Windows Registry

Windows Registry

- a collection of databases that contains the system's configuration data
- This configuration data can be about the hardware, the software, or the user's information.
- It also includes data about the recently used files, programs used, or devices connected to the system.
- The registry on any Windows system contains the following five root keys:

Folder/predefined key	Description
HKEY_CURRENT_USER	- Contains the root of the configuration information for the user who is currently logged on The user's folders, screen colors, and Control Panel settings are stored here This information is associated with the user's profile This key is sometimes abbreviated as HKCU .
HKEY_USERS	- Contains all the actively loaded user profiles on the computer HKEY_CURRENT_USER is a subkey of HKEY_USERS HKEY_USERS is sometimes abbreviated as HKU .
HKEY_LOCAL_MACHINE	- Contains configuration information particular to the computer (for any user) This key is sometimes abbreviated as HKLM .
HKEY_CLASSES_ROOT	- Is a subkey of HKEY_LOCAL_MACHINE\Software The information that is stored here makes sure that the correct program opens when you open a file by using Windows Explorer This key is sometimes abbreviated as HKCR Starting with Windows 2000, this information is stored under both the HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER keys. 1. The HKEY_LOCAL_MACHINE\Software\Classes key contains default settings that can apply to all users on the local computer. 2. The HKEY_CURRENT_USER\Software\Classes key has settings that override the default settings and apply only to the interactive user HKEY_CLASSES_ROOT key provides a view of the registry that merges the information from these two sources HKEY_CLASSES_ROOT also provides this merged view for programs that are designed for earlier versions of Windows To change

	the settings for the interactive user, changes must be made under HKEY_CURRENT_USER\Software\Classes instead of under HKEY_CLASSES_ROOT To change the default settings, changes must be made under HKEY_LOCAL_MACHINE\Software\Classes If you write keys to a key under HKEY_CLASSES_ROOT , the system stores the information under HKEY_LOCAL_MACHINE\Software\Classes If you write values to a key under HKEY_CLASSES_ROOT , and the key already exists under HKEY_CURRENT_USER\Software\Classes , the system will store the information there instead of Under HKEY_LOCAL_MACHINE\Software\Classes .
HKEY_CURRENT_CONFIG	Contains information about the hardware profile that is used by the local computer at system startup.

Accessing registry hives offline (regedit.exe)

Registry Editor				-	×
File Edit View Favorites Help					
Computer\HKEY_LOCAL_MACHINE\SECU	IRITY				
Computer Comput	Name	Type REG_SZ	Data (value not set)		

Accessing registry hives online

- if you only have access to a **disk image**, you must know where the registry hives are located on the disk.
- The majority of these hives are located in the **C:\Windows\System32\Config** directory and are:
- 1. **DEFAULT** (mounted on **HKEY_USERS\DEFAULT**)
- 2. **SAM** (mounted on **HKEY_LOCAL_MACHINE\SAM**)

- 3. **SECURITY** (mounted on **HKEY_LOCAL_MACHINE\Security**)
- 4. **SOFTWARE** (mounted on **HKEY_LOCAL_MACHINE\Software**)
- 5. **SYSTEM** (mounted on **HKEY_LOCAL_MACHINE\System**)

Hives containing user information:

- For Windows 7 and above, a user's profile directory is located in <u>c:\Users\</u> <username>\ where the hives are:
- 1. **NTUSER.DAT** (mounted on **HKEY_CURRENT_USER** when a user logs in)
 - located in the directory C:\Users\<username>\
- 2. USRCLASS.DAT (mounted on HKEY_CURRENT_USER\Software\CLASSES)
 - located in the directory C:\Users\<username>\AppData\Local\Microsoft\Windows
- Remember that NTUSER.DAT and USRCLASS.DAT are hidden files.

The Amcache Hive:

- Windows creates this hive to save information on programs that were recently run on the system.
- This hive is located in C:\Windows\AppCompat\Programs\Amcache.hve.

Transaction Logs and Backups:

Transaction Logs (Yet to be done)

- The transaction logs can be considered as the journal of the changelog of the registry hive.
- Windows often uses transaction logs when writing data to registry hives.
- This means that the transaction logs can often have the latest changes in the registry that haven't made their way to the registry hives themselves.
- The transaction log for each hive is stored as a **.LOG** file in the same directory as the hive itself. It has the same name as the registry hive, but the extension is .LOG.
- For example, the transaction log for the SAM hive will be located in
 C:\Windows\System32\Config in the filename SAM.LOG.
- Sometimes there can be multiple transaction logs as well. In that case, they will have .LOG1, .LOG2 etc., as their extension.

Backups

- Registry backups are the **opposite** of Transaction logs.
- These are the backups of the registry hives located in the C:\Windows\System32\Config directory.
- These hives are copied to the C:\Windows\System32\Config\RegBack directory every ten days.
- It might be an excellent place to look if you suspect that some registry keys might have been deleted/modified recently.

Data Acquisition Tools

KAPE

<u>KAPE</u> is a live data acquisition and analysis tool which can be used to acquire registry data. It is primarily a command-line tool but also comes with a GUI.

📌 gl	ape v1.1	.0.0								- 6	3 ×
File	Fools										
🗸 U:	e Target op	tions			Use Module opti	ions					
Та	get option	15			- Module option	s					
Targ	et source	C:\	·		Module source						
Targ	et destinatio	n D:\target	· 🗹	Flush 🗌 Add %d 🗌 Add %m	Module destination	1		Flush Add %d Add %m Zip			
		Targets (Do	uble-click to edit a target)								
Dra	g a column h	eader here to group by that colu	mn × registry	🛛 🔻 Find							
	Selected	Name	Folder	Description							
ę		• O ¢	*@c	•@c ^	Y 🔳 x0c						^
		MiniTimelineCollection	Compound	MFT, Registry and Event							
	\checkmark	Registry ^{Hives}	Compound	System and user related							
	\checkmark	Registry HivesOther	Windows	Other Registry Hives							
	\checkmark	RegistryHivesSystem	Windows	System level/related Regi 🗸	AppCo						\checkmark
F	rocess VSCs	Deduplicate	Container None	○ VHDX ○ VHD ○ Zip	Export format	Default CS					
SHA	1 exclusions		Base name		Module variables				Кеу		
		*	··· Zip cont	tainer Transfer					Value		
п	urnet varia	bles Transfer options									
	inger vun										
Tar	get variable	s	Key	· ·						Add	
			Value	•							
					Other options						
				📑 Add	Debug messag	es 🗌 Trace mes	sages	Ignore FTK warning			
					Zip password			Retain local copies			
- 60	rent com	nand line									
		tsourco C:tdost D:\	targettfluchtarget	Pogistovilivos Amcacho	Pagisto/HivosOt	hor Dogistry His	occustom Pogistrulliu	vosl leor qui			
	perene	bource e. tuest b.i	anger and ange	regise inves, medere,	region friteson	inci ji cegisti ji in	cooyoccin,regiou yini	gui			
٥	Copy comma	ind			6	Sync with GitHub				0	Execute!
Docum	entation	Targets available: 235	argets selected: 5 Modules	available: 232 Modules select	ted: 0					Disable flu	ush warning:

