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 Eidtor

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						-	- 0	×
File Home Share	View							^ (
Pin to Quick Copy Paste	Cut Copy path Paste shortcut	name New item •	▼ Properties ▼ History	Select all Select none				
Clipboard	Organize	New	Open	Select				
← → ~ ↑ 📙 > TI	his PC > Windows (C:) > Windows > System3	32 → config			~ Ū	Search config		P
10:1	Name	Date modified Type	Size					
Cuick access	bbimigrate	6/9/2018 5:26 PM File	older					
Desktop 📌		4/11/2018 6:38 PM File	older					
Uownloads 🖈	RegBack	6/9/2018 2:27 PM File	older					
📋 Documents 🛛 🖈	systemprofile	4/11/2018 6:38 PM File	older					
Pictures 📌	TxR	12/19/2019 5:42 PM File	older					
- Homework	L] BBI	1/14/2020 5:56 PM File	1,280	KB				
E IE	BCD-Template	6/9/2018 5:26 PM File	28	KB				
Lab 6		1/23/2020 5:41 PM File	49,920	KB				
os		1/14/2020 5:50 PIVI File	1,024	KB				
This PC		7/9/2018 3:17 PM File	32	KB				
2D Objects	netlogon.ftl	1/24/2020 12:24 PM FTL	File 1	KB				
Dealstern	SAM	1/14/2020 5:56 PM File	72	KB				
Desktop	SECURITY	1/14/2020 5:56 PM File	112	KB				
Documents	SOFTWARE	1/15/2020 1:26 PM File	145,664	KB				
Downloads	SYSTEM	1/14/2020 5:56 PM File	26,112	KB				
Music	userdiff	6/9/2018 5:24 PM File	8	KB				
Pictures								
Videos								
🏪 Windows (C:)								
I Network								
-								
17 items								

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

	onfia					 ×
	char	10				
File Home	Share	View				~ 🔮
🖈 🖻	Ê.	🔏 Cut 📃 🛄) 🗙 📫 📔 🦞 New item 🔹 🖓 🕑 Open 👻 💾 Select all			
Pin to Quick Copy	Paste	Copy path Move Copy	Delete Rename New Properties			
access		Paste shortcut to • to •				
CI	ipboard	0	rganize New Open Select			
$\leftarrow \rightarrow \land \land$	> Thi	s PC > Windows (C:) > Windov	vs > System32 > config	~ 0	Search config	م
🖈 Ouick access		Name	Date modified Type Size			
Deckton		bbimigrate	6/9/2018 5:26 PM File folder			
Desktop	<u></u>	Journal	4/11/2018 6:38 PM File folder			
- Downloads	Я.	RegBack	6/9/2018 2:27 PM File folder			
Documents	Ŕ	systemprofile	4/11/2018 6:38 PM File folder			
Pictures	*	TxR	12/19/2019 5:42 PM File folder			
		BBI	1/14/2020 5:56 PM File 1,280 KB			
E IE		BCD-Template	6/9/2018 5:26 PM File 28 KB			
Lab 6			1/23/2020 5:41 PM File 49,920 KB			
os		DEFAULT	1/14/2020 5:56 PM File 1,024 KB			
_		DRIVERS	1/23/2020 5:40 PM File 5,156 KB			
This PC		ELAM	7/9/2018 3:17 PM File 32 KB			
3D Objects		netlogon.ftl	1/24/2020 12:24 PM FTL File 1 KB			
📃 Desktop		SAM	1/14/2020 5:56 PM File /2 KB			
🔮 Documents			1/14/2020 5:56 PM File 112 KB			
👆 Downloads			1/15/2020 1:20 PINI FILE 145,004 KB			
h Music		SYSTEM	6/0/2019 5:24 DMA Ella 8 KP			
Pictures		userain	0/9/2010 3:24 PWI PHE 0 KD			
Videos						
Windows (C	3)					
Network						
17 items 4 items	selected	167 MB				

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

📙 🛃 🚺 🖵 sł	nao106															-	×
File Home	Share	View															~ 🕐
Pin to Quick Copy access	Daste Paste	 ✓ Cut ✓ Copy path ✓ Paste shortcut 	Move to •	Copy to •	Delete Rer	name f	New folder	™ New it 1 Easy a	em • ccess •	Properties	→ Open → Definit S Arrow History	2	elect all elect none nvert selection				
Cli	pboard			Org	anize			New		C	Open		Select				
← → ~ ↑	> Th	is PC → Windows	(C:) → l	Jsers →	shao106									v ©	Search sha	o106	P
		Name	^			Date	modifi	ied	Type		Size						
📌 Quick access						Dute			1700		U.L.C						
E Desktop	*	3D Objects				1/13/	2020 2:	:58 PM	File fold	ler							
👃 Downloads	*	AppData				1/12/	2018 3:2	50 PIVI	File fold	ier Ior							
Documents	*	Deskton				1/13/	2020 2:	-58 DM	File fold	ler							
Pictures	*	Documents				1/13/	2020 2:	:58 PM	File fold	ler							
Homework		Downloads				1/13/	2020 2:	:58 PM	File fold	ler							
IF		Favorites				1/13/	2020 2:	:58 PM	File fold	ler							
Lab 6		n Links				1/13/	2020 2:	:58 PM	File fold	ler							
00		🎝 Music				1/13/	2020 2:	:58 PM	File fold	ler							
0s		OneDrive				3/27/	2018 10	0:39 AM	File fold	ler							
💻 This PC		Pictures				1/13/	2020 2:	:58 PM	File fold	ler							
🧊 3D Objects		🕐 Saved Game	25			1/13/	2020 2:	:58 PM	File fold	ler							
📃 Desktop		Searches				1/13/	2020 2:	:58 PM	File fold	ler							
Documents		Videos	-			1/13/	2020 2:	:58 PM	File fold	ler	4 700	1KD					
🕹 Downloads		NTUSER.DA	1			1/23/	2020 3:	:58 PM	DAI File	e	1,792	KB					
Music																	
Pictures																	
Videos																	
. Windows (C	9																
in standows (c	.,																
Network																	
15 items 1 item :	selected	1.75 MB															:==

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

associated UsrClass.dat file for this user

I Image: Imag	View			-		<
Pinto Quick Copy Paste	Cut Copy path Paste shortcut	Rename New Tolder New				
	C > Windows (C) > Users > shao106	AppData > Local > Microroft > Windowr	14 71	Search Windows		
	······································	Appbala / Local / Microsoft / Windows	~ 0	Search windows	~	<u></u>
📌 Quick access	Name	Date modified lype Size				
📃 Desktop 🛛 🖈	0	9/20/2019 1:06 PM File folder				
L Downloads	1033	9/20/2019 12:58 PM File folder				
Documents	ActionCenterCache	1/15/2020 1:56 PM File folder				
Distures	Application Shortcuts	1/13/2020 2:58 PM File folder				
Pictures y	Burn Cashas	9/20/2019 12:08 PM File Tolder				
Homework	CloudStore	4/11/2019 6:29 DM File folder				
IE IE	Evplorer	10/11/2010 0:50 PM File folder				
Lab 6	GameExplorer	4/11/2018 6:38 PM File folder				
os	History	3/27/2018 10:29 AM File folder				
This PC	Notifications	3/27/2018 10:38 AM File folder				
3D Objects	PPBCompatCache	9/20/2019 1:07 PM File folder				
Deskton	PPBCompatUaCache	9/20/2019 1:07 PM File folder				
Desuments	PRICache	9/20/2019 12:58 PM File folder				
Documents	Ringtones	9/20/2019 12:58 PM File folder				
- Downloads	RoamingTiles	3/27/2018 10:25 AM File folder				
Music	Safety	9/20/2019 12:59 PM File folder				
Pictures	SchCache	9/20/2019 12:57 PM File folder				
Videos	Shell	4/11/2018 6:38 PM File folder				
Windows (C:)	UPPS	10/19/2019 1:57 PM File folder				
A Network	WER	9/20/2019 1:00 PM File folder				
	WinX	3/18/2017 4:03 PM File folder				
	Usrciass.dat	1/15/2020 3:50 PM DAT File 3,072 KB				
23 items 1 item selected 3.	00 MB					

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.

📕 🛃 📕 🖛 Pr	rograms	;								-	×
File Home	Share	View									~ 🕐
Pin to Quick Copy access	📋 Paste	<mark>‰ Cut</mark> ₩ Copy path Paste shortcut	Move Copy to v to v	elete Rename	New New folder	tem • access •	Properties	Select all Select none			
Cli	pboard		Organiz	:e	New		Open	Select			
← → • ↑	→ Th	is PC → Windows	(C:) → Windows →	appcompat >	Programs				~ 0	Search Programs	Q
🕹 Quick access		Name	^	Da	te modified	Туре	Size				
Deckton		🔄 Install		9/7	20/2019 1:18 PM	File folde	r				
Desktop		Amcache.hv	ve	1/1	14/2020 5:56 PM	HVE File	7,168	KB			
- Downloads	ж	Amcache.hv	ve.tmp.LOG1	3/2	29/2018 11:27 AM	LOG1 File	e 0	КВ			
Documents	*	Amcache.hv	ve.tmp.LOG2	3/3	29/2018 11:27 AM	LOG2 File	e 0	KB			
Pictures	Я										
Homework											
L IE											
Lab 6											
os											
This PC											
🧊 3D Objects											
📃 Desktop											
🔮 Documents											
👆 Downloads											
👌 Music											
Pictures											
📕 Videos											
🏪 Windows (C	:)										
鹶 Network											
-											
4 items 3 items s	elected	7.00 MB									

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

e\Settings. View the associated settings.dat for this application. This is not a registry file

📕 🛃 📕 🗢 Settings				-	\Box ×
File Home Sha	e View				~ 🕐
Pin to Quick Copy Paste access Clipboar	Coty Copy path Paste shortcut Copy Dath Copy Dath	ne New folder New	Properties Open ~ Poperties Open	Select all Select none Invert selection Select	
← → • ↑ <mark> </mark> « /	AppData > Local > Packages > Microsoft.Window	sStore_8wekyb3d8bbwe ⇒ Se	ettings v ひ	Search Settings	<i>م</i>
Quick access Desktop Downloads Documents Pictures Lab 6 os This PC 3D Objects Desktop Viewondas Music Viewondas	Name roaming.lock settings.dat	Date modified 6/6/2018 1:10 PM LOCK 1/23/2020 3:57 PM DAT Fi	Size File 0 K	B	
2 items					

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





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.

