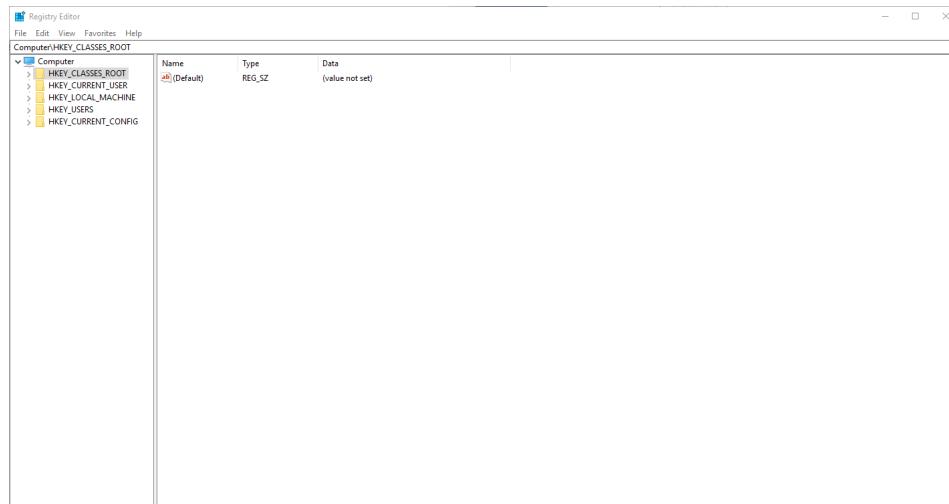
Part 2 Viewing the Registry Structure in Regedit

1. Open Regedit. Click on the Ask Me Anything box (Circle next to the Start button).

Type in Regedit

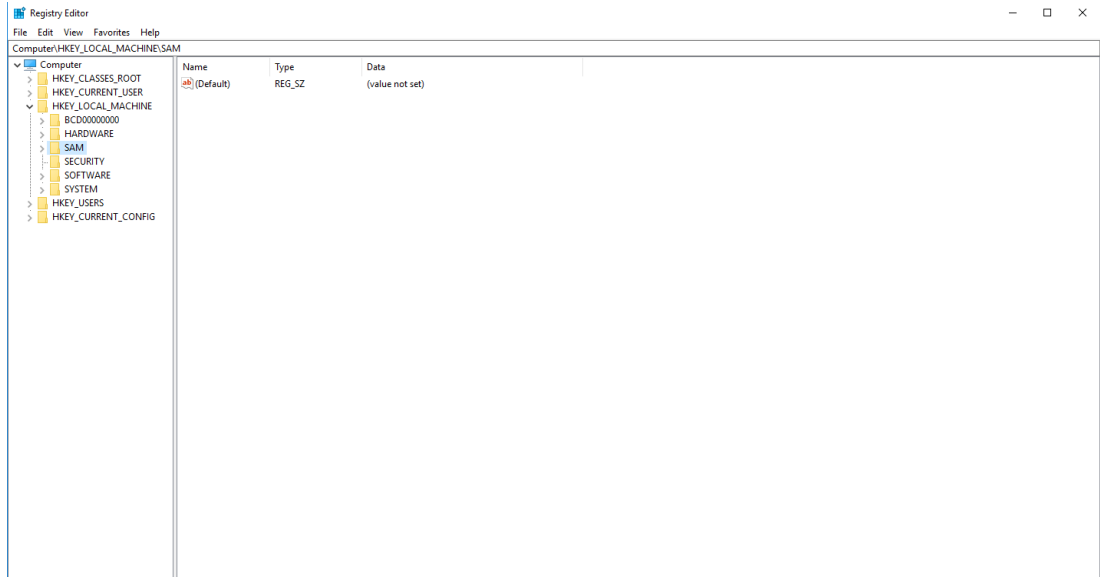


2. Note the basic Hive structure

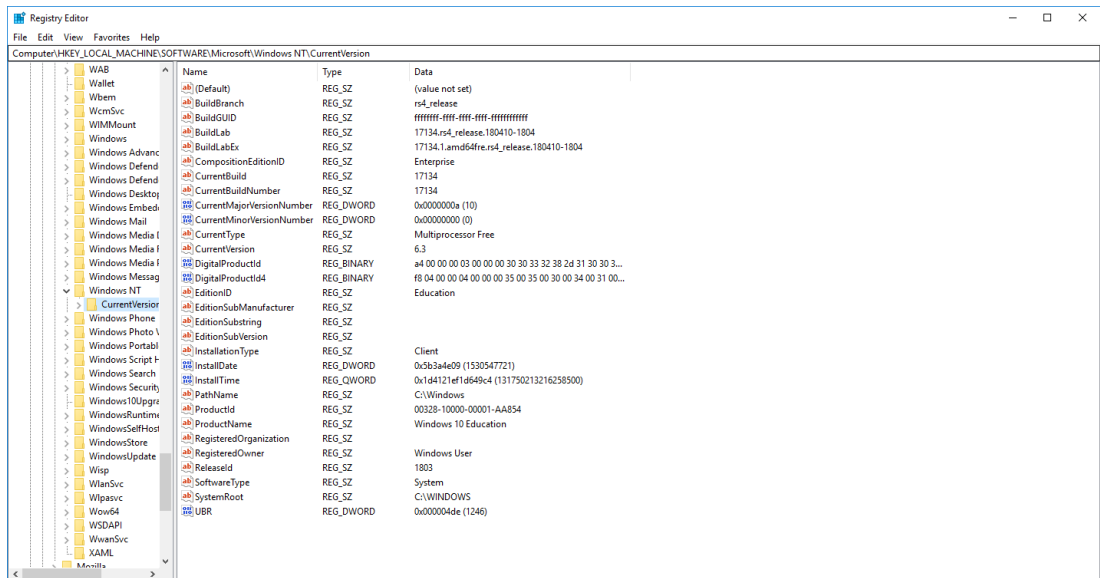


3. The HKEY_CLASSES_ROOT data is stored in the SOFTWARE file. The HKEY_CURRENT_USER is the NTUSER.DAT file information. HKEY_LOCAL_MACHINE stores the SAM, SECURITY, SOFTWARE and

SYSTEM registry files. See below capture.





- Click on the SOFTWARE root key under HKEY LOCAL MACHINE and navigate to the following path: **HKLM_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion**



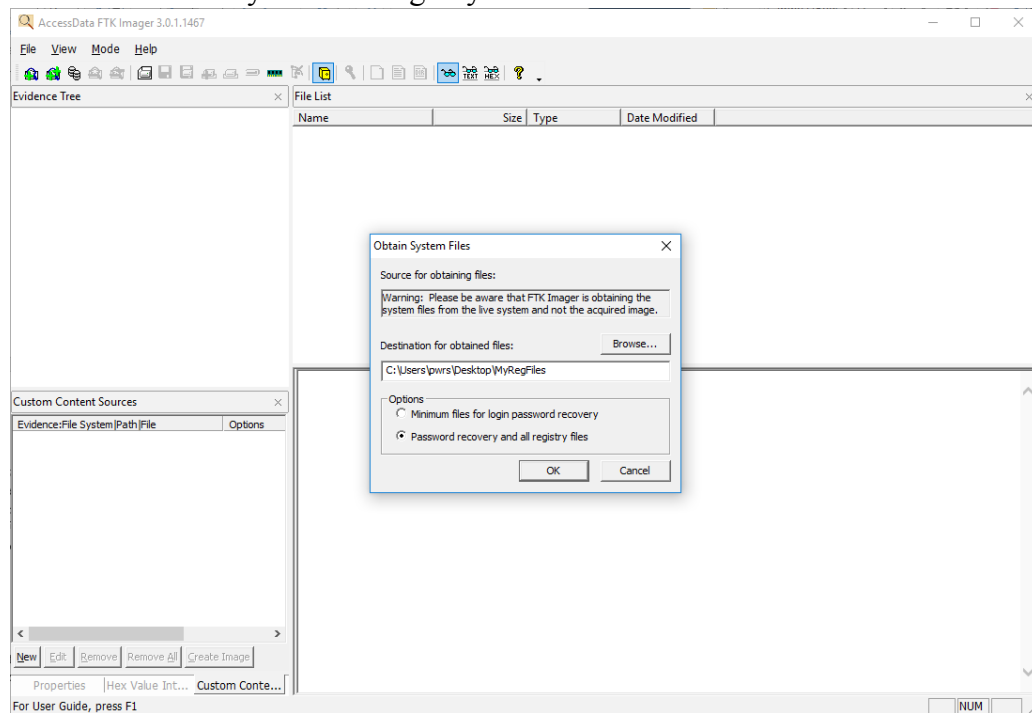
This location tracks the registered owner of the system, the operating system name and version, and the installation time.

- Note the value called InstallDate. This is a 32-bit Unix date and time stamp.

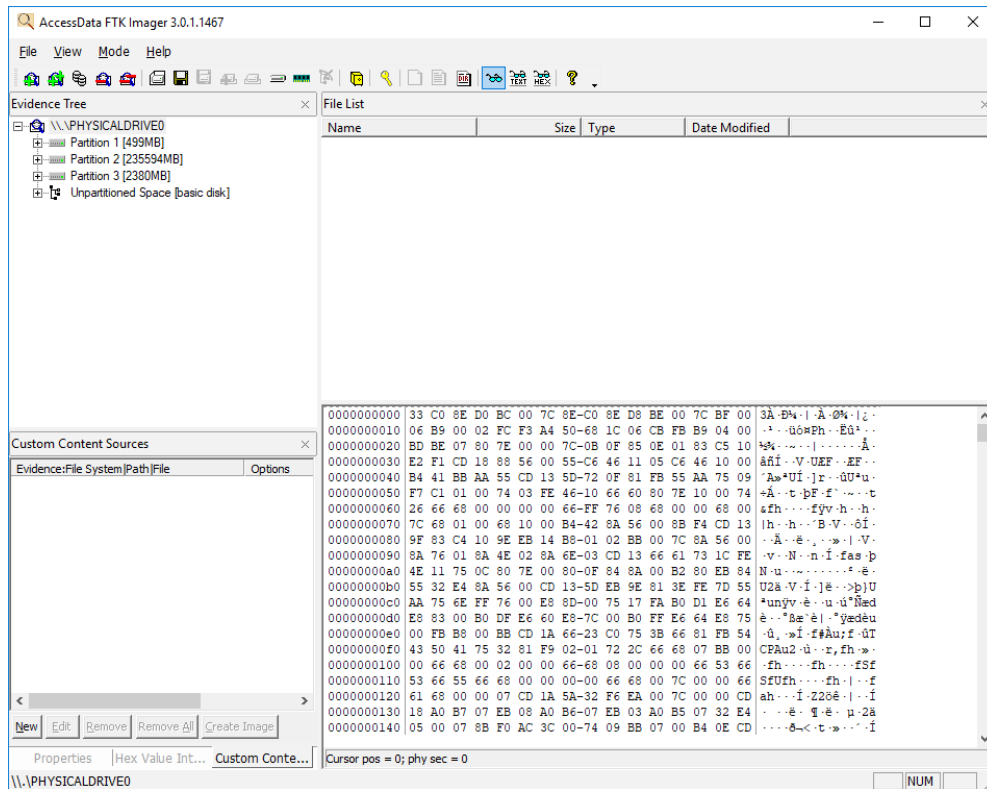
 InstallDate	REG_DWORD	0x5b3a4e09 (1530547721)
 InstallTime	REG_QWORD	0x1d4121ef1d649c4 (131750213216258500)