Autopsy

<u>Autopsy</u> gives you the option to acquire data from both live systems or from a disk image. After adding your data source, navigate to the location of the files you want to extract, then right-click and select the Extract File(s) option.

id Data Source	e 📠 Images/Videos 🔣 Communications ♀ Ge	olocation 🗮 Timeline 🔏 Discovery 🗽 Gen	erate Report 💊 Close Case								Keyword List		Keyword Sear
>		C Listing											F
		/LogicalFileSet1//Users/U	mair										36 F
	Documents and Settings (0)	Table Thumbnail Sur	nmary										
	Drivers (8)											\$	Save Table as
	Intel (1)	Name			0	Madfied Time	Change Time	Access Time	Created Time	Cine	Elsee(Dir)	Elsee(Mots)	Keene
· · ·	MSOCache (1)	Name		5 0	0	Modified Time	Change Time	Access Time	Created time	Size	Flags(Dir)	riags(meta)	Known
1.	PerfLogs (0)	Pictures				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown
👜 🗓	Program Files (30)	PrintHood				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown
÷.	Program Files (x86) (25)	Recent				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown
🕀 - 📜	ProgramData (25)	Saved Games				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00.00:00:00	0000-00-00 00:00:00	n	Allocated	Allocated	unknown
÷.	Recovery (1)	Searches				0000-00-00.00:00:00	0000-00-00 00-00-00	0000-00-00.00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown
	System Volume Information (0)	SandTo				0000-00-00-00-00-00	0000-00-00-00-00-00	0000-00-00-00-00-00	0000.00.00.00.00.00	0	Allocated	Allocated	unknown
	Users (b)	a sentro				0000-00-00 00.00.00	0000-00-00 00.00.00	0000-00-00 00.00.00	0000-00-00 00.00.00	0	Allocated	Allocated	GINIOMI
	Default (29)	Start Menu				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	U	Allocated	Allocated	unknown
	Default Liser (0)	July Templates				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown
÷.	Public (9)	👃 Tracing				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown
Ē.	📙 Umair (36)	📜 Videos				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown
	icesoft (1)	gitconfig			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	126	Allocated	Allocated	unknown
	📜 3D Objects (1)	NTUSER.DAT				0,000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2359296	Allocated	Allocated	unknown
	🕀 📜 AppData (3)	ntuser.dat.LC	Properties			00:00:00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	688128	Allocated	Allocated	unknown
	Application Data (0)	ntuser.dat.LC				100-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	524288	Allocated	Allocated	unknown
	Contacts (1)	NTI ISER DAT	Open in External Viewer	Ctrl+E		00-00-00-00-00-00	0000-00-00-00-00-00	0000-00-00-00-00-00	0000-00-00 00-00-00	65536	Allocated	ollocated	unknown
	Decktes (12)						0000 00 00 00.00.00	0000 00 00 00:00:00	0000 00 00 00:00:00	524200	Allegated	Allegated	
	Desktop (13)	NIUSER.DATI	Extract File(s)			00-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	524200	Allocated	MIDCateu	unnown
	Downloads (59)	NTUSER.DAT	Export Selected Rows to	CSV		00-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	524288	Allocated	Allocated	unknown
	Favorites (3)	Intuser.ini					0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20	Allocated	Allocated	unknown
	IntelGraphicsProfiles (3)		Add File Tags			>							
	📜 Links (3)												
	📜 Local Settings (0)	Hex Text Applic	Add Files to Hash Set (N	o MD5	Hash)	> sults Context Ann	otations Other Occurre	nces					
	Image: MicrosoftEdgeBackups (1)	Strings Indexed Text	Translation										
	🐊 Music (1)												
	J My Documents (0)												
	OneDrive (1)												
	Pictures (3)												
	PrintHood (U)												
	Equal Campa (1)												
	Saved Games (1)												
	SendTo (0)												

FTK Imager

<u>FTK Imager</u> is similar to Autopsy and allows you to extract files from a disk image or a live system by mounting the said disk image or drive in FTK Imager.

AccessData FTK Imager 4.3.0.18					-	×
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp						
🏩 🏩 🗣 🛳 🚖 🗇 🖶 🗮 🚛 🚑 🗁 🚥	🖪 🥄 🛄 🖹 🖻 🐱 😹 🦹 🖕					
Evidence Tree \times	File List					
HP Universal Print Driver	Name Export Files	Size	Туре	Date Modified		
H- Intel	NTUSER.DAT	2,304	Regular File	10/31/2021 4:53:07		
PerfLogs	NTUSER.DAT.FileSlack	136	File Slack			
Program Files Program Files	ntuser.dat.LOG1	603	Regular File	10/27/2021 7:33:02		
ProgramData	ntuser.dat.LOG1.FileSlack	236	File Slack			
Recovery	ntuser.dat.LOG2	603	Regular File	10/27/2021 7:33:02		
System Volume Information	ntuser.dat.LOG2.FileSlack	112	File Slack			
All Users	NTUSER.DAT{1c2b59c6-c5f5-11e	64	Regular File	10/27/2021 7:33:02		1.1
	NTUSER.DAT{1c2b59c6-c5f5-11e	512	Regular File	10/27/2021 7:33:02		- 1
	NTUSER.DAT{1c2b59c6-c5f5-11e.	512	Regular File	10/27/2021 7:33:02		- 1
🗄 🗀 Umair	1 ntuser.ini	1	Regular File	10/28/2021 8:55:15		 -
Custom Content Sources $\qquad imes$	000010 00 00 00 00 01 00 00 00-05	00 00 00 00 00 00	00 00 regi			1.1
Evidence:File System Path File Options	000020 01 00 00 00 20 00 00 00-00 000030 5C 00 3F 00 3F 00 5C 00-43	D0 21 00 01 00 00 3A 00 5C 00	55 00 \.?.?.\	··Ð!·····		- 1
	000040 73 00 65 00 72 00 73 00-5C	00 55 00 6D 00	61 00 s·e·r·s	·\·U·m·a·		
	000060 72 00 2E 00 64 00 61 00-74	00 00 00 00 00 00	00 00 rd.a	-t		
	000070 C5 59 2B 1C F5 C5 EB 11-BA	CB 00 0D 3A 96	48 8E ÅY+ ·õÅë	-°Ё··:-Н·		
	0000000 00 00 00 00 C6 59 2B 1C-F5	C5 EB 11 BA CB	00 0DEY+	·őÅë ·°Ë · ·		
	0000a0 3A 96 48 8E 72 6D 74 6D-16	DD 92 6B 67 CB	D7 01 : H .rmt	m·Ý·kgË×·		
	0000b0 4F 66 52 67 01 00 00 00-00	00 00 00 00 00	00 00 OfRg · · ·			
		00 00 00 00 00	00 00			
	0000e0 00 00 00 00 00 00 00 00 00-00	00 00 00 00 00	00 00			
	0000f0 00 00 00 00 00 00 00 00 00-00	00 00 00 00 00	00 00			
	000100 00 00 00 00 00 00 00 00 00-00	00 00 00 00 00	00 00			
New Edit Remove Remove All Create Image		00 00 00 00 00 00	00 00			
Properties Hex Value In Custom Con	Cursor pos = 0; clus = 9165267; log sec	= 73322136	00 001			
Exports files from the image to a local folde	r					