Registry Editor						-	×
File Edit View Favorites Help Computer\HKEY LOCAL MACHINE\S/	AM						
Computer\HKEY_LOCAL_MACHINESS Computer Computer HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT SECOND SECOND SECOND SECOND HKEY_CLASSES SECONTY SOFTWARE SOFTWARE SOFTWARE HKEY_CURRENT_CONFIG	Marne @ (Default)	Type REG_SZ	Data (value not set)				

4. Click on the SOFTWARE root key under HKEY LOCAL MACHINE and navigate to the flowing path: HKLM_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

📑 Registry Editor			-	×
File Edit View Favorites Help				
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\	CurrentVersion			
> WAB ^ Name	Туре	Data		
- Wallet (Default)	REG SZ	(value not set)		
> Wbem ab BuildBranch	REG SZ	rs4 release		
> WcmSvc ab BuildGUID	REG SZ			
> WIMMount Dia BuildLab	REG SZ	17134,rs4 release.180410-1804		
> Windows ab BuildLabEx	REG SZ	17134.1.amd64fre.rs4 release.180410-1804		
Windows Advanc	REG_SZ	Enterprise		
Windows Defend	REG_SZ	17134		
Windows Decktor	REG_SZ	17134		
Windows Embed	REG_DWORD	0x0000000 (10)		
Windows Mail 🛛 🐯 CurrentMinorVersionNumber	REG_DWORD	0x00000000 (0)		
> Windows Media (🛛 💐 Current Type	REG_SZ	Multiprocessor Free		
> Windows Media F ab CurrentVersion	REG_SZ	6.3		
> Windows Media F 🕺 DigitalProductId	REG_BINARY	a4 00 00 03 00 00 03 30 33 32 38 2d 31 30 30 3		
> Windows Messag BigitalProductId4	REG_BINARY	f8 04 00 00 04 00 00 03 5 00 35 00 30 00 34 00 31 00		
Vindows NT 🐠 EditionID	REG_SZ	Education		
> CurrentVersion EditionSubManufacturer	REG_SZ			
> Windows Phone ab EditionSubstring	REG_SZ			
Windows Photo \ Description Edition SubVersion	REG_SZ			
> Windows Portabl and Installation Type	REG_SZ	Client		
Windows Script F	REG_DWORD	0x5b3a4e09 (1530547721)		
Windows Search 🕮 InstallTime	REG_QWORD	0x1d4121ef1d649c4 (131750213216258500)		
Windows Security	REG_SZ	C:\Windows		
WindowsRuntime Moductid	REG_SZ	00328-10000-00001-AA854		
WindowsSelfHost ProductName	REG_SZ	Windows 10 Education		
WindowsStore MegisteredOrganization	REG_SZ			
WindowsUpdate 🛛 🔊 RegisteredOwner	REG_SZ	Windows User		
> Wisp ab Released	REG_SZ	1803		
> WlanSvc 🚵 SoftwareType	REG_SZ	System		
> WIpasvc	REG_SZ	C:\WINDOWS		
> 📙 Wow64 🛛 🐻 UBR	REG_DWORD	0x000004de (1246)		
> WSDAPI				
> WwanSvc				
L XAML				
< Monilla >				
A A				

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

5. 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.

🔍 AccessData FTK Imager 3.0.1.1467	_		\times
<u>File V</u> iew <u>M</u> ode <u>H</u> elp			
🚯 🎎 🗣 🖄 🖄 🖸 🖬 🖬 🗛 💷 🚥	• 🕅 📴 🔍 🗋 📾 🐱 😹 📓 🖕		
Evidence Tree ×	< File List		×
	Name Size Type Date Modified		
Custom Content Sources × Evidence:File System Path File Options New Edt Bemove Remove Al Create Image Properties Hex Value Int Custom Conte For User Guide, press F1	Obtain System Files X Source for obtaining files: Warning: Please be aware that FTK Imager is obtaining the pystem files from the live system and not the acquired image. Destination for obtained files: Browse C: Users Dwrs/Desktop MyRegFiles Options Options OK OK Cancel	NUM	

- 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.

🔍 AccessData FTK Imager 3.0.1.1467		-		(
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp				
	a =	🕅 📴 🥄 🗋 🖹 📾 🐱 鼹 🦉 🛓		
Evidence Tree	×	File List		×
Pertain 1[499MB] Partition 1[499MB] Partition 1[235594MB] Partition 2[235594MB] Partition 3[2300MB] D=1 Unpartitioned Space [basic disk]	A	Name Size Type Date Modified		
Custom Content Sources	×	000000000 33 C0 8E D0 BC 00 7C 8E-C0 8E D8 BE 00 7C BF 00 3Å BA+ -Å-64+ ; 0000000010 0 6 B9 00 02 FC F3 A4 50-68 IC 06 CB FB B9 04 00 -* - 000FD 00		^
Evidence:File System Path File	Options	0000000030 E2 F1 CD 18 88 56 00 55-C6 46 11 05 C6 46 10 00 âñÍ · V·UEF · EF ·		
< Edt Bemove Remove All Greate Properties Hex Value Int., Oust	> Image om Conte	$ \begin{array}{c} 0000000000 \ Ba \ 41 \ Bb \ Ak \ 55 \ Cb \ 15 \ 5b^{-1} \ 20 \ c1 \ Fb \ 53 \ Ak \ 75 \ 00 \ 74 \ Ab \ -tb^{-1} \ Ff \ \cdots \ t \\ 0000000000 \ 26 \ 66 \ 68 \ 00 \ 00 \ 00 \ 66 \ Fb \ 10 \ 00 \ 74 \ Ab \ -tb^{-1} \ Ff \ \cdots \ t \\ 0000000000 \ 26 \ 66 \ 68 \ 00 \ 00 \ 00 \ 00 \ 66 \ Fb \ 10 \ 00 \ 74 \ Ab \ -tb^{-1} \ Ff \ \cdots \ t \\ 0000000000 \ 76 \ 83 \ C1 \ 10 \ 9E \ Fb \ 14 \ Ab \ -tb^{-1} \ Fb \ -tb^{-1} \ t \ -tb^{-1} \ Fb^{-1} \ t \ -tb^{-1} \ -tb^{-1} \ Fb^{-1} \ t \ -tb^{-1} \ -tb^{-1} \ Fb^{-1} \ t \ -tb^{-1} \$		<
V VPHYSICAL DRIVEO	on contem	porior pos - o, pry sec - o	NUM	
III IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIII				

12. Open that and navigate to the UsrClass.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.

Q AccessData FTK Imager 3.0.1.1467	X
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp	
🗛 🍕 🗣 🗠 🚖 🖨 🖬 🖬 🚛 🚙 👄	译 📵 🔧 🗋 🖻 📴 🐱 證 🦿 🖕
Evidence Tree	× File List ×
Evidence Tree Evidence Tree Vindows AdminArsenal AdminArsenal Approprime Install AdminArsenal Approprime Install AppReadmess AdminArsenal AppReadmess AdminArsenal AppReadmess AdminArsenal AppReadmess Custom Content Sources Evidence:File System/Path/File Options New Edit Remove Remove All Create Install Custom Content Sources Evidence:File System/Path/File	File List X Name Size Type Date Modified Install 1 KB Directory 1/17/2020 114 SI30 4 KB NTFS Index All 9/10/2018 4:01: Amacche.hve 4,608 KB Regular File 6/10/2018 104 Browse For Folder X 9/10/2018 104 6/10/2018 104 Select the destination folder X/2/2018 4:184 7/2/2018 4:184 Desktop I.bibraries X 7/2/2018 4:184 Desktop I.bibraries Network fifterfox Lab09 Visers All Users Visers All Users X Grancel
Properties Hex Value Int Custom Conte	<u></u>

 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.

