Windows Forensic

What is windows forensic

Windows Forensics, include the process of conducting or performing forensic investigations of systems which run on Windows operating systems, It includes analysis of incident response, recovery, and auditing of equipment used in executing any criminal activity.

Forensic Process

The general phases of the forensic process are: the identification of potential evidence; the acquisition of that evidence; analysis of the evidence; and production of a report.



You can go to the link > <u>https://bluecapesecurity.com/</u> > Free tutorials > Build your forensic workstation.

Setup for windows forensic

- 1. Download the virtualbox https://www.virtualbox.org/wiki/Downloads and download vhd iso 2019 <u>https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019</u> and install the server 2019.
- Start the powershell as a administrator and paste the command of the link Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux . And restart the server 2019.
- 3.Download the ubuntu iso file in this link <u>https://learn.microsoft.com/en-us/windows/wsl/install-manual#downloading-distributions</u>
- 4. Install ubuntu as a commandline in server 2019.
- 5. Install windows10, open powershell as a administrator paste the command in this following link <u>https://learn.microsoft.com/en-us/windows/wsl/install-manual</u> and install ubuntu linux from Microsoft store.

Administrator: Windows PowerShell Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. PS C:\Users\Administrator> Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux_

k

Run this command in power shell on server 2019.



File Home Share	View					× 0
$\leftarrow \rightarrow \neg \uparrow \equiv \rightarrow$ This	PC > Documents (\\VBaxSvr) (Z:) >				~ Õ	Search Documents (\\VBoxSvr 🔎
 ✓ Quick access ✓ Desktop ✓ Downloads ✓ Documents ✓ Pictures 	Name Analysis Evidence WF System Volume Information	Date modified 5/17/2022 9:16 PM 5/17/2022 10:27 AM 5/19/2022 5:07 PM 6/3/2022 8:32 AM 5/12/2022 10:44 AM	Type File folder File folder File folder File folder File folder	Size		
This PC	VirtualBox VMs VMWare VMs Ubuntu2004-220404.rio	6/6/2022 3:58 PM 2/14/2022 3:42 PM 6/6/2022 8:04 PM	File folder File folder APPXBUNDLE File	965 922 KB		
	Ubuntu file	convert zi	ip file.			
8 items 1 item selected 94	13 MB					E =



File Home	Share	View										- °
to Quick Copy access	Paste	6 Cut ■ Copy path] Paste shortcut	Move Copy to+ to+ Organiz	e e	New Folder New	item • access •	Properties •	Dpen •	Select all Select none Invert selection Select			
→ - ↑	🕨 > This	PC > Downloads	5 >							~ Ö	Search Downloads	Q,
Quick access Desktop Downloads Documents Pictures This PC Network	* * * *	Name AppxMetada Content_Typ AppxBlockM AppxSignatu Ubuntu_2004 Ubuntu_2004 Ubuntu_2004 Ubuntu_2004 Ubuntu_2004	ta pes] ap re.p7x 1.4.2.0_ARM64.appx 1.4.2.0_{\alpha}e=100.appx 1.4.2.0_scale=125.appx 1.4.2.0_scale=150.appx 1.4.2.0_scale=400.appx 1.4.2.0_scale=400.appx	Da 6// 6// 6// 6// 1 1 1 1 1 1 1 1 1 1 1 1	te modified 5/2022 8:06 PM 5/2022 8:06 PM 5/2022 8:05 PM 5/2022 8:05 PM 5/2022 8:05 PM 5/2022 8:05 PM 5/2022 8:05 PM 5/2022 8:05 PM	Type File fol XML D XML D P7X Fil APPX F APPX F APPX F	der ocument ocument e ile ile ile ile	Size 11 12 463,879 57 69 81 81 176	KB KB KB KB KB			
				Extra	ct the	ubu	intu	file iı	n downl	oad		
			t	folder	•			-				
items 1 item	selected 1	75 KB										

PS

Mod

-a

-a

-a

PS

Administrato	r: Windows PowerShell				-	×
C:\Users	\Administrator	<pre>>Downloads></pre>	• dir			î
Directo	ory: C:\Users\/	Administrato	or\Downloads			
e::	Last	VriteTime	Length	Name		
	c. (c. (2022)	0.00 00				
	0/0/2022	8:00 PM	220	Appxnetadata		
	6/6/2022	8:06 PM	338	AppxBlockMap.xml		
	6/6/2022	8:06 PM	11955	AppxSignature.p7x		
	6/6/2022	8:05 PM	475011248	Ubuntu_2004.4.2.0_ARM64.appx		
	6/6/2022	8:05 PM	58246	Ubuntu_2004.4.2.0_scale-100.appx		
	6/6/2022	8:05 PM	69891	Ubuntu_2004.4.2.0_scale-125.appx		
	6/6/2022	8:05 PM	81939	Ubuntu_2004.4.2.0_scale-150.appx		
	6/6/2022	8:05 PM	179710	Ubuntu 2004.4.2.0 scale-400.appx		
	6/6/2022	8:06 PM	513691210	Ubuntu 2004.4.2.0 x64.appx		
	6/6/2022	8:06 PM	469	[Content Types].xml		

Open the power shell and run this command then after ubuntu installation will be start.



Recycle Bin

Ubuntu

Installing, this may take a few minutes...

Please create a default UNIX user account. The username does not need to match your Windows username. For more information visit: https://aka.ms/wslusers Enter new UNIX username:

> Create a username – forensic Create a password – Admin@123 (Any..)





Recycle Bin



- 0 \times ~ 0 ✓ ♂ Search Downloads ø

Windows PowerShell Rec Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart

Deployment Image Servicing and Management tool Version: 10.0.19041.844

Image Version: 10.0.19044.1288

Enabling feature(s) [-----74.0%------74.0%-------

Run this command in power shell on target machine.



Windows 10 Enterprise Evaluation Windows License valid for 90 days



Windows 10 Enterprise Evaluation Windows License valid for 90 days

- Efficient command line utilities including bash, ssh, git, apt, npm, pip and many more



Install a complete Ubuntu terminal environment in minutes with Windows Subsystem for Linux (WSL). Develop cross-platform applications, improve your data science or web development workflows and manage IT infrastructure without leaving Windows.

Key features: - Efficient command line utilities including bash, ssh, git, apt, npm, pip and many more

Windows 10 Enterprise Evaluation Windows License valid for 90 days

6.Open server 2019 and chage the following setting.

setting > date and time setting > select (UTC) Coordinated Universal time. Go to the c drive and create a two folder Cases and Tools.

setting > virus and threat protection off > cloud-delivered protection off > Exclution – Add click and select cases and tools folder one by one. And create a snapshort.

7. Install the tools in server 2019 for windows Forensic.

1.Download the Arsenal Image Mounter-<u>https://arsenalrecon.com/downloads</u> 2.Download the KAPE Tool- <u>https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape</u>

- 3. Download the Eric Zimmerman Tools <u>https://ericzimmerman.github.io/#index.md</u>
- 4. Download the Regripper tool <u>https://github.com/keydet89/RegRipper3.0</u>
- 5. Download the event log explorer <u>https://eventlogxp.com/</u>
- 6. Download Notepad++ <u>https://notepad-plus-plus.org/downloads/</u>
- All tool copy in c drive Tools folder.
- Install the setup of Event log and Notepad++.

Go to the C:/Tools/Get Zimmer tools > open powershell > .\Get-ZimmermanTools.ps1 – Netversion 4.

O

L. Open:

Edit

Open v. Cr.

Type

Eile folder

File folder

File tolder

File Folder

File folder

File folder

File folder

File Folder

Application

Application

Application

Text Document

Windows Powerfi ...

Properties

2022 T1-36 PM. File folder 2022 11-37 PM

2022 11:37 PM. File folder

2022 11:37 PM. File Folder 2022 11:37 PM

2022 11:38 P6A File folder 2023 11:38 PM

2022 11:38 PM File toldes 2022 11-38 PM

2022 11:39 PM CSV File

Item +

access *

modified

2022 T1:37 PM

2032 T1-38 PM

2022 11:37 PM

2022 11/39 PM

2022 12-30 PM

2022 T1 28 AM

2022 12-31 PM

2022 11-39 PM

2022 10-58 PhA

Windows2019-FOR (Initial install) [Running]



Firefas

Event Log

Explorer



PS C:\Tools\EZTools>



11:39 PM

5 KB

4.545 KB

à.417 KB

3,994 KB

31.68

32.KB

0

p

Select all

Search EZTools

Size

Select none

invert selection

Select



Manage

View

SDT_x64FREE_EN-US_VHD (C:) Drive Tools

File Home \rightarrow

←

 \mathbf{T}

÷

Share

This PC > SDT_x64FREE_EN-US_VHD (C:)

đ \times _ ~ 🕐

Search SDT_x64FREE_EN-US_V... 🔎

~ Ō

📃 Desktop 🛛 🖈 ^	Name	Date modified	Туре	Size
🕂 Downloads 🖈	Cases	30-06-2023 09:12	File folder	
🚆 Documents 🖈		15-09-2018 07:19	File folder	
📰 Pictures 🛛 🖈	📙 Program Files	07-07-2023 07:52	File folder	
Evidence	Program Files (x86)	28-06-2023 13:23	File folder	
Execution	ProgramData	29-06-2023 16:46	File folder	
	📊 Tools	28-06-2023 13:25	File folder	
Projeta	Users	27-06-2023 16:59	File folder	
Registry	Windows	29-06-2023 21:43	File folder	

- 🗸 💻 This PC 3D Objects >
 - 🛛 Desktop >
 - 4 Documents >
 - Downloads >
 - Music >
- > 📰 Pictures
- > 📑 Videos
- > L SDT_x64FREE_EN
- > 👸 CD Drive (D:) Vir
- > 👳 Downloads (\\VI
- 💣 Network >

8 items



 \checkmark

(



:== 💌

2	Ŧ	Tools
~	•	10013

¥

←

File Home Share

 \mathbf{T}





_

> This PC > SDT_x64FREE_EN-US_VHD (C:) > Tools >



Q

E Desktop	* ^	Name	Date modified	Туре	Size
🖊 Downloads	*	Arsenal-Image-Mounter-v3.9.239	28-06-2023 13:25	File folder	
Documents	*	Get-ZimmermanTools	28-06-2023 13:44	File folder	
Pictures	*	kape	28-06-2023 13:26	File folder	
Evidence		RegRipper3.0-master	28-06-2023 13:25	File folder	
Execution		📱 Arsenal-Image-Mounter-v3.9.239	28-06-2023 05:08	Compressed (zipp	34,023 KB
		📩 elex_setup	28-06-2023 05:35	Application	9,193 KB
- Progins		🔢 Get-ZimmermanTools	28-06-2023 05:07	Compressed (zipp	11 KB
Registry		📱 kape	28-06-2023 05:10	Compressed (zipp	1,36,288 KB
💻 This PC		🏶 npp.8.5.4.Installer.x64	28-06-2023 05:37	Application	4,553 KB
3D Objects		🕌 RegRipper3.0-master	28-06-2023 05:30	Compressed (zipp	5,058 KB

All tool show Here.

- Desktop
- Documents
- Downloads
- h Music
- Pictures
- Videos
- SDT_x64FREE_EN
- 🔞 CD Drive (D:) Vir
- 👳 Downloads (\\VI
- Network

ρ

10 items



(3)

v

Ξī

Updates are available e Required updates need to be installed.

View updates



. _ _ _

8. Install the windows 10 Enterprise version as a Target Sysytem and create a snapshort. <u>https://bluecapesecurity.com/prepare-your-target-system/</u>

Go to the setting > Windows Update > Advance option > Update off. Virus and threat protection > manage setting > Real-time protection off and Cloud delivered protection off.

<u>Attack Script Preparation</u> - Go to the url <u>https://github.com/bluecapesecurity/PWF</u> zip file download and extract file.

2 script is execute here.

1. Sysmon script – C:\users\denisha\Desktop\PWF-main\PWF-main/Install-Sysmon > powershell as administrator > .\Install-sysmon.ps1.

2. ART Attack script - C:\users\denisha\Desktop\PWF-main\PWFmain\AtomicRedTeam > open powershell as Administrator > .\ART-attack.ps1.

Sysmon Script Run



OpenDir Cloud

ART Attack Script

	27 Administrator: Windows PowerShell	1		×
cycle Bin	PS C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam> .\ART-attack.psl Installing invoke-atomicredteam			î
	Running Atomic Tests Progress: [ooodooodooo			
eula	<pre>'C:\Users\IEUser\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet p running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShells and import the NuGet provider now? [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function See Wiki at https://github.com/redcanaryco/invoke-atomicredteam/wiki for complete details Starting ART attack simulation</pre>	rovider Set to :	by install	
(F-main	Using Logger: Default-ExecutionLogger All logging commands found Executing test: T1566.001-1 Download Macro-Enabled Phishing Attachment Done executing test: T1566.001-1 Download Macro-Enabled Phishing Attachment T1078.003 Atomic Test #1 - Create local account with admin privileges PathToAtomicsFolder = C:\AtomicRedTeam\atomics			
	Using Logger: Default-ExecutionLogger All logging commands found Executing test: T1078.003-1 Create local account with admin privileges The command completed successfully. The command completed successfully. The command completed successfully. Done executing test: T1078.003-1 Create local account with admin privileges T1059.001 Atomic Test #11 - PowerShell Fileless Script Execution PathToAtomicsFolder = C:\AtomicRedTeam\atomics			
	Using Logger: Default-ExecutionLogger All logging commands found Executing test: T1059.001-11 PowerShell Fileless Script Execution The operation completed successfully. Done executing test: T1059.001-11 PowerShell Fileless Script Execution T1547.001 Atomic Test #1 - Reg Key Run PathToAtomicsFolder = C:\AtomicRedTeam\atomics			
	Using Logger: Default-ExecutionLogger All logging commands found Executing test: T1547.001-1 Reg Key Run			

OpenDir.Cloud

Data Collection

9.Memory Acquisition of the target system

Step for Memory Acquisition :

1. Create a Evidence Folder in Main PC.

2. Go to C:\Users\Documents\Evidence > open cmd > "C:\program Files\Oracle\Virtual Box\VBoxManage.exe"

- 3. SET PATH=%PATH%;"C:\Programs Files\Oracle\Virtual Box"
- 4. vboxmanage.exe
- 5. vboxmanage list vms

6. Vboxmanage debugvm id paste machine(target machine) dumpvm core –filename win10memory.raw

7. Certutil – hashfile win10-memory.raw > win10.memory – hash.txt.



P

3

Ţ,

[]]

е

へ 臣 (1) 14:14 へ 臣 (1) 09-07-2023 ロ

10.Disk Acquisition target system

🗿 Oracle VM VirtualBox Manager						—	đ	\times
File Machine Medium Help								
Tools 🖉 🗄	Add Create	copy Move	Remove Release	Search Properties	Refresh			
win2019-for (34 practical)	🔒 Hard disk	s Optical d	lisks 🛛 💾 Floppy d	disks				
2019 🔶 Running	Name		~			Virtual Size	Actual Sit	70
		26ccea-dfd7-4e08-	hd93-7a85hd797974	S conv vbd		vii tuai Size	Actual 312	~
windows 10 (fresh installation)	> 17763.7	37.amd64fre.rs5_r	elease_svc_refresh.	190906-2324_server_se	rverdatacente	40.00 GB	8.31 GB	
Powered Off	✓ Target s	ysteam.vdi				50.00 GB	50.00 GB	\$
	✓ {0e	Copy	Ctrl+Shift+C	di ka vdi		50.00 GB	1.09 GB	
Target systeam (After attack shutdown)		Move	Ctrl+Shift+M	cabe}.vdi		50.00 GB	9.42 GB	
	{at	Pomovo	Ctrlushiftun	di		50.00 GB	1.36 GB	
	> window	Remove	CULTSHITTER			50.00 GB	50.00 GB	
		Release	Ctri+Shift+L					
		Search						
		Properties	Ctrl+Shift+P					
	Attributes	Information						
	Type	Normal						
			-			145 0040		-
	Location:	ers (Denisha (Virtua)	Box VMs (Larget syst	eam (Snapshots \{Ue9229	91a-4319-4be6-8	04f-c9213ea20	Jf88}.vdi	
	Description:							
	Size						50.00	GB
	0.20.	1				· · · ·		
		4.00 MB				2.00 TB		
						Apply	Reset	
O Type here to search	ı e	—	🝅 🔹	\$) ~ F	⊒ ⊲») 11 09-07	1:54 7-2023	\neg

🦸 Oracle VM VirtualBox Manager

File Machine Medium Help



🦸 Oracle VM VirtualBox Manager

File Machine Medium Help



Oracle VM VirtualBox Manager Ē \times File Machine Medium Help *s*? 🔚 Tools Release Add Search Refresh Create Copy Move Remove Properties Eloppy disks Hard disks Optical disks win2019-for (34 practical) 🗘 Running Name Virtual Size Actual Size {0926ccea-dfd7-4e08-bd93-7a85bd797974}_copy.vhd _ windows 10 (fresh installation) atacente.. 40.00 GB 8.31 GB Dowered Off Copy Virtual Disk \times ? 50.00 GB 50.00 GB 1.09 GB 50.00 GB Location and size of the disk image 50.00 GB 4.69 GB Target systeam (After attack 50.00 GB 9.42 GB Powered Off 1.36 GB 50.00 GB Please type the name of the new virtual hard disk file into the box below or dick on 50.00 GB 50.00 GB the folder icon to select a different folder to create the file in. ___ get systeam\Snapshots\{0e92291a-4319-4be6-8d4f-c9213ea20f88}_copy.vhd Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk. 50.00 GB . . . 50.00 GB 2.00 TB Back Finish Cancel ype. normal Location: ers\Denisha\VirtualBox VMs\Target systeam\Snapshots\{0e92291a-4319-4be6-8d4f-c9213ea20f88}.vdi Description: Size: 50.00 GB 1 1 . 4.00 MB 2.00 TB Reset Apply \heartsuit O Type here to search Д [[]] へ口の L

09-07-2023

Data Examination

Mounting the disk Image with Arsenal Image Mounter

You can enter the Target system harddisk

^ दिये <mark>17:03</mark> ↓









'iew SDT_x64FREE_EN-US_VHD (C:) → Too me Arsenal-Image-Mounter-v3.9.239 Get-ZimmermanTools kape RegRipper3.0-master Arsenal-Image-Mounter-v3.9.239	Date modified 28-06-2023 13:25 28-06-2023 13:24 28-06-2023 13:26 28-06-2023 13:26 28-06-2023 13:26	O Search Tools Type File folder File folder File folder	> 🛛 > Size	File Home Share $\leftarrow \rightarrow \checkmark \uparrow$ \checkmark \land Arse \checkmark Quick access	View nal-Image-Mount > Arsenal-Image-Mounter- Name	v3.9.239 > 🗸	ල Search Arsenal-In Type	age-Mour Size
> SDT_x64FREE_EN-US_VHD (C:) > Too me Arsenal-Image-Mounter-v3.9.239 Get-ZimmermanTools kape RegRipper3.0-master Arsenal-Image-Mounter-v3.9.239	Date modified 28-06-2023 13:25 28-06-2023 13:44 28-06-2023 13:26 28-06-2023 13:26 28-06-2023 13:25	Search Tools Type File folder File folder	م Size	← → ~ ↑ 🚺 « Arse	nal-Image-Mount > Arsenal-Image-Mounter-	v3.9.239 > V	ල Search Arsenal-Im	iage-Mour Size
me Arsenal-Image-Mounter-v3.9.239 Get-ZimmermanTools kape RegRipper3.0-master Arsenal-Image-Mounter-v3.9.239	Date modified 28-06-2023 13:25 28-06-2023 13:44 28-06-2023 13:26 28-06-2023 13:25	Type File folder File folder	Size	 Quick access 	Name	Date modified	Туре	Size
Arsenal-Image-Mounter-v3.9.239 Get-ZimmermanTools kape RegRipper3.0-master Arsenal-Image-Mounter-v3.9.239	28-06-2023 13:25 28-06-2023 13:44 28-06-2023 13:26	File folder File folder		🖈 Quick access				
Get-ZimmermanTools kape RegRipper3.0-master Arsenal-Image-Mounter-v3.9.239	28-06-2023 13:44 28-06-2023 13:26	File folder			lib	02-06-2022 10:50	File folder	
kape RegRipper3.0-master Arsenal-Image-Mounter-v3.9.239	28-06-2023 13:26			Desktop 🖈	runtimes	21-11-2022 20:48	File folder	
RegRipper3.0-master Arsenal-Image-Mounter-v3.9.239	20.06.2022 12:25	File folder		🔶 Downloads 🖈	📄 aim_cli	27-08-2022 20:45	File	
Arsenal-Image-Mounter-v3.9.239	20-00-2023 13:23	File folder		og 🔮 Documents 🖈	🚳 aim_cli.dll	28-02-2023 17:02	Application extens	5
	28-06-2023 05:08	Compressed (zipp	34,023 KB	er 📰 Pictures 🖈	im_cli	28-02-2023 17:03	Application	11/
l elex_setup	28-06-2023 05:35	Application	9,193 KB	/ 📃 Downloads (\\VBox	📄 aim_cli.runtimeconfig.json	26-11-2022 16:01	JSON File	
Get-ZimmermanTools	28-06-2023 05:07	Compressed (zipp	11 KB		📄 Arsenal Recon - End User License Agree	10-08-2022 06:16	Text Document	2/
kape	28-06-2023 05:10	Compressed (zipp	1,36,288 KB	This PC	Arsenal.ImageMounter.dll	28-02-2023 17:03	Application extens	52
npp.8.5.4.Installer.x64	28-06-2023 05:37	Application	4,553 KB	++ 🧊 3D Objects	🚳 Arsenal.ImageMounter.Forms.dll	28-02-2023 17:03	Application extens	4
RegRipper3.0-master	28-06-2023 05:30	Compressed (zipp	5,058 KB	🛄 Desktop	📄 ArsenallmageMounter.deps.json	28-02-2023 17:02	JSON File	7
				🚔 Documents	ArsenallmageMounter.dll	28-02-2023 17:02	Application extens	20,42
				🕹 Downloads	🖀 ArsenallmageMounter	28-02-2023 17:02	Application	49
				Music	ArsenallmageMounter	29-06-2023 16:54	Text Document	
<u> </u>				Pictures	ArsenallmageMounter.runtimeconfig.json	28-02-2023 17:02	JSON File	
Open ima	age mou	nter.		Video	DiscUtils.BootConfig.dll	28-02-2023 17:03	Application extens	57
T	U				DiscUtils.Btrfs.dll	28-02-2023 17:03	Application extens	6
				SD1_x64FREE_EN-US	DiscUtils.Core.dll	28-02-2023 17:03	Application extens	26
				👸 CD Drive (D:) Virtua	🚳 DiscUtils.Dmg.dll	28-02-2023 17:03	Application extens	4
				👳 Downloads (\\VBox	DiscUtils.Ext.dll	28-02-2023 17:03	Application extens	5
				A Network	DiscUtils.Fat.dll	28-02-2023 17:03	Application extens	8
				INCLIVOIR	DiscUtils.HfsPlus.dll	28-02-2023 17:03	Application extens	5/
				53 items	Γ.θ .			
	npp.8.5.4.Installer.x64 RegRipper3.0-master Open ima	npp.8.5.4.Installer.x64 28-06-2023 05:37 RegRipper3.0-master 28-06-2023 05:30	npp.8.5.4.Installer.x64 RegRipper3.0-master 28-06-2023 05:30 Compressed (zipp Open image mounter.	npp.8.5.4.Installer.x64 28-06-2023 05:37 Application 4,553 KB RegRipper3.0-master 28-06-2023 05:30 Compressed (zipp 5,058 KB Open image mounter.	npp.8.5.4.Installer.x64 28-06-2023 05:37 Application 4,553 KB RegRipper3.0-master 28-06-2023 05:30 Compressed (zipp 5,058 KB Open image mounter. Open image mounter.	npp.8.5.4.Installer.x64 28-06-2023 05:37 Application 4,553 KB RegRipper3.0-master 28-06-2023 05:30 Compressed (zipp 5,058 KB Open image mounter. Open image mounter. Uideos Vise Vitis. Bortotiis.Ext.dll Music Videos	npp.8.3.4.Installer.x64 28-06-2023 05:37 Application 4,553 KB Image: Notepade + Image: Notep	npp.8.3.4.Installer.x64 RegRipper3.0-master 28-06-2023 05:30 Compressed (zipp 5,058 KB Compressed (zipp 2,058 KB

다 🖪 오 片 🙆 📄

(

^ ╦ 4<mark>≥</mark> 29-06-2023





Firefox

Event Log

Explorer

Notepad++

+



Windows Server 2019 Datacenter Evaluation Windows License valid for 178 days Build 17763.rs5_release.180914-1434



브



Ē

No

ecycle Bin		a de la compañía de l			
		i 🗖 🗕 I	 Arranal Image Mounter v2.0.220	 \sim	
🚔 Arsenal	Image Mounter			_	\times
File BitLoo	ker Advanced	Help			





N

e Bin						
		Arranal Image	Maumtar v2 0 220	—		
Arsenal Image Mounter					- 0	>
Mount image file			×			
	wnloads (\\ > Evidence v 💍 Sear	ch Evidence	Q			
Organize 🔻 New folde	r					
This PC	Name	Date modified	Туре			
3D Objects	40926ccea-dfd7-4e08-bd93-7a85bd79797	29-06-2023 15:38	Hard Disk			
Desktop	win10-memory.raw	29-06-2023 09:00	RAW File			
 Downloads Music Pictures Videos SDT_x64FREE_EN CD Drive (D:) Vir Downloads (\\VE 	Select the disk of target	t machine				
🎒 Network 🗸 👻	<		>			
File na	me: {0926ccea-dfd7-4e08-bd93-7a85bi ~ Sup	ported formats	~			
		Open Ca	ncel			
+ Mount disk i	image Mount VSCs Launch VM	🖶× Remove	a Remove all 🕄 Refresh	AF	RSENAL RE	с
53 items	Discliftle Ntfs dll tem selected 493 KB		28-02-2023 17·04 Δnnlicatio	n extens 280 k		
				Windows Serv Windo Build	er 2019 Datacente ows License valid 17763.rs5_release.	er Ev for 1809
오 터 🧲	🣻 ڬ 🕿			へ 門		22

Mount options

Disk device, read only

Mount the disk image as a read-only disk device. No write operations will be allowed.