• Another way you can extract Registry files from FTK Imager is through the **Obtain Protected Files option.**

• This option is only available for live systems and is highlighted in the screenshot below. This option allows you to extract all the registry hives to a location of your choosing. However, it will not copy the Amcache.hve file

AccessData FTK Imager 4.3.	0.18				_	×
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp						
		🖸 🍳 🗋 🖹 📾 🐱 👬 😹 🦿 🖉				
Evidence Tree	×	File List				 ×
	<u> </u>	Obtain Protected Files	C: T	D I M I'C I		
		obtain Protected Tiles	Size Type	Date Modified		
		0000000000 FB 52 90 4F 54 46 53 20	-20 20 20 00 02 08 00 00 58	NTES		 _
Custom Content Sources	×	0000000010 00 00 00 00 00 F8 00 0	-3F 00 FF 00 00 38 13 00	···ø··?·ÿ··8··		1.1
Evidence Eile System Bath Eile	Ontions	000000020 00 00 00 00 80 00 80 00	-7E ED 3C 18 00 00 00 00 ···	·····~i<····		
Evidence: File System (Path) File	options		-02 00 00 00 00 00 00 00 00 ···			
		0000000050 00 00 00 00 FA 33 C0 8	-D0 BC 00 7C FB 68 C0 07	· ·ú3À ·Đ¾ · ûhÀ ·		
		0000000060 1F 1E 68 66 00 CB 88 1	-0E 00 66 81 3E 03 00 4E ··h	hf·Ë····f·>··N		
		0000000070 54 46 53 75 15 B4 41 B	-AA 55 CD 13 72 OC 81 FB TFS -75 03 F9 DD 00 1F 83 FC UP	Su · ´A≫≛UI · r · ·ŭ u . ÷1. · . u .≑Ý · · . ì		
		0000000090 18 68 1A 00 B4 48 8A 16	-OE 00 8B F4 16 1F CD 13 -h	··´H····ô··Í·		
		00000000a0 9F 83 C4 18 9E 58 1F 72	-E1 3B 06 0B 00 75 DB A3 Z	Ä··X·rá;···uÛ£		
		0000000000 0F 00 CI 2E 0F 00 04 10 0000000000 66 FF 06 11 00 03 16 01	-5A 33 DB B9 00 20 2B C8 -4 -00 8E C2 FF 06 16 00 E8 fV	A. · · · · Z3U* · +E · · · · · · · · Âÿ · · · è		
		00000000d0 4B 00 2B C8 77 EF B8 0	-BB CD 1A 66 23 C0 75 2D K -+	+Èwï, ·»Í ·f#Àu-		
		00000000e0 66 81 FB 54 43 50 41 7	-24 81 F9 02 01 72 1E 16 f ú	ûTCPAu\$ ·ù · ·r · ·		
		0000000010 68 07 BB 16 68 52 11 10 0000000100 55 16 16 16 68 B8 01 66	-68 09 00 66 53 66 53 66 A.x -61 0E 07 CD 1A 33 C0 BF U.	»·nR··n··ISISI ··h ·fa··Í·3À:		
New Edit Remove Remove All	Create Image	0000000110 0A 13 B9 F6 0C FC F3 A	-E9 FE 01 90 90 66 60 1E	¹ö∙üóªép···f`		
	- F	0000000120 06 66 A1 11 00 66 03 00	-1C 00 1E 66 68 00 00 00 .f;	; · ·f · · · · ·fh · · ·		
Properties Hex Value In Cu	stom Con	Cursor pos = 0; log sec = 0				
Exports selected system files for	facilitating a	SAM attack				1

Tools to read/Parse registry

Registry Viewer

• It only loads one hive at a time, and it can't take the transaction logs into account.

AccessData Registry Viewer (Demo Mode)	- [NTUSER.DA	νT]		_		
🔛 File Edit Report View Window H	Help				- 8 :	×
📽 🚊 B. 🖛 🖶 🗑 🖻 🖻 🗭 💡						_
I A NTUSER.DAT	Name	Туре	Data			_
AppEvents	🍓 (default)	REG_TYPE_SZ	(value not set)			
Console						
Control Panel						
Keyboard Layout						
Microsoft						
Network						
Printers						
🗄 🗀 Software						
🗊 🚍 System						
- 🗀 Uninstall						
						_
Key Properties					4	ħ.
Last Written Time 10/31/2021 10:34:14 L						
AccessData Registry Viewer						.13

Zimmerman's Registry Explorer

• It can load multiple hives simultaneously and add data from transaction logs into the hive to make a more 'cleaner' hive with more up-to-date data.