22 4										- V
AccessData Registry Viewer									_	U X
	_								_	
	🖉 Open								×	
	← → ∽ ↑ [→ This PC → Deskto	op → MyRegFiles			v ©	Search MyRegFile		P	
	Organize 🔻 Ne	ew folder					85	•	0	
		Name	^	Date modified	Туре	Size				
	Quick access	Users		1/24/2020 3:11 PM	File folder					
	Downloads	Amcach	e.hve	1/17/2020 5:45 PM	HVE File	4,608 KI				
	🗄 Documents	SAM		1/17/2020 5:45 PM	File	2,048 KI 72 KI				
	E Pictures	* SECURIT	Y	1/17/2020 5:45 PM	File	112 Ki				
	Homework	settings.	dat	1/22/2020 6:18 PM	DAT File	8 KI				
	New folder	software system		1/17/2020 5:45 PM	File	24,064 KI				
	seperate	s (xob) userdiff		6/10/2018 8:42 PM	File	8 KI				
	This DC	UsrClass	.dat	1/22/2020 6:18 PM	DAT File	3,584 KI				
	inis PC									
	Network									
		File name: software				~	All Files		~	
							Open	Cancel		
					_	_			.1	
AccessData Registry Viewer										
K AccessData Registry Viewer - [software]								-) ×
File Edit Report View Window Help										- 8 ×
🚔 🚇 🗣 🗁 🗑 🖻 🔍 🖛 🤗										
⊡ 🚍 software	^ Name	Туре	Data							
) (default)	REG_SZ	(value not set)							
Accessbata										
Autodesk										
Classes										
Clients										
Hewlett-Packard										
🖶 🦳 Intel										
IXXAT										
JavaSoft										
Khronos										
🖶 🧰 Macromedia										
🗄 🧰 Microsoft										
Mozilla										
MozillaPlugins										
Wance										
NVIDIA Corporation										
- Partner	v									
Key Properties	0 00 00									~
Last Written Time 9/9/2019 16:41:52 UTC										
2,2,2,2,2,2,2,0,1,1,2,2,0,1										
										~
										~

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

17. Click on InstallDate value.

K AccessData Registry Viewer - [software]				-	ΟX
💬 File Edit Report View Window Help					- 5 ×
🖆 🚇 🗟 📭 📄 🗑 📑 💷 🕪 🤶					
Visual JSharp Setup	Name	Туре	Data		^
UsualStudio	ab SystemRoot	REG_SZ	C:\WINDOWS		
ia- iai WAB	ab BuildBranch	REG_SZ	rs4_release		
Wallet	ab BuildGUID	REG_SZ	ffffffff-ffff-ffff-ffff-ffffffffffffff		
B- Ween	ab BuildLab	REG_SZ	17134.rs4_release.180410-1804		
WithMount	ab BuildLabEx	REG_SZ	17134.1.amd64fre.rs4_release.180410-1804		
Windows	ab CompositionEditionID	REG_SZ	Enterprise		
Windows Advanced Threat Protection	ab CurrentBuild	REG_SZ	17134		
Windows Defender	ab CurrentBuildNumber	REG_SZ	17134		
Windows Defender Security Center	CurrentMajorVersionNumber	REG_DWORD	0x0000000A (10)		
- Windows Desktop Search	CurrentMinorVersionNumber	REG_DWORD	0x00000000 (0)		
🗄 🦲 Windows Embedded	(ab) CurrentType	REG_SZ	Multiprocessor Free		
Windows Mail	(ab) CurrentVersion	REG_SZ	6.3		
Windows Media Device Manager	ab) EditionID	REG_SZ	Education		
Windows Media Foundation	EditionSubManufacturer	REG_SZ	(value not set)		
Windows Media Player NSS Windows Media Player NSS	ab EditionSubstring	REG_SZ	(value not set)		
Windows Messaging Subsystem	ab EditionSubVersion	REG_SZ	(value not set)		
ia- 🖸 Windows NT	ab InstallationType	REG_SZ	Client		
CurrentVersion	践 InstallDate	REG_DWORD	0x5B3A4E09 (1530547721)		
Windows Phone	ab ProductName	REG_SZ	Windows 10 Education		
Windows Photo Viewer	ab Releaseld	REG_SZ	1803		
Windows Script Hort	ab SoftwareType	REG_SZ	System		
Windows Search	A UBR	REG_DWORD	0x000004DE (1246)		~
i i i i i i i i i i i i i i i i i i i		DEC 07			
Key Properties	0 09 4E 3A 5B		-N: [^
Last Written Time 1/22/2020 23:49:46 UTC					
OS Instal Date (UTC) Mon Jul 02 16:08:41 2018					
OS Install Date (Local) Mon Jul 02 11:08:41 2018					
software\Microsoft\Windows NT\CurrentVersion		С	Offset: 0		

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

🔏 AccessData Reg	istry Vi	ewer - [software]				_		
🕎 File Edit Re	port	View Window Help					- 5	×
🔊 🚊 🖪 🖛		7 R* 8 0= 8 ?						
🗊 🧰 Visua	l JSharj	o Setup 🔦	Name	Туре	Data			^
😥 🧰 Visua	IStudio	1	ab] SystemBoot	REG SZ	C:\WINDOWS			
🔋 🧰 WAB			ab BuildBranch	REG SZ	rs4 release			
Walle	t		BuildGUID	REG SZ	ffffffff-ffff-ffff-fffff-ffffffffffff			
i Wbe	n		BuildLab	REG SZ	17134.rs4 release.180410-1804			
i 🛛 🔤 Wcm	Svc		BuildLabEx	REG SZ				
Hex Interpreter			× CompositionEditionID	REG SZ	Enterprise			
Tune	Size	Value	CurrentBuild	REG SZ	17134			
signed integer	1.8	1530547721	CurrentBuildNumber	REG SZ	17134			
unsigned integer	1.8	1530547721	CurrentMajorVersionNumber	REG DWORD	0x0000000A (10)			
FILETIME (Stored)	8		CurrentMinorVersionNumber	REG DWORD	0x00000000 (0)			
FILETIME (As Local)	8		CurrentType	REG SZ	Multiprocessor Free			
DOS date	2	·	CurrentVersion	REG SZ	6.3			
DOS time	2	•	ditionID	REG SZ	Education			
DOS date/time	4	9/26/2025 9:48:18 AM	ditionSubManufacturer	REG_SZ	(value not set)			
time_t (Stored)	4	Mon Jul 02 15:08:41 2018 Mon Jul 02 11:09:41 2019	ditionSubstring	REG_SZ	(value not set)			
Unicode string	2+	= #	ditionSubVersion	REG_SZ	(value not set)			
Chicode cang			nstallationType	REG_SZ	Client			
			nstallDate	REG_DWORD	0x5B3A4E09 (1530547721)			
			ProductName	REG_SZ	Windows 10 Education			
			Releaseld	REG_SZ	1803			
			oftwareType	REG_SZ	System			
Byte order:	Little	endian i 🔘 Big endian	JBR	REG_DWORD	0x000004DE (1246)			
	0003 50	uren v	late and	BEC 67	6007 I			<u> </u>
Key Properties			0 09 4E 3A 5B		-28 : [\wedge
Last Written Tim	e	1/22/2020 23:49:46 UTC						
OS Install Date (UTC)	Mon Jul 02 16:08:41 2018						
OS Install Date (Local)	Mon Jul 02 11:08:41 2018						
I]					4
software\Microsoft\	Window	vs NT\CurrentVersion		C	Start: 0 Selected: 4			



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.

-			1	
🔀 AccessData Registry Viewer - [software]				- 🗆 X
💬 File Edit Report View Window Help				_ 8 ×
🛎 😹 🖲 📭 📑 🗉 🖻 🖛 🗎	8			
🗊 🦲 Visual JSharp Setup	^ Name	Туре	Data	^
Hex Interpreter	rrentBuildNumber	REG_SZ	17134	
•	urrentMajorVersionNumber	REG_DWORD	0x0000000A (10)	
Type Size Value	rrentMinorVersionNumber	REG_DWORD	0x00000000 (0)	
signed integer 1-8 13175021321625850	0 irrentType	REG_SZ	Multiprocessor Free	
unsigned integer 1-8 13175021321525850	urrentVersion	REG_SZ	6.3	
FILETIME (Stored) 8 7727201816:08:41	itionID	REG_SZ	Education	
DDS date 2	itionSubManufacturer	REG_SZ	(value not set)	
DOS time 2 ·	itionSubstring	REG_SZ	(value not set)	
DOS date/time 4 ·	itionSubVersion	REG_SZ	(value not set)	
time_t (Stored) 4 ·	stallationType	REG_SZ	Client	
time_t (As Local) 4 ·	stallDate	REG_DWORD	0x5B3A4E09 (1530547721)	
Unicode string 2 + 않니까ů	oductName	REG_SZ	Windows 10 Education	
	leaseld	REG_SZ	1803	
	ftwareType	REG_SZ	System	
	3R	REG_DWORD	0x000004DE (1246)	
	thName	REG_SZ	C:\Windows	
Puta order: I little endine O Pie e	oductld	REG_SZ	00328-10000-00001-AA854	
byte order. C Elice erichan O big er	-gitalProductId	REG_BINARY	A4 00 00 00 03 00 00 00 30 30 33 32 38 2D 31 30 30 30	
Windows Phone	III DigitalProductId4	REG_BINARY	F8 04 00 00 04 00 00 00 35 00 35 00 30 00 34 00 31 00 2	
Windows Photo Viewer	RegisteredOrganization	REG_SZ	(value not set)	
Windows Portable Devices	a RegisteredOwner	REG_SZ	Windows User	
Windows Script Host Windows Search	InstallTime	REG_QWORD	0x F1D649C4 (17426196914349806110)	~
E Key Properties	0 C4 49 D6 F1 1E 12 D4 01-		АТО́Я · ·Ô ·	^
Last Written Time 1/22/2020 23:49:46	UTC			
OS Instal Date (UTC) Mon Jul 02 16:08:41	2018			
OS Instal Date (Local) Mon Jul 02 11:08:41	2018			
, , , , , , , , , , , , , , , , , , , ,				
]			~

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.