Part 3 View the Registry Structure in Registry Viewer

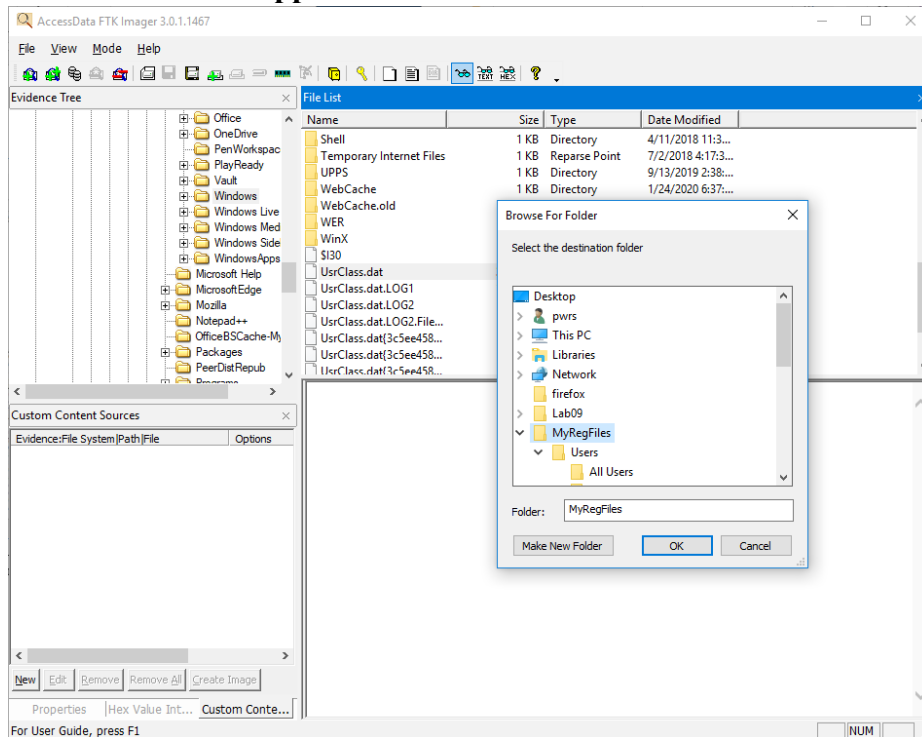
1. Capture the standard registry files on the local machine.
2. Right click on the Desktop and create a new folder called MyRegFiles
3. Open FTK Imager
4. Click on the Obtain Protected Files button to capture the following:
 - i. NTUSER.DAT
 - ii. SAM
 - iii. SECURITY
 - iv. SOFTWARE
 - v. SYSTEM
5. Select the MyRegFiles folder as the Destination for Obtained Files and select the Password Recovery and All Registry Files radio button.



6. Capture the Non-Standard Registry files in FTK Imager
7. In Imager, select File > Add Evidence Item.
8. Use the default Physical Drive radio button selection and hit Next.
9. Wait for the physical drives to draw up in the selection drop down menu.
10. When open, select the System drive which in most labs is the Toshiba or M4 device.
11. Hit finish.

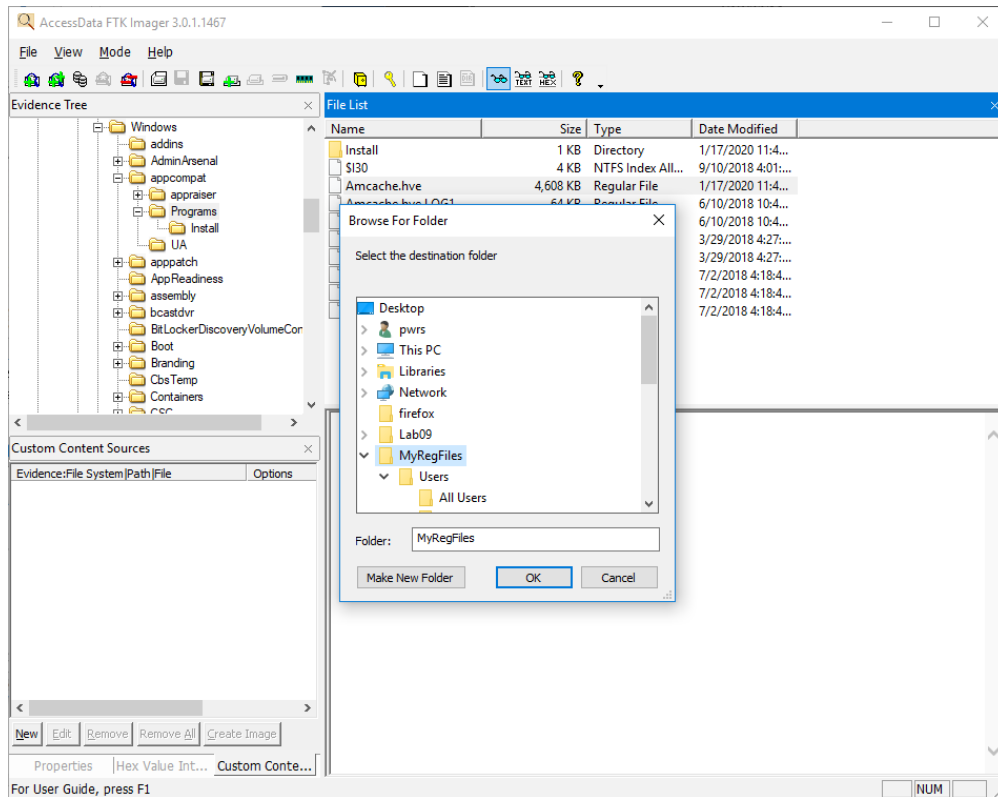


12. Open that and navigate to the **UserClass.dat** file for student at **C:\Users\Student\AppData\Local\Microsoft\Windows**

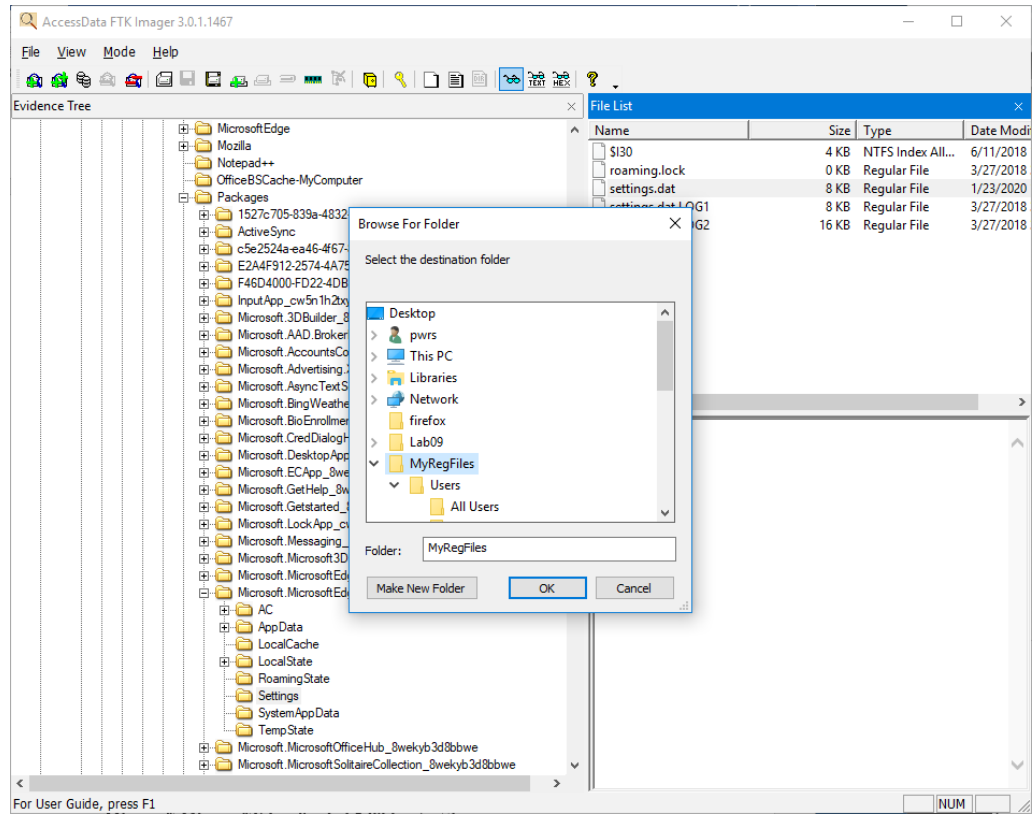


13. Navigate to the Amcache.hve file at: **C:\Windows\appcompat\Programs** and

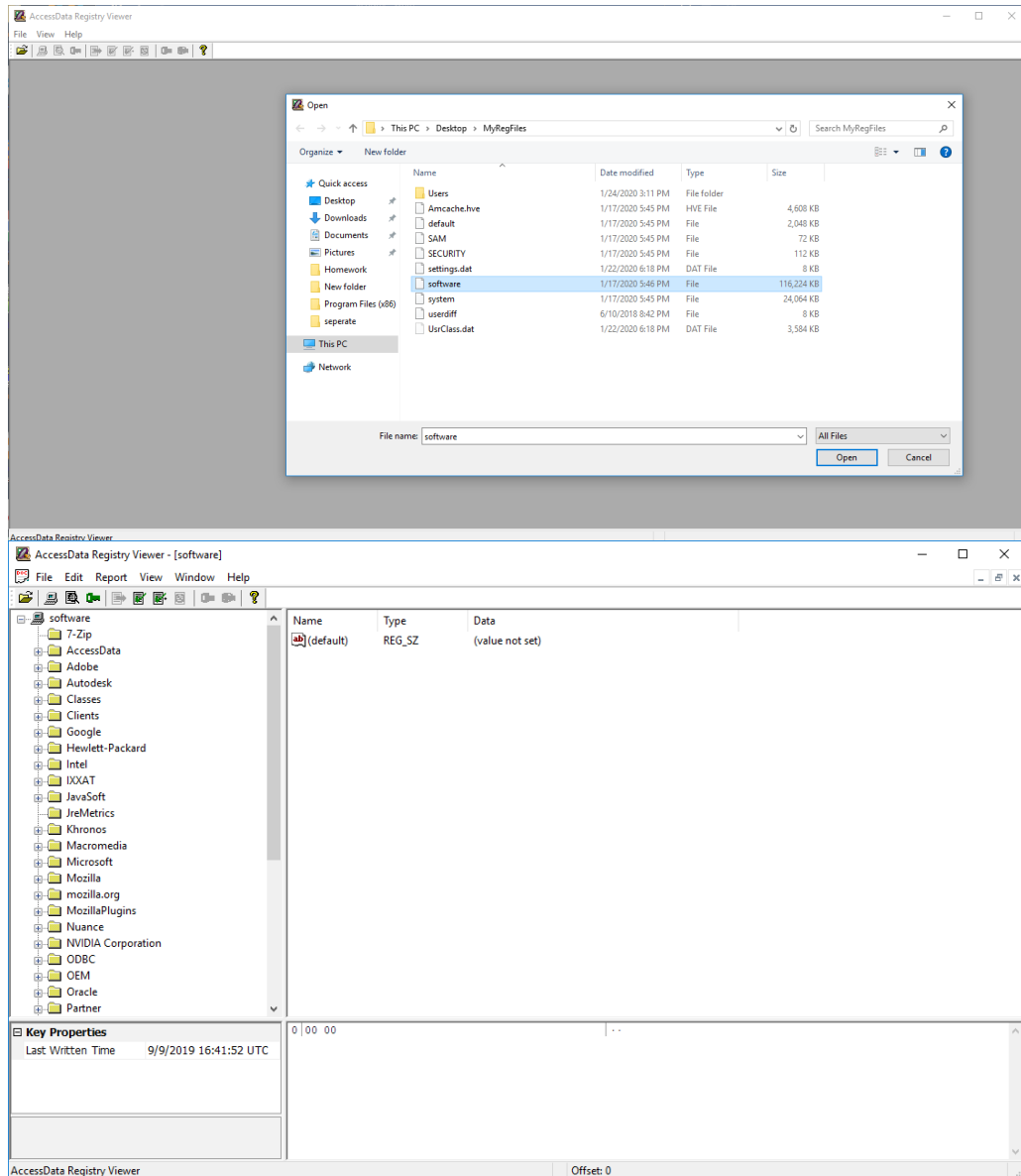
export that to the MyRegFiles folder.