Disk device, write temporary

Mount the disk image as a writable disk device using the AIM write filter. Modifications will be written to a write-overlay differencing file and the original disk image will not be changed. Sometimes referred to as write-overlay or write-copy mode. (Note - required for launching virtual machines.)

Specify alternate differencing file location

Delete differencing file after unmount

Store differencing data in host RAM only (not in a file)

Windows file system driver bypass, read only

Mount the disk image as a virtual read-only file system, using DiscUtils rather than Windows file system drivers. This mount option is often used to bypass file system security, expose NTFS metafiles and streams, and recover deleted files. May also be useful to read files from disk images containing corrupted file systems. Please note, BitLocker-protected volumes are not supported and disk size values are an approximation of each volume's total file size (including things like multiple links to the same file and files with sparse allocation) so the size may appear larger than the expected volume size.

Disk device, write original

Mount the disk image as a writable disk device. Caution, modifications will be written to the original disk image.

Windows file system driver bypass, write original

Mount the disk image as a virtual writable file system. Caution, modifications will be written to the original disk image. This mount option bypasses file system security but does not expose most NTFS metafiles and streams.

Sector size: 512 ~

Fake disk signature

Report a random disk signature to Windows. Useful if the disk image contains a zeroed-out disk signature or you are attempting to mount a duplicate disk signature. (Note - requires a valid MBR and partition table.)

Create "removable" disk device

Цi

+

Emulate the attachment of a USB thumb drive, which may facilitate the successful mounting of images containing partitions rather than complete disks or images without partition tables. (Caution - see relevant FAQ on our website for caveats.)

Automatically remount at Arsenal Image Mounter startup



Windows License valid for 178 days Build 17763.rs5_release.180914-1434



 \times



Firefox

Event Log

Explorer

e

Ω



Windows Server 2019 Datacenter Evaluation Windows License valid for 178 days Build 17763.rs5_release.180914-1434



<u>Creating a triage data collection with KAPE Tool</u>







File Tools												
Use Target op	ions			Us	e Module options							
Target option	s			Managa	KAPE						-	
Target source	E:\		182000 0200	Manage	Nor C							
Target destination	C:\Cases	File Home	Share View	Application Tools								0
	Taroets (Double-	*	Cut		X 🛋	New item •	🗸 🔳 Open 🔹	Select all				
Dran a column h	and as have to serve by that column	Pin to Quick Copy	Paste	Move Copy	Delete Rename	New Easy access *	Properties	Select none				
Calculated	enter nelle to group by this column	access	Paste shorto	ut to • to •	•	folder	•	invert selection				
Selected	Name I		lipboard	U	iganize	New	Open	Select				
	ng.	← → ~ ↑	This PC > Local I	Disk (C:) > Tools	> KAPE				~ 0	Search KAPE		م
	CombinedLogs			□ Name	A	Date modified	d Type	Size				
	EventLogs	🖈 Quick access			100		- Jar-					
	EventLogs-RDP	Tools	1	Documer	ntation	3/19/2022 11:	31 PM File folder					
	EventTraceLogs	Carer		Modules		3/23/2022 9:5	8 PM File folder					
	EventTranscriptDB	- caes		Targete		3/23/2022 9:5	8 PM File folder					
I	KapeTriage	Desktop	*	Char Dat	e created: 3/19/2022	2 11:31 PM	Text Document	21 KB				
	MiniTimelineCollection	Downloads	*	Get- Size	: 372 KB	Antiving Appr Process	Windows Power	S 17 KB				
		Documents	5 <i>1</i>	gkar File	s: CompoundTarget	a, Anuvirus, Apps, Browsers Guide.guide,	Application	61,623 KB				
Process VSCs	Dedupicate	Fictures	*	gkape.set	ttings	3/23/2022 10:	24 PM SETTINGS File	1 KB				
FUA 1 auch rises		Evidence		📌 kape.exe		3/10/2022 10:	38 AM Application	7,038 KB				
Srta-1 excusions	121/171	- condence										
	*	This PC										
Target varia	bles Transfer options	3D Objects										
Target variables		Desktop										
		Pocument										
		Developed			-	Using kar	ne tool sta	are the				
		Downloads	1			Using Kap		one the				
		Music			-	nermaner	nt data of	target o	vete	m		
		Pictures				permaner	n uata OI	larger	syste	,111		
		Videos				in forenci	o worket	otion				
		Local Disk	(C:)				C WUIKSLA	illon.				
Current comm	and line	- Windows 1	0 (E-)									
Unner comm	the sume French Colores		AND C. 1071									
. wape.exe -	-tsource E:tdest C:\Case	T Document	s (1/vB0xSvr) (Z:)									
		Network										
		1.7556770799773										
Copy comma	nd											
Documentation	Tarnets available: 254 Tarnets											Forma .
No. of Concession, Name of Street, or other Distances of Street, o	inders.	AL 14	1 1 1 1 1 1 1 1 1 1 1									Contract of the
All Data is store in Cases Folder.







le Tools									
Use Target o	ptions			Use Module of	otions				
Target optic	ons			- Module optio	105				
Target source	E:\	-	***	Module source			*		
Target destinat	tion C:\Cases		Flush Add %d Add %m	Module destinate	Ion T		Melsh TA	dd %d 🗌 Add %m	20
	Targets (Dor	uble-click to edit a ta	arget)		Hod	ules (Double-click to)	edit a module)		
Drag a column	header here to group by that column	x event	© * Find						P
Selected	Name	Folder	Description						
•	10:	×D:	10: A	y (8)					* *
	CombinedLogs	Compound	Collect Event logs, Trace I	¥ (1)					
	EventLogs	Windows	Event logs		EZParşar				vera
	EventLogs-RDP	Windows	Collect Win7+ RDP relate						Y
	EventTraceLogs	Windows	Event Trace Logs		AbaCbingatCacheParser	EIYoolu	ProgramExecution	AppCompatCachePa	V Contraction of the local distance of the l
	EventTranscriptDB	Win Kape Triage	collections that will collect most of the files nee	ded for a DFIR Invi	estigation. This module pulls	evidence from File System	m files, Registry Hives, E	vent Logs, Scheduled Ta	asks, Evidence of Execution, SRUM data, SUM data, Web Browser data (IE)
F	KapeTriage	Com		iote access softly	ore wys, are party anovirus	automare logs, villidows	ao milenie datadase, an	a at recyce on data file	
	MiniTimeIneCollection	Compound	MrT, Registry and event						
			×		nitmes RhConWaler	Uniferrinal	Kamerrienthes.		
Process VSC	Cs 🗹 Deduplicate	Container 🥘	None VHDX VHD Zp	Export format	🖲 Default 🗌 CSV	O HTML O JSON			
HA-1 exclusion	ns	Base name		Module variables	¥.		Key		
	*		öp container Transfer				Volum		
Tarret	inblas Transformer								
rarget var	transfer options		1						
Target variab	Nes		Key 🔹					Add	
			Value +						
			[Ph. 444	Other option	15			_	
			EF ADD	Debug messa	ages 🗌 Trace message.	8		Ignore FTK wart	ming
				Zin national	1	+		Retain local control	ies
				- i sup potentiti				Contraction of the	
Current com	nmand line								
\kape.exe	tsource E:tdest C:\C	asestflushc	iur						
AND SPECIFIC		and and a second state of	and a second						
				with chiral 1					
p Lopy com	mand		Syn.	c with GitHub				6	Execute1

-	1
63	
2	
Firefo	x



Event Log Explorer

File Tools										
Use Targ	et options			Use Module	options					
Target o	ptions			Module opt	0125					
Target sour	ce E:\	*		Module source		1	-			
Target dest	ination C:\Cases	·	Plush Add %d Add %m	Module destina	tion	-	• El Flush 🗔 A	idd %d 🗌 Add %m 🗌 Zip		
	Targets (Do	uble-click to edit a targ	et)		Plot		edit a module)			
Drag a col	umn header here to group by that colum	nn 🗙 event	🕲 * Find					٩,		
Select	ed Name	Folder	Description							
۲ (10×	×0:	•D: ^	× (8)				· · · · ·	Windows	Q
E] CombinedLogs	Compound	Collect Event logs, Trace I	11 1						
	EventLogs	Windows	Event logs							î
	EventLogs-RDP	Windows	Collect Win7+ RDP relate							
	EventTraceLogs	Windows	Event Trace Logs					AppCompatCachePar .		
	EventTranscriptDB	DATA DESTRUC	TION WARNING!			×	Renote Access			
> 2	KapeTriage	Critic La rito v					Mochiles.			
	MiniTimeIneCollection	A III WA	RNING III				KeywordSearches			
Target Target va	variables Transfer options	v	alue 💽	Cancel]			🗃 Add		
			EP Add	Other optio	ns iages Trace messagi	es		Ignore FTK warning Retain local conies		
Current	command line exetsource E:tdest C:\(Casestflushtar	get KapeTriageifwgui							
Сорус	ommand		الله الله الله الله الله الله الله الله	nc with GitHub				S Execute	1	

Select Total execution time: 115.0	162 seconds		- 0	×				
rget 'ApplicationEvents' rget 'ApplicationEvents' rget 'ApplicationEvents' rget 'ApplicationEvents' und 675 files in 10.536	with Id '2da16dbf-ea47-448e-a00f-fc with Id '2da16dbf-ea47-448e-a00f-fc with Id '2da16dbf-ea47-448e-a00f-fc with Id '2da16dbf-ea47-448e-a00f-fc seconds. Beginning copy	442c3109ba' already processed. Skipping 442c3109ba' already processed. Skipping 442c3109ba' already processed. Skipping 442c3109ba' already processed. Skipping		^		*		
Deferring 'E:\\$MF1	I' due to UnauthorizedAccessException	· · ·				🔹 📖 🗹 Fluth 🗌 A	dd %d 🗌 Add %m	Zp
Deferring 'E:\\$Log	File' due to UnauthorizedAccessExcep	tion		Hode				
Deferring 'E:\\$Ext	tend\\$UsnJrn1:\$Max' due to NotSupport	redException		and the second second				0
Deferring 'E:\\$Sec	ure:\$SDS' due to NotSupportedExcepti	.01						-
Deferring 'E:\\$Ext	tend\\$RmMetadata\\$TxfLog\\$Tops:\$T' du	ue to NotSupportedException						ŏ
ferred file count: 7. Co	opying locked files							
Copied deferred fi	<pre>lle 'E:\\$MFT' to 'C:\Cases\E\\$MFT'. H</pre>	lashing source file						
Skipping sparse de	ile E:(\$cogrife to C:\Cases\E\\$cog	File . Hashing source file		1.07				
Copied deferred fi	<pre>ile 'E:\\$Extend\\$UsnJrnl:\$J' to 'C:\C</pre>	ases\E\\$Extend\\$J'. Hashing source file		CarlyParent	ezrode			
Copied deferred fi	<pre>Lle 'E:\\$Extend\\$UsnJrnl:\$Max' to 'C: Lle 'E:\\$Secure:\$SDS' to 'C:\Carec\E\</pre>	\Cases\E\\$Extend\\$Max'. Hashing source \$Secure \$SDS' Hashing source file	file	CPD/maol artis		Renote Access		
Copied deferred fi	<pre>ile 'E:\\$Boot' to 'C:\Cases\E\\$Boot'.</pre>	Hashing source file						
Copied deferred fi	lle 'E:\\$Extend\\$RmMetadata\\$TxfLog\\$	Tops:\$T to 'C:\Cases\E\\$Extend\\$RmMeta	data\\$TxfLog\\$T'.	Hurthalet				
shing source file				Continuint				N
ppied 601 (Deduplicated:	74) out of 675 files in 114,9477 sec	conds. See '* CopyLog.csv' in 'C:\Cases'	for copy details	and the second of the	These country	-		
ress any key to exit	Target variables			v		Value	B. 14	
		Key *	1				EP ADD	
		Value						
			- Other options					
		Add	Debug messages	Trace messages			🗹 Ignore FTK warr	ing
			Zip password		Ψ.		Retain local copi	es
	Current command line							
	Vkape eve atsource E: atdect C:\C	acestflushtarget Kane Triageifu gui						0
	- Mapelene - Source L West C. IC	ases "utushi "target kapernage "nw "gui						
			na antina 1				14	V
	Copy command	٠	Sync with GitHub				6	Execute
	Documentation Targets available: 254 Tar	gets selected: 1 Modules available: 253 Modules sel	ected: 0				Disable flush wa	mings

Firefax

Notepad++

Event Log Explorer Firefax







......

1000









Cleud

Disk Analysis Process

Go to the link and Download the materials.

https://github.com/bluecapesecurity/PWF/blob/main/Resources/Analysis-Notes-Template.docx



The **registry** or **Windows registry** is a <u>database</u> of information, settings, options, and other values for <u>software</u> and <u>hardware</u> installed on all versions of <u>Microsoft</u> <u>Windows</u> operating systems. When a program is installed, a new subkey is created in the registry. This subkey contains settings specific to that program, such as its location, version, and primary executable.

Registry Explorer with Eric Zimmerman Tools

🔒 🛛 🛃 🖛 🗸 🛛 Get-Zimme	rmanTools					- 0	\times	
File Home Share	View						\sim (?
\leftarrow \rightarrow \checkmark \uparrow \square \Rightarrow Thi	s PC > SDT_x64FREE_EN-US_VHD (C:) > Tools >	Get-ZimmermanToo	ols >		~ ∂	Search Get-ZimmermanTools	Q]
	Name	Date modified	Туре	Size				^
📌 Quick access	E + FC and	20.05.2022.12.40	File Celler					
📃 Desktop 🛛 🖈	EVEC md	28-00-2023 13:40	File folder					
👆 Downloads 🛛 🖈	Lasher	28-00-2023 13:40	File folder					
Documents 🖈	üsGeolocate	28-06-2023 13:41	File folder					
Pictures 🖈		28-06-2023 13:44	File folder					
	METExplorer	28-06-2023 13:41	File folder					
	RECond	28-06-2023 13:41	File folder					
Downloads (\\VBox	BegistryExplorer	28-06-2023 13:47	File folder					
Evidence		28-06-2023 13:42	File folder					
This PC	ShellBagsExplorer	28-06-2023 13:43	File folder					
3D Objects	SOLECmd	28-06-2023 13:43	File folder					
Deskton	TimelineExplorer	28-06-2023 13:43	File folder					
	XWFIM	28-06-2023 13:44	File folder					
Documents	IllRemoteFileDetails	28-06-2023 13:44	CSV File	5 KB				
Downloads	Gamma AmcacheParser	21-05-2023 11:49	Application	4,661 KB				
Music	AppCompatCacheParser	07-03-2023 15:13	Application	4,523 KB				
Pictures	m bstrings	20-05-2022 12:38	Application	3,997 KB				
Videos	ChangeLog	28-06-2023 13:44	Text Document	33 KB				
SDT_x64FREE_EN-US	Get-ZimmermanTools	18-05-2023 14:24	Windows PowerS	24 KB				
😵 CD Drive (D:) Virtua	🛃 JLECmd	13-03-2023 17:06	Application	4,792 KB				
Downloads (\\VBox	🕎 LECmd	04-03-2023 10:30	Application	5,063 KB				
-	MFTECmd	20-10-2022 13:37	Application	4,409 KB				
💣 Network	🜆 PECmd	28-01-2022 12:08	Application	3,885 KB				
	🔄 RBCmd	05-08-2022 13:05	Application	3,607 KB				
	PrecentFileCacheParser	15-06-2022 11:03	Application	3,283 KB				
	😽 rla	28-11-2022 13:16	Application	4,261 KB				
	SBECmd	23-02-2022 08:38	Application	4,800 KB				
	SrumECmd	26-10-2022 09:41	Application	4,517 KB				\sim
32 items							i== 🕒	

Q

Шi

e

(1)

08:26 ヘ 닫다 ↓<mark>⊗</mark> <u>30-06-2023</u>

 \Box



6 items





:== 📼



SOFTWARE

SYSTEM

Documents 🖈

Downloads (\\VE

*

*

Pictures

💻 This PC

Cases

Evidence

3D Objects

Desktop Documents Downloads

Music



512 KB

64 KB

32 KB

68,608 KB

11,008 KB

Size

0

^ 뛷 ◁⊗

 \sim

مر

olumn header here to group b

۷	Data	Valu
=	=	=

 \Box

30-06-2023

Go to this path and load all Registry hives on Registry Explorer.

29-06-2023 09:08

29-06-2023 09:08

5 ~

Type

File

File

File

File

File

Search config



Event Log

Explorer

Notepad++

ρ

Цi



File Tools Options Bookmarks (4/0) View Help

Recycle Bin

2 Firefox

Event Log Explorer



Notepad++

R	egistry hives (5) Available bookmarks (73/0)				_	Va	alues
1	Enter text to search		Find	i		Dra	ag a colu
	Key name	# values # subkeys Last write timestamp					Va V.
ę	RBC	_	=	=		9	
	C:\Cases\F\Windows\System32\config\SEC						
►	N ROOT	0	3	2023-06-29 08:01:15			
	C:\Cases\F\Windows\System32\config\DEF						
	ROOT	0	9	2023-06-29 08:27:03			
	Associated deleted records	0	0				
	👒 Unassociated deleted values	2	0				
	C:\Cases\F\Windows\System32\config\SAM						
	▶ 💳 ROOT	0	1	2023-06-28 16:04:43			
	Associated deleted records	0	0				
	⊿ 👹 C:\Cases\F\Windows\System32\config\SY						
	▶ 💳 ROOT	0	17	2023-06-29 08:00:59	1		
	Associated deleted records	0	0				
	Unassociated deleted records	0	0				
	Unassociated deleted values	146	0				
	C:\Cases\F\Windows\System32\config\50						
	▶ 💳 ROOT	0	17	2023-06-29 08:14:27			
	Associated deleted records	0	0				
	Unassociated deleted records	0	0			т	me view
	😪 Unassociated deleted values	46	0			13	/pe view

Orag a column header here to group by that column

	Va	۷	Data	Value Slack	Is Deleted
۴	—	—	=	=	=

....