 To see the Internet Explorer artifacts, navigate to: HKCU\SOFTWARE\Microsoft\Internet Expolrer .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

G Google	https://www.goo	sgls.com/?gvs_rd=ssl#spf=1500250536323		× 8 🙂
About	Store		Gmail Images 🗰 Sign in	^
		Google ^{Sv}	witch to Chrome for Windows uilt for Windows. Hide annoying ads Id protect against malware on the eb	
		Q Google Search I'm Feeling Lucky		
		It's Data Privacy Day. Take a quick Checkup to review your settings		J
Advertisi	ng Business	How Search works	Privacy Terms Settings	~

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.

iii Registry Editor	-	E	2	×
File Edit View Favorites Help				
Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs				
Compared Natry CURSH 1/USKSHumen Report NyedRit Compared Natry CursH 1/USKSHumen Report NyedRit Patters yournal Carter of the second Carter of the sec				

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

Registry Ed	litor	witer Hele				-	×
omputer\HKF	V CURRE	INT USER\Software\Microsoft	(Windows) CurrentVersion) Explore	n/MenuOrder/Favorites	8		
	-	BannerStore ^	Name	Туре	Data		 _
		BitBucket	(Default)	REG_SZ	(value not set)		
		CabinetState	100 Order	REG_BINARY	08 00 00 02 00 00 08 4 01 00 00 1 00 00 03 00		
	2	CD Burning					
	2	CIDOpen					
	2	CIDSave					
	1 2	CLSID					
	>	ComDig32					
	>	Desktop					
	12	Discardable					
	2	FileExts					
	2	FolderTypes					
	>	HideDesktoplcons					
		LogonStats					
		LowRegistry					
	×	MenuOrder					
		 Favorites 					
		- Links					
	>	Modules					
	>	MountPoints2					
		OperationStatusManag					
		Package Installation					
	>	RecentDocs					
		Ribbon					
		RunMRU					
	5	SearchPlatform					
	5	SessionInfo					
		Shell Folders					
		Shutdown					
		StartPage					
	>	StartupApproved					
		StreamMRU					
		Streams					
		StuckRects3					
		Taskband					
		TWinUI					
		TurnardDather					

- 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



Value name:									
Order									
Value data:									
0120	00	00	6A	00	00	00	02	00	j
0128	00	00	5C	00	32	00	00	00	\ . 2
0130	00	00	3C	50	F3	B3	20	00	< P ó ³ .
0138	47	6F	6F	67	6C	65	2E	75	Google.u
0140	72	6C	00	00	42	00	08	00	rlB
0148	04	00	EF	BE	00	00	00	00	ï ¾
0150	00	00	00	00	2A	00	00	00	*
0158	00	00	00	00	00	00	00	00	
0160	00	00	00	00	00	00	00	00	
0168	00	00	00	00	00	00	47	00	G .
0170	6F	00	6F	00	67	00	6C	00	o.o.g.l.
0170					75				
Edit Dinana'	65 Velue	аа	2E	ии	15	ии	- 13	ии	OK Cancel
Edit Binary	Value	aa	2F	ии		ии	73	ии	OK Cancel
Edit Binary Value name: Order	Value	AA	2F					ии	OK Cancel
Edit Binary Value name: Order Value data:	Value	- AA	2F						OK Cancel
Edit Binary Value name: Order Value data: 0190	65 Value	00	2F	00	D2	00	36	00	OK Cancel
Edit Binary Value name: Order Value data: 0190 0198	65 Value 	00	9F 00 00	00	D2 3C	00	36 76	00 B4	0K Cancel
Edit Binary Value name: Order Value data: 0190 0198 0140	04 00 20	00 00 00	2F 00 00 50	00 00 00	D2 3C 4E	00 50 00	36 76 57	00 84 00	P II P OK Cancel
Edit Binary Value name: Order Value data: 0190 0198 01A0 01A8	65 Value 04 00 20 20	00 00 00 00	00 00 50 13	00 00 00 20	D2 3C 4E 20	00 50 00	36 76 57 50	00 84 00	P I P OK Cancel
Edit Binary Value name: Order Value data: 0190 0198 0140 0148 0140 0148	65 Value 04 00 20 75	00 00 00 00 00	00 00 50 13 72	00 00 00 20 00	D2 3C 4E 20 64	00 50 00 00	36 76 57 50 75	00 B4 00 00	P II P OK Cancel
Edit Binary Value name: Order Value data: 0190 0198 01A0 01A8 01B0 01B8	65 Value 04 00 20 20 20 5 5 65	00 00 00 00 00 00	00 00 50 13 72 20	00 00 00 20 00 00	D2 3C 4E 20 64 55	00 50 00 00 00 00	36 76 57 50 75 6E	00 B4 00 00 00	P I P OK Cancel
Edit Binary Value name: Order Value data: 0190 0198 0140 0148 0140 0188 0160	65 Value 04 00 20 20 75 65 69	00 00 00 00 00 00 00	00 00 50 13 72 20 76	00 00 00 20 00 00 00	D2 3C 4E 20 64 55 65	00 50 00 00 00 00	36 76 76 57 50 75 6E 72	00 B4 00 00 00 00	P II P OK Cancel
Edit Binary ' Value name: Order Value data: 0190 0198 01A0 01A8 01A8 01B0 01A8 01B0 01A8 01C0	65 Value 04 00 20 75 65 65 9 73	00 00 00 00 00 00 00 00 00 00 00	00 00 50 13 72 20 76 69	00 00 00 00 00 00 00 00	D2 3C 4E 20 64 55 65 74	00 50 00 00 00 00 00	36 76 57 50 75 6E 72 79	00 B4 00 00 00 00 00 00	P II P OK Cancel
Edit Binary ' Value name: Order Value data: 0190 0198 01A0 0188 0160 0188 01C0 0128	65 Value 04 00 20 20 20 20 5 65 69 73 20	00 00 00 00 00 00 00 00 00 00 00	2F 00 00 50 13 72 20 76 69 4E	00 00 00 20 00 00 00 00 00 00	D2 3C 4E 20 64 55 65 74 6F	00 50 00 00 00 00 00 00 00 00	36 76 57 50 75 6E 72 79 72	00 84 00 00 00 00 00 00 00	P II P OK Cancel
Edit Binary Value name: Order Value data: 0190 0198 01A0 01A8 0180 0160 01C0 01C0 0108	65 Value 04 00 20 75 69 73 20 74	00 00 00 00 00 00 00 00 00 00 00 00 00	2F 00 00 50 13 72 20 76 69 4E 68	00 00 00 00 00 00 00 00 00 00 00	D2 3C 4E 20 64 55 65 74 6F 77	00 50 00 00 00 00 00 00 00 00 00	36 76 57 50 75 6E 72 79 72 65	00 B4 00 00 00 00 00 00 00 00 00	P II P OK Cancel
Edit Binary Value name: Order Value data: 0190 0198 01A0 0180 0180 0180 0160 0160 0160 0160	65 Value 04 00 20 20 20 20 20 20 75 65 69 73 20 73 20 74	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 50 13 72 20 76 69 4E 68 74	00 00 00 00 00 00 00 00 00 00 00 00	D2 3C 4E 20 64 55 65 74 6F 77 2E	00 50 00 00 00 00 00 00 00 00 00 00 00	36 76 57 50 75 6E 72 79 72 65 75	00 B4 00 00 00 00 00 00 00 00 00 00 00	P II P Cancel OK Cancel

8. 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

👫 Registry Edite	or					_	×
File Edit View	Favorites Help						
Computer\HKEY	CURRENT_USER\Software\Micros	oft	Office				
	Internet Connection Wizard	^	Name	Туре	Data		
>	Internet Explorer		ab (Default)	REG SZ	(value not set)		
>	Keyboard						
>	MediaPlayer						
>	Messaging						
>	Microsoft Management Console						
>	MicrosoftEdge						
>	MS Design Tools						
2	MSDAIPP	-1					
2	MSF						
2	Multimedia						
>	Narrator						
	Notepad						
Y	Office						
>	15.0						
>	16.0						
>	Common						
>	Excel						
>	Outlook						
2	PowerPoint						
> >	Word						
>	OneDrive						
	Usk						
· · · · · ·	Payment						
	PeerNet						
	Personalization						
2	Phone						
2	Pim						
2	Poom						
	RAS AutoDial						
	RAS PROREBOOK						
	Remote Assistance						
	screeniviagnitier	~					
<	> >						

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.