Fil	Registry Exp	lorer v1.6.0.0 ns Bookmarks (29/0) View Help	p											-		×
R	egistry hives (1)	Available bookmarks (30/0)					V	/alues								
Γ	Enter text to search	h			Find		Dr	rag a column h	eader he	re to group by	that column					Q
_								Value Name		Value Type	Data	Value Slack	Is Deleted	Data	Record Re	allocated
	Key name		# values	# subkeys	Last write timestamp		9	BIC		REC	REC	* O C				
9	R C		-	-	-	^		MystDeviceV	/erify	ReaDword	512	-				
	Conso	le	48	3	3 2021-10-27 19:34:19		1	Consistentab	reiny.	DeeDword	1					
	Contro	ol Panel	1	14	4 2021-10-28 08:56:41			ServicesTab		Regoword	1					
	Enviro	nment	4	0	2021-10-27 19:33:14			OnlineDiagno	ostics	RegDword	1					
	EUDC		0	4	4 2021-10-27 19:33:02			OnlineSuppo	ort	RegDword	1					
	🕨 🧮 Keybo	ard Layout	0	3	3 2021-10-27 19:33:07			ProductManu	uals	RegDword	1					
	Micros	oft	0	1	1 2021-10-27 19:33:02			DriverUpdat	es	RegDword	1					
	🚞 Netwo	rk	0	0	2021-10-27 19:33:02			OrderSupplie	ES	RegDword	1					
	🕨 🚞 Printer	rs	0	6	5 2021-10-31 04:40:08			CurrentProfi	ile	RegSz	Default Location	ED-E6				
	a 🚞 Softwa	are	0	23	3 2021-10-31 05:14:46			ReadInOldPr	rofiles	RegDword	1					
	💳 7-Zi	ip	2	0	2021-10-27 19:33:15			ReadInM 1Pr	ofiles	ReqDword	1					
	🕨 🧮 Acc	essData	0	2	2 2021-11-04 02:06:07		-	ChangedDer	ta	ReeDword	-					
	🕨 🚞 App	DataLow	0	1	1 2021-10-27 19:33:15			changeur or		Regoword						
	🕨 🧮 Bitv	ise	0	6	5 2021-10-27 19:33:15			SNPRUNCOUR	nt	RegDword	1					
	🚞 Cha	angeTracker	0	0	2021-10-28 08:56:46			SNP-TMLast	Run	RegDword	132450847					
	🕨 🧮 Clie	nts	0	2	2 2021-10-31 05:13:07			SNPTriggerM	larketing	RegDword	0					
	🕨 🚞 Disc	cord	0	1	1 2021-10-27 19:33:15			SNPShowTM	Privacy	RegDword	0					
	🚞 fcdf	f0d7f-424b-5f10-a1c7-a8f643f21adf	3	0	2021-10-27 19:33:15											
	▶ 🚞 Goo	ogle	0	3	3 2021-10-31 05:28:27			Supe viewer	Piezeru	lawar						
	⊿ 🚞 Hev	vlett-Packard	0	4	4 2021-11-01 14:31:56		1	ype viewer	Binary	viewer						
) 🕨 🚞 3	35e03c50-e9f4-49e0-cb96-5d48742d	2	1	1 2021-10-31 04:45:39		Va	alue name	MystDev	viceVerify						
Þ	4 🚞 I	IP Print Settings	15	1	1 2021-11-02 19:23:25		Va	lue type	RegDwg	rd						
)	Default Location	1	1	1 2021-10-31 04:45:36				- cgono							
	E H	IP SSNP	3	0	2021-11-01 14:32:30		Va	alue	512							
) 🚞 т	M	0	2	2 2021-10-31 04:46:40											
	🕨 🧮 Inte		0	1	1 2021-10-27 19:33:15											
	🕨 🧮 Len	0V0	0	2	2 2021-10-27 19:33:15	\sim	R	aw value	00-02-0	0-00						
<	Key: ROO	T\Software\Hewlett-Packard\HP Pri	int Settings									Valu	e: MystDevi	ceVerify	Collapse	all hive
Se	lected hive: NTUS	ER.DAT clean Last write: 202	1-11-02 19:23	:25 15 of	15 values shown (100.0	0%)	Loa	ad complete						Hidden	keys: 0	59

RegRipper

• takes a registry hive as input and outputs a report that extracts data from some of the forensically important keys and values in that hive. The output report is in a text file and shows all the results in sequential order.

• One shortcoming of RegRipper is that it does not take the transaction logs into account.

RegRipper,	v.3.0		_		×
File Help					
Hive File:	D:\target\NTUSER.DAT_clean		E	Browse	
Report File:	D:\target\ntuserreport.txt		E	Browse	
sysintemals1 tsclientDone typedpathsDo typedurlsDo typedurlstime. uninstallDon userassistDo wc_sharesD winrarDone. winscpDone winzipDone wordwheelque 0 plugins com	Done. b. Done. ne. Done. e. Done. bone. e. eryDone. pleted with errors.				
		Rip	!	Close	
Done.					10

Investigating

System Information and System Accounts

OS Version

SOFTWARE\Microsoft\Windows NT\CurrentVersion

		_ [Value Name	Value Type	Data	Value Slack
	Key name	-11	P 80C	RBC	RBC	all c
_		^	SystemRoot	RegSz	C:\WINDOWS	00-00-00-00-00
	Windows Media Foundation		BaseBuildRevisionNumber	RegDword	1	
	Windows Media Player NSS		BuildBranch	RegSz	vb release	00-00-00-00-00
	Windows Messaging Subsystem		BuildGUID	RegSz		00-00
	CurrentVersion		BuildLab	RegSz	19041.vb release.191206-1406	00-00
	Windows Performance Toolkit		BuildLabEx	RegSz		00-00-00
	Windows Photo Viewer		CompositionEditionID	RegSz	Enterprise	00-00-00-00-05
	Windows Portable Devices		CurrentBuild	ReaSz	19044	
	Windows Script Host		CurrentBuildNumber	RegSz	19044	
	Windows Search		CurrentMajorVersionNumber	RegDword	10	
	Windows Security Health		CurrentMinorVersionNumber	RegDword	0	
	Windows 10Upgrader		CurrentTune	Regenera	Multiprocessor Erea	65-00-64-00-00-00-00-00-00-00-00-00-00-00-00-00
	WindowsRuntime		CurrentType	DeeCe	6 a	
	WindowsSelfHost		Currentversion	Reysz	0.5	00-00-00
	WindowsStore		EditionID	Regsz	Protessional	00-00
	WindowsUpdate		EditionSubManufacturer	RegSz		
	Wisp		EditionSubstring	RegSz		
	WianSvc		EditionSubVersion	RegSz		
	Wipasvc		InstallationType	RegSz	Client	00-00-00-00-00
			InstallDate	RegDword	1637778211	
	WUSDAPI		ProductName	RegSz	Windows 10 Pro	72-00-70-00-72-00-69-00-73-00-65-00-
			ReleaseId	RegSz	2009	00-00
			SoftwareType	RegSz	System	00-00-00-00-00

Autostart Programs (Autoruns)

The following registry keys include information about programs or commands that run when a user logs on.

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

SOFTWARE\Microsoft\Windows\CurrentVersion\Run

	Enter text to search Find	D	rag a column header here to group by	that column				م
			Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
_	Key name		* # D C	8 0 0	RBC	RBC		
Y			SecurityHealth	RegExpandSz	%windir%\system32\Secu	00-00-00		
	Retaillemo		VMware User Process	RegSz	"C:\Program Files\VMware	00-00		
ŕ	RunOnce		VMware VM3DService Process	RegSz	"C:\WINDOWS\system32\	47-00		
	SecondaryAuthEs							

Services info

SYSTEM\CurrentControlSet\Services

• Notice the Value of the Start key in the screenshot below.

R	egistry hives (7) Available bookmarks (108/0)		1	alues					
[Enter text to search Find		D	ag a column header h	ere to group by	that column			
-		-		Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
-	Key name	_	Ŷ	R C	R C	RBC	REC		
٩		^	•	DependOnService	RegMultiSz	FltMgr	00-00-00		
	Beep			Description	RegSz	@%systemroot%\system	00-00-00		
	> DFE			DisplayName	RegSz	@%systemroot%\system	00-00-00		
ſ				ErrorControl	ReaDword	1			
	BluetoothilserService			Group	RegSz	ESEIlter Top	00-00		
	Bluetooth IserService Za6b6			ImageDath	DegEvpandSz	SvetamPoot/svetam32/d	00-00		
	boxser			Start	RegExpanusz	pystemotor pystemoz (u	00-00		
	BrokerInfrastructure			Start	Reguword	2			
	▶ == Browser			Supportedheatures	Reguword	/			
	PTACSaprica			Туре	RegDword	2			

In this registry key, if the start key is set to 0x02, this means that this service will start at **boot**.