14. Navigate to the settings.dat file for the Edge Browser at: **C:\Users\Student\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\settings**
Export that to the MyRegFiles folder

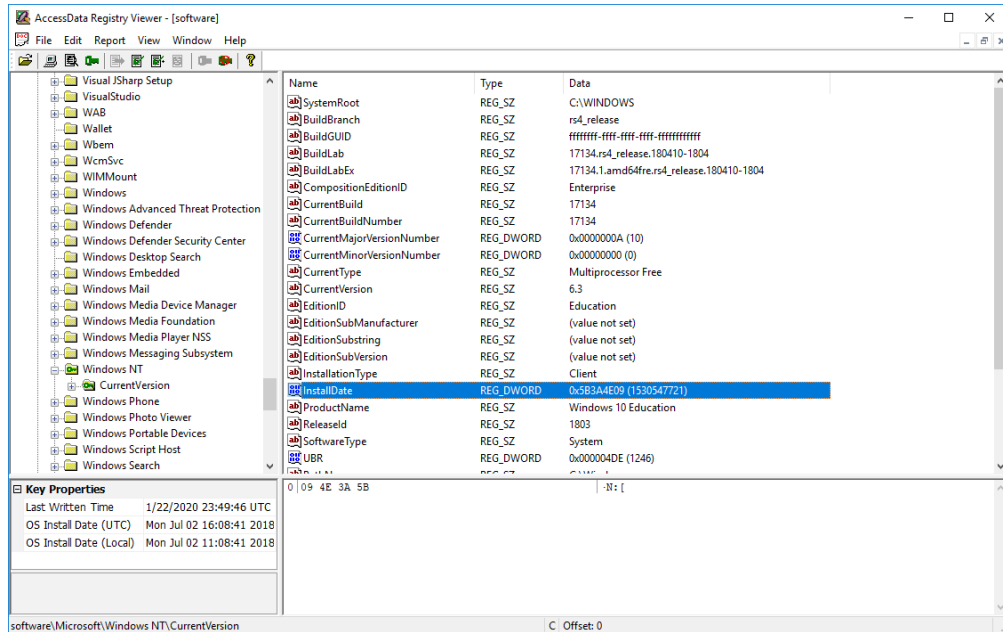


15. Open Registry Viewer and do a File > Open and select the SOFTWARE registry file in the MyRegFiles folder.



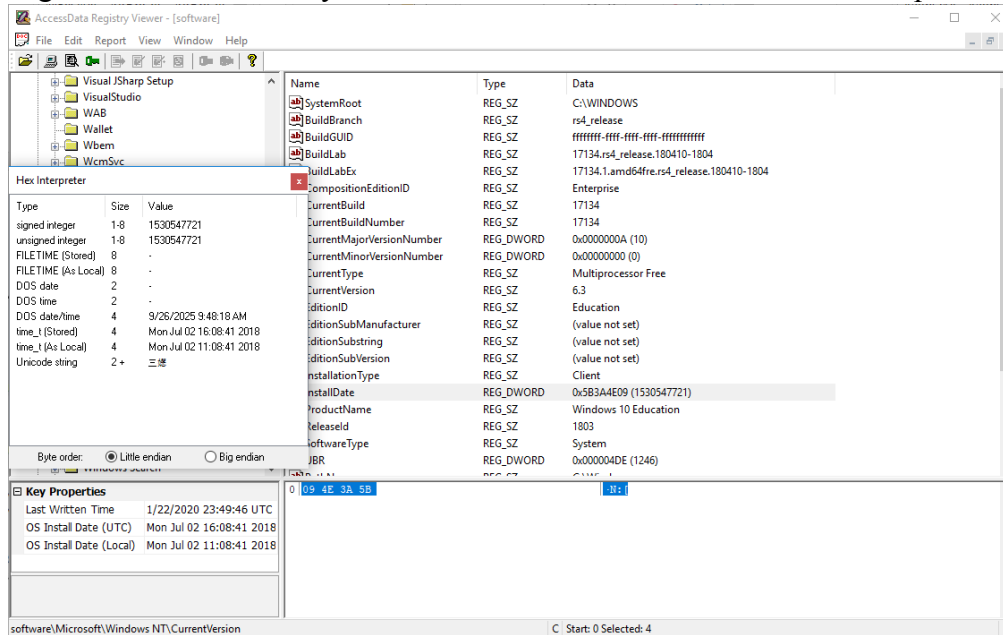
16. When open, navigate to the same location we were in for Regedit at:
SOFTWARE\Microsoft\Windows NT\CurrentVersion

17. Click on InstallDate value.

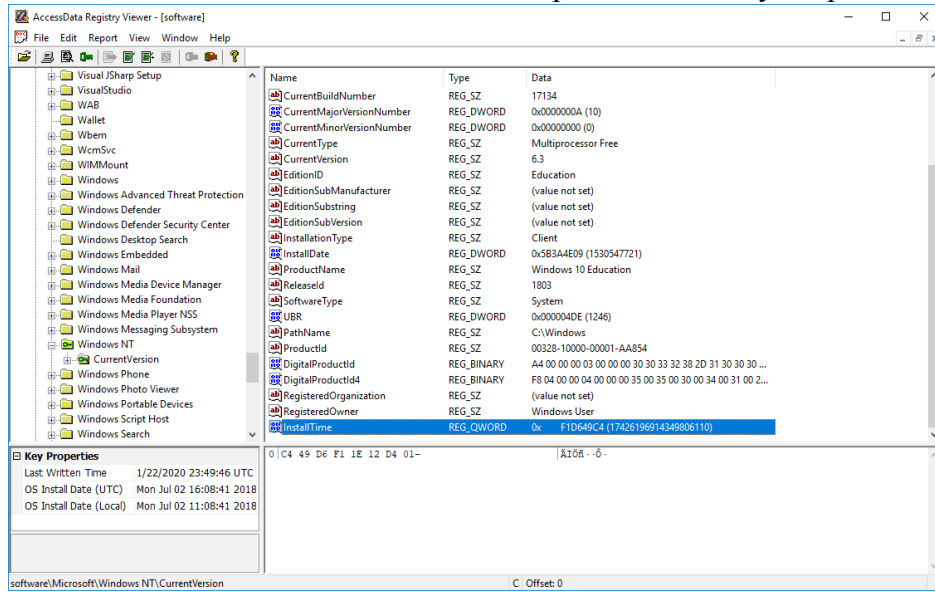


Note that in Key Properties there is a Last Written Time which references when the subkey you are in was last updated.

18. Right click on the four byte value and select the Show Hex Value Interpreter link

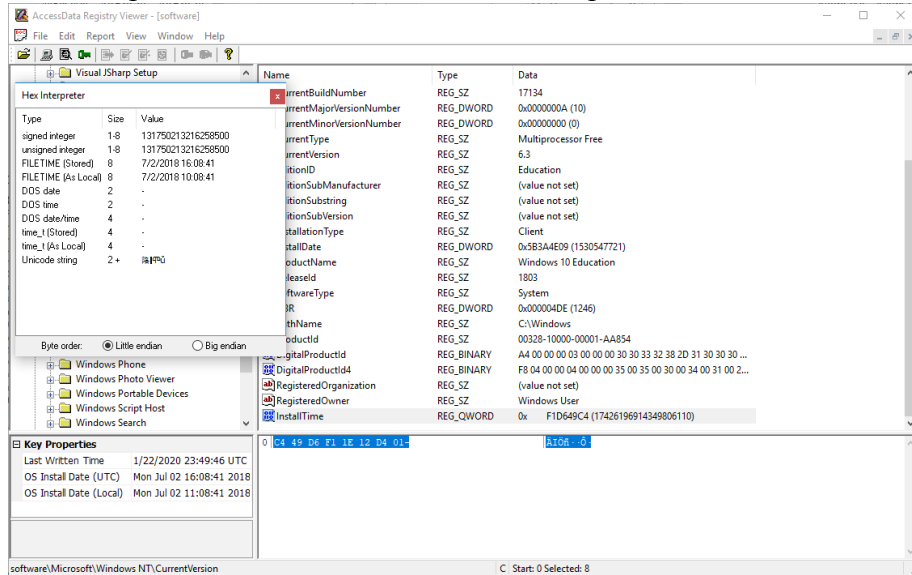


19. View the date/time of installation and compare it to the Key Properties



20. Windows 10 has added a new time stamp called InstallTime. This is a 64-bit Windows FILE TIME date and time stamp.

21. Select the InstallTime value, highlight the 8 byte set of data and right click for the Hex Interpreter to see this date and time stamp translated.



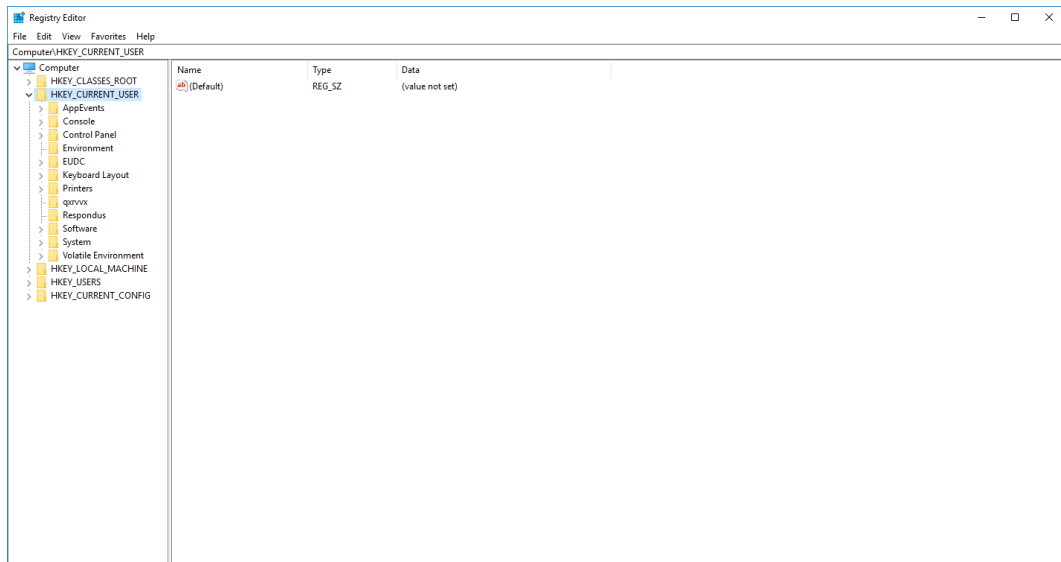
Part 3 NTUSER.DAT Information

The objective of this lab is to familiarize the student with the Windows registry user profile; NTUSER.DAT.