🎬 Registry I	Editor					-	×
File Edit \	/iew	Favorites Help					
Computer\H	KEY_CL	JRRENT_USER\Software\Microsoft	Office\16.0\Word\File MR	J			
>	M	1ediaPlayer ^	Name	Туре	Data		^
>	M	lessaging	ab (Default)	REG SZ	(value not set)		
>	M	licrosoft Management Console	ab Item 1	REG SZ	[F000000001[T01D5D62C8A60C3401[O000000001*C:		
>	M	licrosoftEdge	ab Item 10	REG SZ	[F00000000][T01D5D17EEE6E2CE2][O000000001*C:\		
>	M	1S Design Tools	ab Item 11	REG SZ	[F00000000][T01D5C737E7A952A0][O00000000]*C:\		
>		ISDAIPP	ab Item 12	REG SZ	[F00000000][T01D5C736B529BAF0][O00000000]*C:\		
>		ISF	ab Item 13	REG SZ	[F00000000][T01D5C73149607200][O000000001*C:\		
2		luitimedia	ab Item 14	REG SZ	[F00000000][T01D5B52491859AC0][O00000000]*C;\		
>		otenad	ab Item 15	REG SZ	[F00000000][T01D5B51AB30E8CB0][O00000000]*C		
		ffice	ab Item 16	REG SZ	[F00000000][T01D5B51A3EF57AF0][O00000000]*C:\		
		15.0	ab Item 17	REG SZ	[F00000000][T01D5A0C6D64E92A0][O00000000]*C:		
	÷ 🗍	16.0	ab Item 18	REG_SZ	[F00000000][T01D5A0C6B1C5B2B0][O00000000]*C:		
	5	Access	ab Item 19	REG_SZ	[F00000000][T01D5A0C63A5845D0][O00000000]*C:		
	>	Common	ab Item 2	REG SZ	[F00000000][T01D5D6255FD05340][O00000000]*C:\		
	>	Excel	ab Item 20	REG_SZ	[F00000000][T01D5A0C54784BAA0][O00000000]*C:		
	>	Groove	ab Item 21	REG_SZ	[F00000000][T01D5A0C4DD90B4A0][O00000000]*C:		
	>	PowerPoint	ab Item 22	REG_SZ	[F00000000][T01D5A0C44D67CC60][O00000000]*C:		
	>	Registration	ab Item 23	REG_SZ	[F00000000][T01D5A0C3DFB314E0][O00000000]*C:		
		SyncProc	ab Item 24	REG_SZ	[F00000000][T01D5A0C3196B0A90][O00000000]*C:		
	>	User Settings	ab Item 25	REG_SZ	[F00000000][T01D5A0C2AB899DC0][O00000000]*C:		
	>	WEF	ab Item 26	REG_SZ	[F00000000][T01D5A0C2304C8B40][O00000000]*C:		
	~	Word	ab Item 27	REG_SZ	[F00000000][T01D5A0BFA82173E0][O00000000]*C:\		
		AddinLoad Times	ab Item 28	REG_SZ	[F00000000][T01D591CBCEFC0870][O00000000]*C:		
		Eile MPLL	ab Item 29	REG_SZ	[F00000000][T01D591C6CF75E5A0][O00000000]*C:\		
		Ontions	ab Item 3	REG_SZ	[F00000000][T01D5D30973157490][O00000000]*C:\		
		Place MRI	ab Item 30	REG_SZ	[F00000000][T01D47AC5606BCAD0][O00000000]*C:		
		Reading Locations	ab Item 31	REG_SZ	[F00000000][T01D47AC52C2D9DC0][O00000000]*E:		
		Recent Templates	ab Item 32	REG_SZ	[F00000000][T01D476E4507F0631][O00000000]*E:\l		
		Resiliency	ab Item 33	REG_SZ	[F00000000][T01D476E434628580][O00000000]*C:\		
		> Security	ab Item 34	REG_SZ	[F00000000][T01D4755004B60C20][O00000000]*C:\		
		Wizards	ab Item 35	REG_SZ	[F00000000][T01D475415D244890][O00000000]*E:\l		
	1	Common Y	ab Item 36	REG_SZ	[F00000000][T01D4749C7E0D2D60][O00000000]*C:\		
<		>			······································		~

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

Registry Editor				-	\times
le Edit View Favorites Help					
omputer\HKEY_CURRENT_USER\Software\Microso	ft\Windows\CurrentVersion\Explorer				
V Explorer	Name	Туре	Data		
Accent	ab (Default)	REG_SZ	(value not set)		
> Advanced	AppReadinessLogonCompl	REG_DWORD	0x00000001 (1)		
> AppContract	👪 Browse For Folder Height	REG_DWORD	0x0000015a (346)		
AutoComplete	Browse For Folder Width	REG_DWORD	0x0000013e (318)		
> AutoplayHandlers	ExplorerStartupTraceRecorded	REG DWORD	0x00000001 (1)		
Baminrottling	Still FirstRunTelemetryComplete	REG DWORD	0x00000001 (1)		
Bannerstore	110 GlobalAssocChangedCounter	REG DWORD	0x0000006e (110)		
Sitbucket	10 LocalKnownFoldersMigrated	REG DWORD	0x00000001 (1)		
Cabinetstate	200 PostAppinstallTasksComple	REG DWORD	0v0000001 (1)		
S CD Burning	Reason Setting	REG DWORD	0-0000000ff (255)		
CiDOpen	2 ChallState	PEG PINARY	24 00 00 00 24 28 00 00 00 00 00 00 00 00 00 00 00 00 00		
CIDSave	CID La data dOa Liberrian	REG_DINARY	24 00 00 00 58 28 00 00 00 00 00 00 00 00 00 00 00 00 00		
S CLSID		REG_DWORD			
> Combigsz	SlowContextMenuEntries	REG_BINARY	60 24 62 21 ea 3a 69 10 a2 dc 08 00 26 30 30 9d 9d 0		
Desktop	TelemetrySalt	REG_DWORD	0x0000002 (2)		
> Discardable	👸 UserSignedIn	REG_DWORD	0x00000001 (1)		
> FileExts					
> Folder lypes					
> HideDesktopicons					
LogonStats					
LowRegistry					
> MenuOrder					
> Modules					
> MountPoints2					
OperationStatusManac					
Package Installation					
> RecentDocs					
Ribbon					
RunMRU					
> SearchPlatform					
SessionInto					
Shell Folders					
Shutdown					
StartPage					
> StartupApproved					
StreamMRU					
> Streams					
StuckRects3					
> Taskband					

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

Registry Edit	or			-	- 🗆)
Edit Viev	v Favorites Help					
nputer\HKEY	_CURRENT_USER\Software\Micro	soft\Windows\CurrentVer	sion\Explorer\RecentDocs			
	> CIDSave	^ Name	Type	Data		
	> 📙 CLSID	18 67	REG BINARY	66 00 69 00 72 00 65 00 2e 00 64 00 6f 00 63 00 78 00		
	> ComDlg32	18 68	REG BINARY	4c 00 61 00 62 00 20 00 31 00 2e 00 64 00 6f 00 63 00		
	> Desktop	88 69	REG BINARY	46 00 69 00 72 00 65 00 66 00 6f 00 78 00 20 00 46 00		
	> Discardable	110 7	REG BINARY	53 00 59 00 30 00 2d 00 34 00 30 00 31 00 20 00 43 0		
	> FileExts	11 70	REG BINARY	62 00 6f 00 6f 00 6b 00 20 00 6d 00 61 00 72 00 6b 00		
	> Folder lypes	18 71	REG BINARY	66 00 69 00 72 00 65 00 66 00 6f 00 78 00 00 00 6e 00		
	> HideDesktopicons	200 72	REG BINARY	44 00 65 00 73 00 6b 00 74 00 6f 00 70 00 00 00 62 00		
	LogonStats	88 73	REG BINARY	4c 00 61 00 62 00 20 00 39 00 00 00 68 00 32 00 00 00		
	LowRegistry	88 74	REG BINARY	49 00 54 00 53 00 34 00 37 00 32 00 24 00 4c 00 61 0		
	> Medulae	88 75	REG BINARY	31 00 32 00 33 00 00 00 56 00 32 00 00 00 00 00 00		
	> MountPoints?	88 76	REG BINARY	31 00 32 00 33 00 2e 00 66 00 74 00 66 00 00 00 00 62 0		
	OperationStatusMana		REG BINARY	6c 00 61 00 62 00 20 00 33 00 2e 00 64 00 65 00 62 0		
	Package Installation	20 70	PEG PINARY	52 00 65 00 67 00 60 00 73 00 74 00 72 00 70 00 20 00		
	RecentDocs	20 70	PEG PINARY	72 00 65 00 67 00 09 00 73 00 74 00 72 00 65 00 00 00		
	Ribbon	200 0	PEG PINARY	42 00 72 00 61 00 72 00 68 00 20 00 52 00 65 00 70 00		
	RunMRU	200	PEG PINARY	45 00 61 00 67 00 73 00 00 20 00 52 00 52 00 05 00 70 00		
	> SearchPlatform	200	PEG PINARY			
	> SessionInfo	0000	REG_BINARY	4-00 51 00 52 00 70 00 00 70 00 00 00 50 00 52 00 00 00		
	- Shell Folders	0002	REG_BINARY	40 00 01 00 02 00 20 00 50 00 20 00 55 00 79 00 75 00		
		10 85	REG_BINARY	34 00 22 00 70 00 62 00 67 00 00 00 50 00 32 00 00 00		
		200 05	REG_BINARY	40 00 61 00 62 00 20 00 37 00 20 00 50 00 61 00 73 00		
	> StartupApproved	00000	REG_BINARY			
	StreamMRU	100 80	REG_BINARY	35 00 2e 00 70 00 6e 00 67 00 00 00 50 00 32 00 00 00		
	> 🔤 Streams	1008/	REG_BINARY	31 00 2e 00 70 00 6e 00 67 00 00 00 50 00 32 00 00 00		
		.00 88	REG_BINARY	70 00 69 00 63 00 00 06 56 00 32 00 00 00 00 00 00 00 00		
	> 📙 Taskband	100 89	REG_BINARY	41 00 52 00 50 00 20 00 50 00 6f 00 69 00 73 00 6f 00		
	> 🔤 TWinUI	<u>100</u> 9	REG_BINARY	/4 00 68 00 /5 00 6d 00 62 00 6e 00 61 00 69 00 6c 0		
		100	REG_BINARY	32 00 2e 00 70 00 6e 00 67 00 00 00 50 00 32 00 00 00		
	User Shell Folders	88 91	REG_BINARY	41 00 52 00 50 00 20 00 50 00 6f 00 69 00 73 00 6f 00		
	> UserAssist	88 92	REG_BINARY	36 00 2e 00 50 00 4e 00 47 00 00 00 50 00 32 00 00 00		
	··· VirtualDesktops	88 93	REG_BINARY	4c 00 61 00 62 00 20 00 35 00 20 00 45 00 74 00 68 00		
	> VisualEffects	88 94	REG_BINARY	42 00 61 00 73 00 69 00 63 00 20 00 43 00 50 00 55 00		
	Wallpapers	88 95	REG_BINARY	37 00 2e 00 70 00 6e 00 67 00 00 00 50 00 32 00 00 00		
	WordWheelQuery	88 96	REG_BINARY	42 00 61 00 73 00 69 00 63 00 20 00 43 00 50 00 55 00		
	> Ext	88 97	REG_BINARY	53 00 63 00 72 00 69 00 70 00 74 00 73 00 00 00 62 00		
	Extensions	88 98	REG_BINARY	39 00 2e 00 70 00 6e 00 67 00 00 00 50 00 32 00 00 00		
	> FileAssociations	88 99	REG_BINARY	4e 00 65 00 74 00 77 00 6f 00 72 00 6b 00 20 00 43 00		
	riteristory	✓ I MRUListEx	REG_BINARY	4e 00 00 00 79 00 00 00 4f 00 00 00 76 00 00 00 69 00		