Current control set

- The hives containing the machine's configuration data used for **controlling system startup.**
- Commonly, we will see two Control Sets, **ControlSet001** and **ControlSet002**, in the SYSTEM hive on a machine.
 - In most cases, **ControlSet001** will point to the Control Set that the machine **booted with**
 - SYSTEM\ControlSet001
 - ControlSet002 will be the last known good configuration.
 - SYSTEM\ControlSet002
- Windows creates a volatile Control Set when the machine is **live**, called the CurrentControlSet (HKLM\SYSTEM\CurrentControlSet). For getting the most accurate system information, this is the hive that we will refer to.
- We can find out which Control Set is being used as the CurrentControlSet by looking at the following registry value: SYSTEM\Select\Current
- Similarly, the last known good configuration can be found using the following registry value: SYSTEM\Select\LastKnownGood

1	Enter text to search Find	
	Key name	
۴	REC	^
÷.	Select	
	🕨 💳 Setup	
	Software	
	🕨 💳 State	
	🕨 💳 WaaS	
	▶ 🚞 WPA	
	😭 Unassociated deleted values	
	🛯 🔐 C:\Users\THM-4n6\Desktop\UsrClass.dat clean	

Dra	Drag a column header here to group by that column												
	Value Name	Value Type	Data	Valu									
۴	RBC	RBC	RBC	R B C									
F	Current	RegDword	1										
	Default	RegDword	1										
	Failed	RegDword	0										
	LastKnownGood	RegDword	1										

Computer Name

SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

	Enter text to search Find	1	
	Key name		
٩	R B C	\wedge	+
÷	ComputerName		

l	Drag a column header here to group by that column											
		Value Name	Value Type	Data	Value Slack	I						
ł	٩	RBC	RBC	RBC	RBC							
l	+	(default)	RegSz	mnmsrvc	02-00-B0-00							
I		ComputerName	RegSz	THM-4N6	00-00-00							

Time Zone Information

SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Enter text to search Find		Drag a column header here to group by that colu	mn	م
l er	-11	Value Name	Value Data	Value Data Raw
Key name	_ [9 8BC	a 🗖 c	R C
REC	^	Bias	-300	4294966996
Terminal Server		DaylightBias	-60	4294967236
		DaylightName	@tzres.dll,-871	@tzres.dll,-871
▶ 💳 UnitedVideo		DaylightStart	Month 0, week of month 0, day of week 0, Hours:Minutes:Seconds:Milliseconds 0:0:0:0	00-00-00-00-00-00-00-00-00-00-00-00-00-
▶ Construction		StandardBias	0	0
Isothermalian		StandardName	@tzres.dll872	@tzres.dll,-872
usbstor		StandardStart	Month 0, week of month 0, day of week 0	00-00-00-00-00-00-00-00-00-00-00-00-00-
▶ 🚞 VAN		Stanuarustant	Hours:Minutes:Seconds:Milliseconds 0:0:0:0	00-00-00-00-00-00-00-00-00-00-00-00-00-
Version		TimeZoneKeyName	Pakistan Standard Time	Pakistan Standard Time
Video	:	ActiveTimeBias	-300	4294966996

Network Interfaces and Past Networks

SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces

E	Enter text to search Find	n I.	Dra	ag a column header here to grou	up by that colu	mn			م
_		_		Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
	Key name	_	9	R C	R C	RIC	8 0 C		
9		^	+	EnableDHCP	RegDword	1			
	DNSRegisteredAdapters			Domain	RegSz				
	Interfaces			NameServer	RegSz				
	[44d5640f-2572-40d5-a87f-51d5055b82e6]			DhcpIPAddress	ReaSz	192, 168, 100, 58	BA-00-B8-16-0A-00		
	{49cc068d-4d9d-11ec-a780-806e6f6e6963}			DhcpSubnetMask	RegSz	255,255,255,0			
	{61988577-c1a8-41f1-a283-21cc83b7435a}			DhonServer	RegSz	192, 168, 100, 1	35-00-00-00-65-00-7		
Þ	{7b1e8ddb-fc33-43b1-8cd5-7f0e3afa9ecb			Lease	RegDword	86400			
	NsiObjectSecurity			LeaseObtainedTime	RegDword	1637778828			
	= PersistentRoutes			T1	RegDword	1637822028			
	Winsock	Ι.		11	Regbword	1627954429			
	Performance	:		12	RegDword	1037054420			
	E Security			LeaseTerminatesTime	RegDword	1637865228			
	ServiceProvider			AddressType	RegDword	0			
	🕨 🚞 Tapip6			IsServerNapAware	RegDword	0			
	F CPIP6TUNNEL			DhcpConnForceBroadcastFlag	RegDword	0			
	💳 tcpipreg			DhcpNameServer	RegSz	192.168.100.1			
				DhcpDefaultGateway	RegMultiSz	192.168.100.1	00-00-00-00-00-00		
	💳 tdx			DhcpSubnetMaskOpt	RegMultiSz	255.255.255.0	00-00-00-00-00-00		
	Telemetry			DhcpInterfaceOptions	RegBinary	FC-00-00-00-00-0	00-00-00-00		
	terminpt			DhcpGatewayHardware	RegBinary	C0-A8-64-01-06-00	2E-00-30-00-00-00		
	TermService			DhcpGatewayHardwareCount	RegDword	1			
	Themes				-				

The past networks a given machine was connected to can be found in the following locations

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed

R	egistry hives (/) Available bookmarks (108/0)		Vi	alues										
	Enter text to search Find		Dra	ag a column header he	a column header here to group by that column									
_				Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated					
_	Key name	_	9	RBC	8 8 C	RBC	RBC							
٩	RBC	^	-	ProfileGuid	RedSz	{A3D7C922-7D34-4688	CA-63-7E-00-CA-99							
	🚞 Managed		1	Description	Deefe	Mahurah D								
	⊿ 🚞 Unmanaged			Description	Regsz	Network 2								
Þ	010103000F0000F008000000F0000F04			Source	RegDword	8								
	0 10 10 3000F0000F008000000F0000F05D50D	i		DnsSuffix	RegSz	eu-west-1.compute.int	F5-48-B1-00-F5-57							
	0 10 10 3000F0000F008000000F0000F07444C0			FirstNetwork	RegSz	Network 2								
	0 10 10 3000F0000F008000000F0000F07BEDE9			DefaultGatewayMac	RegBinary	02-D4-D8-FF-33-74	87-01-C0-51-87-01							
	NoImeModeImes													

• These registry keys contain past networks as well as the last time they were connected.

SAM hive and user information

• The SAM hive contains user account information, login information, and group information.