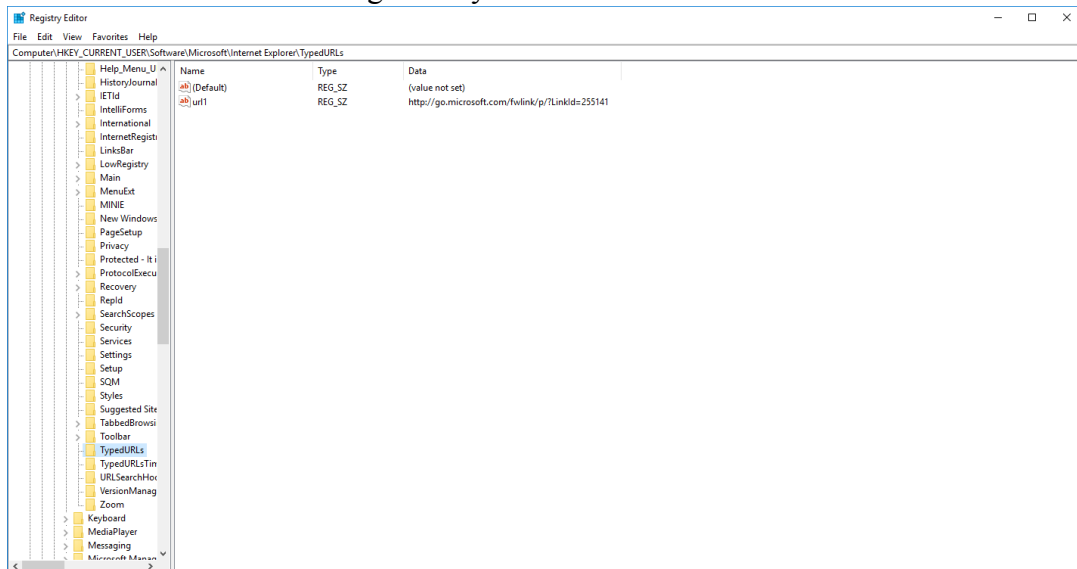
This lab uses Windows 10, File Explorer, Regedit, and Registry Viewer

Section 1 — Internet Explorer

1. Open Regedit and navigate to the HKCU root key. This is the same as navigating to the NTUSER.DAT file.

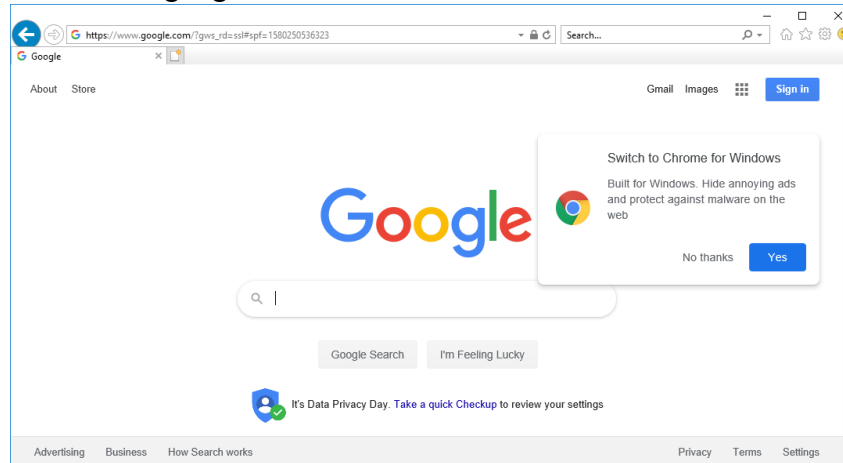


2. To see the Internet Explorer artifacts, navigate to: **HKCU\SOFTWARE\Microsoft\Internet Explorer**. Open the **TypedURLs** subkey and view the recent browsing activity

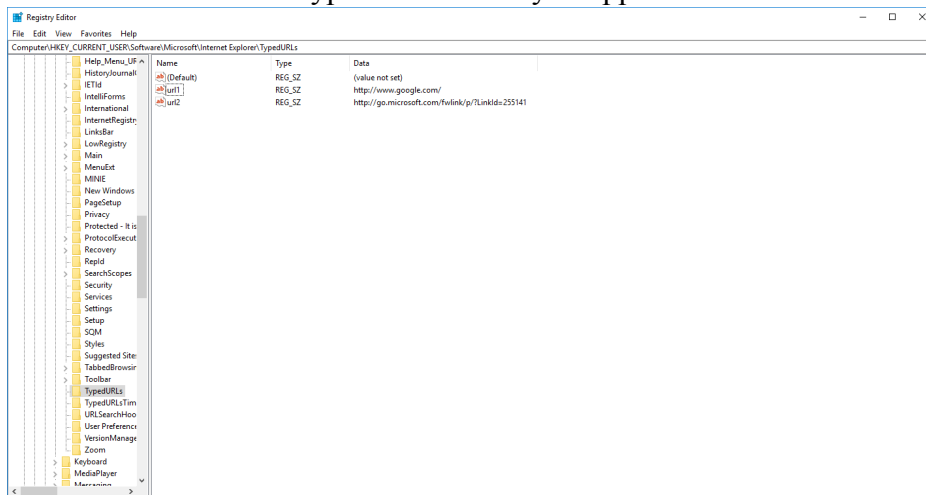


Also note the associated TypedURLsTime below TypedURLs

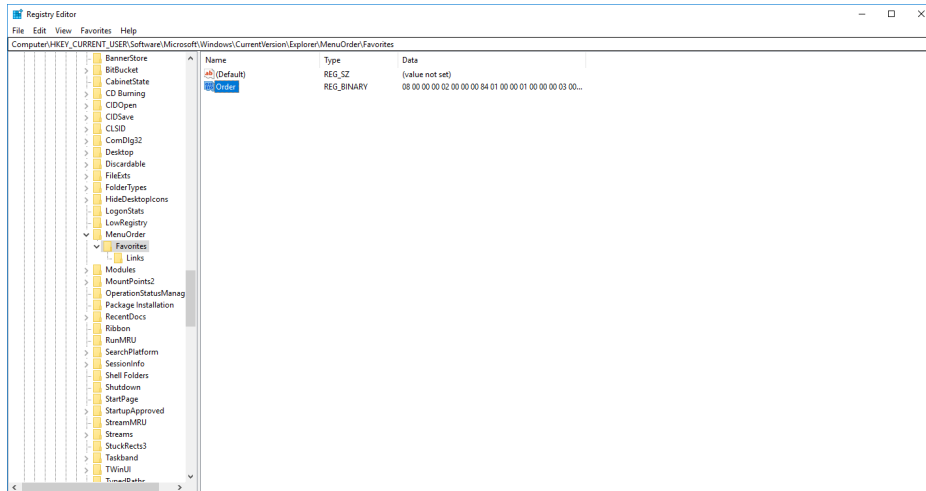
3. 5. NOTE: If no TypedURLs subkey is present, it likely hasn't been used yet. To create a series of Typed URL entries:
 1. In the Start / Ask Me Anything box, type in Internet Explorer.
 2. Select IE when the choice is displayed at the top of the list.
 3. Enter `www.google.com` into the browser address bar and hit enter



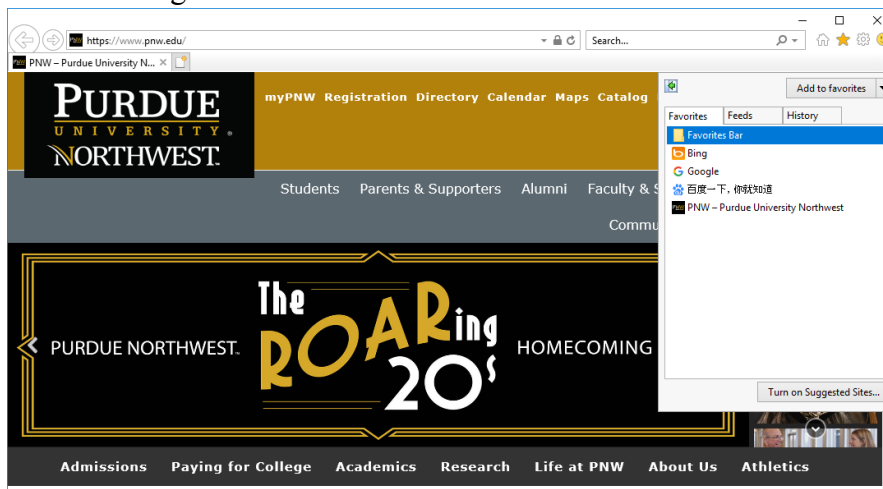
4. Return to Regedit and click View > Refresh or use the F5 key to refresh the screen. This should cause the TypedURLs subkey to appear and have the entries loaded.

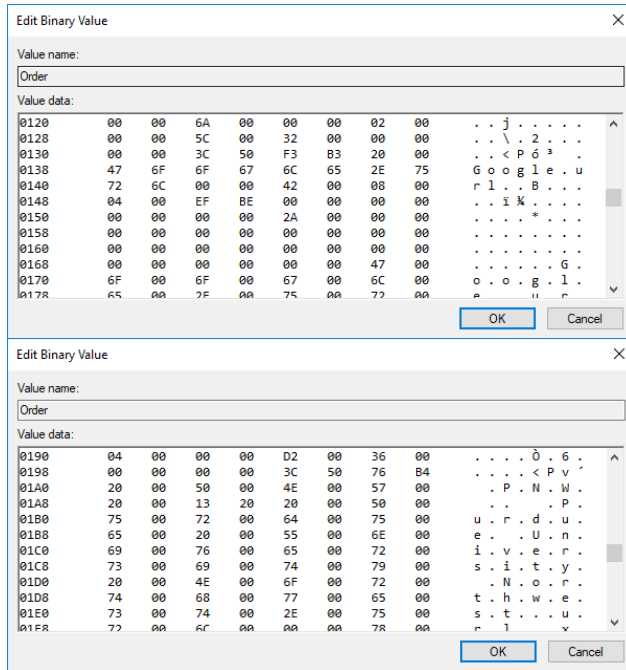


5. To view the user favorites for IE navigate to:
NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Favorites\Order

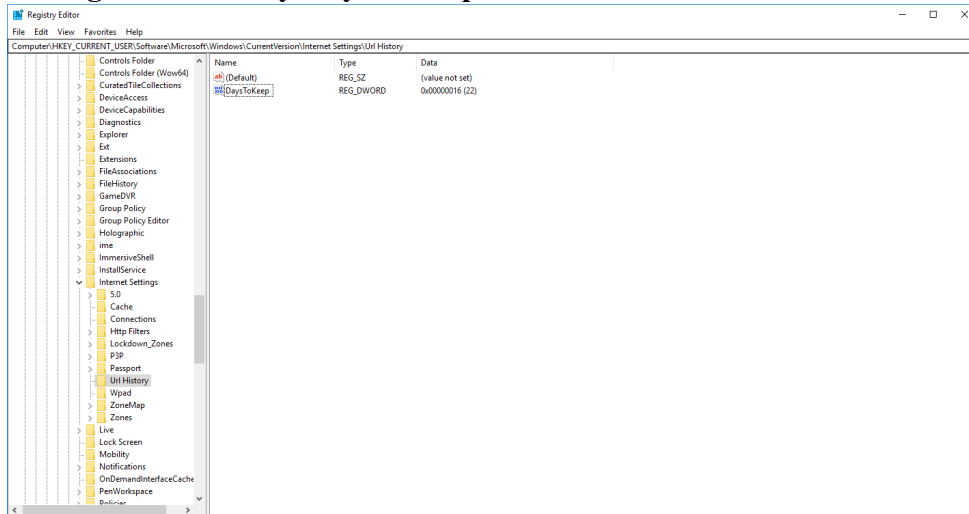


6. If no favorites are available other than the default root entries, add a folder to the IE favorites and browse to the pages entered above in the TypedURLs section. Add them to the Favorites folder.
7. Return to Regedit and refresh the screen to view the added favorites