3. View the contents of the ComD1g32. 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

📫 Registry Ec	litor						-	>
ile Edit Vi	ew Fa	avorites Help						
omputer\HK	Y_CUF	RENT_USER\Software\Micro	soft	\Windows\CurrentVersion	\Explorer\ComDlg32\ClDSize	eMRU		
	-	Controls Folder	^	Name	Type	Data		
		Controls Folder (Wow64)		ab (Default)	REG SZ	(value not set)		
	>	CuratedTileCollections		w o	REG BINARY	63 00 68 00 72 00 6f 00 6d 00 65 00 2e 00 65 00 78 00		
	>	DeviceAccess		88 1	REG BINARY	52 00 65 00 67 00 69 00 73 00 74 00 72 00 79 00 56 00		
	>	DeviceCapabilities		88 10	REG BINARY	44 00 42 00 20 00 42 00 72 00 66 00 77 00 73 00 65 00		
	>	Diagnostics		200 10	PEG DINARY	76 00 20 00 45 00 46 00 45 00 20 00 41 00 26 00 41 0		
	~	Explorer		200 12	REG DINARY	76 00 24 00 25 00 25 00 44 00 24 00 25 00 24 00 20 0		
		Accent		90 12	DEC DIMARY	76 00 34 00 35 00 35 00 44 00 35 00 35 00 36 00 30 00 30 00		
		Advanced		90 14	REG_DINART	70 00 54 00 55 00 42 00 51 00 44 00 44 00 42 00 50 0		
		> AppContract		00 14	REG_DINART	10 00 04 00 00 00 43 00 01 00 02 00 70 00 03 00 72 00		
		AutoComplete		200 10	REG_BINARY	41 00 70 00 6F 00 77 00 65 00 72 00 73 00 6F 00 66 00		
		> AutoplayHandlers		200 17	REG_BINARY	50 00 69 00 63 00 60 00 65 00 72 00 48 00 61 00 73 00		
		Bam I hrottling		10 17	REG_BINARY	52 00 65 00 75 00 70 00 6F 00 6E 00 64 00 2E 00 65 00		
		BannerStore		18	REG_BINARY	46 00 54 00 46 00 20 00 49 00 66 00 61 00 67 00 65 0		
		> BitBucket		19	REG_BINARY	53 00 6e 00 69 00 70 00 70 00 69 00 6e 00 67 00 54 00		
		CabinetState		100 Z	REG_BINARY	/6 00 6d 00 // 00 61 00 /2 00 65 00 2e 00 65 00 /8 0		
		CIDO and		100 20	REG_BINARY	/b 00 30 00 43 00 34 00 38 00 36 00 46 00 46 00 46 0		
		CIDOpen		100 B	REG_BINARY	66 00 74 00 6b 00 2e 00 65 00 78 00 65 00 00 00 00 0		
		CLSID		100 4	REG_BINARY	7b 00 36 00 44 00 30 00 43 00 30 00 34 00 34 00 46 0		
		ComDia32		200 5	REG_BINARY	6e 00 6f 00 74 00 65 00 70 00 61 00 64 00 2e 00 65 00		
		CIDSizeMPLL		80 6	REG_BINARY	66 00 69 00 72 00 65 00 66 00 6f 00 78 00 2e 00 65 00		
		FirstFolder		200 7	REG_BINARY	45 00 53 00 45 00 44 00 61 00 74 00 61 00 62 00 61 00		
		LastVisitedPidIMRI		8008	REG_BINARY	4f 00 70 00 65 00 6e 00 57 00 69 00 74 00 68 00 2e 00		
		LastVisitedPidIMRL		88 9	REG_BINARY	45 00 73 00 65 00 44 00 62 00 56 00 69 00 65 00 77 00		
		OpenSavePidIMRU		🕮 MRUListEx	REG_BINARY	01 00 00 00 00 00 00 00 14 00 00 00 13 00 00 00 0d 0		
		Desktop						
		Discardable						
		FileExts						
		> FolderTypes						
		> HideDesktoplcons						
		LogonStats						
		LowRegistry						
		> MenuOrder						
		> Modules						
		> MountPoints2						
		OperationStatusMana	iç 🛛					
		- Ackage Installation						
		> RecentDocs						
		Ribbon	~					

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.

	Registr	y Edito	r						-	Х
File	Edit	View	Favorites	Help						
Com	nputer\	HKEY_O	CURRENT_	USER\Software\Micros	ioft)	Windows\CurrentVersion\Exploi	er\ComDlg32			
			👻 📙 F	ileExts	^	Name	Туре	Data		
			>			ab (Default)	REG SZ	(value not set)		
			×	.3g2			-	. ,		
			2	.3gp						
			>	.3gp2						
			>	.3gpp						
			>	.3mf						
			2	.aac						
			2	.ac3						
				.accdb						
			2	acrobatsecuritysett						
				adt						
			113	adte						
			113	aif						
				aifc						
				aiff						
			1 5	amr						
				.api						
			>	.arw						
			>	.asf						
			>	.asx						
			>	.au						
			>	.avi						
			>	.bak						
			>	.bat						
			>	.bin						
			>	.bmp						
			>	.bpdx						
			>	.BTR						
			2	.cab						
			2	.cdxml						
			>	.cfg						
			>	.chm						
			2	.cnq						
				.contact						
			2	.02						
			2	.crw						
				.05						
			114		۷					

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; Winl0 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

👫 Registry Editor				- 🗆 X
File Edit View Favorites Help				
Computer\HKEY_CLASSES_ROOT\Local Settings\Soft	ware			
LicLua.LicLuaObject.15	Name	Type	Data	
LicLua.LicLuaObject.16	ab (D-f-ult)	1700	(unliss mathemath)	
LISTNET.Listnet	(Derault)	KEG_5Z	(Value hot set)	
LISTNET.Listnet.11				
LISTNET.Listnet.12				
LISTNET.Listnet.15				
LISTNET.Listnet.16				
ListPad.ListPad				
ListPad.ListPad.1				
> LiveScript				
> LiveScript Author				
> Inkfile				
Local Settings				
> ImmutableMuiCache				
> MrtCache				
> MuiCache				
> Software				
> LocalPathSearchProvider				
> LocationApi				
> LocationApi.1				
> LocationDisp.CivicAddressReportFact				
> LocationDisp.CivicAddressReportFact				
LocationDisp.DispCivicAddressReport				
LocationDisp.DispCivicAddressReport				
LocationDisp.DispLatLongReport				
LocationDisp.DispLatLongReport.1				
LocationDisp.LatLongReportFactory				
LocationDisp.LatLongReportFactory.1				
> 📙 Logagent.Logagent				
Logagent.Logagent.1				
Logging.Logger				
Logging.Logger.2				
> LpkSetup.1				
> LR.LexRefBilingualService.1.0				
> LR.LexRefBilingualService.1.0.1				
> LR.LexRefBilingualServiceAttribute.1.0				
> LR.LexRefBilingualServiceAttribute.1.0				
> LR.LexRefBilingualTextContext.1.0				
> LR.LexRefBilingualTextContext.1.0.1				
> LR.LexRefEnglishStemmer.1.0 🗸				
< >>				

- 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.

Registry Editor			-	×
e Edit View Favorites Help				
omputer\HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows	\CurrentVersion			
> LicLua.LicLuaObject.15 ^ Name	Type	Data		
> LicLua.LicLuaObject.16	1990			
> LISTNET.Listnet	KEG_SZ	(value not set)		
> LISTNET.Listnet.11				
> LISTNET.Listnet.12				
> LISTNET.Listnet.15				
> LISTNET.Listnet.16				
> ListPad.ListPad				
> ListPad.ListPad.1				
> LiveScript				
> LiveScript Author				
> 🔄 Inkfile				
🗸 🔄 Local Settings				
> ImmutableMuiCache				
> MrtCache				
> MuiCache				
V Software				
V Microsoft				
V Windows				
CurrentVersion				
> AppContainer				
> AppModel				
> SyncMgr				
> TrayNotify				
₩orkFolders				
> Shell				
> LocalPathSearchProvider				
> LocationApi				
S LocationApi.1				
> LocationDisp.CivicAddressReportFact				
LocationDisp.CivicAddressReport				
LocationDisp.DispCivicAddressReport				
LocationDisp.Displetiondatessiteport				
LocationDisp.DispLatLongReport 1				
LocationDisp.Latl.ongReportFactory				
LocationDisp.Latl.ongReportFactory.1				
> Logagent.Logagent				
> Logagent.Logagent.1				
> Logging Logger				

6. Navigate to: HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\micr osoft.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.