			-	F



Fil	e To	ols Opti	ons Bo	ookmarks (4/0) Vie	ew Help								
R	egistry	hives (5)	Availa	ble bookmarks (73/0)									
	Enter te	ext to sear	ch		Find								
	Key na	ame											
۴	RBC				^								
	- F - 🦉	C:\Case	s\F\Wi	ndows\System32\c	config\SECURITY								
	C:\Cases\F\Windows\System32\config\SECURITY C:\Cases\F\Windows\System32\config\DEFAULT C:\Cases\F\Windows\System32\config\SAM												
 C:\Cases\F\Windows\System32\config\DEFAULT C:\Cases\F\Windows\System32\config\SAM C:\Cases\F\Windows\System32\config\SYSTEM 													
C:\Cases\F\Windows\System32\config\SAM C:\Cases\F\Windows\System32\config\SYSTEM													
	- A 🦉	C:\Case	s\F\Wiı	ndows\System32\c	config\SOFTWARE								
		Chan	nels										
		comm	and										
	•	Contr	ol Panel										
►	►	Curr	entVers	ion	Using Software hives								
	Þ	Curre	ntVersio	n	asthering the information								
	►	Windo	ows Defe	ender	gathering the mormation								
		Windo	ows Defe	ender	about current version of OS								
		E Devic	es										
<					>								
— В	ookmar	k informatio	on										
H	ve			C:\Cases\F\Windows	s\System32\config\SOFTWARE								

Va	alues					
Dra	ag a column header here to gr	oup by that co	lumn			
	Value Name	Value Type	Value	Is Del	Data Rec	
۴	RBC	RBC	RBC	RBC		
►	ProgramFilesDir	RegSz	C:\Pr	00-00		
	CommonFilesDir	RegSz	C:\Pr			
	ProgramFilesDir (x86)	RegSz	C:\Pr	00-00		
	CommonFilesDir (x86)	RegSz	C:\Pr	00-00		
	CommonW6432Dir	RegSz	C:\Pr			
	DevicePath	RegExpan	%Sys	00-00		
	MediaPathUnexpanded	RegExpan	%Sys	00-00		
	ProgramFilesPath	RegExpan	%Pro	00-00		
	ProgramW6432Dir	RegSz	C:\Pr	00-00		
	SM_ConfigureProgramsN	RegSz	Set P	00-00		
	SM_GamesName	RegSz	Games			

Bookmark information									
Hive	C:\Cases\F\W	indows\System32\config\SOFTWA	ARE						
Category	Operating sys	tem		Type viewer	Slack viewer	Binary vie	wer		
Name	CurrentVersion	n		Value name	ProgramFilesDir				
Key path	Microsoft\Wine	ows version information (Windows key)			RegSz				
Short description Windows version information (Windows key)				Value	C:\Program Files	:			_
Long description		^			·				
			~	Raw value	43-00-3A-00-5C 0-00-46-00-69-0	-00-50-00-7 00-6C-00-65	72-00-6F-00-67-00- -00-73-00-00-00	72-00-61-00-6D-0	0-2
Key: Microsoft\V	Vindows\Curr	entVersion				Value:	ProgramFilesDi	r Collapse all I	nives
Selected hive: SECURITY	Last write:	28-06-2023 17:12:44 +00:00	11 of 11 values shown (100.00%)					Hidden keys: 0	1
	e .	- 📫 😭 🗠					^ 탓 ◁≈	08:39	

 \Box

08:39 30-06-2023

⊲∞

Fil	e Tools Options	Bookmarks (4/0) View He	elp										
Re	egistry hives (5) Ava	ilable bookmarks (73/0)				Va	alues						
E	Enter text to search			Find		Dra	ag a column head	der here to gro	up by that	column			
	14						Value Name	Value Type	Data		Value	Is Del	Data Re
-	Key name				-	٩	RBC	RBC	RBC		RBC		
*		Windows \ System 32 \ config	SECURITY		-		(default)	RegSz	mnmsrvc	:	02-00		
	C:\Cases\F\W	Vindows (System 32) config			-	•	ComputerName	RegSz	DESKTOP	P-MD2HC	01-00		
	C:\Cases\F\W	Vindows\System32\config	-										
	C:\Cases\F\W	Vindows\System32\config	SYSTEM										
	▶ 🚞 {4d36e972-	e325-11ce-bfc1-08002be10318	3}										
	▶ 🚞 {53f56307-ł	b6bf-11d0-94f2-00a0c91efb8b}	}	Using System hive									
	6bdd1fc6-8	310f-11d0-bec7-08002be2092f	}	asthering the									
	AppCompate	Cache		gaulering uie	_								
	bam		1	information about	_								
Þ	Computer	Name		computer name of									
	CrashContre	ol											
	DeviceClass	es		target system.	~								
c				2	>								
Bo	ookmark information —												
HI	ve	C: (Cases (F) (Windows (5))ster	m32\config\SYSTEM							•			
Ca	ategory	Operating system				Ту	/pe viewer S	lack viewer	Binary vie	wer			
Na	ame	ComputerName				Valu	Je name Co	omputerName					
Ke	ey path	ControlSet001\Control\Com	puterName\Compute	erName		Valu	ue type Re	egSz					
Sł	nort description	The name of the computer				Valu	ue DE	SKTOP-MD2H	OPT				
Lo	ong description	The name of the computer		^									
						Ray	w value	+-00-45-00-53- 00-48-00-43-0	00-48-00-5 0-50-00-54	4-00-4F-00	-50-00-2D	-00-4D-00	0-44-00-3
				· · · · · · · · · · · · · · · · · · ·						-			
	Key: ControlSe	et001\Control\ComputerNam	ne\ComputerNam	e					Value:	Comput	erName	Collaps	se all hives
Se	lected hive: SECURITY	Last write: 28-06-2023	3 16:12:11 +00:00	2 of 2 values shown (100.00%)	Сорі	ied V	/alue data to cl	ipboard			Hi	dden key	ys: 0 1
E		🥭 🔚 📫		A						~ 토] ⊲ <mark>⊗</mark> 20	08:51	, 🖵

Gathering system information with RegRipper

Follow the Step for Regripper

- 1. Go to the C:\Tools\RegRipper\> open cmd > dir > rip.exe
- 2. You can create a folder in c drive with Analysis and also create registry folder in Analysis
- 3. Insert the file in Analysis folder: C:\Cases\F\Windows\system32\config - DEFAULT

SAM SECURITY SOFTWARE SYSTEM

C:\Cases\F\users\Denisha - NTUSER.DAT

C:\Cases\F\users\Denisha\Appdata\Local\Microsoft\Windows\- UserClass.dat 4. Back to cmd and type rip.exe -r C:\Cases\Analysis\Registry\SOFTWARE -p winver 5. rip.exe -r C:\Cases\Analysis\Registry\SOFTWARE -p nic2 6. rip.exe -r C:\Cases\Analysis\Registry\SYSTEM -p timezone 7. rip.exe -r C:\Cases\Analysis\Registry\SYSTEM -p shutdown 8. rip.exe -r C:\Cases\Analysis\Registry\SOFTWARE -p defender

📊 🛃 📙 🖛 RegR	lipper	3.0-master					_	ð	×
File Home	Share	e View							~ 🕐
← → ~ ↑ 📘	C:\To	ools\RegRipper3.0-master\RegRipper3.0-mas	ter		~ Ō	Search RegRipper3.0-ma	aster	Q,	
	^	Name	Date modified	Туре	Size				
🖈 Quick access		plugins	01-07-2023 06:42	File folder					
E Desktop	*		21-03-2023 11:46	GITATTRIBUTES File	1 KB				
👆 Downloads 🗦	*	Base.pm	21-03-2023 11:46	PM File	27 KB				
Documents	*	File.pm	21-03-2023 11:46	PM File	9 KB				
Pictures	*	Key.pm	21-03-2023 11:46	PM File	14 KB				
Evidence		license.md	21-03-2023 11:46	MD File	2 KB				
Execution		license	21-03-2023 11:46	Text Document	2 KB				
plugins		p2x5124.dll	21-03-2023 11:46	Application extens	417 KB				
- Progins		🔊 q	21-03-2023 11:46	lcon	6 KB				
Registry		README.md	21-03-2023 11:46	MD File	2 KB				
💻 This PC		💿 regrip	21-03-2023 11:46	Windows Batch File	1 KB				
🧊 3D Objects		rip	21-03-2023 11:46	Application	1,857 KB				
Desktop		🧾 rip	21-03-2023 11:46	PL File	17 KB				
Documents		📳 rip_bulk	21-03-2023 11:46	Compressed (zipp	1,591 KB				
		o rr	21-03-2023 11:46	Application	2,492 KB				
Musia		гг	21-03-2023 11:46	PL File	16 KB				
Pictures									
Videos									
SDT_x64FREE_E	EN	G	o to this path and	open cmd.					
👸 CD Drive (D:) \	Vir		*	-					
🛖 Downloads (\\	VE								
a	\checkmark							_	
16 items									:== 🛌

H 🤶 🔚 🝅

ρ

 \Box



Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved.

C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe Rip v.3.0 - CLI RegRipper tool

Rip [-r Reg hive file] [-f profile] [-p plugin] [options] Parse Windows Registry files, using either a single module, or a profile.

NOTE: This tool does NOT automatically process Registry transaction logs! The tool does check to see if the hive is dirty, but does not automatically process the transaction logs. If you need to incorporate transaction logs, please consider using yarp + registryFlush.py, or rla.exe from Eric Zimmerman.

a [bive] Desistary bive file to serve
-r [nive]
-dCheck to see if the hive is dirty
-gGuess the hive file type
-aAutomatically run hive-specific plugins
-aTAutomatically run hive-specific TLN plugins
-f [profile]use the profile
-p [plugin]use the plugin
-llist all plugins
-cOutput plugin list in CSV format (use with -]
-s systemnamesystem name (TLN support)
-u usernameUser name (TLN support)
-uPUpdate default profiles
-hHelp (print this information)

015-

Ex: C:\>rip -r c:\case\system -f system C:\>rip -r c:\case\ntuser.dat -p userassist C:\>rip -r c:\case\ntuser.dat -a

net Downloads (\\VE

e

ρ

16 items



Ē

09:16

09-07-2023

^ 🏷 🕼

 \times

~ 🕐

 \times

```
Administrator: C:\Windows\System32\cmd.exe
```

-s systemname.....System name (TLN support) -u username.....User name (TLN support) -uPUpdate default profiles -h.....Help (print this information) Ex: C:\>rip -r c:\case\system -f system C:\>rip -r c:\case\ntuser.dat -p userassist C:\>rip -r c:\case\ntuser.dat -a C:\>rip -l -c All output goes to STDOUT; use redirection (ie, > or >>) to output to a file. copyright 2020 Quantum Analytics Research, LLC C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r C:\Cases\Analysis\Registry\SOFTWARE -p winver Launching winver v.20200525 winver v.20200525 (Software) Get Windows version & build info

ProductName	Windows 10 Enterprise Evaluation
ReleaseID	2009
BuildLab	19041.vb_release.191206-1406
BuildLabEx	19041.1.amd64fre.vb_release.191206-140
CompositionEditionID	EnterpriseEval
RegisteredOrganization	
RegisteredOwner	Denisha
InstallDate	2023-06-28 16:13:27Z
InstallTime	2023-06-28 16:13:27Z

C:\Tools\RegRipper3.0-master\RegRipper3.0-master>

目

Using plugins gathering more details Here using winver plugin show detail about windows version.





Г

 \times

^

```
Administrator: C:\Windows\System32\cmd.exe
```



Ъ

 \times



C:\Tools\RegRipper3.0-master\RegRipper3.0-master≻rip.exe -r C:\Cases\Analysis\Registry\SYSTEM -p networklist Launching networklist v.20200518 Launching networklist v.20200518 (Software) Collects network info from NetworkList key

Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles not found.

C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r C:\Cases\Analysis\Registry\SYSTEM -p shutdown Launching shutdown v.20200518 shutdown v.20200518 (System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value LastWrite time: 2023-06-29 09:08:05Z ShutdownTime : 2023-06-29 09:08:05Z Detail about last shutdown time of target system.

C:\Tools\RegRipper3.0-master\RegRipper3.0-master≻rip.exe -r C:\Cases\Analysis\Registry\SOFTWARE -P defender Launching defender v.20200427 defender v.20200427 (Software) Get Windows Defender settings

Key path: Microsoft\Windows Defender LastWrite Time 2023-06-29 09:07:52Z

Key path: Microsoft\Windows Defender\Exclusions\Paths

Key path: Microsoft\Windows Defender\Exclusions\Extensions

Key path: Microsoft\Windows Defender\Exclusions\Processes

Key path: Microsoft\Windows Defender\Exclusions\TemporaryPaths

Key path: Microsoft\Windows Defender\Exclusions\IpAddresses

Key path: Microsoft\Windows Defender\Features TamperProtection value = 1 If TamperProtection value = 1, it's disabled

Key path: Microsoft\Windows Defender\Real-Time Protection



Detail about Microsoft defender



Ъ

 \times

Parsing registry hives in bulk with RegRipper

1. Go to the Registry folder location > open cmd > dir > attrib * > attrib -h NTUSER>DAT > attrib -h UserClass.dat

2. For /r %i in (*) do (C:\Tools\RegRipper\rip.exe -r %i -a > %i.txt).

3. Show in Registry folder text file automatic created then after all file selected and edit with Notepad++ and show the all detail of target system.

이 것이 같은 것이 같은 것이 같은 것이 같은 것이 같은 것이 같이		
📊 🔁 📙 = Registry —	þ	\times
File Home Share View		~ 🕐
← → × ↑ → This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > Analysis > Registry v O Search Registry		2
Administrator: C:\Windows\System32\cmd.exe -		×
C:\Cases\Analysis\Registry>attrib -h NTUSER.DAT		^
C:\Cases\Analysis\Registry>attrib -h UsrClass.dat		
C:\Cases\Analysis\Registry>		
		~
14 items		
モーク 目: C III 😂 🔲 🔛 - ^ 空 🕫 09:39 クロ つの:39 09-07-2	9 2023	$\overline{}$

Administrator: C:\Windows\System32\cmd.exe

29-06-2023	09:08	524,288	DEFAULT	
29-06-2023	09:08	65,536	SAM	
29-06-2023	09:08	32,768	SECURITY	
29-06-2023	09:08	70,254,592	SOFTWARE	
29-06-2023	09:08	11,272,192	SYSTEM	
	5 File(s)	82,149,	,376 bytes	
	2 Dir(s)	22,986,297,	,344 bytes	fr

C:\Cases\Analysis\Registry>attrib *

A		C:\Cases\Analysis\Registry\DEFAULT
A	н	C:\Cases\Analysis\Registry\NTUSER.D4
A		C:\Cases\Analysis\Registry\SAM
A		C:\Cases\Analysis\Registry\SECURITY
A		C:\Cases\Analysis\Registry\SOFTWARE
Δ		C:\Cases\Analysis\Registry\SYSTEM

C:\Cases\Analysis\Registry>attrib -h NTUSER.DAT

C:\Cases\Analysis\Registry>for /r %i in (*) do (C:\Tools\RegRipper3.0-master\RegRipper3.0-master\rip.exe -r %i -a > %i.txt)

20

015-

C:\Cases\Analysis\Registry>(C:\Tools\RegRipper3.0-master\RegRipper3.0-master\rip.exe -r C:\Cases\Analysis\Registry\DEFAULT -a 1>C:\Cases\Analysis\Registry\DEFAULT.txt)

Launching adobe v.20200522 Launching allowedenum v.20200511 Launching appassoc v.20200515 Launching appcompatflags v.20200525 Launching appkeys v.20200517 Launching applets v.20200525 Launching apppaths v.20200511 Launching appspecific v.20200515 Launching appx v.20200427 Launching arpcache v.20200515 Launching attachmgr v.20200525 Launching cached v.20200525 Launching cmdproc v.20200515 Launching comdlg32 v.20200517 Launching compdesc v.20200511 Launching DDO v.20140414 Launching disablemru v.20190924 Launching environment v.20200512 Launching featureusage v.20200511 [*] Launching heidisql v.20201227 [*] Launching iconlayouts v.20211001 Launching identities v.20200525

Execute the command for create the text file of registry hives.

Ъ

 \times

📊 🛃 📊 🖛 Registry						_	ð	×
File Home Share	View							~ 🕐
\leftarrow \rightarrow \checkmark \uparrow \square \Rightarrow This	PC > SDT_x64FREE_EN-US_VHD (C:) >	4		~ Ō	Search Registry		Q	
^	Name	Date modified	Туре	Size				
🖈 Quick access		01 07 2022 10 55	T	15 KD				
📃 Desktop 🛛 🖈	UsrClass.dat	01-07-2023 10:55	Text Document	15 KB				
🖶 Downloads 🖈	UsrClass.dat	29-06-2023 09:07	DAT File	3,328 KB				
		01-07-2023 10:55	Text Document	373 KB				
		29-06-2023 09:08	File	11,008 KB				
Pictures 🖈	SOFTWARE	01-07-2023 10:55	Text Document	2,476 KB				
Evidence	SOFTWARE	29-06-2023 09:08	File	68,608 KB				
Execution		01-07-2023 10:55	Text Document	4 KB				
plugins	SECURITY	29-06-2023 09:08	File	32 KB				
Registry	SAM	01-07-2023 10:55	Text Document	8 KB				
	SAM	29-06-2023 09:08	File	64 KB				
💻 This PC	NTUSER.DAT	01-07-2023 11:02	Text Document	39 KB				
3D Objects	NTUSER.DAT	29-06-2023 09:07	DAT File	1,024 KB				
Desktop	DEFAULT	01-07-2023 10:55	Text Document	16 KB				
Documents	DEFAULT	29-06-2023 09:08	File	512 KB				
🖶 Downloads								
👌 Music								
Pictures					Show	the all text file	of	
📑 Videos					regist	try hives.		
SDT_x64FREE_EN								
🥳 CD Drive (D:) Vir								
🛖 Downloads (\\VI								
14 items							-	:

오 H 🤶 🗔 🗳

^ 문 4≥ 09:36 09-07-2023

	×
	~ 🕐
	o
ind	
•	
5 1	and

a. . . 14 items | 1 item selected 2.41 MB

Цi

e

ρ

(







User Accounts and SIDs Overview

🖾 Administrator: Command Prompt	_	ð	\times
Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved.			^
C:\Users\Administrator>net The syntax of this command is:			
NET [ACCOUNTS COMPUTER CONFIG CONTINUE FILE HELPMSG LOCALGROUP PAUSE SESSION SHARE STATISTICS STOP TIME USE USER VIEW]	GROUP HELP START		
C:\Users\Administrator>net accounts Force user logoff how long after time expires?: Minimum password age (days): Maximum password age (days): Minimum password length: Length of password history maintained: Lockout threshold: Lockout duration (minutes): Lockout observation window (minutes): Computer role: The command completed successfully.	Never 0 42 0 None Never 30 30 SERVER		
C:\Users\Administrator>net user User accounts for \\WIN-AJDB7GOIQEJ			
Administrator DefaultAccount Gue WDAGUtilityAccount The command completed successfully.	st		
C:\Users\Administrator>net localgroup Aliases for \\WIN-AJDB7GOIQEJ			
*Access Control Assistance Operators *Administrators *Backup Operators *Certificate Service DCOM Access *Cryptographic Operators			- -
🔳 🔎 🛱 🥭 🧮 🗠 📰	~ 〒 √ <mark>∞</mark> 05	:25 7-2023	

C:\Users\Administrator>net localgroup

Aliases for \\WIN-AJDB7GOIQEJ

*Access Control Assistance Operators *Administrators *Backup Operators *Certificate Service DCOM Access *Cryptographic Operators *Device Owners *Distributed COM Users *Event Log Readers *Guests *Hyper-V Administrators *IIS IUSRS *Network Configuration Operators *Performance Log Users *Performance Monitor Users *Power Users *Print Operators *RDS Endpoint Servers *RDS Management Servers *RDS Remote Access Servers *Remote Desktop Users *Remote Management Users *Replicator *Storage Replica Administrators *System Managed Accounts Group *Users The command completed successfully.

C:\Users\Administrator>whoami win-ajdb7goiqej\administrator

C:\Users\Administrator>whoami /user

USER INFORMATION

User Name

SID

Ъ

へ む 🕫

01-07-2023

 \times



🔤 Administrator: Command Prompt		—	þ	\times
*Users				
The command completed success	fully.			
C:\Users\Administrator>whoami win-ajdb7goiqej\admini strator				
C:\Users\Administrator>whoami	/user			
USER INFORMATION				
User Name	SID			
win-ajdb7goiqej\administrator	S-1-5-21-3369172402-319990300-3115234934-500			

C:\Users\Administrator>





 \sim

~

1

Analysis of user accounts, groups and profiles

All Hives load in Registry Explorer and open SAM hive and click the on the user folder.

4	Registry Explorer v1.6.0.0																						-	_	Ć	p	\times	
Fil	le Tools Option	ns Bookm	narks (0/0) Vi	iew Help																								
Re	Registry hives (5) Available bookmarks (73/0)							Va	alues	Us	er ad	coun	ts															
E	Enter text to search Find							Dra	ag a c	olumn	head	der he	ere to	o grou	ip by	that	colum	n	_		_						کر	C
	Key name																							••••			••••	····
ę	RBC															D		•				r						
	🕨 🦉 C:\Cases	\Analysis\A	Registry\DEF	AULT							′ [–]					en		d				- N	2					
	⊿ 🦉 C:\Cases	\Analysis\I	Registry\SAM	4			_									is ha		mi				rs Of	i n					
	Aliases	S																st										
►	Users	5																to				1						
	C:\Cases	(Analysis (I	Registry (SEC				_											rs				u st	2 i					
	C:\Cases	\Analysis \r	Registry\SOF	TWARF																		0						
	C: \Cases \Analysis \Registry \SOFT WARE																					s :[1					
<	< >																					}						
-										0	3					fa												
— B(ookmark Information	n	Cacec\Apalysic\	Peoistry\S/	M											ult												
	ive	0.10		ycegisu y pr	4-1 -											er												
Ca	ategory	Ope	erating system													0												
Na	ame	User	rs																									~
Ke	ey path	SAM	1\Domains\Acco	ount\Users				<																			>	
Sł	hort description	User	er accounts					Тс	otal re	ows: 6																Export	: ?	!
Lo	ong description	User	r accounts in SA	AM file					vpe vi	iewer																		
								Valu		me	Co.	ofault	F)															-
								Valu	ue typ	pe	Re	egDwo	ord															
	Key: SAM	1\Domains\A	Account\Users	s																Val	lue:	(d	efaul	t)	Colla	pse al	l hive	es
Se	lected hive: DEFA	ULT Last	t write: 28-0	06-2023 16	:32:29 +00:00	1 of 1 values s	hown (100.0	0%)															Hid	lden k	eys: 0	1	
	0	H: /	s	-																		H	-1	(05:48			
		דו 🤇																			\sim	Τ	Ч×	01-	07-20	23	1	

File Tools Options Bookmarks (0/0) View Help

R	egistry hives (5)	Available b	able bookmarks (73/0)						V	Values User accou																									
Enter text to search Find							Drag a column header here to group by that column														Q														
	Key name											9																							^
											0	4					D	0		Α					{"						-				
	C:\Cases	\Cases \Analysis \Registry \DEFAULT						_										e	en s		d					ve									
		(Analysis (Registr	y (SAPI							_										ł	na		ni					on						
Þ	Users	;									_													ra					: 1,						
	> 🍘 C:\Cases	\Analysis \	Regis										\checkmark	_	_	_	_			_	-	_	_	to		_			"q ue						
	C:\Cases	\Analysis\	Regis	Export	succ	cessfi	ul																		\times	(sti						
	🕨 🎁 C:\Cases	\Analysis\	Regis																										on s"						
-		_	_) va	alues (exporte	d to 'C	:\User	s\Adminis	trator\D	eskto	p\Us	er ad	cour	nts_V	/alue	s_E	xpor	t_20	230	7010	5483	1.xls	x'				;0						
<			_																										3						-
B	ookmark information	n																																	
н	live	C:\(Cases								ļ	OK																							
С	ategory	Ope	erating sy	/stem																	(D													
N	lame	Use	rs																																~
ĸ	ey path	SAM	1\Domain	s\Account	t\Use	rs						<																					_	>	
s	hort description	Use	r accoun	ts								Т	otal	row	s: 6																		Expo	rt	?
	ona description	Use	r accoun	ts in SAM	file																														
_													ype	view	er		C 10																		_
												Va	ilue n	name		(de	fault	:)																	
							Value type RegDword																												
	Key: SAM	l\Domains\/	Account	Users																						Va	alue	:	(def	ault))	Colla	pse a	all hi	ves
Se	elected hive: DEFA	ULT Last	t write:	28-06-	-2023	16:32	:29 +0	0:00	1 of	1 values	shown	(100.	.00%)																1	Hid	den l	eys:	0	1
F	0	=: 🧹	3																									म			0	5:48			
																												۲.		× (01-0)7-20	23	0)

– 🗆 🗡

🍡 📙	↓ Desk	top							Ð	×
File	Home	Share	e View							~ 🕐
$\leftarrow \rightarrow$.	~ 🛧 🗖	> Th	his PC > Desktop				~ Ō	Search Desktop		Q
		^	Name	Date modified	Туре	Size				
 ✓ Puick Desile Dov Dov Doc Pict Evid Evid Evid Evid Reg Reg V This F 3D (C) Doc SDT SDT 	k access ktop wnloads cuments tures dence cution gins gistry PC Objects ktop cuments wnloads usic tures eos [_x64FREE_	* * EN	 book Event Log Explorer User accounts_Values_Export_2023070105 Open this file in timeline explorer 	05-07-2023 05:18 28-06-2023 13:23 01-07-2023 05:48	Office Open XML Shortcut XLSX File	8 KB 2 KB 7 KB				
> 👳 Cor	wnloads (\	\VE								
3 items		~								
× *	р Ц	i	🨂 🚍 🖕					^ 탓 ੍∞ ₀9	10:04 -07-2023	\Box





Timeline Explorer v1.3.0.0

File Tools Tabs View Help











book



user accounts_V...





Loading file 'User accounts_Values_Export_20230701054831.xlsx'...



a,	Timeline Explorer v1.3.	0.0				- 0	×
ile	Tools Tabs V	iew Help					
lse	r accounts_Values_Exp	ort_20230701054831.xlsx					×
)r	ag a column b	neader here to grou	up by that column		Enter text to sear	dh	Find
	Created On	Last Login Time	Last Password Change	Last Incorrect Password	Expires On	User Name	
r	=	=	=	RBC	RBC	RBC	
•	2023-06-28					Administrator	`
	2023-06-28					Guest	
	2023-06-28					DefaultAccour	nt
	2023-06-28		2023-06-28 16:04:43			WDAGUtilityAd	count
	2023-06-28	2023-06-29 08:01				Denisha	
	2023-06-28	2023-06-28 16:18	2023-06-28 16:12:17			defaultuser0	

Show the detail about Target system user.