- To view the History, navigate to:
NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\URLHistory\DaysToKeep

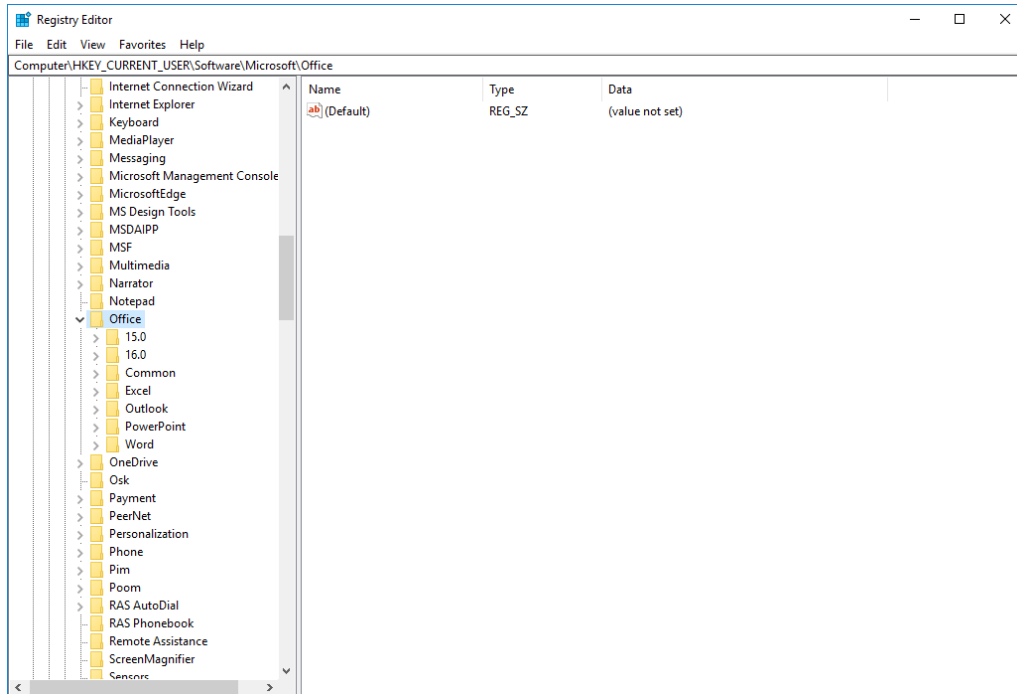


The setting by default is 0x 16 or decimal 22 days

Section 2 Microsoft Office

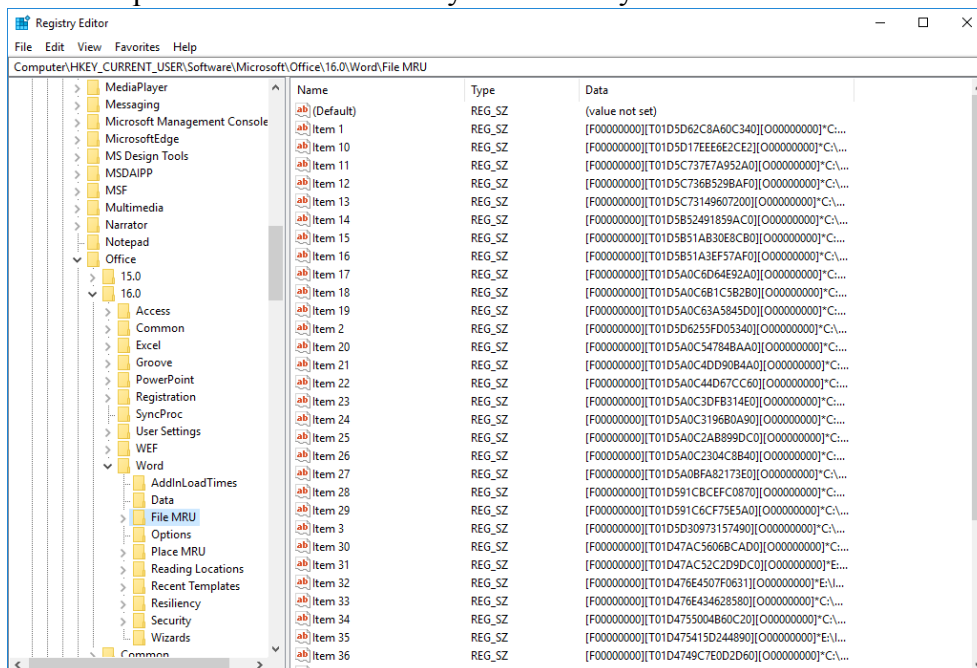
1. In Registry Viewer and the NTUSER.DAT, navigate to:

NTUSER.DAT\SOFTWARE\Microsoft\Office



Note the version number present where Version 12 = Office 2007, Version 14 = Office 2010 and Version 15 = Office 2013

2. Open the version number available in the lab machine
3. The common Office utilities are here; Access, Excel, PowerPoint, Word; along with their accompanying artifacts.
4. Open the Word subkey.
5. Note the File MRU where standard logon accounts (non-live account) store their most recently used information
6. Click to open the File MRU subkey and note any entries.

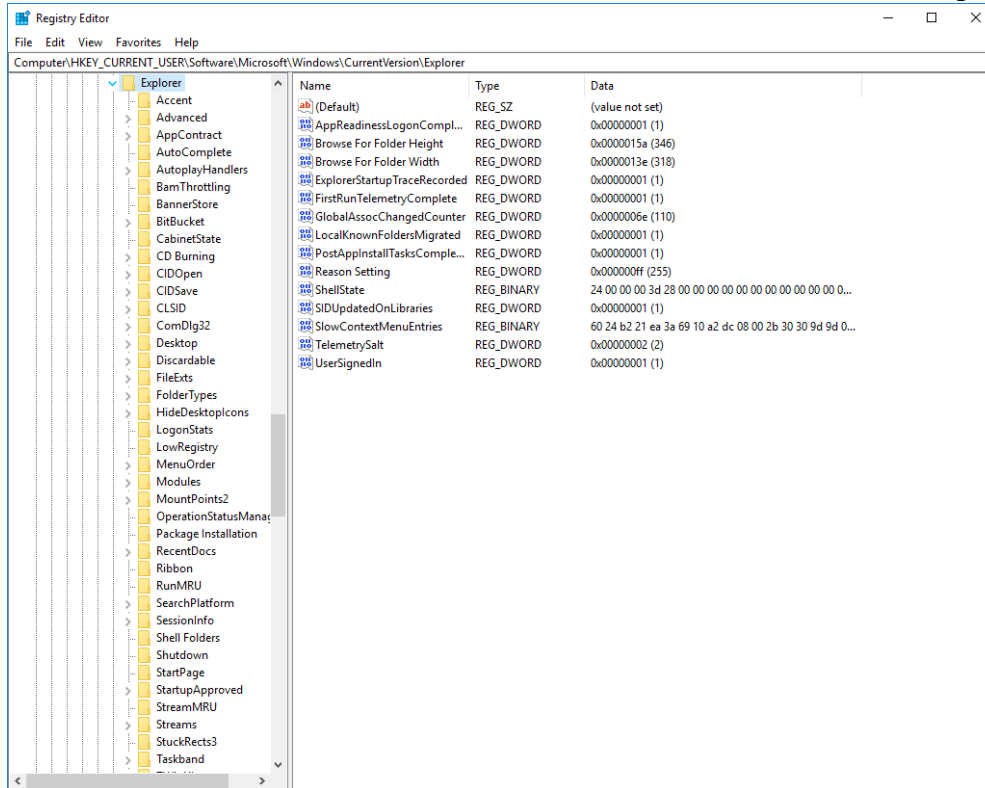


If no one exist, open Microsoft Word and create/save a new document to the Desktop, return to Regedit and refresh the view

7. Note within these MRUs are a 64-bit Windows FILE TIME date and time stamp, however it is stored in big endian / Unicode format rather than the traditional little endian / ASCII format.