🛎 🚨 🕼 🖛 🖻 🖥 🗟 🕨 🕬	8				
	^	Name	Туре	Data	
🖶 🛄 *		ab (default)	REG_SZ	5636b142	
🖶 🧰 .3g2			-		
ф-🧰 .3gp					
i⊒- [3gp2					
🖶 🦲 .3gpp					
👜 🦲 .3mf					
iaac					
🕀 🦲 .adt					
🔅 🦲 .adts					
👜 🦲 .amr					
⊕- 🦲 .arw					
🔅 🦲 .asf					
🗓 🦲 .avi					
🕀 🦲 .bmp					
🖶 🦲 .cr2					
🗓 🦲 .crw					
idib. 🧰 🧰					
🖶 🦲 .divx					
🔅 🦲 .erf					
🗓 🦲 .flac					
🖶 🦲 .gif					
🔃 🛄 .htm					
👜 🧰 .html	~				
<	>				
Kev Properties		00 35 00 36 0	0 33 00 36 00-	62 00 31 00 34 00 32 00 5 · 6 · 3 · 6 · b · 1 · 4 · 2 ·	

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

		21				2	
÷	Internet Setting	gs	^		Name		Туре
	InternetRegistr	у			ab]url1		REG_SZ
<u>ب</u>	LowRegistry				ab url2		REG_SZ
	Main				ab]url3		REG SZ
۵.	New Windows				ab]url4		REG SZ
	OnlineHistory				abluds		REG SZ
	OpenSearch				abluste		DEC 57
	PageSetup				Eguno Esta a		NEG_3Z
	PhishingFilter				egurl/		REG_SZ
	PivotIndex				@Jurl8		REG_SZ
	Privacy				趟)url9		REG_SZ
🧰	Protected - It i	s a violation of Windows P	oli		赳url10		REG_SZ
÷- 🚞	Recovery				釶]url11		REG_SZ
	ServiceUI				ط)url12		REG_SZ
÷- 🗀	TabbedBrowsi	ng			赴 url 13		REG_SZ
÷- 🚞	Toolbar			U	ab]url14		REG_SZ
	TypedURLs			1	abjurl15		REG_SZ
	TypedURLsTim	e			ab url16		REG SZ
	TypedURLsVisi	tCount			ab]url17		REG SZ
	UrlBlock				ablurl18		REG SZ
÷ 🚞	UserStateMigra	ation			ab]url10		REG SZ
`	Zoom				ab]		REG SZ
📄 Sof	ftware				abluel21		DEC SZ
micros	oft.microsofto	ficehub_8wekyb3d8bbwe	~		abluiza		NEG_SZ
			>		eguri22		KEG_SZ

Data http://www.hotmail.com/ http://www.google.com/ http://www.audubon.com/ http://www.shaddboncom/ http://www.sharks.org/ http://www.beallsoutlet.com/ http://www.deansourier.com/ http://www.divessi.com/ http://www.scubadiving.com/ http://www.bigfishexpeditions.com/ http://www.whatcomcounty.us/200/Sheriff http://www.olympus.com/ http://www.nikon.com/ http://www.canon.com/ http://www.bhphotovideo.com/ http://www.adorama.com/ http://www.scuba.com/ http://www.dan.org/ http://www.bp.com/ http://www.arco.com/ http://www.shelloil.com/ http://www.genius.com/ 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:

First Eits Report View Window Help SMA SMA Consistent Consolition	- 🗆 X				🖉 AccessData Registry Viewer - [SAM]
Sold Image: Type Data Sold Sold Image: Type Data Sold Sold Image: Type Data Image: Type Data Image: Type Type Image: Type Type Data Image: Type Type Image: Type Type Type Data Image: Type Type Image: Type Type Type Type Type Type Type Image: Type	- 7 ×				File Edit Report View Window Help
Image: State of the state o					
SMA Rig_DWORD		Data	Type	Name	B-B SAM
B (within Time 5/24/2018 17:17:51 UTC		(value not ret)	PEG DWORD	(default)	🗄 🚞 SAM
3 Key Properties Last Written Time 5/24/2018 17:17:51 UTC					Count C
					I Key Properties Last Written Time 5/24/2018 17:17:51 UTC

- 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

🖉 AccessData Registry Viewer - [SAM]					-	• ×
🔛 File Edit Report View Window Help						- 6 ×
🚔 🚊 🖪 🖛 🗁 🗑 🕾 🗟 🕩 🖦 🎙	?					
	Name	Type	Data			
🛓 🧰 SAM	e c	DEC DINARY	03 00 01 00 00 00 00 00 00 00 00 00 00 00			
- Domains	BR V	REG RINARY				
Accunt Alase Groups Groups						
	_					
Key Properties	A 000 00 00 010 10 00	00 00 0C 01 00 0	0-03 00 01 00 0C 01 00 00			^
Last Written Time 3/29/2018 15:58:40 UT	020 00 00	00 00 28 01 00 0	0-4A 00 00 00 00 00 00 00(J			
SID unique identifier 503	030 74 01	00 00 00 00 00 0	0-00 00 00 00 74 01 00 00 tt.			
User Name DefaultAccount	040 00 00	00 00 00 00 00 00	0-74 01 00 00 00 00 00 00 ·····t			
Description A user account manage	d 060 74 01	00 00 00 00 00 00 00	0-00 00 00 00 74 01 00 00 tt.			
Logon Count 0	070 00 00	00 00 00 00 00 0	0-74 01 00 00 00 00 00 00 ·····t···			
Last Logon Time Never	V 080 00 00	00 00 74 01 00 0				
	0a0 18 00	00 00 00 00 00 00 00	0-94 01 00 00 18 00 00 00			
	060 00 000	00 00 AC 01 00 0	0-18 00 00 00 00 00 00 00			
	0c0 C4 01	00 00 18 00 00 0	0-00 00 00 00 01 00 14 80 Å			~
SAM\SAM\Domains\Account\Users\000001F7				Offset: 0		

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

🚨 AccessData Registry Viewer - [SAM]				- 🗆 ×
💬 File Edit Report View Window Help				- 6 ×
📽 🍠 📴 📭 🗑 🗑 📾 👘 🌹				
SAM S	Name 题F 题V 题FercePassw.	Type REG_BINARY REG_BINARY REG_BINARY REG_BINARY	Due 00 001 00 000 000 00 00 FA 40 24 FA 34 6E DS 01 000 0 00 00 00 00 F4 40 00 00 03 00 01 00 F4 00 00 00 66 00 0. 00 00 00 00	
Key Properties	00 03 00 01 10 00 00 00 00	00 00 00 00 00-	-F8 A9 E4 FA 34 6E D5 01	^
Last Written Time 9/18/2019 15:23:10 UT	20 00 00 00	00 00 00 00 00 00-	-7A DD 7B A0 94 69 D5 01	
SID unique identifier 1002	30 EA 03 00	00 01 02 00 00-	-14 02 00 00 00 00 00 00 ê	
User Name cit	40 00 10	00 01 00 00 00-	-00 00 00 00 00 00 00 00 00	
Logon Count 22				
Last Logon Time 9/18/2019 15:23:10 U				
Last Password Change (III 5/24/2018 17:18:08 0)	~ ~			

7. Close the SAM file in Registry Viewer and open the SOFTWARE file.

8. Navigate to:

SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI

🔏 AccessData Registry Viewer - [software]			- 🗆 X
🖼 File Edit Report View Window Help			- 5
AppModelUnlock AppModelUnlock AppModelUnlock AppModelUnlock AppModelUnlock AppModelUnlock AppModelUnlock AppModelUnlock AppModelUnlock Authentication Credential Provider Filters LockScreenContent Credential Provider Signal Authentication Creative Background BootAnimation ClearAutologon FingerprintLogon NgcPin PicturePassword Creative ValidateUsername ValidateUsername ValidateUsername ValidateUsername	Name Type BhowTablet	Data 0x00000000 (0) (6087888-EAD8-445C-9CFD-0887F74EA6CD) .\pwrs .\pwrs .>p3:5-13-21-4171667097-16694073-3857598102-1004 S-1-5:21-4171667097-16694073-3857598102-1004 .0000040C2 (16578) .00000000 (0) .000000000 (0)	
Key Properties Last Written Time 1/28/2020 21:52:33 UTC	0 00 00 00 00		
	-		
L software\Microsoft\Windows\CurrentVersion\Authentica	i I ation\LogonUI	Offset: 0	

- 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

_ 8 x

_

2. Navigate to: SYSTEM/ControlSet001/Enum/USBSTOR AccessData Registry Viewer - [SYSTEM] File Edit Report View Window Help HDAUDIO HDAUDIO HTTEE File Coll File Edit Report View Window Help File Edit Report View Window

PCI PCI PCIDE RODT SCSI STORAGE SVD USB USB USSTOR Disk&Ven_Senen&AProd_Disk Disk&Ven_Senen&AProd_Disk Disk&Ven_SanDisk&Prod_Exte Disk&Ven_SanDisk&Prod_Exte Disk&Ven_SanDisk&Prod_Exte Disk&Ven_TOSHIBA&Prod_Exte Disk&Ven_VD&Prod_Exte Disk&Ven_VD&Prod_Exte	
Key Properties	
Las written i me 12/17/2019 21:53:23 010	
SYSTEM\ControlSet001\Enum\USBSTOR	Offset: 0

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

K AccessData Registry Viewer - [SYSTEM]				-	□ ×
File Edit Report View Window Help					- 8 ×
Image: Second regions / received recei	Name DeviceDesc Capabilities	Type REG 52 REG	Data @disk.inf %disk.devdesc%;Disk.drive 0x00000010 (16) 0x0000003 (3) (c235ffe4.7155.569c-8360-7cd724d501fe) USBSTORDisk_USBSTORR;Bw/ GenDisk USBSTORDisk_USBSTORR;Bw/ GenDisk (d366e97-e325-11ce-bfc1-08002be10318) disk (d366e97-e325-11ce-bfc1-08002be10318) disk 005 USB Disk.20 SB Device 0x00000000 (0)		
< >					
E Key Properties Last Written Time 11/10/2018 17:17:12 UTC	00 40 00 64 0 10 66 00 2C 0 20 64 00 65 0 30 38 00 44 0 40 69 00 76 0	0 69 00 73 00 0 25 00 64 00 0 76 00 64 00 0 69 00 73 00 0 65 00 00 00-	68 00 20 68 00 8 -1 </td <td></td> <td>~</td>		~
SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_&Pro	USB_DISK_2.0ℜ	v_PMAP\070769EF	2A43E511&0 Offset: 0		

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.