Þ

📙 🔄 📴 🖛 🗧 Registry						- 0	\times							
File Home Share	View						~ 🕐							
← → × ↑ 🔒 > This P	C > SDT_x64FREE_EN-US_VHD (C:) > Cases >	Analysis > Registr	У		~ ∂	Search Registry	Q							
🛄 Desktop 🛛 🖈 ^ 🛛	Name	Date modified	Туре	Size										
🕂 Downloads 🖈 Documents 🖈	DEFAULT	29-06-2023 09:08 30-06-2023 17:18	File Text Document	512 KB 16 KB										
Evidence	NTUSER.DAT NTUSER.DAT	29-06-2023 09:07 30-06-2023 17:18 29-06-2023 09:08	DAT File Text Document File	1,024 KB 39 KB 64 KB										
 plugins Registry RegRipper3.0-m This PC 3D Objects Desktop Documents Documents 	SA Open SEC Print SEC Edit SO Edit with Notepad++ SO SY: SY: Open with Restore previous versions	 6-2023 17:18 6-2023 09:08 6-2023 17:18 6-2023 17:18 6-2023 09:08 6-2023 17:19 6-2023 09:08 6-2023 17:19 	Text Document File Text Document File Text Document File Text Document	8 KB 32 KB 4 KB 68,608 KB 2,476 KB 11,008 KB 373 KB										
 Music Pictures Videos SDT_x64FREE_EN CD Drive (D:) Vir Downloads (\\VE Network 	Send to Cut Copy Create shortcut Delete Rename Properties	> SAM file notepad	e open with ++											
12 items 1 item selected 7.0	оэкв													
1	C:\Cas	es\Analysis\Registry\SAN	1.txt - Notepad++	[Administrato	r]						_	đ	×	
------	----------	--------------------------	-------------------	------------------	-----------	---------	--------------	-------------	-------------	-----------------	--------------------------	-----------------	-----	---
File	Edit	Search View Enco	ding Language	Settings To	ols Macro	Run P	Plugins Wind	low ?				+	•	×
	<u>-</u>	3 🖻 🗟 📭 📥 🖌	66 2	± # 🏂	R 🗟 🖉		5 N 🎩 🐺	I 💹 🌃 🖉) 🔚 👁 📘					
	all 🗵	💾 SYSTEM.txt 🛛 🔡	DEFAULT.txt 🗵	📑 NTUSER.DA	T.txt 🗵 🔚	SAM.txt	🗵 🔚 SECUR	ITY.txt 🗵 🖁	SOFTWARE.tx	t 🗵				
	1	samparse v.20220	921											~
	2	(SAM) Parse SAM	file for use	er & group	mbrshp :	info								
	3													
	4													
	5	User Information	L											
	6													
	7	Username	: Administra	ator [500]				_						
	8	SID	: S-1-5-21-3	3331464962	-2147846:	31-3394	1824829-50	0						
	9	Full Name	:											
	0	User Comment	: Built-in a	account to	r adminis	stering	g the comp	uter/doma	in					
	1	Account Type	· Wed Tup 20	16.12.16	2022 7									
	2	Name	. wea oun 20	5 10.15.10	2023 2									
1	4	Last Login Date	· · Never											
1	5	Pwd Reset Date	· Never											
1	6	Pwd Fail Date	· Never							01 1	4 . •4			
1	7	Login Count	: 0							Show the us	ser detail			
l î	8	> Password d	loes not exp	re						using Mator				
1	9	> Account Di	sabled							using Noter	pau++.			
2	0	> Normal use	r account											
2	1													
2	2	Username	: Guest [50]	1]										
2	3	SID	: S-1-5-21-3	- 3331464962	-2147846	31-3394	824829-50	1						
2	4	Full Name	:											
2	5	User Comment	: Built-in a	account fo	r guest a	access	to the co	mputer/do	main					
2	6	Account Type	:											
2	7	Account Created	: Wed Jun 20	3 16:13:16	2023 Z									
2	8	Name	:											
2	9	Last Login Date	: Never											
3	0	Pwd Reset Date	: Never											
3	1	Pwd Fail Date	: Never											~
Norr	mal tex	t file	ler	ngth : 7,269 lin	nes : 202		Ln:20 Co	1:26 Pos:5	83	Windows (CR LF)) UTF-8		INS	
		오 텔: 🧲	i	()	्र 🔛						∧ 투 4 ⁰ 01-0	6:01)7-2023		

RecentDocs Analysis

Information about the files that were recently opened/saved and the folders that were opened are maintained in the RecentDocs registry key.

Load the Ntuser.dat hive on Registry Explorer. And open Recent Doc.







```
👆 Downloads
```

👌 Music

Pictures



SDT_x64FREE_EN

🧃 CD Drive (D:) Vir

👳 Downloads (\\VE

6 items



 \sim



:==

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (29/0) View Help

Registry hives (1) Available bookmarks (29/0) Recent documents Values Q Drag a column header here to group by that column Enter text to search... Find Extension Value Name Target Name Lnk Name Mru Position Opened On Extension Las. Key name # valu A B C A 8 C A B C A B C ~ 9 =_ _ 9 8 B C $= \land$ invoke-atomicr 0 2023-06-28 2023-06-28 1 RecentDocs 8 invoke-atomicr PrinterPorts edteam edteam (2).Ink RecentDocs Invoke-Atomic RecentDocs 9 Invoke-Atomic 1 2023-06-28 1 ... RedTeam RedTeam.psm .par (3).Ink .ps1 RecentDocs 7 Invoke-Atomic Invoke-Atomic 2 2023-06-28 1 .psd1 RedTeam.psd1 RedTeam.lnk RecentDocs 3 .psm1 3 AtomicRedTea AtomicRedTea m.lnk m .zip RecentDocs 2 ART-attack.ps ART-attack.lnk 4 2023-06-28 1... Folder \sim 1 > < RecentDocs 6 Resources Resources.Ink 5 RecentDocs PracticalWindo PracticalWindo 6 5 2023-06-28 1... Bookmark information wsForensics-c wsForensics-c C:\Cases\Analysis\Registry\NTUSER.DAT Hive heat-sheet.pd heat-sheet.Ink User files and folders Category RecentDocs PWF-main.lnk 7 4 PWF-main.zip 2023-06-28 1 ... RecentDocs Name 8 RecentDocs 1 The Internet The Internet.lnk Software Microsoft Windows Current Version Explore Key path 1 1 1 1 1 1 Total rows: 19 Export ? Recently opened files by extension Short description ----See MRU key for order of opening Long description Type viewer 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 00 \sim 00000000 08 00 00 00 09 00 00 00 07 00 00 03 00 00 Data interpreter Current offset: 0 (0x0) Bytes selected: 0(0x0)? SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs Value: MRUListEx Collapse all hives Key: Selected hive: NTUSER.DAT Last write: 28-06-2023 17:58:22 +00:00 11 of 11 values shown (100.00%) Hidden keys: 0 1 10:19 Ω e Ξi ^ 뛰 ◁≈

o ×

Open Ntuser.dat file in Notepad++.

👔 C:\Cases'	s\Analysis\Registry\NTUSER.DAT.txt - Notepad++ [Administrator] —	đ	\times
File Edit	Search View Encoding Language Settings Tools Macro Run Plugins Window ?	+ '	• ×
e 🔁 🔁	🖻 🕞 🕼 🚔 🔏 🛍 Ə C # 🦕 🍳 🔍 🖬 🚘 三, 1 📑 🐼 🔟 🖓 💷 👁 • 🗉 🗈 🖻 🖻		
📑 all 🗵 📔	🚍 DEFAULT.txt 🗵 🔚 NTUSER.DAT.txt 🗵 📇 SECURITY.txt 🗵 🔚 SOFTWARE.txt 🗵 🔚 SAM.txt 🗵 🔚 UsrClass.dat.txt 🗵 🔚 SYSTEM.txt 🗵 🔚 NTUSER.DAT		
726 <mark>S</mark>	oftware\Microsoft\Windows\CurrentVersion\Search\RecentApps not found.		~
727 -			
728 r	ecentdocs v.20200427		
729 ()	NTUSER.DAT) Gets contents of user's RecentDocs key		
730			
731 R	lecentDocs		
732	All values printed in MKUList(MKUListEx order.		
733 30	artWrite Time: 2022-06-29 17.59.227		
735	$8 = invoke_stomicredtesm$		
736	9 = Invoke-AtomicRedTeam.psml		
737	7 = Invoke-AtomicRedTeam.psdl		
738	3 = AtomicRedTeam		
739	2 = ART-attack.psl		
740	6 = Resources		
741	5 = PracticalWindowsForensics-cheat-sheet.pdf		~
<			>
earch result	ts - (10 hits)		×
Search	"RecentDocs" (10 hits in 1 file of 1 searched)		~
C:\Ca	ases Analysis Degistry NTHSED DAT tot (10 bits)		
	ases (Analysis (Registry (MIOSER. DAT. CRC (10 MICs)		
Lin	ne 728: recentdocs v.20200427		
Lin Lin	ne 728: recentdocs v.20200427 ne 729: (NTUSER.DAT) Gets contents of user's RecentDocs key		
Lin Lin Lin	ne 728: recentdocs v.20200427 ne 729: (NTUSER.DAT) Gets contents of user's RecentDocs key ne 731: RecentDocs		
Lin Lin Lin Lin	ne 728: recentdocs v.20200427 ne 729: (NTUSER.DAT) Gets contents of user's <u>RecentDocs</u> key ne 731: <u>RecentDocs</u> ne 733: Software\Microsoft\Windows\CurrentVersion\Explorer\ <mark>RecentDocs</mark>		
Lin Lin Lin Lin Lin	ne 728: recentdocs v.20200427 ne 729: (NTUSER.DAT) Gets contents of user's RecentDocs key ne 731: RecentDocs ne 733: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs ne 746: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf		
Lin Lin Lin Lin Lin	<pre>ne 728: recentdocs v.20200427 ne 729: (NTUSER.DAT) Gets contents of user's RecentDocs key ne 731: RecentDocs ne 733: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs ne 746: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf ne 751: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl</pre>		
Lin Lin Lin Lin Lin Lin	<pre>ne 728: recentdocs v.20200427 ne 729: (NTUSER.DAT) Gets contents of user's RecentDocs key ne 731: RecentDocs ne 733: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs ne 746: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf ne 751: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl ne 756: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psdl</pre>		
Lin Lin Lin Lin Lin Lin	<pre>ne 728: recentdocs v.20200427 ne 729: (NTUSER.DAT) Gets contents of user's RecentDocs key ne 731: RecentDocs ne 733: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf ne 751: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl ne 756: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl ne 761: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl </pre>		
Lin Lin Lin Lin Lin Lin Lin	<pre>ne 728: recentdocs v.20200427 ne 729: (NTUSER.DAT) Gets contents of user's RecentDocs key ne 731: RecentDocs ne 733: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs ne 746: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf ne 751: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl ne 756: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psdl ne 761: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psml ne 766: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psml ne 766: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psml</pre>		
Lin Lin Lin Lin Lin Lin Lin Lin	<pre>ne 728: recentdocs v.20200427 ne 729: (NTUSER.DAT) Gets contents of user's RecentDocs key ne 731: RecentDocs ne 733: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs ne 746: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf ne 751: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl ne 756: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl ne 761: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl ne 766: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psml ne 766: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.zip ne 771: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder</pre>		~
Lin Lin Lin Lin Lin Lin Lin Lin Lin	<pre>ne 728: recentdocs v.20200427 ne 729: (NTUSER.DAT) Gets contents of user's RecentDocs key ne 731: RecentDocs ne 733: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf ne 746: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf ne 751: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl ne 756: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl ne 761: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl ne 766: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl ne 766: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpsl ne 766: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.zip ne 771: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder file length:39,529 lines:1,000 ln:728 Col:11 Sel:10 1 Windows(CRLF) ANSI</pre>	11	~ VS

ShellBags Analysis

Analysis of shellbags is useful as it can aid in the creating a broader picture of an investigation, providing indications of activity, acting as a history of what directory items may have since been removed from a system, or even evidence access of removable devices where are no longer attached. And also store Malicious Activity.

Usrclass.txt file edit with Notepad++.

📔 C:\	Case	s\Analysis\Regist	ry\UsrClass.	dat.txt -	- Notepad++	Adminis	trator]						—	o ;	×
File	Edit	Search View	Encoding	Langu	uage Setting	s Tools	Macro	Run Plugins	Window ?					+ 🔻	×
		🗈 🖻 🖻 🖉	b 🖈 🖻			b		F2 5 1	TE 🖂 🕅 TR		📾 👁 🗖 🔳				
						63 V	• -								
🔚 all	×	DEFAULT.txt	🗵 💾 NTU	SER.DA	T.txt 🗵 🔚 🤅	ECURITY	.bd 🗵 📙	SOFTWARE.txt	🛛 🔛 SAM.txt	t 🗵	😸 UsrClass.dat.txt	🔀 🔚 SYSTEM.txt 🗵			
127				1						- 1 -					^
128				- E			I			1.1		My Games [Deskto	[/0/qc		
129				- I.						1		My Computer [Des	sktop\1\]		
130				- E			I			1		My Computer\D:\	[Desktop\1]	(0)]	
131				- I						1		My Computer\Z:\	[Desktop\1]	(1)]	
132				- I						1		My Computer\CLS]	[D_Desktop	[Deskt(0]
133		2023-06-28	16:33:3	4	2023-06-2	8 16:3	33:32			1 9	99809/3	My Computer\CLS]	[D_Desktop\]	PWF-ma:	i:
134		2023-06-28	16:33:3	6	2023-06-2	8 16:3	33:32			1 9	99812/2	My Computer\CLS]	[D_Desktop\]	PWF-ma:	i:
135		2023-06-28	16:33:3	6	2023-06-2	8 16:3	33:36			1 9	99845/2	My Computer\CLS]	Desktop	PWF-ma:	i:
136		2023-06-28	16:33:3	6	2023-06-2	8 16:3	33:34			1 9	99830/3	My Computer\CLS]	Desktop	PWF-ma:	i:
137		2023-06-28	17:45:0	0	2023-06-2	8 17:4	15:00			1 9	99852/3	My Computer\CLS]	[D_Desktop\]	PWF-ma:	i:
138		2023-06-28	16:33:3	6	2023-06-2	8 15:2	27:16			1.1		My Computer\CLS]	Desktop	PWF-ma:	i:
139				- E			1	2023-04-2	7 13:32:14	1.1		My Computer\CLS]	[D_Desktop\]	PWF-ma:	i:
140				- E			1	2023-04-2	7 13:32:14	1.1		My Computer\CLS]	[D_Desktop\]	PWF-ma:	i:
141				- E			1			1.1		My Computer\C:\	[Desktop\1]	\3\]	
142		2023-06-28	17:56:4	6	2023-06-2	8 16:4	12:32			1 9	99671/3	My Computer\C:\/	AtomicRedTea	am [De:	s:
143		2023-06-28	17:57:0	4	2023-06-2	8 16:4	12:38			1 9	99737/4	My Computer\C:\/	AtomicRedTea	am\inv(o:
144	1	2023-06-28	17:57:0	4	2023-06-2	8 16:4	12:38			1 9	99868/3	My Computer\C:\/	AtomicRedTea	am\inv(o:
145		2023-06-28	17:57:0	4	2023-06-2	8 16:4	12:38			1 1	100972/4	My Computer\C:\/	AtomicRedTea	am\inv(o:
146		2023-06-28	17:57:1	6	2023-06-2	8 17:5	57:08			1 1	104667/10	My Computer\C:\A	AtomicRedTea	am\ator	m:
147	1	2023-06-29	08:01:1	8	2019-12-0	7 09:1	4:54			1.6	50/1	My Computer\C:\H	Program File	es [De:	s:
148		2023-06-29	08:09:5	6	2023-06-2	8 16:3	30:32			1 1	102703/2	My Computer\C:\H	Program File	es\Ora	c:
149		2023-06-29	08:09:5	0	2023-06-2	8 16:3	30:32			j 1	102704/2	My Computer\C:\H	Program File	es\Ora	c:
150		2023-06-29	08:01:1	8	2019-12-0	7 09:1	14:54			1 1	1223/1	My Computer\C:\H	Program File	es (x8)	6
151		2023-06-28	16:33:2	2	2023-06-2	8 15:2	27:16			i i		PWF-main.zip [20	510224] [De:	sktop\;	2
152				i i			i i	2023-04-2	7 13:32:14	- i -		PWF-main.zip\PWH	-main [Des]	ktop(2)	χi –
153				i i			i i	2023-04-2	7 13:32:14	i i		PWF-main.zip\PWH	-main\Insta	all-Sy:	sı
154		2023-06-28	16:33:3	2	2023-06-2	8 16:3	33:32			i s	99809/3	PWF-main [Deskto	[/8/qa	-	
155		2023-06-28	17:39:2	2	2023-06-2	8 16:3	33:32			i s	99812/2	PWF-main\PWF-mai	in [Desktop]	\3\0\1	
156		2023-06-28	17:45:0	o i	2023-06-2	8 17:4	15:00 i			i s	99835/3	PWF-main\PWF-mai	in\Install-	Sysmon	
<				- :			-			1.1					×
1 -		<i>c</i> 1					4.65						175.0		
Norma	l text	file			length : 14,	338 line	s:163	Ln : `	Col:1 Pos:	1		Windows (CR LF)	J1F-8	INS	,
		р Цi	6		🍅 🔛							<u>へ</u> 『	고 ଏ <mark>ଛ</mark> 09-07-2	023]

Usrclass.txt file edit with Notepad++.

📔 C:	\Cases\Analysis\R	egistry\UsrClass.	dat.txt - Notepad++ [Admir	nistrator]			– 0 ×
File	Edit Search V	iew Encoding	Language Settings To	ols Macro Run Plugir	s Window ?		+ v ×
		🔉 👝 🛛 🧶 👘		💽 😪 TR. FR. 🚍 🦷			
all 🔚	🛛 🔀 🔚 DEFAULT	.txt 🛛 🔚 NTUS	SER.DAT.txt 🛛 🔚 SECURI	TY.txt 🛛 🔚 SYSTEM.txt	🗵 🔚 SOFTWARE.txt 🛛 🔚 SA	AM.txt 🗵 🔚 UsrClass.dat.txt 🛽	3
124	(USRCLAS:	S.DAT) Shell	/BagMRU traversal	in Win7+ USRCLASS	.DAT hives		^
125							
126	MRU Time		Modified	Accessed	Created	Zip_Sub	folder MFT
127							
128						I	
129	2023-06-2	29 08:12:06					
130							
132							
133	2023-06-	28 16:50:50	12023-06-28 16:33	3.32 2023-06-28	16:33:34 2023-06-2	28 16:33:32	9980
134	2023-06-2	28 16:33:44	12023-06-28 16:33	3:36 2023-06-28	16:33:36 2023-06-2	8 16:33:32	9981
135			12023-06-28 16:33	3:36 2023-06-28	16:33:36 2023-06-2	8 16:33:36	9984
136	2023-06-	28 17:56:18	2023-06-28 16:33	3:36 2023-06-28	16:33:36 2023-06-2	8 16:33:34	9983
137			2023-06-28 17:45	00 2023-06-28	17:45:00 2023-06-2	8 17:45:00	9985
138			2023-06-28 15:27	7:30 2023-06-28	16:33:36 2023-06-2	8 15:27:16	
139	2023-06-2	28 16:49:10		i i	i i	2023-04	-27 13:32:14
140	2023-06-2	28 16:49:53	1	1	1	2023-04	-27 13:32:14
141	2023-06-2	29 08:11:52	1	1	1	I. I.	1
142			2023-06-28 17:50	5:46 2023-06-28	17:56:46 2023-06-2	28 16:42:32	9967
143			2023-06-28 16:42	2:38 2023-06-28	17:57:04 2023-06-2	8 16:42:38	9973
144			2023-06-28 16:42	2:38 2023-06-28	17:57:04 2023-06-2	8 16:42:38	9986
145	2023-06-2	28 17:57:29	2023-06-28 16:42	2:38 2023-06-28	17:57:04 2023-06-2	8 16:42:38	1009
146	2023-06-2	28 18:06:27	2023-06-28 17:57	7:16 2023-06-28	17:57:16 2023-06-2	28 17:57:08	1046
147			2023-06-28 16:30	0:32 2023-06-29	08:01:18 2019-12-0	07 09:14:54	60/1
148	2023-06-2	29 08:11:56	2023-06-28 16:30	0:32 2023-06-29	08:09:56 2023-06-2	28 16:30:32	1027
149	2023-06-2	29 08:11:58	2023-06-28 16:30	0:54 2023-06-29	08:09:50 2023-06-2	28 16:30:32	1027
150	2023-06-2	29 08:12:06	2021-10-06 13:59	9:00 2023-06-29	08:01:18 2019-12-0	07 09:14:54	1223
151			2023-06-28 15:2	/:30 2023-06-28	16:33:22 2023-06-2	8 15:27:16	07.10.00.14
152	2023-06-2	28 16:48:32				2023-04	-27 13:32:14
153	2023-06-2	28 16:48:55	· · · · · · · · · · · · · · · · · · ·		<u></u>	2023-04	-27 13:32:14
<							>
Norm	al text file		length : 14,338 li	ines : 163 Ln	:1 Col:1 Pos:1	Windows (CR LF)	UTF-8 INS
	л Ц	6	- 🧉 🛸 -	😜 🔛		^	ि मि व <mark>⊗</mark> 11:03 11:03 कि 01-07-2023 कि

Open the ShellBagsExplorer



Insert the UsrClass.dat

💐 ShellBags Explorer v1.4	4.0.0					_				_	o ×	
📚 Select a registry hive to o	pen. Hold SHIFT to ignore a	dirty Registry hiv	es		\times							
← → × ↑ 📙 « Ar	nalysis > Registry	~ ē	Search Registry		Q						Q	,
Organize 🔻 New fold	er			-		ion	Created On	Modified On	Accessed On	First Interac	ted L	.a
This DC	Name		Date modifie	ed	Type ^	-	=	=	=	=		_
2D Objects	NTUSER.DAT		29-06-2023 0	9:07	DAT Fi							
	NTUSER.DAT		01-07-2023 1	1:02	Text D							
Desktop	SAM		29-06-2023 0	9:08	File							
Documents			01-07-2023 1	10:55	Text D							
👆 Downloads			29-06-2023 0	9:08	File							
👌 Music			01-07-2023 1	10:55	Text D							
Pictures	SOFTWARE		29-06-2023 0	9:08	File						3	
📕 Videos	SOFTWARE		01-07-2023 1	10:55	Text D						-	
SDT x64FREE EN	SYSTEM		29-06-2023 0	9:08	File							
CD Drive (D·) Vir	SYSTEM		01-07-2023 1	10:55	Text D						~	-
Develoade ().)/(UsrClass.dat		29-06-2023 0	9:07	DAT Fi							
Downloads (\\vt	UsrClass.dat		01-07-2023 1	0:55	Text Di 🧹							
鹶 Network 🛛 👻	<				>							
File n	ame: UsrClass.dat				~							
			Open	Can	cel							
NIA .									Times		Q =€ Q = i = i = i = i	1
NA									Time z	one: UTC	0 of 0 visible	-
📕 🔎 🛱 🥻	ê 🥅 🍅 i	🖐 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -							~ 臣	d⊗ 09-07-2	$\frac{2}{2023}$	

-	ShellBag	gs Explorer v1.4.0.0							—	o ×
File	e Tools	Help								
	Value		D	orag a column hea	der here	to group by that colur	mn			م
	4 🏠 🛄	Desktop		Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On
	4.2	My Computer	9	P RBC	No im	RBC	=	=	=	=
		Program Files (v86)		Home Folder	-	Root folder: GUID	1	1		
	u ا	Program Files		My Computer	Ť	Root folder: GUID		1		
		AtomicRedTeam		PWE-main.zin		File		2023-06-28 15:27:16	2023-06-28 15:27:30	2023-06-28 16:33:2
	• 🛱	Desktop		PWE-main		Directory		2023-06-28 16:33:32	2023-06-28 16:33:32	2023-06-28 16:33:3
	- E	Z:		P VVI HIGHT		Directory	2	2023-00-20 10.33.32	2023-00-20 10.33.32	2023-00-20 10.33.3
		D:								
	*	Home Folder								
	4 📄	PWF-main								
	Þ 🧰	PWF-main	<	1						>
	- 4 🖹	PWF-main.zip								
	> > ==	PWF-main		Summary Det	ails H	lex				
	Show the output			ShellBag ite	ms: 4					
'Us	rClass.dat	' Registry hive loaded in 2.3714 seconds!	4 shellbags lo	baded in 0.0092	seconds			Time zo	ne: UTC 4 of 4 row	/s visible (100.00%)
	۶) 🛱 🥭 🧮 🗉	-						^ 맏 ੍∞ ₀	11:13 9-07-2023

NTFS- File system Analysis

NT file system (NTFS), which is also sometimes called the New Technology File System, is a process that the Windows NT operating system uses for storing, organizing, and finding files on a hard disk efficiently

Hard Disk Structure



Simple hard drive logical parts

MFT(Master File Table) records

Master File Table (MFT) MFT or \$MFT can be considered one of the most important files in the NTFS file system. It keeps records of all files in a volume, the files' location in the directory, the physical location of the files in on the drive, and file metadata.