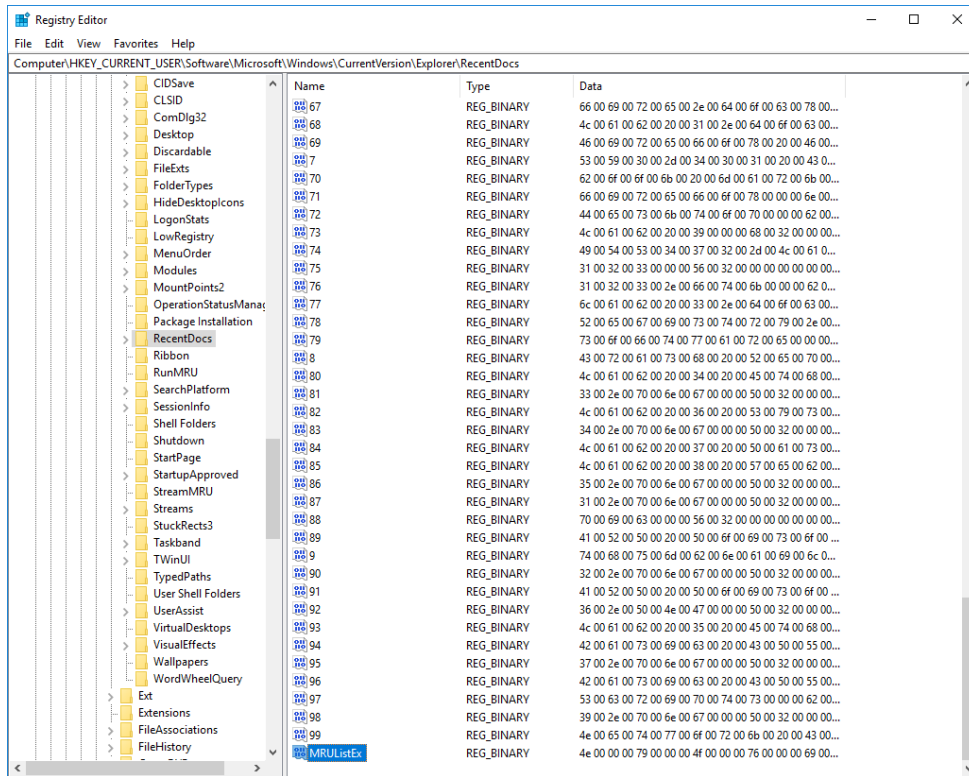
Section 3 Explorer Subkey

1. In Registry Viewer and the NTUSER.DAT, navigate to:
NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

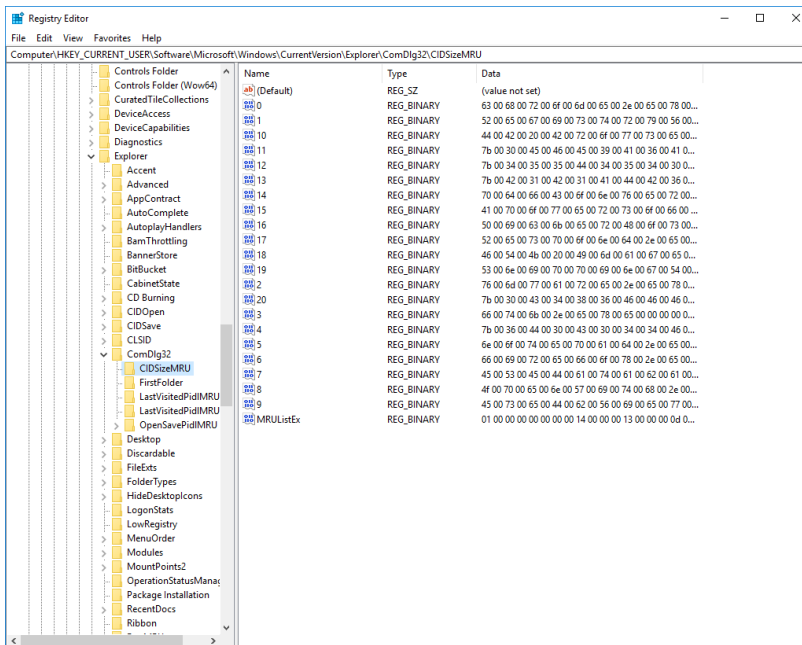


2. View the contents of the RecentDocs. This is storing references to documents accessed by extension. We can see the order opened through the MRUListEx; however dates and times are not available for each access. The last one on top is presumed to be the last modification of the subkey; hence that date/time can be read

from Key Properties

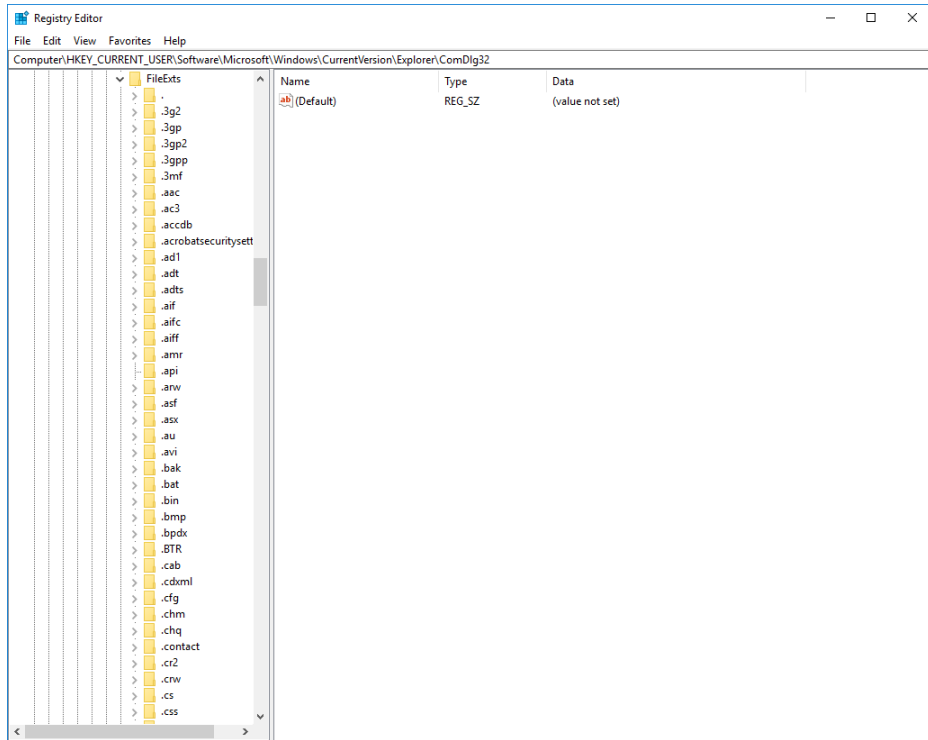


- View the contents of the ComDlg32. It is similar to RecentDocs in that it tracks the data in the same manner; however the data itself is not pulled from accessing documents. It is archived through the use of the Microsoft Common Save-As dialog box.



4. Open the FileExts subkey. This shows file extension associations for applications. In

Windows 10 it is also used for storing user searches in Cortana.



Part 4 UsrClass.dat Information

The objective of this lab is to familiarize the student with the Windows registry user profile; UsrClass. dat.

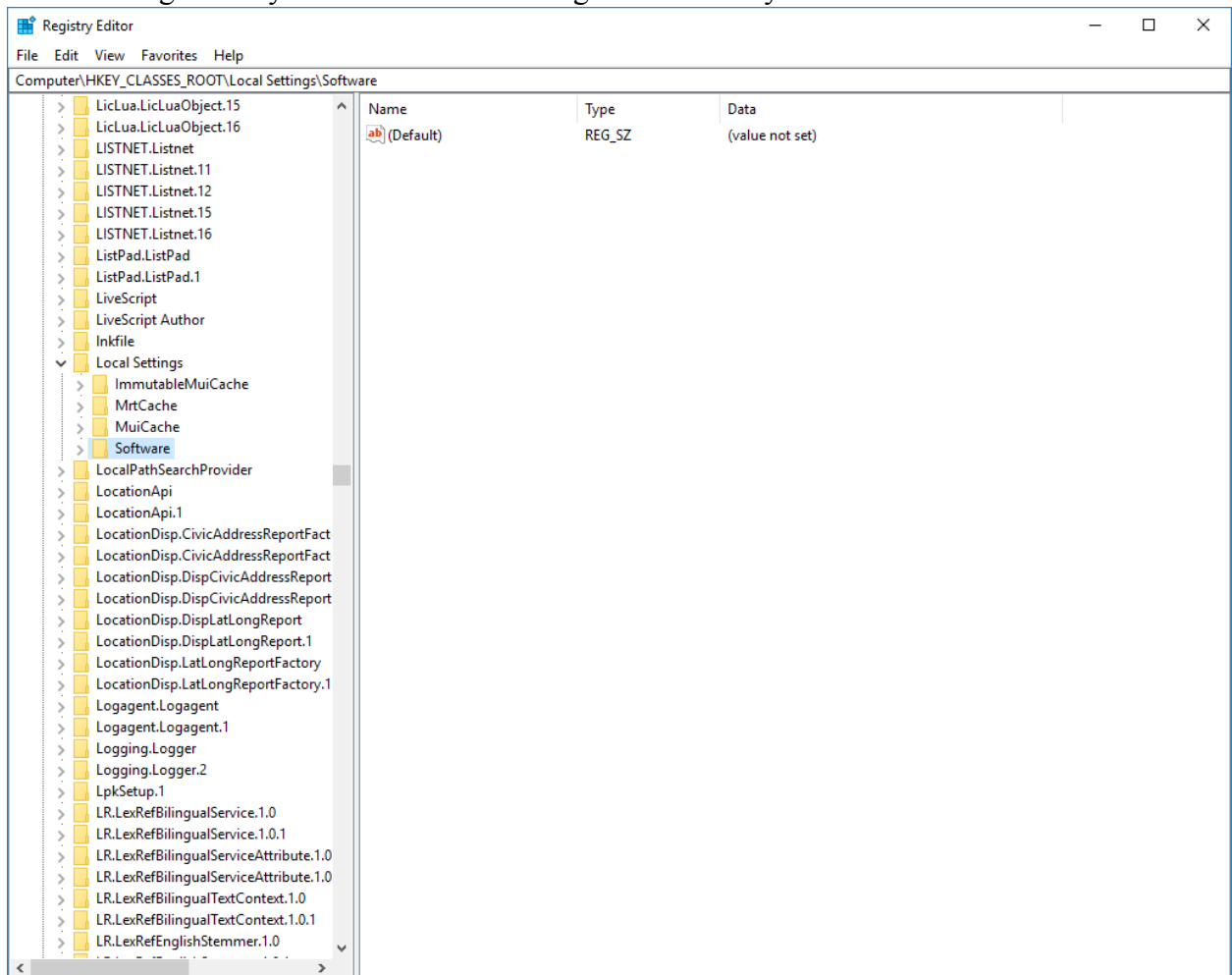
This lab uses Windows 10, File Explorer, Regedit, Registry Viewer, and the Lab Files folder; Win10 Reg Files.

Section 1 UsrClass.dat

1. Open Regedit and navigate to the HKCR root key. Navigate to:

HKEY_CLASSES_ROOT\Local Settings\Software

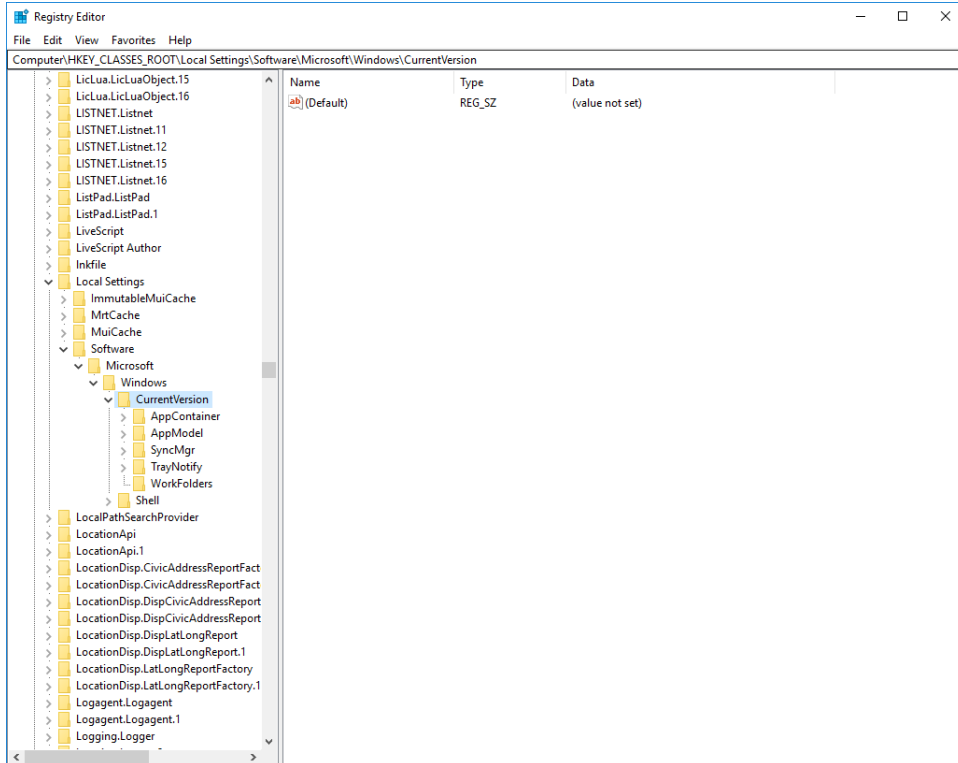
NOTE: There is a type down feature in Regedit. Place the cursor anywhere in the key navigation pane under the HKCR and type in “LO” quickly. This will take you to the Local Settings subkey which is in a rather large list of subkeys in the root of HKCR



2. This is the same as navigating to the UsrClass.DAT file.
3. Note the AppX entries in the root of the Local Settings subkey. These are identifiers for Windows Apps.
4. Navigate to:

HKCR\Local Setting\Software\Microsoft\Windows\CurrentVersion

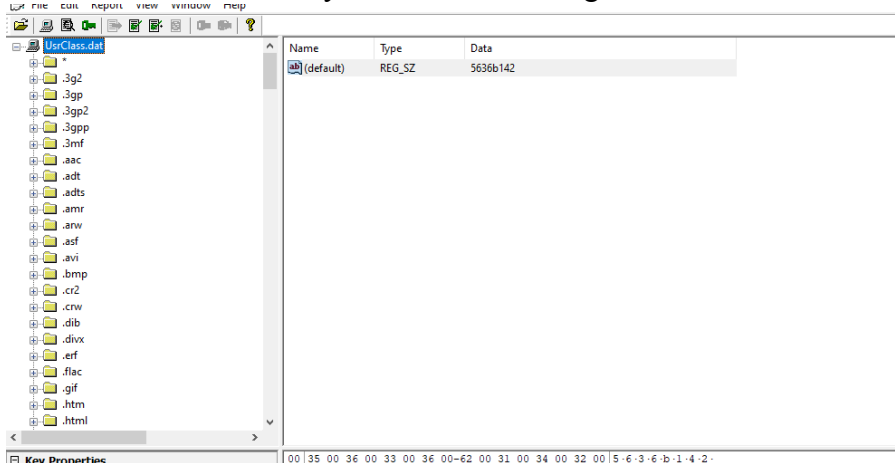
5. Note, both of these hold information regarding the Windows Apps.