AccessData Registry Viewer - [SYSTEM]					-	×
👺 File Edit Report View Window Help						- 8 ×
🚅 🚚 🗟 🖛 📄 🗑 🗃 🗐 🕩 🕪 🤶						
SWD SSWD SWD SSWD SSWD		Name Capabilities Capabilities Address ContainerID ClassGUID ClassGUID ClassGUID PriendlyName ConfigFlags	Type REG_SZ REG_DWORD REG_SZ REG_DWORD REG_SZ REG_MULT_SZ REG_MULT_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_DWORD	Data @disk.inf,%disk_devdesc%;Disk drive 0x0000002 (2) (0)4716-210a-11ea-bbb2-744609a988f) USBSTOR;Diskcenel, UDisk		
Key Properties	~	00 40 00 64 00	69 00 73 00-	6B 00 2E 00 69 00 6E 00 🕅 d.i.s.ki.n.		 /
Last Written Time 12/17/2019 21:53:23 UTC		20 66 00 20 0 20 64 00 65 00 30 3B 00 44 00 40 69 00 76 00	25 00 64 00- 76 00 64 00- 69 00 73 00- 65 00 00 00	5 00 73 00 65 00 57 00 [*,4*4.1.**. 5 00 73 00 63 00 25 00 [4***4.4.**.*. EB 00 20 00 64 00 72 0] ivre		
WSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_General&Prod_UDisk&Rev_5.0	00\7	&11a0ec1b&0&&) Offset:	0		~

- 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

g. WPDBUSENUM (In the SWD subkey in Windows 10)
🚋 🧰 {5d624f94-8850-40c3-a3fa-a4fd2080baf3}
🚋 🧰 ACPI
🗄 🧰 ACPI_HAL
DISPLAY
HDAUDIO
HID
HTREE
🖶 💼 PCI
🖶 🧰 PCIIDE
🗄 🧰 ROOT
🗄 💼 SCSI
🗄 🧰 STORAGE
🗄 💼 SWD
🗄 💼 USB
🖕 🧰 USBSTOR

6. Move up to the USB subkey above the USBSTOR.

Pile Edit Report View Window Help Pile Window Help	⊐ ×
Image: Solution Image: Sol	_ 8 ×
Image: Second Hubbo Name Type Data Image: Second Hubbo Recond Hubbo Mechanit Recip Works Mechanit	
Image: Biology Hulls and State Stat	^
Image: Biology Hulls and Hyperboly Biology Hyperboly	
Image: With Display Dis	
B W10, 393899, 064A W10, 39389, 00, 664A, MU, 01 W10, 39389, 00, 464A, MU, 01 W10, 95428, 00, 464A, MU, 01 W10, 95428, 00, 464A, MU, 00 W10, 95428, 00, 12484, MU, 00 W10, 97814, 00, 1248 W10, 97814, 00, 1538 W10, 17814, 00, 1541 W10, 17814, 00, 1541 W10, 17814, 00, 1541 W10, 17814, 00, 1541 W10, 17814, 00, 1241 <t< td=""><td></td></t<>	
Image: Windowskie Window	
Image: Windows and Wind	
Image: Windows and Wind	
Image: Section of the sectio	
Image: Solution of the	
Image: Solution of the	
Image: Section 122828ML00 Image: Section 122828ML00 Image: Section 122828ML00 Image: Section 122828ML00 Image: Section 122828ML00 Image: Section 122828ML00 Image: Section 122828ML00 Image: Section 122828ML00 Image: Section 122828ML00 Image: Section 122828ML00 Image: Section 122828ML00 Image: Section 122828ML00 Image: Section 122828ML00	
Image: State Processing St	
Image: Mark Program	
Image: Mark Programmer Line Reg DWORD 5388 Image: Reg DWORD 540000001 (1) Image: Mark Programmer Line Reg DWORD 540000001 (1) Image: Reg DWORD 5400000001 (1) Image: Mark Programmer Line Reg DWORD 5400000001 (1) Image: Reg DWORD 5400000001 (1) Image: Mark Programmer Line Reg DWORD 500000001 (1) Image: Reg DWORD 5400000001 (1) Image: Mark Programmer Line Reg DWORD 500000001 (1) Image: Reg DWORD 500000001 (1) Image: Mark Programmer Line Reg DWORD 500000001 (1) Image: Reg DWORD 500000001 (1) Image: Mark Programmer Line Reg DWORD 500000001 (1) Image: Reg DWORD 500000001 (1) Image: Mark Programmer Line Reg DWORD 500000001 (1) Image: Reg DWORD 50000001 (1) Image: Mark Programmer Line Reg DWORD 500000001 (1) Image: Reg DWORD 50000001 (1) Image: Mark Programmer Line Reg DWORD 500000001 (1) Image: Reg DWORD 50000001 (1) Image: Mark Programmer Line Reg DWORD 500000001 (1) Image: Reg DWORD 500000001 (1) Image: Mark Programmer Line Reg DWORD 500000001 (1) Image: Reg DWORD 500000001 (1) Image: Mark Programmer Line Reg DWORD 5000000001 (1) Image: Reg DWORD 5000000000000000000000000000000000000	
Image: Control (Control (Contro) (Contro) (Control (Contro) (Contro) (Contro) (Contro) (Contro) (
Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description Image: Model Description	
Image: Wind DetRAPID_3019 Image: Wind DetRAPID_40001 Image: Wind DetRAPID_40001 Image: Wind DetRAPID_40001 Image: Wind DetRAPID_40001 Image: Wind DetRAPID_4000 Image: Wind DetRAPID_4000 Image: Wind MetRAPID_4000 Image: Wind DetRAPID_4000 Image: Wind MetRAPID_40000 Image: Wind DetRAPID_40000 Image: Wind MetRAPID_4000000000000000000000000000000000000	
Image: Wide Job Constraint Image: Wide Job Constraint <td< td=""><td></td></td<>	
Image: With UD_1058ABPID_2561 Image: WextParentLine REG_DWORD 0x0000001 (1) Image: With UD_14Cb&PID_1212 Image: WextParentLine REG_DWORD 0x0000001 (1) Image: With UD_1575ABPID_0621 Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: With WID_1415C&PID_301D Image: WID_1	
Image: Work of the sector of the se	
Image: With the second secon	
Image: With the time 1/9/2020 21:30:30 UTC Image: With the time 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
Image: Second	
El Key Properties 0 02 00 00 00 Last Written Time 1/9/2020 21:30:30 UTC 0 02 00 00 00	~
Last Written Time 1/9/2020 21:30:30 UTC	^
	~
SYSTEM: ControlSet011/Enum	

- 7. Each of the subkeys here represent devices inserted into the system, not just storage units. Each has an identifier called a VID/PID or Vendor ID and Product ID. Each half of the VID/PID ID uses a four hexadecimal character set to identify the device. For example, the VID_413C&PID_8161 identifies a Dell Computer Corp. device (413C) that is an integrated keyboard (8161).
- 8. Navigate to:

SYSTEM\ControlSet001\Services\W32Time

KccessData Registry Viewer - [SYSTEM]				-	o x
File Edit Report View Window Help					- 8 ×
🖆 🔜 🖻 🖙 🖹 🗃 🕼 의 🕩 🖦 🤶					
Keyson Skejstry Viewer - [SYSTEM] File Edit Report View Window Help Image: Sket Skejstry Viewer - [SYSTEM] Image: Skej Skejstry Viewer - [SYSTEM] Image: Skej Skejstry Viewer - [SYSTEM] Image: Skejstry Viewer - [Syste	Name DisplayTon Transform DisplayTon Transform	Type REG_SZ REG_SD REG_BINARY REG_EXPAND_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Data @%SystemRoot%kysystem32(w32time.dll,-201 @%SystemRoot%kystem32(w32time.dll,-201 0.00000001 (1) 80 51 10 00 00 00 00 00 00 00 00 00 00 00 00		
Last written ime 6/10/2018 22:45:25 UTC	20 73 00 74 0 30 33 00 32 0 40 6C 00 6C 0	0 65 00 6D 00-3 0 74 00 69 00-4 0 2C 00 2D 00-4	33 00 32 00 5C 00 77 00 a t = t = m 3 2 \.v= ED 00 65 00 25 00 46 00 3 2 t : t = m e. d. 32 00 30 00 31 00 00 00 1 1 1 = 2 .0 .1		~
SYSTEM\ControlSet001\Services\W32Time		Offset: (D		

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.

K AccessData Registry Viewer - [SYSTEM]				– 🗆 X
💬 File Edit Report View Window Help				_ 8 ×
🚅 💂 🕒 🖿 🗑 🗑 🗐 🕩 🖦 🤶				
VMware NAT Service Vmware Volumar Volumar Voluma Volume Vol	Name NtpServer ServiceDIUn ServiceMin Type	Type REG_SZ REG_EXPAND_SZ REG_DWORD REG_SZ REG_SZ	Data time.windows.com,0x9 %systemroot%system32\w32time.dll 0x0000001 (1) SvchostEntry_W32Time NT5DS	
Key Properties Last Written Time 6/10/2018 22:48:16 UTC	00 74 00 69 0 10 64 00 6F 0 20 2C 00 30 0	0 6D 00 65 00-: 0 77 00 73 00-: 0 78 00 39 00-:	2E 00 77 00 69 00 6E 00 t.i.m.eee 2E 00 63 00 6F 00 6D 00 d.o.w.so.m. 00 00 ,	~
SYSTEM\ControlSet001\Services\W32Time\Parameters		Offset:	0	