Analysis of MFT Records with MFTECmd

📊 🛃 📕 🖛 F						_	o ×
File Home Share View							~ 🕜
Pin to Quick Copy Paste Paste s	hortcut to v	Delete Rename	New item • 1 Easy access •	Properties	Select all	e	
Clipboard	Organ	nize	New	Open	Select		
← → × ↑ 📙 > This PC > S	DT_x64FREE_EN-US_VHD (C:)) → Cases → F →			~ Ū	Search F	م
🔜 Desktop 🛷 ^ Name	^	Date	modified Type	Size			
- Downloads 🖈 📃 er.	tand	20.06	2022.09.21 Eile fel	dor			
🗄 Documents 🖈 📃 Pro	nend pgramData	30-06	5-2023 08:30 File fol	der			
E Pictures 🖈 Use	ers	30-06	5-2023 08:30 File fol	der			
Cases Win	ndows	30-06	-2023 08:30 File fol	der			
Evidence SBG	oot	30-06	5-2023 08:31 File	8	КВ		
Execution SLo	ogFile	30-06	5-2023 08:31 File	65,536	KB		
Begistry SM	IFT	29-06	5-2023 05:02 File	1,14,432	КВ		
\$Se	acure_\$SDS	29-06	5-2023 05:02 File	2,007	KB		
💻 This PC							
3D Objects							
E. Desktop		You can s	show MFT file	in Cases folder.	This		
Documents		file is use	in MET Decor	de Analycie	-		
👆 Downloads		1110 15 450		us Allalysis.			
👌 Music							
Pictures							
Julieos							
SDT_x64FREE_EN							
8 items 1 item selected 111 MB							

^ 范 ☆

Ч

28-07-2023

e

0

ρ

📊 l 🛃 📊 🖘 l	Manage			- 6	×
File Home Share	View Application Tools				~ 🕐
Pin to Quick Copy Paste	Cut Copy path Paste shortcut Copy path	me New folder [™] New item ▼ [™] Easy access ▼	Properties	Select all Select none Invert selection	
Clipboard	Organize	New	Open	Select	
← → × ↑ 🔒 > This P	C > SDT_x64FREE_EN-US_VHD (C:) > Tools >	Get-ZimmermanTools		✓ Ö Search Get-ZimmermanTo	ols 🔎
Desktop 🖈 ^	Name	Date modified Type	Size		^
Downloads *	METExplorer	28-06-2023 13:41 File fold	ar		
Documents	BECmd	28-06-2023 13:41 File fold	ler		
	RegistryExplorer	28-06-2023 13:42 File fold	ler		- 18
Evidence	SDBExplorer	28-06-2023 13:42 File fold	ler		- 18
	ShellBagsExplorer	01-07-2023 10:36 File fold	ler		
Execution	SQLECmd	28-06-2023 13:43 File fold	ler	Open the	
NIFS	TimelineExplorer	01-07-2023 05:43 File fold	ler	MFTExplorer in	
Registry	XWFIM	28-06-2023 13:44 File fold	ler	cmd	
💻 This PC	🔜 !!!RemoteFileDetails	28-06-2023 13:44 CSV File	e 5	KB	
3D Objects	Carl AmcacheParser	21-05-2023 11:49 Applica	tion 4,661	KB	
Desktop	AppCompatCacheParser	07-03-2023 15:13 Applica	tion 4,523	KB	
Documents	m bstrings	20-05-2022 12:38 Applica	tion 3,997	KB	
	ChangeLog	28-06-2023 13:44 Text Do	cument 33	KB	
Music	Get-Zimmerman lools	18-05-2023 14:24 Windov	vs PowerS 24	KB	
		13-03-2023 17:00 Applica	tion 4,792	KB	
Pictures	METEC md	20-10-2022 13:37 Applica	tion 3,003	KB	
Videos	PECmd	28-01-2022 12:08 Applica	tion 3,885	KB	
SDT_x64FREE_EN	RBCmd	05-08-2022 13:05 Applica	tion 3.607	KB	
32 items 1 item selected 4.3	0 MB				
📲 오 🛱 🌔	i 🚍 ڬ			へ 🛐 🆫 🔩 05:54 へ 🛐 🆫 🕼 02-08-202	23 🖥

```
Administrator: C:\Windows\System32\cmd.exe
```

Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved.

C:\Tools\Get-ZimmermanTools>MFTECmd.exe Description: MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com) https://github.com/EricZimmerman/MFTECmd You can go in Get-ZimmermanTools path and open cmd and type this command for all helps Б

11:48

튀

 \times

~

```
Examples: MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out" --csvf MyOutputFile.csv
MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\jsonout"
MFTECmd.exe -f "C:\Temp\SomeMFT" --json "c:\temp\bout" --bdl c
MFTECmd.exe -f "C:\Temp\SomeMFT" --de 5-5
MFTECmd.exe -f "C:\temp\SomeJ" --csv c:\temp
MFTECmd.exe -f "c:\temp\SomeBoot"
MFTECmd.exe -f "c:\temp\SomeBoot"
MFTECmd.exe -f "c:\temp\SomeSecure_SDS" --csv c:\temp
MFTECmd.exe -f "c:\temp\SomeI30" --csv c:\temp
```

Usage:

MFTECmd [options]

Options:

-f <f></f>	File to process (\$MFT \$J \$Boot \$SDS \$I30). Required
-m <m></m>	\$MFT file to use when -f points to a \$J file (Use this to resolve parent path in \$J CSV output)
json <json></json>	Directory to save JSON formatted results to. This orcsv required unlessde orbody is specified
jsonf <jsonf></jsonf>	File name to save JSON formatted results to. When present, overrides default name
csv <csv></csv>	Directory to save CSV formatted results to. This orjson required unlessde orbody is specified
csvf <csvf></csvf>	File name to save CSV formatted results to. When present, overrides default name
body <body></body>	Directory to save bodyfile formatted results tobdl is also required when using this option
bodyf <bodyf></bodyf>	File name to save body formatted results to. When present, overrides default name
bdl <bdl></bdl>	Drive letter (C, D, etc.) to use with bodyfile. Only the drive letter itself should be provided
blf	When true, use LF vs CRLF for newlines [default: False]



Ē	Administrator: C:\Wi	ndows\System32\	cmd	.exe		
	CEV (CEV)	Directory	to	cave	CSV	formatted

csv <csv></csv>	Directory to save CSV formatted results to. This orjson required unlessde orbody is
couf (couf)	specified
CSVT (CSVT)	Pirestery to save CSV formatted results to when present, overrides default name
body < body >	File name to save body formatted negults to When present exempides default name
DOUYT (DOUYT)	Prive letter (C. D. etc.) to use with bedufile. Only the drive letter itself chould be provided
DUI (DUI)	When thus use IF we CBLE for neulines [default, Felce]
	When true, use LF VS CKLF for newlines [default: raise] Directory to cave experted (MET FILE record do is also required when using this ention
	Offect of the furt FILE record,do is also required when using this option
40 <40>	offsets
	See offsels Dump full details for fMFT ontru/converse # Format is 'Entru' on 'Entru' for' as desimal on how
de (de)	Dump full details for smill entry/sequence #. Format is Entry or Entry-seq as detimal or nex.
d 5	Example: 5, 024-5 OF 0X2/0-0X5.
ar	when true, dump pmri resident files to dir specified bycsv, in Resident Subdirectory. Files
£1.c	Will be named (EntryNumber>- <sequencenumber>_<filename>.Din</filename></sequencenumber>
+15	when true, displays contents of directory from smrl specified byde. Ignored whende points to a
	THE [detault: False] Dump full details for Security Id from #SDS as desiral on how Everplay 624 on 0v270
	Dump full details for Security 10 from \$505 as decimal or nex. Example: 624 or 6x2/6
at Kats	ontions [default: www.MM dd UU.mm.cs fffffff]
5P	The second
SII	Components condensed file listing of mansed \$MET contents. Requirescsv [default: Falce]
11	When thus include all timestamos from 0x20 attribute vs only when they differ from 0x10 in the \$MET.
at	Idefault. Falsal
25	[Uerault, raise] When thus, nacework clack share from FILE neconds when processing \$MET files. This ention has no
1'5	offect for \$120 files [default: False]
	Process all Valume Shadow Conjes that exist on drive specified by fildefaulty Falsal
vss dodupo	Deduplicate of & VSCs based on SHA 1. First file found wins [default: False]
dedupe	Show dobug information during processing [default: False]
debug	Show debug information during processing [default: False]
vension	Show version information
	Show help and usage information
-,, -n,neip	Show help and usage information

-f is required. Exiting

ρ

Show all option you can use in Analysis.

þ

_

 \times

~

 \sim

14:08

28-07-2023

^ 灯 🗤

C:\Tools\Get-ZimmermanTools>_

e

PIN_

Administrator: C:\Windows\System32\cmd.exe

```
C:\Tools\Get-ZimmermanTools>MFTECmd.exe -f c:\Cases\F\$MFT --de 0
MFTECmd version 1.2.2.1
```

Author: Eric Zimmerman (saericzimmerman@gmail.com) https://github.com/EricZimmerman/MFTECmd

```
Command line: -f c:\Cases\F\$MFT --de 0
```

File type: Mft

Processed c:\Cases\F\\$MFT in 21.7731 seconds

c:\Cases\F\\$MFT: FILE records found: 1,12,778 (Free records: 1,394) File size: 111.8MB

Dumping details for file record with key 0000000-00000001

Entry-seq #: 0x0-0x1, Offset: 0x0, Flags: InUse, Log seq #: 0x1A155FD3, Base Record entry-seq: 0x0-0x0 Reference count: 0x1, FixUp Data Expected: 93-00, FixUp Data Actual: 00-00 | 00-00 (FixUp OK: True)

```
**** STANDARD INFO ****
Attribute #: 0x0, Size: 0x60, Content size: 0x48, Name size: 0x0, ContentOffset 0x18. Resident: True
Flags: Hidden, System, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x100, Quota charged: 0x
0, Update sequence #: 0x0
```

```
Created On:2023-06-2905:02:52.1527466Modified On:2023-06-2905:02:52.1527466Record Modified On:2023-06-2905:02:52.1527466Last Accessed On:2023-06-2905:02:52.1527466
```

**** FILE NAME ****

ρ

Attribute #: 0x3, Size: 0x68, Content size: 0x4A, Name size: 0x0, ContentOffset 0x18. Resident: True

File name: \$MFT Flags: Hidden, System, Name Type: DosWindows, Reparse Value: 0x0, Physical Size: 0x4000, Logical Size: 0x4000

Using this command gathering the information about this file.

Р

 \times



Administrator: C:\Windows\System32\cmd.exe

Last Accessed On: 2023-06-29 05:02:52.1527466

**** FILE NAME ****

Attribute #: 0x3, Size: 0x68, Content size: 0x4A, Name size: 0x0, ContentOffset 0x18. Resident: True

File name: \$MFT Flags: Hidden, System, Name Type: DosWindows, Reparse Value: 0x0, Physical Size: 0x4000, Logical Size: 0x4000 Parent Entry-seq #: 0x5-0x5

Created On:2023-06-2905:02:52.1527466Modified On:2023-06-2905:02:52.1527466Record Modified On:2023-06-2905:02:52.1527466Last Accessed On:2023-06-2905:02:52.1527466

**** DATA ****

Attribute #: 0x6, Size: 0x50, Content size: 0x0, Name size: 0x0, ContentOffset 0x0. Resident: False

Non-Resident Data

Starting Virtual Cluster #: 0x0, Ending Virtual Cluster #: 0x6FBF, Allocated Size: 0x6FC0000, Actual Size: 0x6FC0000, Initi alized Size: 0x6FC0000

DataRuns	Entries	(Cluster	offset	->	#	of	clusters))
0xC0000				->			0x67C0	
0x2886D0				->			0x800	

**** BITMAP ****

Attribute #: 0x5, Size: 0x48, Content size: 0x0, Name size: 0x0, ContentOffset 0x0. Resident: False

Non-Resident Data

Starting Virtual Cluster #: 0x0, Ending Virtual Cluster #: 0x4, Allocated Size: 0x5000, Actual Size: 0x4008, Initialized Si ze: 0x4008

DataRuns Entries (Cluster offset -> # of clusters) 0x7B048 -> 0x5

C:\Tools\Get-ZimmermanTools>_





 \times

 \sim

MFT parsing and in-depth analysis with MFTECmd

Administrator: C:\Windows\System32\cmd.exe

	•
ds <ds></ds>	Dump full details for Security Id from \$SDS as decimal or hex. Example: 624 or 0x270
dt <dt></dt>	The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for
	options [default: yyyy-MM-dd HH:mm:ss.fffffff]
sn	Include DOS file name types in \$MFT output [default: False]
fl	Generate condensed file listing of parsed \$MFT contents. Requirescsv [default: False]
at	When true, include all timestamps from 0x30 attribute vs only when they differ from 0x10 in the \$MFT
	[default: False]
rs	When true, recover slack space from FILE records when processing \$MFT files. This option has no
	effect for \$I30 files [default: False]
VSS	Process all Volume Shadow Copies that exist on drive specified by -f [default: False]
dedupe	Deduplicate -f & VSCs based on SHA-1. First file found wins [default: False]
debug	Show debug information during processing [default: False]
trace	Show trace information during processing [default: False]
version	Show version information
-?, -h,help	Show help and usage information

-f is required. Exiting

C:\Tools\Get-ZimmermanTools>MFTECmd.exe -f c:\Cases\F\\$MFT --csv c:\Cases\Analysis\NTFS --csvf MFT1.csv MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com) https://github.com/EricZimmerman/MFTECmd

```
Command line: -f c:\Cases\F\$MFT --csv c:\Cases\Analysis\NTFS --csvf MFT1.csv
```

File type: Mft

Processed c:\Cases\F\\$MFT in 11.7887 seconds

c:\Cases\F\\$MFT: FILE records found: 1,12,778 (Free records: 1,394) File size: 111.8MB CSV output will be saved to c:\Cases\Analysis\NTFS\MFT1.csv Using this command all MFT file entry store in one file (MFT.csv) and then after show the details open using timeline explorer.

_

Б

 \times













DOCX

book



NTFS

Share

01N-

View

Home

~

File

e

User accounts_V...

ρ

Ш

Windows Server 2019 Datacenter Evaluation Windows License valid for 149 days Build 17763.rs5_release.180914-1434

 \times

~ 🕐



Timeline Explorer v1.3.0.0

File Tools Tabs View Help

MFT1.csv

Dr	ag	g a col	lumn header here to group by that column		PWF-main >	K 👻 Find
	-	In U	Parent Path	File Name		Extensio
Ŧ			REC	ROC		R B C
	3	~	.\Users\Denisha\Desktop\ <mark>PWF-main</mark>	PWF-main		
	4	\checkmark	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main	Investigation-roadmap.pn	g	.png
	4	\checkmark	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main	License.md		.md
	4	\checkmark	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main	README.md	7 1	.md
	4	\checkmark	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main	AtomicRedTeam	You can show any	
	3	\checkmark	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main\Atomic	ART-attack-cleanup.ps1	nalicious activity and	.ps1
	3	\checkmark	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main\Atomic	ART-attack.ps1	show detail, Here we	.ps1
	3	\checkmark	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main\Atomic	PWF_Analysis-MITRE.png f	ind PWF-main script	.png
	3	\checkmark	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main\Atomic	PWF_Analysis-MITRE.svg	because this is run on	.svg
	4	~	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main	Install-Sysmon	arget system.	
	3	~	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main\Instal…	Install-Sysmon.ps1		.ps1
	4	~	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main	Resources		
	3	~	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main\Resour	Analysis-Notes-Template.	docx	.docx
	3	~	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main\Resour	PracticalWindowsForensic	s-cheat-sheet.pdf	.pdf
	3	~	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main\Resour	Analysis-Notes-Template.	docx	.docx
	3	\checkmark	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main\Resour	PracticalWindowsForensic	s-cheat-sheet.pdf	.pdf
	3	\checkmark	.\Users\Denisha\Desktop\ <mark>PWF-main</mark> \PWF-main\Resour	RegRipper-plugins.csv		.csv
•						Þ

_

 \times

►

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

MFT1.csv

4

Dr	ag a column	header here to group	by that column		PWF-main		× • Find
	File Size	Created0x10	Created0x30	Last Modified0x10	Last Modified0x30	Last Record	Change0x:
Ŧ	=	=	=	=	=	=	
	0	2023-06-28 17:44:57		2023-06-28 17:44	2023-06-28 17:44:57	2023-06-28 1	17:44:58
	77340	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:57	2023-06-28 1	17:44:57
	34523	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:57	2023-06-28 1	17:44:57
	8345	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:57	2023-06-28 1	17:44:57
	0	2023-06-28 17:44:57		2023-06-28 17:44	2023-06-28 17:44:57	2023-06-28 1	17:56:29
	2635	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:57	2023-06-28 1	17:44:57
	3360	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:57	2023-06-28 1	17:56:29
	234776	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:58	2023-06-28 1	17:44:58
	113692	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:58	2023-06-28 1	17:44:58
	0	2023-06-28 17:44:58		2023-06-28 17:44		2023-06-28 1	17:44:58
	2673	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:58	2023-06-28 1	17:44:58
	0	2023-06-28 17:44:58		2023-06-28 17:44	2023-06-28 17:44:58	2023-06-28 1	17:52:33
	19183	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:58	2023-06-28 1	17:44:58
	2979904	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:58	2023-06-28 1	17:52:33
	18374	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:58	2023-06-28 1	17:44:58
	22398	2023-04-27 08:02:14	2023-06-28 17:44	2023-04-27 08:02	2023-06-28 17:44:58	2023-06-28 1	17:44:58
	2610224	2023-06-28 17:44:42		2023-06-28 17:43	2023-06-28 17:44:42	2023-06-28 1	17:43:34

— 🗆

 \times

Þ

MACB Timestamps Analysis

M - Modify

A – Access

You can Analysis MFT file so all timestamps are show you like all modifying time ,Access time, creation time, last Access time are known as MACB.

C – Changed(last Access \$MFT)

B - (Birth) / Creation

Finding Evidence of deleted filed with USN Journal analysis

📊 🛃 🛃 🚽 🖌										- 0	\times
File Home	Share	View									~ 🕐
Pin to Quick Copy access Clip	Paste Raste	Cut Copy path Paste shortcut	Move to • Copy to • Org	Delete Rename	New folder New	w item ▼ y access ▼ F	Properties • Open	Select all Select non Invert select Select	e ction		
$\leftarrow \rightarrow \cdot \uparrow$	> This F	PC > SDT_x64FR	EE_EN-US_VHD (C:) > Cases > F	>			~ Ū	Search F		Q
Evidence	^	Name	^	Da	ate modified	Туре	Size				
Execution		SExtend		30	0-06-2023 08:31	File folder	r				
NTFS		ProgramData	а	30	0-06-2023 08:30	File folder	r				
Registry		Users		30)-06-2023 08:30	File folder	r				
💻 This PC		Windows		30	0-06-2023 08:30	File folder	r				
3D Objects		SBoot		30	0-06-2023 08:31	File	65 526 1	(B			
Desktop				20	-06-2023 08:31	File	1 1/ /22 1	(B			
Documents		Secure SSD	s	29	-06-2023 05:02	File	2.007	(B			
Downloads			-				_,				
h Music											
Pictures								T T • .1 •	C1 C		
Videos								Using thi	s file for		
	EN							journalin	lg part.		
	Vie										
Devente ede (0.)											
Pownloads (~										
8 items 1 item se	lected]== 📼
	4. 🧹		~					<u>^</u>	៤ ។	06:02	

02-08-202

📊 🛃 🛄 🛨			Manage	Get-ZimmermanTools					_	þ	>	~
File Home	Share	View	Application Tools								\sim	?
$\leftarrow \rightarrow \cdot \cdot \uparrow$	cmd						~ >		Search Get-Zimm	ermanTool	ls 🔎	
E Pictures	cmd Search for	r "cmd"										^
Evidence]					
Execution		EZViev	ver	28-06-2023 13:40	File folder							
NTFS		Hashe	r	28-06-2023 13:41	File folder							
Registry		iisGeo	locate	28-06-2023 13:44	File folder							
This PC		JumpL	istExplorer	28-06-2023 13:41	File folder							
2D Objects		METE	plorer	28-06-2023 13:41	File folder							
SD Objects		RECm	d 	28-06-2023 13:41	File folder							
Desktop		Regist	ryExplorer	28-06-2023 13:42	File folder							
Documents		SDBEx	plorer	28-06-2023 13:42	File folder							
👆 Downloads		ShellB	agsExplorer	01-07-2023 10:36	File folder		_		4			
👌 Music		SQLEC	imd	28-06-2023 13:43	File folder		Ν	Λ Γ"]	l'Fcmd ope	n		
Pictures		Timeli	neExplorer	01-07-2023 05:43	File folder							
Videos		XWFIN	1	28-06-2023 13:44	File folder							
	ENI 🧀	🛛 !!!Rem	oteFileDetails	28-06-2023 13:44	CSV File	5 KB						
		6 Amca	cheParser	21-05-2023 11:49	Application	4,661 KB						
🥳 CD Drive (D:) V		AppCo	ompatCacheParser	07-03-2023 15:13	Application	4,523 KB						
🕳 System Reserv	red 😭	h bstring	gs	20-05-2022 12:38	Application	3,997 KB						
🕳 Local Disk (F:)		Chang	jeLog	28-06-2023 13:44	Text Document	33 KB						
🕳 Local Disk (G:)		🔋 Get-Zi	mmermanTools	18-05-2023 14:24	Windows PowerS	24 KB						
🛖 Downloads (\\	VE 🕷	JLECm	d	13-03-2023 17:06	Application	4,792 KB						
_	15	LECm	d	04-03-2023 10:30	Application	5,063 KB						
💣 Network		MFTE	Cmd	20-10-2022 13:37	Application	4,409 KB						
	~	PECm	d	28-01-2022 12:08	Application	3,885 KB						~
32 items 1 item sel	lected 4.30	MB									┋══	
	6		e						^ 탓 ੍∞ ₀	12:27 9-07-2023	\Box	

Administrator: C:\Windows\System32\cmd.exe

e

-

(3)

0

ρ

<u>ju</u>

MFTECmd [options]