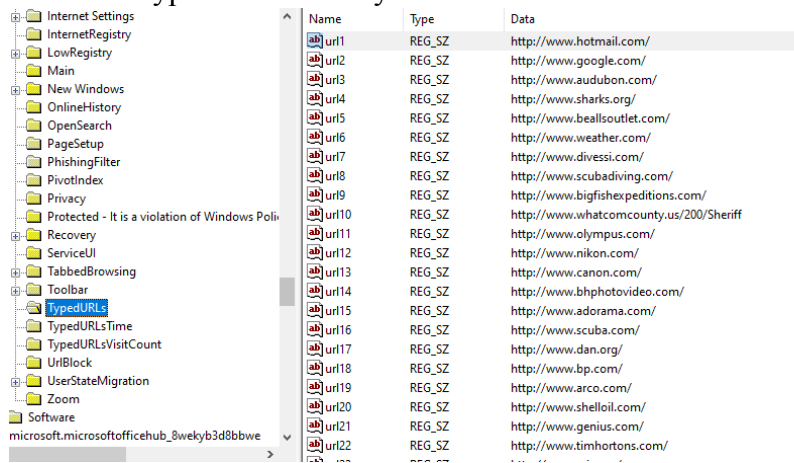
6. Navigate to: **HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppDataContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\Children\001\Internet Explorer\DOMStorage**

This is the TypedURLs for the new Edge browser

7. Open the UsrClass.dat file located in the Lab Files folder called Win10 Reg Files
8. 11. Note the difference between navigating in Regedit and Registry Viewer. In the actual registry being viewed by Regedit, the UsrClass.dat file data is stored as an alias in the HKCR subkey under Local Settings.



9. View the TypedURLs subkey here which has more data in it.



The image shows a screenshot of the Windows Registry Editor. The left pane displays a tree view of the registry, with 'TypedURLs' selected under the 'Internet Settings' folder. The right pane shows a list of registry values for 'TypedURLs'.

Name	Type	Data
url1	REG_SZ	http://www.hotmail.com/
url2	REG_SZ	http://www.google.com/
url3	REG_SZ	http://www.audubon.com/
url4	REG_SZ	http://www.sharks.org/
url5	REG_SZ	http://www.beallsoutlet.com/
url6	REG_SZ	http://www.weather.com/
url7	REG_SZ	http://www.divessi.com/
url8	REG_SZ	http://www.scubadiving.com/
url9	REG_SZ	http://www.bigfishexpeditions.com/
url10	REG_SZ	http://www.whatcomcounty.us/200/Sheriff
url11	REG_SZ	http://www.olympus.com/
url12	REG_SZ	http://www.nikon.com/
url13	REG_SZ	http://www.canon.com/
url14	REG_SZ	http://www.bhphotovideo.com/
url15	REG_SZ	http://www.adorama.com/
url16	REG_SZ	http://www.scuba.com/
url17	REG_SZ	http://www.dan.org/
url18	REG_SZ	http://www.bp.com/
url19	REG_SZ	http://www.arco.com/
url20	REG_SZ	http://www.shelloil.com/
url21	REG_SZ	http://www.genius.com/
url22	REG_SZ	http://www.timhortons.com/

Part 5 SAM File Information

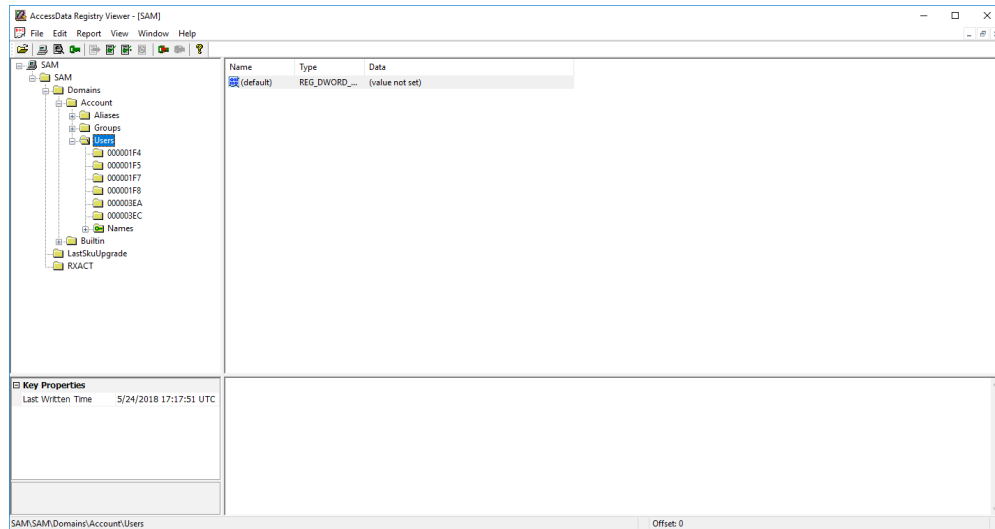
The objective of this lab is to familiarize the student with the Windows registry SAM file.

This lab uses Windows 10, File Explorer, Regedit, Registry Viewer, and the Lab Files folder; Win10 Reg Files.

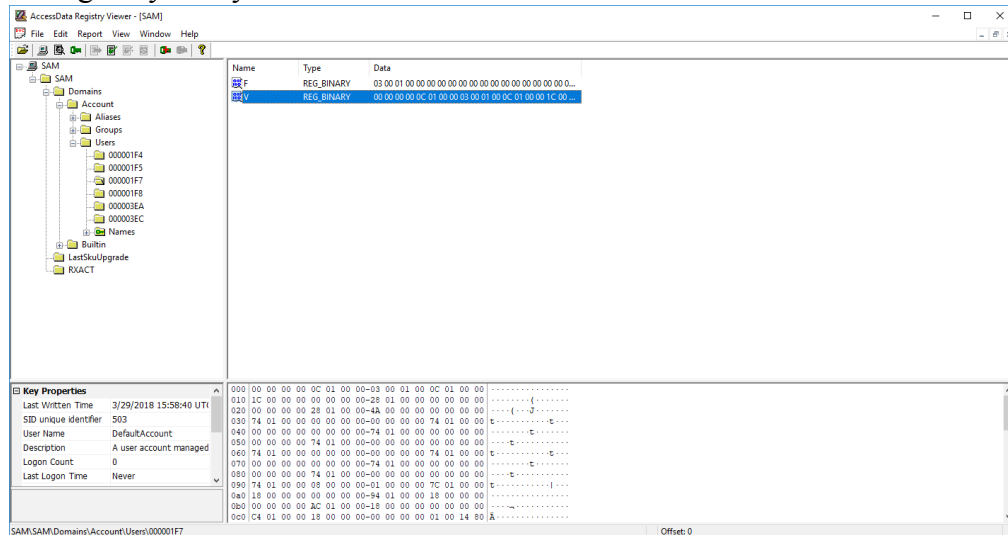
Section 1— SAM File

1. Open Regedit.
2. Open the SAM file located in the Lab Files10 Reg Files folder.
3. Navigate to:

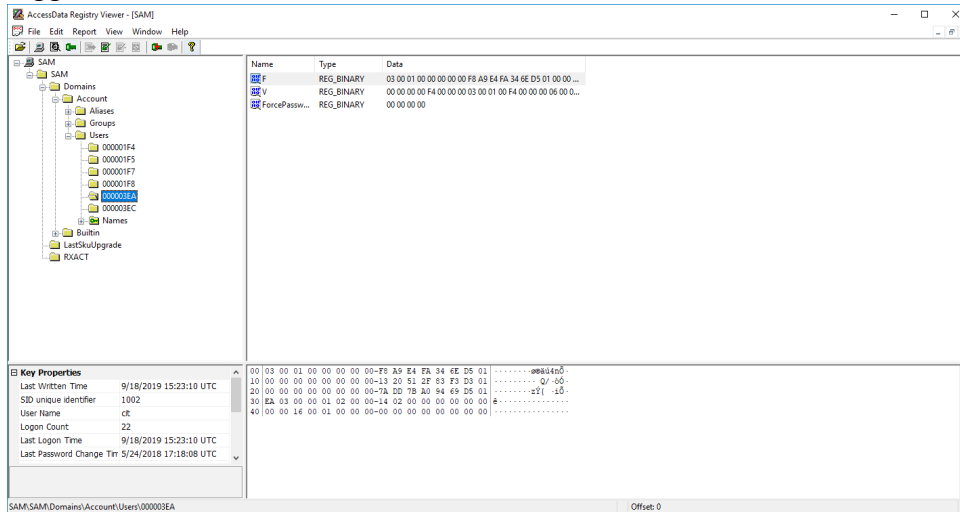
SAM\SAM\Domains\Account\Users



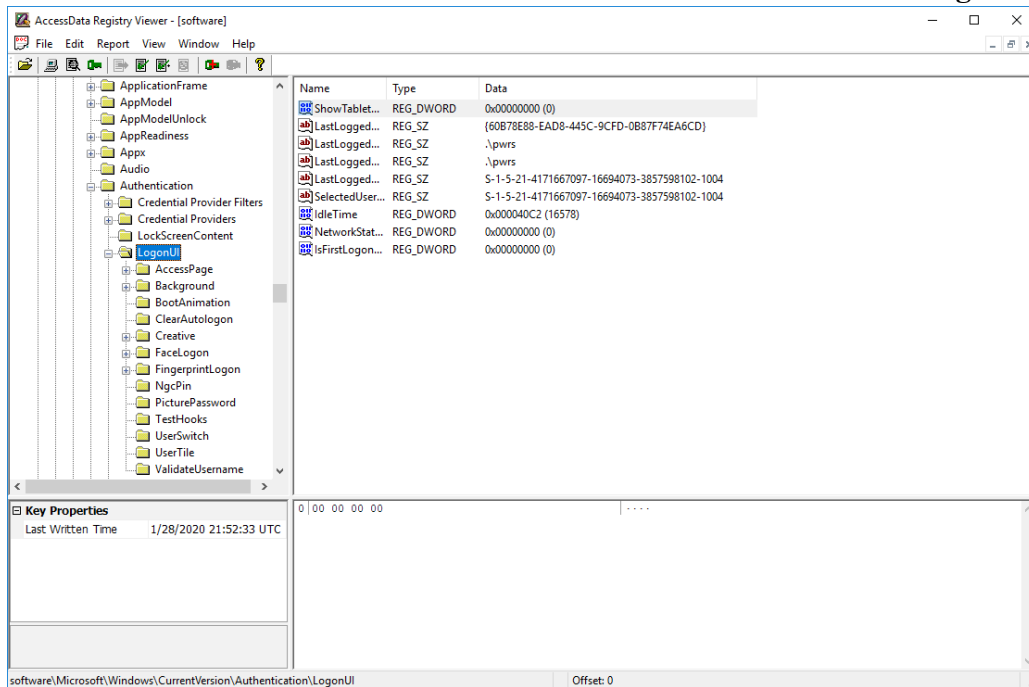
4. Click on the 000001F7 account
5. Click on the V value and scroll towards the bottom of the data. This is a new account setting in Windows 10 called the Default Account and is described as an account managed by the system