SAM\Domains\Account\Users

-																					
E	Enter text to search Find		Dra	ag a columr	n header he	re to group	by that co	olumn													
		- 1		User Id	Invalid	Total L	Create	Last Lo	Last Pa	Last In	Expires	User N	Full Na	Passwo	Groups	Comment	User C	Home	Interne	Accoun	Home .
_	Key name	_	9	-	-	=	-	-	-	-	=	R C	R C	# C	e C	RBC	RUC	R B C	RBC		
-		11		501	0	0	2021-1					Guest			Guests	Built-in					
	Account															account					
	Aliases															access to					
	▶ Groups															the					
•	Users															/domain					
	Builtin			503	0	0	2021-1					DefaultA			System	A user					
	LastSkuUpgrade											ccount			Managed	account					
	KXACI														Group	by the				~	
	C:\USers\Inn-4no\Deskt															system.					
	Consolo			504	0	0	2021-1		2021-1			WDAGUti				A user					
	Control Pagel	11										nt				managed					
	Environment															and used					
	E FUDC															system					
	Keyboard Layout															for Windows				\checkmark	
	Printers															Defender					
	4 Software															Applicati					
	Amazon															scenarios					
	Classes															1.00					
	Microsoft			1001	0	19	2021-1	2021-1	2021-1	2021-1		THM-4n6		count	Administr						

• The information contained here includes the relative identifier (RID) of the user, number of times the user logged in, last login time, last failed login, last password change, password expiry, password policy and password hint, and any groups that the user is a part of.

Usage or knowledge of files/folders

Recent Files

· a list of recently opened files for each user

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

located in the directory C:\Users\<username>\

R	(egistry hives (7) Available bookmarks (108/0)		V	alues Recent do	cuments					
Γ	Enter text to search Find		Dr	ag a column header	here to group by that c	olumn				م
		-		Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
	Key name	_	9	* C C	* D C	8 0 0	REC	-	-	-
٩	REC	^		RecentDocs	7	EZtools	EZtools.lnk	0	2021-12-01 13:00:34	
۲	RecentDocs		1	PecentDocs	6	Settings	Settings lok	1		2021-11-30 10:56:23
	Ribbon			Recenterous		Seconds	Secongstank	-		2021-11-50 10.50.25
	E RunMRU			RecentDocs	5	WallpaperSettings.xml	WallpaperSettings.Ink	2		2021-11-30 10:56:21
	▶ = SearchPlatform			RecentDocs	4	System and Security	System and Security lok	3		
	Shell Folders			RecentDocs	2	··/PP06C0E4-D202-4E	Suctor lok	4		
	Shutdown			Recentbocs	5	75-8A90-CB05B6477E	Systemank			
	StartPage					EE}				
	Streams		-	RecentDocs	1	KAPE	KAPE.Ink	5		
	StuckRects3			RecentDocs	0	Get-KAPEUpdate.ps1	Get-KAPEUpdate.lnk	6		2021-11-24 18:18:48
	TabletMode			RecentDocs	2	ChangeLog.txt	ChangeLog.lnk	7		2021-11-24 18:18:48
	Taskband			Folder	2	Settings	Settings.Ink	0	2021-11-30 10:56:23	
	TypedPaths			Folder	1	System and Security	System and	1		
	C User Shell Folders						Security.Ink			
	▶ 💳 UserAssist			Folder	0	KAPE	KAPE.lnk	2		
				.xml	0	WallpaperSettings.xml	WallpaperSettings.lnk	0	2021-11-30 10:56:21	
	VisualEffects			.txt	0	ChangeLog.txt	ChangeLog.lnk	0	2021-11-24 18:18:48	
	C Wallpapers			.ps1	0	Get-KAPEUpdate.ps1	Get-KAPEUpdate.Ink	0	2021-11-24 18:18:48	

• if we are looking specifically for the last used **PDF(or any extention)** files, we can look at the following registry key:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ .pdf

• located in the directory C:\Users\<username>\AppData\Local\Microsoft\Windows

Office Recent Files

• Microsoft Office also maintains a list of recently opened documents.

NTUSER.DAT\Software\Microsoft\Office\<VERSION_Number>

• An example registry key will look like this:

NTUSER.DAT\Software\Microsoft\Office\15.0\Word

• Starting from **Office 365**, Microsoft now ties the location to the user's <u>live ID</u>. In such a scenario, the recent files can be found at the following location.

NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\FileMRU

ShellBags

- When any user opens a folder, it opens in a specific layout.
- Users can change this layout according to their preferences.
- These layouts can be different for different folders.
- This information about the Windows 'shell' is stored and can identify the Most Recently Used files and folders.
- Since this setting is different for each user, it is located in the user hives. We can find this information on the following locations:

USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

- Registry Explorer doesn't give us much information about ShellBags.
- However, another tool from Eric Zimmerman's tools called the ShellBag
 Explorer shows us the information in an easy-to-use format. We just have to point to the hive file we have extracted, and it parses the data and shows us the results

💐 S	hellBag	s Explorer v1.4.0.	0											-		5
File	Tools	Help														
Val	ue															
+ 41	D	esktop		lu.t												í
	÷.	My Computer		Value	Icon	Shell Type	MRU Positi 4	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has Explored	Misce	laneous	
		KAPE	9	# C	No im	# C	-	-	-	-	-	-		* CC		
	\$	Home Folder		My Computer	\$	Root folder: GUID		0				2021-12-01 13:06:47	×			
	2	Search Folder		KAPE		Directory		1 2021-11-25 03:34:14	2021-11-25 03:34:14	2021-11-25 03:34:14			✓	NTES	file system	
	2	Search Folder	•	Home Folder	*	Root folder: GUID		2			2021-11-24 18:20:02					
	\$	Control Panel		Search Folder	2	Users property view		3			2021-11-30 11:08:01					
		E:\		Search Folder	2	Users property view		4			2021-11-30 11:08:52					
				Control Panel	*	Root folder: GUID		5								
				E:\		Users property view: Drive letter		5			2021-11-24 18:20:02		\checkmark			

Open/Save and LastVisited Dialog MRUs:

- When we open or save a file, a dialog box appears asking us where to save or open that file from.
- It might be noticed that once we open/save a file at a specific location, Windows remembers that location.
- This implies that we can find out recently used files if we get our hands on this information. We can do so by examining the following registry keys

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

[Enter text to search Find		Dra	ag a column header here to group b	y that column			م
	M			Value Name	Mru Position	Executable	Absolute Path	Opened On
	Key name	Ŧ	9	RBC	=	8 8 C	RBC	=
Ŷ	CIDSizeMRU		•	0	0	notepad.exe	My Computer\C:\Program Files\Amazon\Ec2ConfigService\S ettings	2021-11-30 10:56:19
P		Ш					a congo	

Windows Explorer Address/Search Bars:

• the paths typed in the Windows Explorer address bar or searches performed

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

	Enter text to search Find	Dr	ag a column hea	der here to gro	o group by that column					
_			Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated		
_	Key name a	9	RBC	RBC	RBC	8 B C				
9 1	TurnedPaths	•	url1	RegSz	C:\	72-00-6F-00-67-00-72-00-61				
ľ	I liser Shell Folders		url2	RegSz	C:\Program Files	33-00-32-00-00-00-00-00-00-00				
	► UserAssist		url3	RegSz	C:\Windows\System32	60-53-09-00				

Evidence of Execution

UserAssist

- These keys contain information about the **programs launched**, the **time of their launch**, and the **number of times they were executed**.
- However, programs that were run using the command line can't be found in the User Assist keys.
- The User Assist key is present in the NTUSER hive, mapped to each user's **GUID**.

NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count

R	izgistry hives (1) Available bookmarks (31/0) Values UserAssist									
	Enter text to search Find	Dr	Drag a culum header here to group by that culumn 👂							
			Program Name	Run Counter	Focus Count	Focus Time	Last Executed			
_	Key name	9	10:	=	=	RBC	=			
9	R C		UEME_CTLCUACount:ctor	0	0	0d, 0h, 00m, 00s				
F	∡ = {F4E57C4B-2036-4 Count		{Common Programs}\Accessories\Snipping Tool.Ink	9	0	0d, 0h, 00m, 00s	2021-11-25 03:14:34			
	FA99DFC7-6AC2-		UEME_CTLSESSION	54	0	0d, 0h, 00m, 00s				
	Cartual Desktops		{Common Programs}\Accessories\Paint.lnk	7	0	0d, 0h, 00m, 00s	2021-11-25 03:14:34			
	VisualEffects		{Programs}\Accessories\Notepad.lnk	6	0	0d, 0h, 00m, 00s	2021-11-25 03:14:34			
	Calipapers Valpapers		{User Pinned}\TaskBar\File Explorer.Ink	26	0	0d, 0h, 00m, 00s	2021-12-01 13:02:43			
	Ext		{Programs}\Windows PowerShell\Windows PowerShell.Ink	Windows PowerShell\Windows	0	0d, 0h, 00m, 00s	2021-11-25 03:37:24			
	Feeds	:	{User Pinned}\TaskBar\Firefox.lnk	2	0	0d, 0h, 00m, 00s	2021-12-01 12:32:34			
	FileAssociations		{Common Programs}\Accessories\Remote	1	0	0d, 0h, 00m, 00s	2021-11-25 03:59:55			
	FileHistory		Desktop Connection.Ink							
	GameDVR		{User Pinned}\TaskBar\Opera Browser.Ink	1	0	0d, 0h, 00m, 00s	2021-11-25 04:10:02			
	Group Policy		{Common Programs}\Accessories\Notepad.lnk	1	0	0d, 0h, 00m, 00s	2021-11-30 10:55:21			
	Holographic									

ShimCache

- ShimCache is a mechanism used to keep track of application compatibility with the OS and tracks all applications launched on the machine.
- Its main purpose in Windows is to ensure backward compatibility of applications.
- It is also called Application Compatibility Cache (AppCompatCache).
- It is located in the following location in the SYSTEM hive:

SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

- ShimCache stores file name, file size, and last modified time of the executables.
- Our goto tool, the Registry Explorer, doesn't parse ShimCache data in a humanreadable format, so we go to another tool called AppCompatCache Parser, also a part of Eric Zimmerman's tools. It takes the SYSTEM hive as input, parses the data, and outputs a CSV file that looks like this:

Fil	Image: EXVever v1.0.0.0 - 20211202213532_Windows10Creators_SYSTEM_dean_AppCompatCache.csv - CM X File Tools Help - CM X											
	A	В	c	D	E	F	G					
1	ControlSe	CacheEnt	Path	LastModifiedTimeUTC	Executed	Duplicate	SourceFile	^				
2	1	0	C:\Users\THM-4n6\Desktop\KAPE\gkape.exe	6/24/2021 6:23	NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean					
3	1	1	C:\Users\THM-4n6\Desktop\KAPE\kape.exe	6/24/2021 6:23	NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean					
4	1	2	C:\Program Files\Common Files\microsoft shared\ink\TabTip.exe	10/6/2021 13:52	NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean					
5	1	3	C:\Windows\System32\rdpinput.EXE	12/7/2019 9:09	NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean					
6	1	4	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe	10/6/2021 13:45	NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean					
				44 Jac Jacob 3.40			columnation and produced overrage stress					

• We can use the following command to run the AppCompatCache Parser Utility:

AppCompatCacheParser.exe --csv <path to save output> -f <path to SYSTEM hive for data parsing> -c <control set to parse>

AmCache

• This performs a similar function to ShimCache, and stores additional data related to program executions.

- This data includes **execution path**, **installation**, **execution** and **deletion times**, and **SHA1** hashes of the executed programs.
- This hive is located in the file system at:

C:\Windows\appcompat\Programs\Amcache.hve

• Information about the last executed programs can be found at the following location in the hive:

Amcache.hve\Root\File\{Volume GUID}\

This is how Registry Explorer parses the AmCache hive:

Enter text to search Find	Drag a column header here to group by	y that column					
1	Timestamp	Path	Name	Product Name	Publisher	Version	SHA1
Key name	9 —	* 0 t	4 0 4	(D)	10:	1D:	4 0 c
C_Users\THM-4n6\Desktop\NTUSER_E ROOT	2021-12-01 12:45:37	c:\program files\uindowsapps\microsoft.microsoft3dview er_7.2107.7012.0_x648wekyb3d8bbwe\3 dviewer.exe	3DViewer.exe	view 3d	microsoft corporation	7.2107.7012.0	1b3846b00a121040b4a4b2796773ef90899f6 048
C:\Users\THM-4n6\Desktop\SYSTEM_	2021-12-01 12:55:19	c:\program files\7-zip\7z.exe	7z.exe	7-zip	igor pavlov	19.00	6c7ea8bbd435163ae3945cbef30ef8b9872a45 91
C\Users\THM-4n6\Desktop\Amcache (11517870-670-4e20-9618-7548117154)	2021-12-01 12:55:19	c:\program files\7-zip\7zfm.exe	72FM.exe	7-zip	igor pavlov	19.00	e45e198607c8d7398745baa71780e3e7a2f6d eca
A Root	2021-12-01 12:55:19	c:\program files\7-zip\7zg.exe	7zG.exe	7-zip	igor pavlov	19.00	df22612647e9404a515d48ebad49034968525 0de
DeviceCensus DriverPackageExtended InventoryApplication	2021-12-01 13:00:29	c:\program files (x80)\google\update\download\(8a69d345-d 564-463c-aff1-a69d9e530f96)\96.0.4664.45 \96.0.4664.45_chrome_installer.exe	96.0.4664.45_drrome_installer.exe		google Ic	96.0.4664.45	e2b8b2e677152fab11f14d1e192184ca05166e Of
InventoryApplicationAppV	2021-12-01 12:55:49	c: \program files \amazon \ssm \amazon-ssm-agent. exe	amazon-ssm-agent.exe				e57d619197d5937d85d8d702385fd45707a30 809
InventoryApplicationFramework InventoryApplicationShortcut	2021-12-01 12:57:38	c:\programdata\package cache\(71aad)47-faef-4dc7-8d46-60f211aa a9f6)\amazonssmagentsetup.exe	AmazonSSMAgentSetup.exe	amazon som agent	amazon web services	3.1.338.0	9194f54f615d43875ed093b94da70ea596828 16a
InventoryDeviceContainer	2021-12-01 13:00:20	c: \users \thm-4n6 \desktop \amcacheparser.ex	AmcacheParserexe	amcacheparser	eric zimmerman	1.4.0.0	13ab20217dff43326642d9a224e5405db00b3c
InventoryDeviceInterface	Total rows: 596	- A					Export