Options:	
-f <f></f>	File to process (\$MFT \$J \$Boot \$SDS \$I30). Required
-m <m></m>	\$MFT file to use when -f points to a \$J file (Use this to resolve parent path in \$J CSV output)
json <json≻< td=""><td>Directory to save JSON formatted results to. This orcsv required unlessde orbody is</td></json≻<>	Directory to save JSON formatted results to. This orcsv required unlessde orbody is
	specified
jsonf <jsonf></jsonf>	File name to save JSON formatted results to. When present, overrides default name
csv <csv></csv>	Directory to save CSV formatted results to. This orjson required unlessde orbody is
	specified
csvf <csvf></csvf>	File name to save CSV formatted results to. When present, overrides default name
body <body></body>	Directory to save bodyfile formatted results tobdl is also required when using this option
bodyf <bodyf></bodyf>	File name to save body formatted results to. When present, overrides default name
bdl <bdl></bdl>	Drive letter (C, D, etc.) to use with bodyfile. Only the drive letter itself should be provided
blf	When true, use LF vs CRLF for newlines [default: False]
dd <dd></dd>	Directory to save exported \$MFT FILE recorddo is also required when using this option
do <do></do>	Offset of the \$MFT FILE record to dump as decimal or hex. Ex: 5120 or 0x1400 Usede ordebug to
	see offsets
de <de></de>	Dump full details for \$MFT entry/sequence #. Format is 'Entry' or 'Entry-Seq' as decimal or hex.
	Example: 5, 624-5 or 0x270-0x5.
dr	When true, dump \$MFT resident files to dir specified bycsv, in 'Resident' subdirectory. Files
	will be named ' <entrynumber>-<sequencenumber>_<filename>.bin'</filename></sequencenumber></entrynumber>
fls	When true, displays contents of directory from \$MFT specified byde. Ignored whende points to a
	file [default: False]
ds <ds≻< td=""><td>Dump full details for Security Id from \$SDS as decimal or hex. Example: 624 or 0x270</td></ds≻<>	Dump full details for Security Id from \$SDS as decimal or hex. Example: 624 or 0x270
dt <dt></dt>	The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for
	options [default: yyyy-MM-dd HH:mm:ss.fffffff]
sn	Include DOS file name types in \$MFT output [default: False]
fl	Generate condensed file listing of parsed \$MFT contents. Requirescsv [default: False]
at	When true, include all timestamps from 0x30 attribute vs only when they differ from 0x10 in the \$MFT
	[default: False]
rs	When true, recover slack space from FILE records when processing \$MFT files. This option has no
	effect for \$I30 files [default: False]
vss	Process all Volume Shadow Copies that exist on drive specified by -f [default: False]
dedupe	Deduplicate -+ & VSCs based on SHA-1. First file found wins [default: False]
debug	Show debug information during processing [default: False]
trace	Show trace information during processing [default: False]

01**5**-



0 ×

 \mathbf{h}

 \mathbf{v}

 \Box

_

Administrator: C:\Windows\	\System32\cmd.exe	—	o ×					
dedupe Ded debug Sho trace Sho version Sho -?, -h,help Sho	duplicate -f & VSCs based on SHA-1. First file found wins [default: False] ow debug information during processing [default: False] ow trace information during processing [default: False] ow version information ow help and usage information							
-f is required. Exitin	ng							
C:\Tools\Get-Zimmerman MFTECmd version 1.2.2.	nTools>MFTECmd.exe -f C:\Cases\F\\$Extend\\$J -m C:\Cases\F\\$MFTcsv C:\Cases\ .1	\Analysis\NTFS1						
Author: Eric Zimmerman https://github.com/Eri	n (saericzimmerman@gmail.com) icZimmerman/MFTECmd							
Command line: -f C:\Cases\F\\$Extend\\$J -m C:\Cases\F\\$MFTcsv C:\Cases\Analysis\NTFS1 Using this command								
File type: UsnJournal	IOT	store the all journ	al					
Processed C:\Cases\F\\$	\$MFT in 8.5757 seconds							
C:\Cases\F\\$MFT: FILE Path to C:\Cases\Analy CSV output wil	<pre>records found: 1,12,778 (Free records: 1,394) File size: 111.8MB ysis\NTFS1 doesn't exist. Creating ll be saved to C:\Cases\Analysis\NTFS1\20230709123220_MFTECmd_\$MFT_Output.csv</pre>							
Processed C:\Cases\F\\$	\$Extend\\$J in 7.9542 seconds							
Usn entries found in C CSV output wil	C:\Cases\F\\$Extend\\$J: 2,43,185 ll be saved to C:\Cases\Analysis\NTFS1\20230709123240_MFTECmd_\$J_Output.csv							
C:\Tools\Get-Zimmermar	nTools>_							

오 H: 🥝 🚍 🍅 🔄 🔄 🕋

へ EP ↓ 12:33 09-07-2023 $\widehat{}$

~

 \Box

📊 🛛 🔁 📊 🗢 🗍 NTFS1						—	þ	\times
File Home Share	View							~ 🕐
\leftarrow \rightarrow \checkmark \uparrow \square \Rightarrow This	PC > SDT_x64FREE_EN-US_VHD (C:) > Cases >	Analysis > NTFS1			~ Ū	Search NTFS1		Q,
📰 Pictures 🛛 🖈 ^	Name	Date modified	Туре	Size				
Evidence	00230709123220_MFTECmd_\$MFT_Output	09-07-2023 12:32	CSV File	58,903 KB				
Execution	20230709123240_MFTECmd_\$J_Output	09-07-2023 12:32	CSV File	50,449 KB				
NTFS								
Registry								
💻 This PC								
3D Objects								
E Desktop								
Documents								
👆 Downloads		. 1 1 .	1 .1 . 0		1.1	C 1		
b Music	Show the Two file auto cre	ated and gat	her the 1nf	ormation de	leted	file.		
Pictures								
Videos								
SDT_x64FREE_EN								
🥳 CD Drive (D:) Vir								
System Reserved								
Local Disk (F:)								
Local Disk (G:)								
🛖 Downloads (\\VI								
💣 Network								
~								
2 items 1 item selected 49	0.2 MB							
🖶 🤉 🗄	🗧 🧉 🔄 💽 🚑	CO				^ 怇 ੍ <mark>ଛ</mark> 09-0	2:37	\Box

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

20230709123240_MFTECmd_\$J_Output.csv

Dr	ag a	a column header here to g	roup by that column		Enter text to search	Find	
	r	Parent Sequence Number	Update Sequence Number	Update Reasons		File	
Ŧ			=	RBC		RBC	4
	761	1	22959408	HardLinkChange Close		Arcł	
	761	1	22959536	HardLinkChange Close		Arcł	
	761	1	22959664	HardLinkChange Close		Arcł	
	761	1	22959792	HardLinkChange Close		Arcł	
	761	1	22959920	HardLinkChange Close		Arcł	
	761	1	22960048	FileDelete Close		Arcł	
	761	1	22960176	FileDelete Close		Arcł	
	761	1	22960304	FileDelete Close		Arcł	
	761	1	22960432	FileDelete Close		Arcł	
	761	1	22960560	FileDelete Close		Arcł	
	761	1	22960688	HardLinkChange Close		Arcł	
	761	1	22960824	FileDelete Close		Arcł	
	761	1	22961000	FileDelete Close		Arcł	
	761	1	22961168	HardLinkChange Close		Arcł	_
	761	1	22961304	FileDelete Close		Arcł	
	761	1	22961480	FileDelete Close		Arcł	
4	761	1	22961648	HardLinkChangelClose		Arct	-

-0

101**%**____

C:\Cases\Analysis\NTFS1\20230709123240_MFTECmd_\$J_Output.csv

(2)

e

ρ

Ξī

Total lines 2,43,185 Visible lines 2,43,185 Open files: 1 🖽 Search options



 \times

へ 貯 4<mark>∞</mark> 12:40 09-07-2023

 \Box

Evidence of Execution

1. BAM (Background Activity Moderator)

📙 🛃 📴 = 🛛 Registry		Registry Explorer v1.6.0.0					
File Home Share	View	File Tools Options Bookmarks (0/0) View I	Help				
\leftarrow \rightarrow \checkmark \uparrow \square \Rightarrow This	s PC > SDT_x64FREE_EN-US_	Registry hives (0) Available bookmarks (0/0)		Values			
📰 Pictures 🛛 🖈 🐴	Name	Enter text to search	Find	Drag a column header here to group by that column			
Evidence	UsrClass.dat			Value Name			
Execution	UsrClass.dat	e and a subset of the subset o	imestamp	9 REC			
NTFS	SYSTEM						
Registry	SYSTEM						
💻 This PC	SOFTWARE						
3D Objects							
Desktop	SECURITY						
Documents	SAM						
Downloads	SAM	I and the system hive					
Music	NTUSER.DAT	Load the system mye		 Please Wait 			
Pictures	NTUSER.DAT	in Registry Explorer		Loading			
Videos		8 5 1					
SDT_x64FREE_EN							
🥸 CD Drive (D:) Vir							
System Reserved							
Local Disk (F:)							
Local Disk (G:)				Type viewer			
🛖 Downloads (\\VI							
💣 Network							
~							
14 items 1 item selected	10.7 MB						
🛨 🔎 🛱 🥢	😂 🥅 🍅 🖉			^ 탄 4 [×] 09-07-2022			

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (29/0) View Help

R	egistry hives (1) Available bookmarks (29/0)				/alues	BamDam	
[Enter text to search Fin	d		Dr	rag a colum	nn header here to group by that column	
_					Program	Execution Time	
	Key name	# v	alu	9	RBC	=	
9	RBC ▶ 🔚 {4d36e972-e325-11ce-bfc1-08002be10318}	=	^		Microsof	t.Windows.ShellExperienceHost_cw5n1h2txyew 2023-06-28 18:13:5	52
	[53f56307-b6bf-11d0-94f2-00a0c91efb8b]				Microsof	tWindows.Client.CBS_cw5n1h2txyewy 2023-06-28 18:13:	50
	 {6bdd1fc6-810f-11d0-bec7-08002be2092f} AppCompatCache 				\Device\ nFrameH	HarddiskVolume2\Windows\System32\Applicatio 2023-06-29 09:07:4 Host.exe	46
	bam				windows	.immersivecontrolpanel_cw5n1h2txyewy 2023-06-28 18:13:5	50
	⊿ 🔂 State				Microsof	t.Windows.SecHealthUI_cw5n1h2txyewy 2023-06-28 16:47:	51
	UserSettings				Microsof	t.XboxGamingOverlay_8wekyb3d8bbwe 2023-06-28 16:32:4	42
	5-1-5-18		\sim		\Device\	HarddiskVolume2\Windows\System32\cmd.exe 2023-06-28 16:32:4	49
<		>	_	:	\Device \ owerShe	HarddiskVolume2\Windows\System32\WindowsP 2023-06-29 08:05:0 ell\v1.0\powershell.exe	08
- B	ookmark information				Microsof	t.MicrosoftOfficeHub_8wekyb3d8bbwe 2023-06-29 09:07:4	46
Н	ive		_		Microsof	t.WindowsStore_8wekyb3d8bbwe 2023-06-29 08:13:0)7
С	ategory				\Device\ xe	HarddiskVolume2\Windows\System32\notepad.e 2023-06-28 17:58:2	27
N	ame		_		\Device\ exe	HarddiskVolume2\Windows\System32\VBoxTray. 2023-06-29 09:07:4	43
K	ey path			H	otal rows	. 17	_
S	hort description		_	_	otarrows.	• • • • • • • • • • • • • • • • • • • •	_
L	ong description			T	ype viewe	21	
				Va	lue name	Version	
				Va	lue type	RegDword	
	Key: ControlSet001\Services\bam\State\UserSettings\S-1-5	-21-3	3331	4649	962-21478	4631-3394824829-1001	/a
Se	elected hive: SYSTEM Last write: 29-06-2023 09:07:46 + 00:00	19	of	19 va	lues show	vn (100.00%)	
	= 🔎 H; 🧲 🔚 🍅 🔤 🦉						

....

ρ Execution Time ~ _ /ew 2023-06-28 18:13:52 2023-06-28 18:13:50 atio 2023-06-29 09:07:46 2023-06-28 18:13:50 2023-06-28 16:47:51 2023-06-28 16:32:42 2023-06-28 16:32:49 œ wsP 2023-06-29 08:05:08 2023-06-29 09:07:46 2023-06-29 08:13:07 ad.e 2023-06-28 17:58:27

Value:

þ

 \times

5

?

Export

Version Collapse all hives

13:08

ヘ 厈 ↓☆ 09-07-2023

Hidden keys: 0 1

Ļ

📕 🗹 📑 🗸 🗧 Registry								_	đ	×
File Home Share			Analusia	Desist				Canada Daniata (~ •
Pictures * ^	Name	~	Date mo	dified	Туре	Size	~ 0	Search Registry		Q
Evidence	UsrClass.dat		01-07-20	23 10:55	Text Document	15 KB				
NTFS	SYSTEM		29-06-20	23 09:07 23 10:55	DAT File Text Document	3,328 KB 373 KB				
Registry		Open Print		13 09:08	File Text Document	11,008 KB				
This PC		Edit		3 09:08	File	68,608 KB				
Desktop	SECURIT 📓	Edit with Notepad++ Share		23 10:55 23 09:08	Text Document File	4 KB 32 KB				
Documents		Open with	>	23 10:55	Text Document	8 KB				
Downloads Music		Send to	>	3 11:02	Text Document	39 KB				
Pictures		Cut		23 09:07 23 10:55	DAT File Text Document	1,024 KB 16 KB				
Videos SDT_x64FREE_EN	DEFAUL1	Сору		3 09:08	File	512 KB				
🧐 CD Drive (D:) Vir		Delete								
System Reserved Local Disk (F:)		Rename			System.txt f	ile edit with				
Local Disk (G:)		Properties			Notepad++	•				
Downloads (\\VE										
Network										
14 items 1 item selected 3	372 KB									
📲 오 🛱 🕻	🗧 🥅 🛀							^ 탓 ੍ <mark>≈</mark> 09-07	:09 7-2023	\Box

🔐 C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad++ [Administrator] — 🛛 🗇	×
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ? +	• ×
Compared to the second secon	
🔚 all 🗵 🔚 DEFAULT.txt 🗷 🔚 NTUSER.DAT.txt 🗷 📇 SECURITY.txt 🗷 📇 SOFTWARE.txt 🗵 📇 SAM.txt 🗵 🔚 UsrClass.dat.txt 🗵 🔚 SYSTEM.txt 🗵	
424 Pending Rename Operations2 : CurrentControlSet\Control\Session Manager\PendingFileRenameOperations2	~
425	
426 bam v.20200427	
427 (System) Parse files from System hive BAM Services	
428	
$\frac{429}{2000} = \frac{5-1}{2000} = \frac{1}{2000} =$	
430 2023-06-28 16:23:052 - \Device\HarddiskVolume2\Windows\System32\oobe\FirstLogonAnim.exe 431	
432 S-1-5-21-3331464962-214784631-3394824829-1000	
433 2023-06-28 16:20:23Z - \Device\HarddiskVolume2\Windows\explorer.exe	
434 2023-06-28 16:20:23Z - Microsoft.Windows.CloudExperienceHost cw5nlh2txyewy	
435 2023-06-28 16:20:22Z - MicrosoftWindows.Client.CBS cw5nlh2txyewy	
436	
437 S-1-5-21-3331464962-214784631-3394824829-1001	
438 2023-06-29 09:07:45Z - \Device\HarddiskVolume2\Windows\explorer.exe	
439 2023-06-29 09:07:46Z - Microsoft.Windows.StartMenuExperienceHost cw5nlh2txyewy	
440 2023-06-29 09:07:46Z - Microsoft.Windows.Search_cw5nlh2txyewy	
441 2023-06-28 18:13:52Z - Microsoft.Windows.ShellExperienceHost cw5nlh2txyewy	\sim
	>
Search results - (12 hits)	×
Search "bam" (12 hits in 1 file of 1 searched)	^
C:\Cases\Analysis\Registry\SYSTEM.txt (12 hits)	
Line 426: bam v.20200427	
Line 427: (System) Parse files from System hive BAM Services	
Line 1408: Name = bam	
Line 1409: Display = @%SystemRoot%\system32\drivers\ <mark>bam</mark> .sys,-100	
Line 1410: ImagePath = system32\drivers\ <mark>bam</mark> .sys	
Line 5970: 2023-06-29 08:01:14Z,BasicDisplay,,\SystemRoot\System32\DriverStore\FileRepository\basicdisplay.inf_amd64_	65a
Line 6000: 2023-06-29 08:00:59Z, BasicRender, , \SystemRoot\System32\DriverStore\FileRepository\basicrender.inf_amd64_df	49c
Line 6050: 2023-06-28 16:04:29Z, bam, @%SystemRoot%\system32\drivers\bam.sys;-100,system32\drivers\bam.sys,Kernel drive	r, 5 Y
	>
Normal text file length : 3,81,631 lines : 7,241 Ln : 427 Col : 1 Sel : 16 1 Windows (CR LF) UTF-8 II	NS
$\blacksquare \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	\Box

2. AppCompactcache Analysis/Shimcache

The shimcache is a Windows registry entry that records metadata about executed applications, including timestamps and filenames.

_ 🛃 _ ╤			I	Manage		Get-Zimn	nerman	Tools							- 0		×
File Home	Share	View	Appli	ication Too	ols												2
Pin to Quick Copy P access	aste	C ut C opy path Paste shor	tcut	Move to •	Copy to T	Delete R	ename	New folder	The New F Easy	v item ▼ v access ▼	Properties	📧 Open 👻	Select	all none selection	n		
Clipt	board	rd Or					nize New				0	Sel	ect				
\leftarrow \rightarrow \checkmark \uparrow	> This PC	C⇒ SDT	x64FRE	E_EN-US_	VHD (C:) > Too	ls ≽ G	et-Zimm	ermanTo	ols			~ (Se و	arch Get-ZimmermanTo	ols ,	Q
Evidence	^ N	lame		^			Da	ate modif	ied	Type		Size					^
Execution		MFTExplorer				28-06-2023 13:41			13:41	File folder							
NTES		RECmd				28-06-2023 13:41 File fo				File fold	er						
Basistar		RegistryExplore					28	-06-2023	13:42	3:42 File folder							
Registry		SDBEx	SDBExplorer				28	28-06-2023 13:42 File			er						
💻 This PC		ShellB	agsExpl	orer			01	-07-2023	10:36	File fold	ler						
🗊 3D Objects		SQLEC	md				28	-06-2023	13:43	File fold	er			.	.1 • 1 .•		
Desktop		Timeli	neExplo	orer			01	-07-2023	23 05:43 File	File fold	er			US11	ng this location		
Documents		NWFIM SWFIM AmcacheParser					28	-06-2023	13:44	File fold	er			oper	n this file in cm	d.	
Downloads							28	-06-2023	5-2023 13:44 CSV F 5-2023 11:49 Appli			5	KB				
- Downloads	- L - A						21	-05-2023			tion	4,661	KB				
J Music	C	AppCompatCacheParser					07	-03-2023	15:13	Application		4,523	KB	5			
Pictures		bstring	gs				-05-2022	12:38	Application		3,997	KB					
📑 Videos		Chang	jeLog				28-06-2023 13:44			Text Do	Text Document 3		KB				
SDT_x64FREE_E	EN	📓 Get-Zi	mmern	nanTools			18	-05-2023	14:24	Windov	vs PowerS	24	KB				
🔞 CD Drive (D:) V	/in	📕 JLECm	nd				13	-03-2023	17:06	Applica	tion	4,792	KB				
		I LECmd					04-03-2023 10:30			Applica	Application 5,063 KB						
_	Ē	MFTE	Cmd				20	-10-2022	13:37	Applica	tion	4,409	KB				
💣 Network	0	PECm	d				28	-01-2022	12:08	Applica	tion	3,885	KB				
	~	🔄 RBCm	d				05	-08-2022	13:05	Applica	tion	3,607	KB				~
32 items 1 item sel	ected 4.41	MB		• •				06 0000	44.00	a 11		2 202	100				=

🛋 🔎 🛱 🥭 🧮 ڬ

^ 〒 ↓ 02-08-2023 **₹**
Go to the Appcompatcacheparser.exe in cmd

0						
Recycle	Administrator: C:\Windows\Syst	m32\cmd.exe			- 🗆	\times
	Nicrosoft Windows [Versio (c) 2018 Microsoft Corpor	n 10.0.17763.737] ation. All rights reserved.				^
Firef	:\Tools\Get-ZimmermanToo Option 'csv' is require	ls>AppCompatCacheParser.exe				
	Description: AppCompatCache Parser v	ersion 1.5.0.0				
Event	Author: Eric Zimmerman https://github.com/Eric	(saericzimmerman@gmail.com) Zimmerman/AppCompatCacheParse	n			
Explo	Examples: AppCompatCach AppCompatCach	eParser.execsv c:\temp -t eParser.execsv c:\tempc	-c 2 svf results.csv			
	Short options	(single letter) are prefixed	with a single dash. Long comma	nds are prefixed with	two dashe	25
Notepa L	Jsage: AppCompatCacheParser [o	otions]				
Doc	<pre>ptions: -f <f></f></pre>	Full path to SYSTEM hive to p	process. If this option is not	specified, the live Re	gistry wi	i11
DOC	csv <csv> (REQUIRED) csvf <csvf> c <c></c></csvf></csv>	Directory to save CSV format File name to save CSV format The ControlSet to parse. Defi	ted results to. Be sure to incl ted results to. When present, c ault is to extract all control	ude the full path in d overrides default name sets [default: -1]	ouble quo	otes
lice	-t dt <dt></dt>	Sorts last modified timestam The custom date/time format	os in descending order [default to use when displaying time sta	:: False] mps. See https://goo.g	1/CNVqØk	for v
accounts	5_V			Windows Server 2019 Windows Lic Build 17763.r	Datacenter E ense valid for s5_release.18(valuation r 173 days 0914-1434
	📄 🤔 🗄 م	🝅 🗵 🧐 📝 📼		へ 貯 4≥	06:07 05-07-2023	\Box

Create the folder Execution in Analysis and run this command and store the output in Execution folder.



e

-

Шi

ρ

A-

3)

ecycl Administrator: C:\Windows\System32\cmd.exe —													
"	c <c> -t dt <dt></dt></c>	The ControlSet to parse. Default is to extract all control sets [default: -1] Sorts last modified timestamps in descending order [default: False] The custom date/time format to use when displaying time stamps. See https://goo.	gl/CNVq0k	(for									
Fire	nl debug trace version	options [default: yyyy-MM-dd HH:mm:ss] When true, ignore transaction log files for dirty hives [default: False] Show debug information during processing [default: False] Show trace information during processing [default: False] Show version information											
2	-?, -h,help	Show help and usage information											
Event Expl													
	C:\Tools\Get-ZimmermanToo	ls>AppCompatCacheParser.exe -f C:\Cases\Analysis\Registry\SYSTEMcsv C:\Cases\A	nalysis\E	Execut									
-00	ion AppCompatCache Parser ver	sion 1.5.0.0											
otep	¿Author: Eric Zimmerman (s https://github.com/EricZi	aericzimmerman@gmail.com) .mmerman/AppCompatCacheParser											
	Command line: -f C:\Cases	\Analysis\Registry\SYSTEMcsv C:\Cases\Analysis\Execution											
DO	Processing hive 'C:\Cases	\Analysis\Registry\SYSTEM'											
bo	Found 350 cache entries f	or Windows10C_11 in ControlSet001											
	Results saved to 'C:\Case	s\Analysis\Execution\20230705061123_Windows10C_11_SYSTEM_AppCompatCache.csv'											
Us	C:\Tools\Get-ZimmermanToo	ols>											
cour	nts_V	Mindaux Serve 20		Free lands									

015-

N--/

Vindows Server 2019 Datacenter Evaluation Windows License valid for 173 days Build 17763.rs5_release.180914-1434