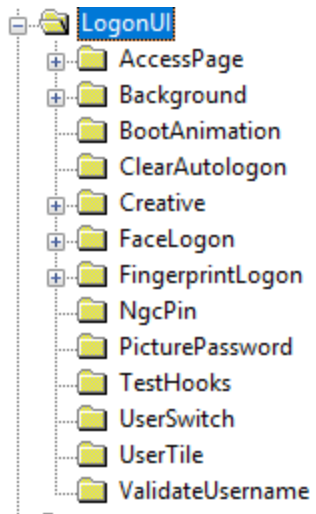
6. Click-on the user: 000003EA. This is a normal Windows account. Note in Key Properties this user name: CPUUser and the number of logons: 22, and the last time logged on: 9/18/2019



7. Close the SAM file in Registry Viewer and open the SOFTWARE file.
8. Navigate to:
SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI



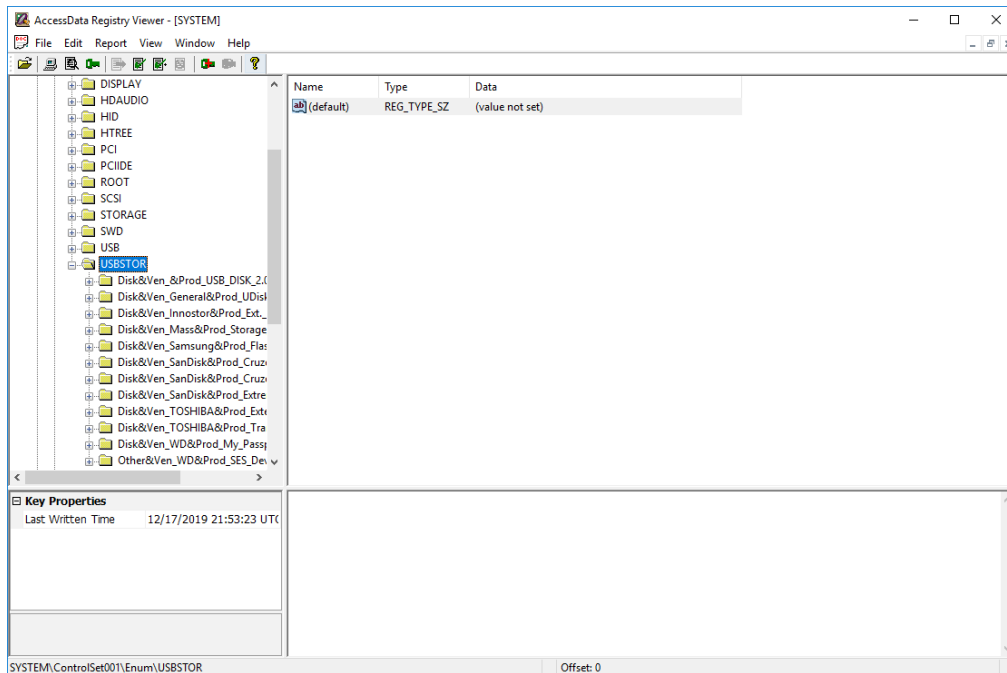
9. Note the logon status of users in the LogonUI values.
10. Note the subkeys for different types of logon authentications under the LogonUI subkey, namely.
 - a. FaceLogon
 - b. FingerprintLogon
 - c. PicturePassword
 - d. PINLogonEnrollment



Part 6 SYSTEM File Information

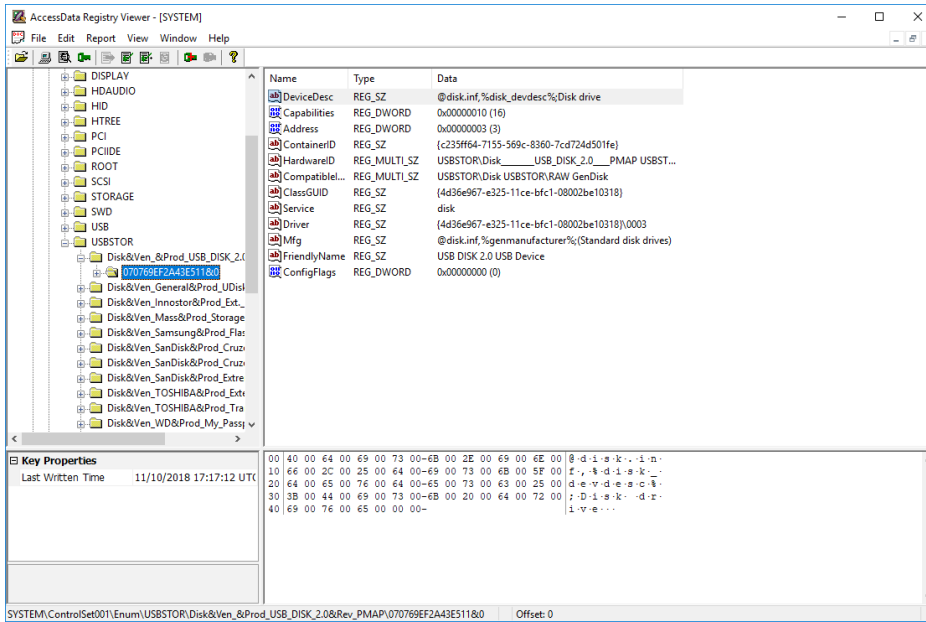
The objective of this lab is to familiarize the student with the Windows registry SYSTEM file. This lab uses Windows 10, File Explorer, Regedit, Registry Viewer, and the Lab Files folder; Win10 Reg Files.

1. Open Registry Viewer and view the SYSTEM registry file located in the Lab Files10 Reg Files folder
2. Navigate to:
SYSTEM\ControlSet001\Enum\USBSTOR

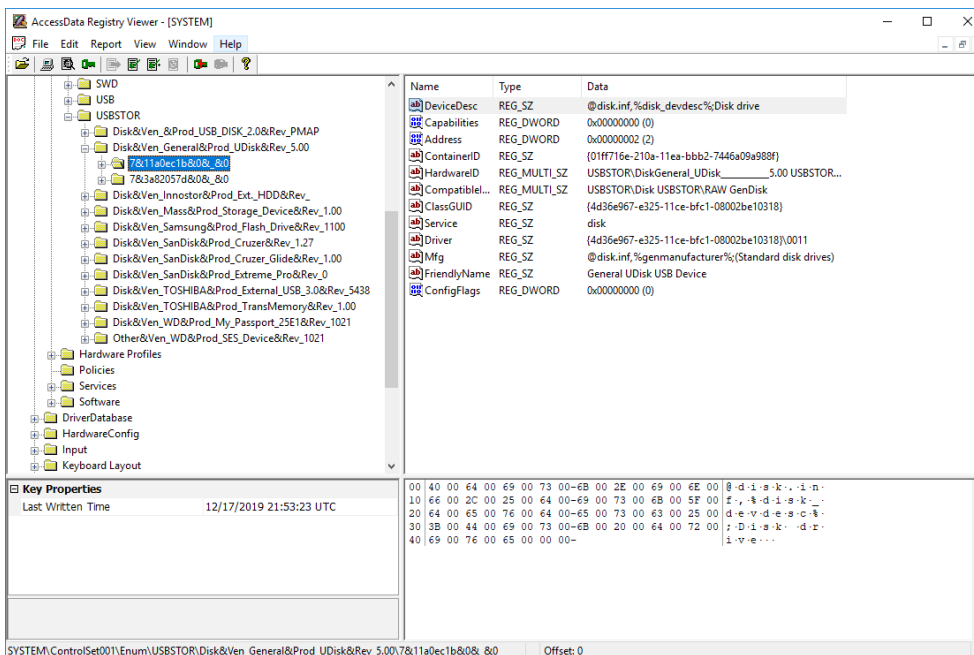


3. Each of the subkeys below USBSTOR represents a Disk and Vendor / Model name. Click on these, such as the WIBU Codemeter-Stick and note that each of the subkey

names are the drive identifiers for each device from that manufacturer



4. Each of the subkeys below USBSTOR represents a Disk and Vendor / Model name. Click on these, such as the WIBU Codemeter-Stick and note that each of the subkey names are the drive identifiers for each device from that manufacturer.



5. There are many other Property subkeys associated with devices that contain this information including but not limited to:
 - a. IDE
 - b. PCI
 - c. SCSI
 - d. STORAGE
 - e. USB
 - f. USBSTOR

SYSTEM\ControlSet001\Services\W32Time

AccessData Registry Viewer - [SYSTEM]

File Edit Report View Window Help

SYSTEM\ControlSet001\Services\W32Time

Name	Type	Data
Description	REG_SZ	@%SystemRoot%\system32\w32time.dll,-201
DisplayName	REG_SZ	@%SystemRoot%\system32\w32time.dll,-200
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	80 51 01 00 00 00 00 00 00 00 00 03 00 00 00 14 00 0...
ImagePath	REG_EXPAND_SZ	%SystemRoot%\system32\svchost.exe -k LocalService
ObjectName	REG_SZ	NT AUTHORITY\LocalService
RequiredPriv...	REG_MULTI_SZ	SeAuditPrivilege SeChangeNotifyPrivilege SeCreateG...
ServiceSidTy...	REG_DWORD	0x00000001 (1)
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000020 (32)

Key Properties

Last Written Time: 6/10/2018 22:45:25 UTC

SYSTEM\ControlSet001\Services\W32Time Offset: 0

9. This service tracks the automatic updating of the local machines time clock to an Internet time clock. Checking the Parameters subkey will display a value of Type. If the Type value data is NTP, the system is autosynching to the Internet. If it is not synching, it will say NoSync. The NtpServer value will show which time clock the system is using.

AccessData Registry Viewer - [SYSTEM]

File Edit Report View Window Help

SYSTEM\ControlSet001\Services\W32Time\Parameters

Name	Type	Data
NtpServer	REG_SZ	time.windows.com,0x9
ServiceDll	REG_EXPAND_SZ	%systemroot%\system32\w32time.dll
ServiceDllUn...	REG_DWORD	0x00000001 (1)
ServiceMain	REG_SZ	SvchostEntry_W32Time
Type	REG_SZ	NTPSDS

Key Properties

Last Written Time: 6/10/2018 22:48:16 UTC

SYSTEM\ControlSet001\Services\W32Time\Parameters Offset: 0