BAM/DAM

- Background Activity Monitor or BAM keeps a tab on the activity of background applications.
- **Desktop Activity Moderator** or **DAM** is a part of Microsoft Windows that optimizes the **power consumption of the device**.
- Both of these are a part of the Modern Standby system in Microsoft Windows.
- In the Windows registry, the following locations contain information related to BAM and DAM.
- This location contains information about **last run programs**, their full paths, and **last execution time.**

SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}

Below you can see how **Registry Explorer** parses data from BAM:

inter te	ext to search Find		Drag a column header here to group by that column	
		11	Program	Execution Time
key na	me	11	9 nBC	-
e c	^	ΙĒ	Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy	2021-11-24 18:02:15
	A Dam		Microsoft. Windows. Cortana_cw5n1h2txyewy	2021-11-24 18:02:15
	State	11	\Device\HarddiskVolume2\Windows\explorer.exe	2021-11-24 18:02:15
	S-1-5-18	11	\Device\HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe	2021-11-24 18:02:15
	S-1-5-21-4174496583-1		windows.immersivecontrolpanel_cw5n1h2txyewy	2021-11-24 15:40:31
	5-1-5-21-417449658		\Device\HarddiskVolume2\Program Files\VMware\VMware Tools\vmtoolsd.exe	2021-11-24 18:02:14
	S-1-5-90-0-1		\Device\HarddiskVolume2\Windows\System32\cmd.exe	2021-11-25 03:23:14
	5-1-5-90-0-2		\Device\HarddiskVolume2\Program Files (x86)\Mozilla Firefox\firefox.exe	2021-11-25 03:46:20
	BasicDisplay		\Device\HarddiskVolume2\Program Files (x86)\Google\Update\GoogleUpdate.exe	2021-11-25 03:43:40
	BasicRender	1.1	\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2021-11-24 17:56:18
	BattC		VDevice Harddisk Volume 2 Windows \System 32 \notepad.exe	2021-11-25 03:42:53
	BcastDVRUserService		\Device\HarddiskVolume2\Users\THM-4n6\AppData\Local\Programs\Opera\opera.exe	2021-11-25 04:12:35
	BcastDVRUserService_7a6b6		VDevice HarddiskVolume2/Program Files/Google/Chrome/Application/chrome.exe	2021-11-25 03:43:50
	DOMTH2		\Device\HarddiskVolume2\Windows\System32\mstsc.exe	2021-11-25 04:00:04
	P Been		Device HarddiskVolume2/Windows/System32\SystemSettingsAdminFlows.exe	2021-11-25 04:00:54
	> C= BEE		VDevice HarddiskVolume2/Windows/System32\SystemPropertiesComputerName.exe	2021-11-25.04:01:35
	bindflt		VDevice HarddiskVolume2/Windows/System32/rundl32.eve	2021-11-24 17:38:19
	BITS		Vevice Harddisk/olume2/Program Files (v86)/WindowsInstallationAssistant/Windows10LingraderApp.ex	2021-11-24 18:01:52
	BluetoothUserService		Vavice Harddisk Volume 2/Drogram Files (v86) Wirroenft Edgel Indate Wirroenft Edgel Indate eve	2021-11-24 15:21:35
	BluetoothUserService_7a6b6		Davice Hardrick/ok ma 20 program Files (v86) Microsoft EdgeOptate Pile 0501 EdgeOptate.exe	2021-11-24 15:23:43
	bowser 🗸	I F	period participation and program in the program in the program of the get public door the second sec	6V61 11 61 14/64/14

External Devices/USB device forensics

Device identification:

- The following locations keep track of **USB keys** plugged into a system.
- These locations store the vendor id, product id, and version of the USB device plugged in, the time the devices were plugged into the system and can be used to identify unique devices.

SYSTEM\CurrentControlSet\Enum\USBSTOR

SYSTEM\CurrentControlSet\Enum\USB

Registry Explorer shows this information in a nice and easy-to-understand way.

Registry nives (5) Available bookmarks (61/0)		dues usosituk										
Enter text to search Find	Find Drag a column header here to group by that column											
Mar		Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed
key name	9	-	n C	#Ec	a 🛛 c	R C	e 🗖 c	* 0 ¢	-	-	-	-
V allc USB	Þ	2021-11-24 18:25	Ven_Kingston	Prod_DataTraveler _2.0	Rev_PMAP	{e251921f-4da2-11 ec-a783-001a7dda 7110}	1C6F654E59A3B0C 179D366AE&0	Kingston DataTraveler 2.0 USB Device	2021-11-24 18:25	2021-11-24 18:25	2021-11-24 18:40	
XENBUS EXENVIF		2021-11-24 18:27	Ven_USB3.0	Prod_External_Devi ce	Rev_SDM1	{f529a9d6-4d9e-11 ec-a782-001a7dda 7110}	0123456789ABCDE 80	USB3.0 External Device USB Device	2021-11-24 18:27	2021-11-24 18:27	2021-11-24 18:27	

First/Last Times:

Similarly, the following registry key tracks the first time the device was connected, the last time it was connected and the last time the device was removed from the system.

```
SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-
97a6-4088-9453-a19231573b29}\####
```

In this key, the *####* sign can be replaced by the following digits to get the required information:

Value	Information

0064	First Connection time
0066	Last Connection time
0067	Last removal time

Although we can check this value manually, as we have seen above, Registry Explorer already parses this data and shows us if we select the USBSTOR key.

USB device Volume Name:

The device name of the connected drive can be found at the following location:

```
SOFTWARE\Microsoft\Windows Portable Devices\Devices
```

R	egistry hives (4) Available bookmarks (92/0)	Va	alues Windows Portable Devices						
	Enter text to search Find		g a column header here to group by that column						
			Timestamp	Device	Serial Number	Guid	Friendly Name		
-	Key name	Ŷ	=	*Bc	*Ec	aBc	a C		
۲ ۲	Windows Portable Devices Windows Portable Devices SWD#WPDBUSENUM#{E2!	•	2021-11-25 07:16:54			{E251921F-4DA2-11EC-A783-001A7DDA7110 }	USB		
			2021-11-25 07:16:54			<pre>{F529A9D6-4D9E-11EC-A782-001A7DDA7110 }</pre>	New Volume		

We can compare the GUID we see here in this registry key and compare it with the Disk ID we see on keys mentioned in device identification to correlate the names with unique devices. Take a look at these two screenshots and answer Question # 3.

Combining all of this information, we can create a fair picture of any USB devices that were connected to the machine we're investigating.

- reg query HKLM /s /f "C:\TMP\mim.exe sekurlsa::LogonPasswords > C:\TMP\o.txt"
 - to search for a specific value in the registry