 \sim



-

Windows License valid for 173 days Build 17763.rs5_release.180914-1434



-0,	Timeline F	Explorer v	/1.3.0.0			Output show in Timeline								
File	E Tools	Tabs	View Help			Fynlore								
202	/30705061	.123_Win	dows10C_11_SYSTEM	1_AppCompatCache.c	.SV	Explorer	-							
Dr	ag a	colum	n header he	re to group	by that column		Enter	r text to search Find						
	Line	Tag	Control S	Duplicate	Cache Entry Posi…	Executed	Last Modified Time UTC	Path						
т	=		=		=	RBC	=	RBC						
►	1		1		0	No	2021-10-06 13:52:38	C:\Windows\system32\s						
	2		1		1	No		00000009 000a564b2739						
	З		1		2	No		00000009 000b08a20000						
	4		1		3	No		00000009 00010000f097						
	5		1		4	No		00000009 000c005f0bb9						
	6		1		5	No		00000009 000b08ff0005						
	7		1		6	No	2023-06-29 08:25:43	C:\Program Files\Wind						
	8		1		7	No		00000009 000f00630c820						
	9		1		8	No		00000009 0012090104c6						
	10		1		9	No	2023-06-29 08:13:18	C:\ProgramData\Micros						
	11		1		10	No	2023-06-29 08:24:59	C:\Program Files\Windo						
	12		1		11	Yes		00000009 00015a0c00790						
	13		1		12	No	2023-06-29 08:24:55	C:\Program Files\Windo						
	14		1		13	No		00000009 000b09000000						
	15		1		14	No		00000009 00015a0c00790						
	16		1		15	No		00000009 0004089c33f70						
	17		1		16	Yes		00000009 07e7272e697a						
	18		1		17	No	2023-06-29 08:22:37	C:\Program Files\Windo						
\square	19		1		18	No		00000009 000b090000020						

Timeline Explorer v1.3.0.0

🖹 c	:\Cases\Analysis\Regi	istry\SYSTEM.txt - Notepad+	+ [Administrator]					o ×
File	Edit Search View	v Encoding Language	Settings Tools Macro Ru	n Plugins	Window ?			+ v ×
	🚽 🗄 🖷 🗟 🐚	😂 🐇 🖻 💼 Ə e) 🛍 🏂 🔍 🔍 🖬 🖬	🗄 🎙 🗍	= 🖉 🔝 🍱 🖉 🖿	🥑 🔲 🖿 🕨 🔤		
🔡 al	II 🗵 🔚 DEFAULT.txt	🛛 🔀 NTUSER.DAT.txt 🔅	🛛 🔚 SECURITY.txt 🛛 🔚 SO	FTWARE.txt	🛛 🔚 SAM.txt 🛛 🔚 U	JsrClass.dat.txt 🛛 🔚 SYSTEI	M.txt 🗵	
10	appcompate	ache v.20220921						
11	l (System) Pa	arse files from Sys	stem hive AppCompatCa	che		Find		
12	2					Find Peolace Find in Files	Find in Projects Mark	
13	3 ControlSet	001\Control\Sessior	1 Manager\AppCompatCa	che		Replace Find in thes	This in Projects Mark	
14	LastWrite :	Time: 2023-06-29 09	9:08:05Z			Find what: appcom	patcache	、 、
15	Signature:	0x34						
16	SIGN.MEDIA	=AIAA6D23 VirtualBo	000-0000179-Win.e	xe 2023-	06-26 05:56:58]		
17	00000000	0002a41723290000	000a000047ba0000	8664	Microsoft.UI.X			
18	G () 25 - 2 - 2	0005077207640000	000a000045630000	8664	Microsoft.Wind			In selecti
19	C:\Windows	\system32\wevtutil.	exe 2021-10-06 13:5	2:38		l	System hives	
20	C:\Windows	\SystemApps\Microso	ort.windows.StartMenu	Lxperienc	enost_cw5n1n2txy	Backward direction	1 1	
		USECHACIUSIIUUUU	00020000000000000000000000000000000000	06 12.52.	Alcrosoft.Wind	Match whole word only	edit with	
22	C:\Windows	System32 (MUSNOTII)	Migrosoft Vhowler 42	40 21001	0 v 64 0 v 6 k v 6 2 d	Match case	Matanadu	
23	C:\Program	riles(windowsapps)	MIGrosoft.XboxApp_48	. 49.31001	.0_x648Wekyb30		ivotepaa++	
25		Varazza (wpem/wmlp	000-00004-540000	9664	Migrosoft Wind			
25	00000009	000=00007f120000	0002000042640000	8664	Microsoft WCL	Search Mode		
20		Microsoft NETLE	ework w4 0 30316 MCa	ooor nTaek eve	2021_10_06_12*	Normal		
20	C:\Program	Files (v86)\Micros	actt\EdgeUndate\Insta	11\117500	469_989D_4132_98			
20	C:\Windows	rites (A00) (HICEOS	solt (Eugeopuate (Insta	12-07 00	•09•05		x)	
30	C:\Windows	System32\mobsurg	2019-12-07 09-09	.47	.05.05	Regular expression	. matches newline	
31	00000000	0002000273480000	000a000027410000	8664	Microsoft NFT			
32	C:\Windows	system32\SearchFil	terHost.exe 2021-10	-06 13.52	:31			
33	3 0000000b	000a00004a6103ff	000a00004a6103ff	8664	Microsoft.Wind	lows.ShellExperience	Host cw5n1h2txv	-wv ne
34	C:\Windows	\svstem32\osk.exe	2019-12-07 09:08:43	0001	110100010.0110	end bierrenper reliee	iero esoninzoky	
35	C:\Windows	\svstem32\wbem\unse	capp.exe 2021-10-06	13:52:05				
36	C:\Windows	\svstem32\cleanmar.	exe 2021-10-06 13:5	3:34				
37	7 00000009	3e8137f653cc0000	000a000047ba0000	8664	Microsoft.Offi	ce.OneNote 8wekv	b3d8bbwe	
38	00000009	000e00007f120000	000a0000273a0000	8664	Microsoft.VCLi	bs.140.00.UWPDesktor	p 8wekvb3d8bbwe	
39	0000009	00015a0c00790000	000a00004a640000	8664	Microsoft.Your	Phone 8wekvb3d8bbwe		
						1		× *
	and the state film	1	4h - 2 01 621 - Kana - 7 241	1	Colu15 Colu1411	14Cm - 1 (1		2
Norm	hal text file	leng	tn : 3,81,031 lines : 7,241	Ln : 10	Col: 15 Sel: 14 1	Windows (0	UTF-8	INS
	ト ク Li ti	🤕 🚍 🧉	🗠 🧳 📝				へ に d <mark>x 06:0</mark>	3 2023 🖓

3.Analyzing the Amcache with AmcacheParser

AmCache. hve is a Windows system file that is created to store information related to program executions. The artifacts in this file can serve as a huge aid in an investigation, it records the processes recently run on the system and lists the paths of the files executed.

Load the Amcache.hve on Registry Explorer

📙 🛃 📘 🖛 Programs			198 1994								_	đ	\times			
File Home Share	2	View										~ 🕐				
← → ~ ↑ 📙 > Tł	his P	PC > SDT_x64FREE_EN-	US_VHD (C:)	> Cases >	F > Windows	> A	pp	Compat > Progra	ims	v Č Sea	arch Programs		Q			
^		Name				Ту	/pe	Size								
🖈 Quick access		Amcache hve			29-06-2023 09:07		H	VE File	1 280 K	B						
📃 Desktop 🛛 🖈					25 00 2025 05.07			VETIC	1,200 N							
👆 Downloads 🖈																
🚆 Documents 🖈																
📰 Pictures 🛛 🖈		Registry Explorer v	1.6.0.0													
Evidence	Fi	le Tools Options B	ookmarks (0)/0) View												
Execution	R	egistry hives (1) Availa	able bookmar	ks (0/0)		_	Values									
NTFS	I	Enter text to search			Find		Drag a column header here to group by that column									
Registry								Value Name	Value Type	Data	Value Slack	Is Delet	ed			
💻 This PC	This PC						۴	RBC	RBC	RBC	R B C					
3D Objects	L_	C:\Cases\F\W		_	2023-06-28 17:12		•	CreatingCommand	RegSz	"C: \Program File	2D-00-32-00-44					
Desktop	•	▶ [{11517B7C	2	1	2023-06-28 17:12	:		CreatingModule	RegSz	C:\Windows\SYS						
Documents		Associated de	0	0												
Downloads																
Music																
Pictures																
Videos																
SDT_x64FREE_EN						:										
😚 CD Drive (D:) Vir																
🛖 Downloads (\\VE																
×																
1 item 1 item selected 1	1															
T ク H	6	🗦 🥅 🍅	*								へ ┞	38 -2023				

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (0/0) View Help

Registry hives (1) Available bookmarks (0/0)						Va	alues Amca	che-InventoryApplica	ationFile					
[Enter text to searc	h		Find		Dra	ag a column hea	ader here to group b	y that column				,	Q
_					-		Timestamp	Path	Name	Product Name	Publisher	Version	SHA1	
	Key name		# values	# subkeys	4	9	=	RBC	RBC	RBC	RBC	RBC	RBC	^
۲			=	= '			2023-06-29 0	c:\program	3DViewer.exe	view 3d	microsoft	6.1908.2042.0	ee05f81b330d2e	2
	C:\Cases		-					files\windowsap			corporation		755d8028ec5da8 59cf9eae1813	3
	▲ {1151/B	/C-E/9D-4e20-961B-75	2					crosoft3dviewe					556156461015	
	A ROOT	in Commun	0			'		r_6.1908.2042.						
) De	viceCensus	1	-				b3d8bbwe\3dvi						
		verPackageExtended	24					ewer.exe						_
		entoryApplication	24	c			2023-06-29 0	c:\program files\windowsap	AppInstaller.ex	microsoft appx click handler	microsoft	1.0.1901.2500	828d5cf25052ad 0686636867130f	i F
			1	17				ps\microsoft.de	-			-	5a8ff4b71a83	
		ventoryApplicationFile	10	14				sktopappinstall er 1.0.30251.0						
		appinstaller evelc736df	19	_				_x648wekyb						
		appinstaller.exe c736df	19					3d8bbwe\appin staller eve						
			10	_			2023-06-29.0	c:\program	AppInstallerEle	microsoft appx	microsoft	1.0.1901.2500	935407d4d0d89	
		calculator evel 724943ch	10					files \windowsap	vatedAppServic	click handler	corporation	1	8f997d5231daff	
		codecnacks heif 17deccd	19					ps\microsoft.de sktopappinstall	eClient.exe				a3329a1443f56	
		codecpacks vp9 el86e4	19					er_1.0.30251.0						
		codecpacks.webp. Idaa3	19					_x648wekyb 3d8bbwe\appin						\sim
	=	compattelrunner, 1732ad	20			То	otal rows: 128						Export	?
	=	cookie exporter, 21e69	19											
	=	cookie exporter. 81014	19			Ty	ype viewer	Binary viewer						
	=	cookie exporter. c1715	19			Valu	ue name	WritePermissionsCheo	:k					
		cortana.exe d59b9eee1	19											_
<				>		Valu	ue type	RegDword						
	Key: Roo	t\InventoryApplicationFil	e							Va	alue: Write	PermissionsCheck	Collapse all hi	ves
Se	lected hive: Amc	ache.hve Last write:	2023-06-2	29 08:12:32	2 0	of 2 v	alues shown	(100.00%) Load	complete			ŀ	lidden keys: 0	1
	م	H 🤶 📄	6	Q. (^ 맏 ੍∞ ₀	17:06 19-07-2023	

o ×



Go to the target system and Download the Amcache in link <u>https://ericzimmerman.github.io/#!index.md</u> and open cmd with Run as a Administrator.

Recycle Bin AmcachePa		
Administrator: Command Prompt —		\times
Microsoft Windows [Version 10.0.19044.1288] (c) Microsoft Corporation. All rights reserved.		î
pwF-mC:\Windows\system32>cd C:\Users\Denisha\Desktop		
C:\Users\Denisha\Desktop>dir Volume in drive C has no label. Volume Serial Number is 4AF5-9951 Directory of C:\Users\Denisha\Desktop		
05-07-2023 14:09 <dir> 05-07-2023 14:09 <dir> 05-07-2023 14:09 <dir> AmcacheParser 05-07-2023 14:03 4,515,977 AmcacheParser.zip 05-07-2023 23:14 <dir> PWF-main 28-06-2023 23:13 2,610,224 PWF-main.zip 2 File(s) 7,126,201 bytes 4 Dir(s) 31,148,974,080 bytes free</dir></dir></dir></dir>		
C:\Users\Denisha\Desktop>AmcacheParser -f C:\Windows\appcompat\Programs\Amcache.hvecsv amcache/ 'AmcacheParser' is not recognized as an internal or external command, Amcacheoperable program or batch file.		
C:\Users\Denisha\Desktop>dir Volume in drive C has no label. Volume Serial Number is 4AF5-9951		
amcac Directory of C:\Users\Denisha\Desktop		
Windows License Build 19041.vb_rele	valid for 8 ase.19120	2 days 6-1406
日 🖓 Type here to search O 首 💽 🦷 🖬 🖬 📾 Rain へ 供 (4) ENG 🕫 🕫	:45	\neg

06-07-2023



All File create in Amcache folder. Amcache folder copy the main pc and open with excel and show the output.

6	📙 🛃 📙 🖛 amcache				– 🗆 ×	
Recyc	File Home Share	e View			~ 🕐	
	← → ~ ↑ 📙 « De	esktop → amcache v Ĉ		e		
	^	Name	Date modified	Type	Size	
PWF-	📌 Quick access	20220706214226 Amcache DeviceContai	06-07-2022 21:42	CSV Eile	2 1/ 2	Programs\Amcache.hve.LO
	📃 Desktop 🛛 🖈	20230706214236 Amcache DevicePons csv	06-07-2023 21:42	CSV File	27 KB	
	👆 Downloads 🖈	20230706214236 Amcache DriveBinaries	06-07-2023 21:42	CSV File	107 KB	
	🔮 Documents 🖈	20230706214236 Amcache DriverPackag	06-07-2023 21:42	CSV File	1 KB	sum: 0x28DD8509
DW/E-	📰 Pictures 🛛 🖈	20230706214236_Amcache_ShortCuts.csv	06-07-2023 21:42	CSV File	8 KB	
6400-	Music	20230706214236_Amcache_Unassociated	06-07-2023 21:42	CSV File	15 KB	
	📑 Videos					
1	 OneDrive 					
Amcac	💻 This PC	All file pa	ste in main pc.			
	3D Objects					
	Desktop					
	Documents					
Amcac	Downloads					
	Music					
	Pictures					
	Videos					
ame	Local Disk (C:)					
Citte	🔀 CD Drive (D:) Vir					
	×	<			>	Windows License valid for 82 days
	6 items					Build 19041.vb_release.191206-1406
		rch O 🛱	Ce 🗖 💼		<u>⊡</u> 27℃ へ(€ \$\cdot) ENG 06-07-2023

🔒 🛛 🔁 📴 🚽 🖬 amcache	2						_	đ	\times
File Home Sha	are Vie	w							~ 🕐
← → ~ ↑ 📙 > `	This PC →	Downloads > amcache				~ Ō	Search ar	mcache	Q
		Name	Date modified	Туре	Size				
Quick access		வ 20230706214236_Amcache_DeviceContai	06-07-2023 21:42	Microsoft Excel C	3 KB				
Desktop	Я	😰 20230706214236_Amcache_DevicePnps	06-07-2023 21:42	Microsoft Excel C	27 KB				
Downloads	R	😰 20230706214236_Amcache_DriveBinaries	06-07-2023 21:42	Microsoft Excel C	107 KB				
Documents	А.	20230706214236_Amcache_DriverPackages	06-07-2023 21:42	Microsoft Excel C	1 KB				
Pictures	*	20230706214236_Amcache_ShortCuts	06-07-2023 21:42	Microsoft Excel C	8 KB				
46		20230706214236_Amcache_Unassociated	06-07-2023 21:42	Microsoft Excel C	15 KB				
48		†	<u> </u>						
49									
Screenshots									
📥 OneDrive		All file shown in	main pc and	open with					
💻 This PC		excel.	-	-					
📃 Desktop									
Documents									
🕂 Downloads									
👌 Music									
Pictures									
🚪 Videos									
Lew Volume (C:)									
New Volume (F:)									
💣 Network									
_									
6 items 1 item selected	d 14.0 KB								

—

[[]]

Ţ,

e

(

P

 $\langle \rangle$

2019

x

9



	≣ਙ੶⊘	~ =	20	0230706214236	5_Amcache_U	Table Tools	Sign	in 🖉 🗄	ē — Ō	\times			
F	ile Home	Insert	Draw	Page Layout	Formula	s Data	Review	View Help	Table Desig	n Ç T	ell me what you wa	unt to do 🖓	
Tab Ta ₁⊕	Table Name: Image: Summarize with PivotTable Table1 Image: Summarize with PivotTable Image: Summarize with PivotTable Image: Summarize with PivotTable					Refresh aal Table Dar	∷	ader Row Fi tal Row La nded Rows Ba Table	rst Column [ast Column anded Columns e Style Options	⊡ Filter Butt	on Quick Styles ~ Table Styles	Amcache Entry	~
AS	5 *	: ×	$\checkmark f_x$	Unassoc	iated								~
	А		В		С		D	E	F	G	н	I.	
1	Column16364	- 💌 F	ProgramId 💌	FileKeyLast	tWriteTime	stamp 💌	SHA1 💌	IsOsComponent	t 💌 FullPath 💌	Name 💌	FileExtension 💌	LinkDate 🗾 💌	Proc
2	Unassociated	C	0006a8dc383d	d	05-07-2	023 08:39	32136ffef(FALSE	c:\users\de	AmcacheF	.exe	24-10-2052 08:04	l amc
3	Unassociated	C	0000f519feec	×	29-06-2	023 08:08	77f2e744c	TRUE	c:\windows	CompatTe	.exe	18-10-2025 04:45	i micr
4	Unassociated	0	0006f3904a4b	0	29-06-2	023 08:09	074349c30	FALSE	c:\program	cookie_ex	.exe	21-06-2023 22:30) micr
5	Unassociated	l	0000f519feec	*	29-06-2	023 08:01	11eba7b1	TRUE	c:\windows	csrss.exe	.exe	25-05-1971 13:07	7 micr
6	Unassociated	To	0000f519feec	×	29-06-2	023 08:08	0646f8653	TRUE	c:\windows	DeviceCer	.exe	19-05-2039 12:13	3 micr
7	Unassociated	C	0006f3904a4b	0	29-06-2	023 08:09	777ac620a	FALSE	c:\program	elevation	.exe	21-06-2023 22:30) micr
8	Unassociated	C	0006f3904a4b	0	29-06-2	023 08:09	872cc644f	FALSE	c:\program	identity_ł	.exe	21-06-2023 22:30) micr
9	Unassociated	C	0006e0870de	4	29-06-2	023 08:09	5dedd60f	FALSE	c:\program	ie_to_edg	.exe	21-06-2023 22:30) ieto
10	Unassociated	C	0006ae478658	8	29-06-2	023 08:09	690897252	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:16	i micr
11	Unassociated	C	0006868509b0	d	29-06-2	023 08:09	7f6daa619	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:15	i micr
12	Unassociated	C	0006868509b0	c	29-06-2	023 08:09	076f72b14	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:16	i micr
13	Unassociated	C	0006868509b0	c	29-06-2	023 08:09	9f5c3fd02	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:22	2 micr
14	Unassociated	C	0006868509b0	c	29-06-2	023 08:09	9f5c3fd02	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:22	2 micr
15	Unassociated	C	00060cab34c3	3	28-06-2	023 17:12	3d26b0dc	FALSE	c:\program	Microsoft	.exe	22-07-2021 01:16	i micr
16	Unassociated	C	0006868509b0	d	29-06-2	023 08:09	b61a5756c	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:16	i micr
17	Unassociated	C	0006868509b0	c	29-06-2	023 08:09	7f7c48ad1	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:16	i micr
18	Unassociated	C	0006868509b0	c	29-06-2	023 08:09	cc92d47f7	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:15	i micr
19	Unassociated	C	000651e5db3	1	29-06-2	023 08:09	7c51ea622	FALSE	c:\program	Microsoft	.exe	21-06-2023 22:30) micr
20	Unassociated	C	000651e5db3	1	29-06-2	023 08:09	7c51ea622	FALSE	c:\program	Microsoft	.exe	21-06-2023 22:30) micr
21	Unassociated	C	0000f519feec	*	29-06-2	023 08:04	7e29a8d98	TRUE	c:\windows	MoUsoCo	.exe	01-05-2068 18:03	micr
22	Unassociated	C	0006f3904a4b	0	29-06-2	023 08:09	fea1f23ec	FALSE	c:\program	msedge.e	.exe	21-06-2023 22:30) micr
23	Unassociated	C	0006707b1ec4	4	29-06-2	023 08:09	92332ecf2	FALSE	c:\program	msedgew	.exe	21-06-2023 22:30) micr 🔻
	4	2023070	6214236_Am	cache_Unass	oci 🤆	Ð			•				Þ
Rea	ady 🖓 Accessi	ibility: Una	wailable						Display Settin	gs 🌐	■ — –		+ 100%
	ОТуре	e here to	o search		Ţ	() 🤇	2 🥽	💼 👈	• 🕎	2019	🔰 🔨 📢	日 日本 10-07-2023	2

Open the task Schedular and click the Application Experience then manually run task.



Administrator: Command Prompt

5 Dir(s) 29,456,506,880 bytes free

C:\Users\Denisha\Desktop>AmcacheParser.exe -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache2 AmcacheParser version 1.5.1.0

0

Author: Eric Zimmerman (saericzimmerman@gmail.com) https://github.com/EricZimmerman/AmcacheParser

Command line: -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache2

Two transaction logs found. Determining primary log... Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1 Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2 Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1 At least one transaction log was applied. Sequence numbers have been updated to 0x0056. New Checksum: 0x28D8E509 'C:\Windows\appcompat\Programs\Amcache.hve' is in use. Rerouting...

Б

 \times

Two transaction logs found. Determining primary log... Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1 Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2 Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1 At least one transaction log was applied. Sequence numbers have been updated to 0x0056. New Checksum: 0x28D8E509

| 其i 💽 🧮 💼 🚖 🕑 🌔 🛹 28°C へ 😘 🖫 🕼 ENG

C:\Windows\appcompat\Programs\Amcache.hve is in new format!

Total file entries found: 145 Total shortcuts found: 50 Total device containers found: 9 Total device PnPs found: 57 Total drive binaries found: 370 Total driver packages found: 2

Found 45 unassociated file entry

Results saved to: amcache2

Total parsing time: 9.353 seconds

Ŧ

📔 🛃 📊 🖛 🛛 amcach	ne2						—	þ	\times						
File Home Sh	e Home Share View														
← → ~ ↑	→ 👻 🚹 > This PC > Downloads > amcache2														
		Name	Date modified	Туре	Size										
Quick access		🔕 20230710103733_Amcache_DeviceContai	10-07-2023 10:37	Microsoft Excel C	3 KB										
	71	😰 20230710103733_Amcache_DevicePnps	10-07-2023 10:37	Microsoft Excel C	32 KB										
👆 Downloads	A	🔊 20230710103733_Amcache_DriveBinaries	10-07-2023 10:37	Microsoft Excel C	108 KB										
🔮 Documents	A	🔊 20230710103733_Amcache_DriverPackages	10-07-2023 10:37	Microsoft Excel C	1 KB										
Pictures	*	20230710103733_Amcache_ShortCuts	10-07-2023 10:37	Microsoft Excel C	8 KB										
46		20230710103733_Amcache_Unassociated	10-07-2023 10:37	Microsoft Excel C	18 KB										

Save the file Amcache2 folder and open with excel.

(2)

Р

e

Ţ,

[[]]

 \mathbf{b}

2019

x

0

^ 맏 ♡)

:== **E**

2

10:40 10-07-2023

48 49

OneDrive

This PC 🔜 Desktop

💧 Music Pictures 📑 Videos

Network

*

Screenshots

Documents Downloads

Low Volume (C:) New Volume (F:)

E	∃•ਙ੶ ੋ	~ =	2023	3071010373	3_Amca	che_Unasso	ciatedFileEr	ntries - E	Excel	denishagohil334@gmail.com 🖸 🧳 🖻 — 🗇 🗙									
F	ile Home	Insert	Draw	Page Lay	/out	Formulas	Data	Review	v View	Help	Table D)esign	Q	Tell me w	hat you v	vant to do			
Tab Tal √⊕	le Name: ble1 Resize Table Properties	IF Summ	aarize with P ve Duplicate ert to Range Toole	PivotTable es	Insert Slicer	Export f	Refresh 🔅		Header Row Fotal Row Banded Row	First	Column Column ded Colum tyle Option	ins is	⊡ Filter Butt ns		Quick tyles ~ ole Styles	Out Up	tput dated.	~	
E1	2 -	: ×	√ f _s	FALS	SE													~	•
	А		В				с		D		E		F	G		н	1		•
1	Application	lame 💌 Pr	ogramId		🕶 FileK	(eyLastWri	teTimest	amp 💌	SHA1 💌	IsOsCon	ponent	Full	Path 💌	Name	🕶 FileÐ	ktension 🔽	LinkDate	- L	_
2	Unassociated	d 00 k	06a8dc383	3d31dcde	22	(07-07-202	3 04:55	32136ffef	E FA	ALSE	c:\us	sers\de	Amcache	eF.exe		*****	## :	
3	Unassociated	d 00	00f519fee	c486de87	7e		29-06-202	3 08:08	77f2e744d	т	RUE	c:\w	indows	Compat	Te.exe		*****	##	
4	Unassociated	d 00	06119b978	889343334	4d	:	10-07-202	3 04:53	42d834da	F/	ALSE	c:\pr	rogram	cookie_e	ex.exe		******	##	
5	Unassociated	d 00	00f519fee	c486de87	7e		29-06-202	3 08:01	11eba7b1	Т	RUE	c:\w	indows	csrss.exe	e .exe		*****	##	
6	Unassociated	d 00	00f519fee	c486de87	7e		29-06-202	3 08:08	0646f8653	Т	RUE	c:\w	indows	DeviceC	er.exe		******	##	
7	Unassociated	00 k	0000f519feec486de87e 0006119b97889343334d 0006119b97889343334d			4d 10-07-2023 04:53 3bd5d28ca			F/	ALSE	c:\pr	rogram	elevatio	n .exe		*****	##		
8	Unassociated	d 00	0006119b97889343334d 0006119b97889343334d			10-07-2023 04:53 cdf846712			F/	ALSE	c:\pr	rogram	identity	<u></u> ł.exe		******	##		
9	Unassociated	00 k	06137d5e	ee4dd1f6	b	10-07-2023 04:53 d97d5b3d			F/	ALSE	c:\pr	rogram	ie_to_eo	dg.exe		*****	##		
10	Unassociated	d 00	065bf2b4f	f348de189	Эа	(08-07-202	3 15:53	6d27b973	F/	ALSE	c:\pr	rogram	Microso	ftl.exe		******	##	
11	Unassociated	00 k	06aa1f899	2cfa6e33	8ł	:	10-07-202	3 04:53	06bac910a	F/	ALSE	c:\pr	rogram	Microso	ftl.exe		*****	##	
12	Unassociated	d 00	06aa1f899	2cfa6e33	8ł	(08-07-202	3 15:53	aa15234f0	F/	ALSE	c:\pr	rogram	Microso	ftl.exe		******	##	
13	Unassociated	00 k	06aa1f899	2cfa6e33	8t		08-07-202	3 15:53	fed2634co	F/	ALSE	c:\pr	rogram	Microso	ftl.exe		*****	##	
14	Unassociated	900 8	06aa1f899	2cfa6e33	8ł		08-07-202	3 15:53	ed6642a2	F/	ALSE	c:\pr	rogram	Microso	ftl.exe		******	##	
15	Unassociated	00 k	06aa1f899	2cfa6e33	8ł		08-07-202	3 15:53	0c5f3e8a7	F/	ALSE	c:\pr	rogram	Microso	ftl.exe		*****	##	
16	Unassociated	d 00	060cab34c	3bd2ce1	cfi		28-06-202	3 17:12	3d26b0dc	F/	ALSE	c:\pr	rogram	Microso	ftl.exe		******	##	
17	Unassociated	00 k	06aa1f899	2cfa6e33	8t		08-07-202	3 15:53	06bac910a	F/	ALSE	c:\pr	rogram	Microso	ftl.exe		*****	##	
18	Unassociated	d 00	06aa1f899	2cfa6e33	8ł	(08-07-202	3 15:53	0a0018108	F/	ALSE	c:\pr	rogram	Microso	ftl.exe		******	##	
19	Unassociated	00 k	060f01fa4	45416eed	18		10-07-202	3 04:53	f705161e7	F/	ALSE	c:\pr	rogram	Microso	ftl.exe		*****	##	
20	Unassociated	900 8	060f01fa4	45416eed	18	:	10-07-202	3 04:53	f705161e7	F/	ALSE	c:\pr	rogram	Microso	ftl.exe		******	##	
21	Unassociated	00 k	00f519fee	c486de87	7e		29-06-202	3 08:04	7e29a8d9	т	RUE	c:\w	indows	MoUsoC	oi.exe		*****	##	
22	Unassociated	d 00	06e71e18	2965d414	6f	:	10-07-202	3 04:53	f92f04998	F/	ALSE	c:\pr	rogram	МрСору	A .exe		******	##	
23	Unassociated	d 00	06dc1a176	5320b5db	be		10-07-202	3 04:53	45d7b8e9	F/	ALSE	c:\w	indows	MpSigSt	ul.exe				•
	< ►	202307101	103733_An	ncache_Ur	nassoci	\oplus					•							►	
Rea	Ready 42 Accessibility: Unavailable										🛱 Display S	ettings			₽ -		+	100%	6
	ОТур		Ļ (נ 🔁			(1)	\mathbf{r}	2019	P	×	~	탄 🕬 10	10:50 0-07-2023	(2)				

4. Windows Prefetch Analysis

Accessing Prefetch Files for Forensic Analysis. A digital forensic investigation often aims to determine the activities of a user on a computer. Prefetch files are an important type of evidence, which provide detailed information about the programs that were run on a computer.

In the windows 10 target system many prefetch files available in this path.

ŵ

A-

3

015-

📊 🛛 🛃 🚽 🛛 prefetch					_	đ	×
File He Customize Qui	ck Access Toolbar						~ 🕐
← → ~ ↑ 📙 <u>C:\Ca</u>	ses\F\Windows\prefetch			~ ē	Search prefetch		Q
^	Name	Date modified	Туре	Size			^
Cuick access	AM_BASE.EXE-808FC880.pf	29-06-2023 08:06	PF File	2 KB			
Desktop 🖈	AM DELTA.EXE-B7261F63.pf	29-06-2023 08:07	PF File	2 KB			
👆 Downloads 🖈	AM_ENGINE.EXE-69ACF71F.pf	29-06-2023 08:06	PF File	3 KB			
🔮 Documents 🖈	APPLICATIONFRAMEHOST.EXE-CCEEF75	29-06-2023 08:05	PF File	15 KB			
📰 Pictures 🛷	AUDIODG.EXE-BDFD3029.pf	29-06-2023 08:03	PF File	6 KB			
Evidence	BACKGROUNDTASKHOST.EXE-145A3777.pf	28-06-2023 16:21	PF File	12 KB			
Execution	BACKGROUNDTASKHOST.EXE-A89D33B8	29-06-2023 08:02	PF File	14 KB			
plugins	BACKGROUNDTRANSFERHOST.EXE-4FEE	28-06-2023 16:24	PF File	14 KB			
Desister	BACKGROUNDTRANSFERHOST.EXE-298E	28-06-2023 16:46	PF File	8 KB			
Registry	BACKGROUNDTRANSFERHOST.EXE-CF5	28-06-2023 16:52	PF File	10 KB			
This PC	BYTECODEGENERATOR.EXE-C1E9BCE6.pf	29-06-2023 08:25	PF File	8 KB			
3D Objects	CLOUDEXPERIENCEHOSTBROKER.EXE-E8	28-06-2023 16:19	PF File	14 KB			
Desktop	CMD.EXE-4A81B364.pf	28-06-2023 16:32	PF File	1 KB			
	COMPATTELRUNNER.EXE-DB97728F.pf	28-06-2023 17:13	PF File	3 KB			
Developede	CONHOST.EXE-1F3E9D7E.pf	29-06-2023 08:25	PF File	10 KB			
Downloads	CONSENT.EXE-531BD9EA.pf	29-06-2023 08:03	PF File	25 KB			
J Music	CSC.EXE-67679278.pf	28-06-2023 16:42	PF File	9 KB			
Pictures	CSRSS.EXE-3FE41F7E.pf	28-06-2023 16:20	PF File	5 KB			
Videos	CVTRES.EXE-F2B7602E.pf	28-06-2023 16:42	PF File	3 KB			
SDT_x64FREE_EN	DLLHOST.EXE-5E46FA0D.pf	29-06-2023 08:14	PF File	4 KB			
🥳 CD Drive (D:) Vir	DLLHOST.EXE-28A8211F.pf	29-06-2023 08:13	PF File	12 KB			
Downloads (\\VF	DLLHOST.EXE-61F58501.pf	28-06-2023 16:19	PF File	8 KB			
v	DLLHOST.EXE-504C779A.pf	29-06-2023 08:11	PF File	5 KB			~
180 items	1 13						:== 🛌

06:07 07-07-2023

 \Box

^ ┞ ₄⊗

ρ

Цi

e

Open the PECmd tool and type the command for particular application.

, I 🌛	- - -			Manage	Get-ZimmermanTools				- 0	×
File	Home	Share	View	Application Tools						~ 🕐
← →	~ ^ [C:\Too	ols\Get-Zimi	mermanTools				~ Ū	Search Get-ZimmermanTo	ols 🔎
		^	Name	^	Date modified	Туре	Size			^
📌 Q	uick access		EvtxE	Cmd	28-06-2023 13:40	File folder				
	Desktop	*	EZVie	wer	28-06-2023 13:40	File folder				
- 🕂 I	Downloads	*	Hash	er	28-06-2023 13:41	File folder				
	Documents	*	iisGeo	olocate	28-06-2023 13:44	File folder				
	Pictures	*	Jump	ListExplorer	28-06-2023 13:41	File folder				
	Evidence		MFTE	xplorer	28-06-2023 13:41	File folder				
	Execution		RECm	nd	28-06-2023 13:41	File folder				
	NTES		Regis	tryExplorer	28-06-2023 13:42	File folder				
	Denista		SDBE:	xplorer	28-06-2023 13:42	File folder				
	Registry		Shell	BagsExplorer	01-07-2023 10:36	File folder				
TI	his PC		SQLE	Cmd	28-06-2023 13:43	File folder				
	3D Objects		Time	lineExplorer	01-07-2023 05:43	File folder				
	Desktop		XWFI	М	28-06-2023 13:44	File folder				
A	Documents		📆 !!!Ren	noteFileDetails	28-06-2023 13:44	CSV File	5 KB			
	Downloade		端 Amca	acheParser	21-05-2023 11:49	Application	4,661 KB			
	Downloads		🕥 АррС	CompatCacheParser	07-03-2023 15:13	Application	4,523 KB			
_	Music		🐪 bstrin	igs	20-05-2022 12:38	Application	3,997 KB			
	Pictures		Chan	geLog	28-06-2023 13:44	Text Document	33 KB			
	Videos		📓 Get-Z	CimmermanTools	18-05-2023 14:24	Windows PowerS	24 KB			
-	SDT_x64FRE	E_EN	🌄 JLECr	nd	13-03-2023 17:06	Application	4,792 KB			
1	CD Drive (D) Vir	LECm	nd	04-03-2023 10:30	Application	5,063 KB			
-	Downloads		MFTE	Cmd	20-10-2022 13:37	Application	4,409 KB			
-		~	PECm	nd	28-01-2022 12:08	Application	3,885 KB			~
32 item	s 1 item	selected	3.79 MB							

32 items 1 item selected 3.79 MB

Цi

e

3

ρ

05:07 ^ 强 🏪 🗤 16-07-2023



```
Administrator: C:\Windows\System32\cmd.exe
```

Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved.

```
C:\Tools\Get-ZimmermanTools>PECmd.exe
Description:
PECmd version 1.5.0.0
```

```
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd
```

```
Examples: PECmd.exe -f "C:\Temp\CALC.EXE-3FBEF7FD.pf"
    PECmd.exe -f "C:\Temp\CALC.EXE-3FBEF7FD.pf" --json "D:\jsonOutput" --jsonpretty
    PECmd.exe -d "C:\Temp" -k "system32, fonts"
    PECmd.exe -d "C:\Temp" --csv "c:\temp" --csvf foo.csv --json c:\temp\json
    PECmd.exe -d "C:\Windows\Prefetch"
```

Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

Б

06:08

07-07-2023

^ 뛷 🕼

 \times

 \sim

Usage:

PECmd [options]

Options:	
-f <f></f>	File to process. Either this or -d is required
-d <d></d>	Directory to recursively process. Either this or -f is required
-k <k></k>	Comma separated list of keywords to highlight in output. By default, 'temp' and 'tmp' are
	highlighted. Any additional keywords will be added to these
-0 <0>	When specified, save prefetch file bytes to the given path. Useful to look at decompressed Win10
	files
- q	Do not dump full details about each file processed. Speeds up processing when usingjson orcsv
	[default: False]
json <json></json>	Directory to save JSON formatted results to. Be sure to include the full path in double quotes
jsonf <jsonf></jsonf>	File name to save JSON formatted results to. When present, overrides default name
csv <csv></csv>	Directory to save CSV formatted results to. Be sure to include the full path in double quotes
csvf <csvf></csvf>	File name to save CSV formatted results to. When present, overrides default name
html <html></html>	Directory to save xhtml formatted results to. Be sure to include the full path in double quotes
dt <dt></dt>	The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for
	options [default: yyyy-MM-dd HH:mm:ss]



Administrator: C:\Windows\System32\cmd.exe

Either -f or -d is required. Exiting

C:\Tools\Get-ZimmermanTools>PECmd.exe -f C:\Cases\F\Windows\prefetch\APPLICATIONFRAMEHOST.EXE-CCEEF759.pf PECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com) https://github.com/EricZimmerman/PECmd

Command line: -f C:\Cases\F\Windows\prefetch\APPLICATIONFRAMEHOST.EXE-CCEEF759.pf

Keywords: temp, tmp

Processing C:\Cases\F\Windows\prefetch\APPLICATIONFRAMEHOST.EXE-CCEEF759.pf

Created on: 2023-06-28 16:24:19 Modified on: 2023-06-29 08:05:09 Last accessed on: 2023-06-29 08:05:09

Executable name: APPLICATIONFRAMEHOST.EXE Hash: CCEEF759 File size (bytes): 63,002 Version: Windows 10 or Windows 11

Run count: 3 Last run: 2023-06-29 08:04:59 Other run times: 2023-06-28 16:35:05, 2023-06-28 16:24:09

Volume information:

Ω

FF-

#0: Name: \VOLUME{01d9aa46f526b4aa-4af59951} Serial: 4AF59951 Created: 2023-06-29 05:02:52 Directories: 20 File references: 3
06

Ы

_

^ ┖⊇ ◁∞

07-07-2023

 \times

 \sim

Directories referenced: 20

Ξi

00: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES

01: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS

02: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_NEUTRAL_SPLIT.SC

0:5-

Administrator: C:\Windows\System32\cmd.exe

06

Directories referenced: 20

- 00: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES
- 01: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS

02: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_NEUTRAL_SPLIT.SC ALE-100_8WEKYB3D8BBWE

Б

^ 뛷 🕼

07-07-2023

×

03: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_NEUTRAL_SPLIT.SC ALE-100_8WEKYB3D8BBWE\IMAGES

04: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X64__8WEKYB3D8BB WE

05: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X64__8WEKYB3D8BB WE\MICROSOFT.SYSTEM.PACKAGE.METADATA

06: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE_11910.1002.5.0_NEUTRAL_SPLIT.SCALE-10
0_8WEKYB3D8BBWE

07: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE_11910.1002.5.0_NEUTRAL_SPLIT.SCALE-10 0_8WEKYB3D8BBWE\ASSETS

08: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE_11910.1002.5.0_NEUTRAL_SPLIT.SCALE-10
0_8WEKYB3D8BBWE\ASSETS\APPTILES

- 09: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS
- 10: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\FONTS
- 11: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\GLOBALIZATION
- 12: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\GLOBALIZATION\SORTING
- 13: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\IMMERSIVECONTROLPANEL
- 14: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\IMMERSIVECONTROLPANEL\IMAGES
- 15: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\RESCACHE
- 16: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\RESCACHE_MERGED
- 17: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\RESCACHE_MERGED\987641329
- 18: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32
- 19: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\EN-US

Files referenced: 80

- 00: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\NTDLL.DLL
- 01: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\APPLICATIONFRAMEHOST.EXE (Executable: True)
- 02: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\KERNEL32.DLL



5. Windows Prefetch Timeline Analysis

In this command all prefetch file store in specific folder and open with timeline explorer

Administrator: C:\Windows\System32\cmd.exe	ð	×
197: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\MSVCP110_WIN.DLL		-
198: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WINDOWS.SYSTEM.DIAGNOSTICS.DLL		
199: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WINMETADATA\WINDOWS.UI.WINMD		
200: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WINMETADATA\WINDOWS.SECURITY.WINMD		
201: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WINDOWS.SECURITY.AUTHENTICATION.WEB.CORE.DLL		
202: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\ONECORECOMMONPROXYSTUB.DLL		
203: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\EN-US\WINDOWS.SECURITY.AUTHENTICATION.WEB.CORE.DLL.MUI		
204: \VOLUME{01d9aa46f526b4aa-4af59951}\USERS\DENISHA\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D8B	BWE \AC	/IN
ETCACHE\MSIMGSIZ.DAT		
205: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WINDOWSCODECS.DLL		
206: VOLUME{01d9aa46+526b4aa-4a+59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X648	VEKYB3	D8B
BWE \MYOFFICE.RUNTIMECOMPONENTS.WINMD		
207: \VOLUME{01d9aa46+526b4aa-4a+59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X648	VEKYB3	D8B
BWE (MYOFFICE.RUNTIMECOMPONENTS.DLL		
208: \VOLUME{01d9aa46+526b4aa-4a+59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.VCLIBS.140.00_14.0.27323.0_X648WEKYB3D8	3BBME /	MSV
CP140_APP.DLL		
209: \V0LUME{0109aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.VCLIBS.140.00_14.0.27323.0_X648WEKYB3D8	SBBME /	VCR
210: \VOLUME{0109aa4of526D4aa-4af59951}\WINDOWS\SYSTEM32\WEBPLATSTORAGESERVER.DLL		
211: $VOLUME{0109aa40T520D4aa-4aT59951}WINDOWS{SYSTEM32}LOGONCLI.DLL242. VOLUME{0109aa40T520D4aa-4aT59951}WINDOWS{SYSTEM32}LOGONCLI.DLL$		1 T.N.
212: (V) C2FC4R2R2WL440T 520044-44T59951} (USERS (DENIARAPPDATA (LOCAL (PACKAGES (MICROSOFT.MICROSOFTOFFICEHOB_8WEKYB3D8BE	SWE \AC	VTN.
ETCACHE \S3FUIB3K\HERU-IMAGE-DESKTUP-F0720A4145[1].JPG		
213: $VOLUME{0109ad40T520D4ad-4dT59951}WINDOWS(STSTEMSZ(EN-OS)WINDOWS(STOLLE.MUI$		A TH
214: \VULUME{01090040075200400-40759951}\USEKS\DENISHA\APPDATA\LUCAL\PACKAGES\MICKUSUFT.MICKUSUFTUFFICEHUB_8WEKYB3D8BE	SWE \AC	VTN .
215: $VOLUME{0109ad40T520D4ad-4dT59951} WINDOWS (SYSTEM32 (CKYPTOWINKT.DLL216: VOLUME{0109ad40T520D4ad-4dT59951} WINDOWS (SYSTEM32 (CKYPTOWINKT.DLL)) ACKACES MTCPOSOFT MTCPOSOFT CELLUP QUEVVP3D0PL$		CAL
210. (VOLUME { 01090040075200400-40759951 } (USEKS (DENISHA (APPDATA (LOCAL (PACKAGES (MICKOSOFT.MICKOSOFTOFFICEHOB_OWEKTBSDODE STATE) THIPDDAPTYNOTICE HTMLTMD (Kowword: True)	SWE (LU	CAL
STATE (THIRDPARTYNOTICE. HTML. ~ TMP (Reyword: True)		
Processed C:\Cases\E\Windows\prefetch\WWAHOST_EXE-DB0D8801 pf in 0 86211480 seconds		
Processed 180 out of 180 files in 76.5676 seconds		
CSV output will be saved to C:\Cases\Analysis\Execution\20230716051531 PECmd Output.csv		
CSV time line output will be saved to C:\Cases\Analysis\Execution\20230716051531_PECmd_Output_Timeline.csv		

へ 🛐 🌄 🗤

16-07-2023

C:\Tools\Get-ZimmermanTools>PECmd.exe -d C:\Cases\F\Windows\prefetch --csv C:\Cases\Analysis\Execution\



🛃 📑 🗧 Execution

File

Home Share View

~ Ō	Search Execution	

← → * ↑	⇒ Th	is PC > SDT_x64FREE_EN-US_VHD (C:) > Cases	> Analysis → Execut	ion		~ Ō
	^	Name	Date modified	Туре	Size	
📌 Quick access						
Deskton		20230/05061123_Windows10C_11_SYSTE	05-07-2023 06:11	CSV File	45 KB	
- Desktop	~	國 20230705080017_Amcache_DeviceContai	05-07-2023 08:00	CSV File	3 KB	
Downloads	*	📆 20230705080017_Amcache_DevicePnps	05-07-2023 08:00	CSV File	27 KB	
Documents	*	📆 20230705080017_Amcache_DriveBinaries	05-07-2023 08:00	CSV File	107 KB	
Pictures	*	🔯 20230705080017_Amcache_DriverPackages	05-07-2023 08:00	CSV File	1 KB	
Evidence		式 20230705080017_Amcache_ShortCuts	05-07-2023 08:00	CSV File	8 KB	
Execution		國 20230705080017_Amcache_Unassociated	05-07-2023 08:00	CSV File	13 KB	
NTFS		🔯 20230707061607_PECmd_Output	07-07-2023 06:16	CSV File	1,374 KB	
Registry		a 20230707061607_PECmd_Output_Timeline	07-07-2023 06:16	CSV File	54 KB	
Registry		30230716051531_PECmd_Output	16-07-2023 05:15	CSV File	1,374 KB	
💻 This PC		a 20230716051531_PECmd_Outpu_Timeline	16-07-2023 05:15	CSV File	54 KB	

Open this file in timeline explorer

0

015-

3





















Q



Цi

e





 \times

~ 🕐

م

D



Show the All prefetch file with time

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

20230716051531_PECmd_Output.csv

Dr	ag a	column header here to group by that column			Enter tex	kt to search		Find
	ote	Source Filename	Volume1Seri	Source Created		Source Modif.	So	ource /
Ŧ]c	RBC	RBC	=		=	=	
►		C:\Cases\F\Windows\prefetch\AM_BASE.EXE-808FC88		2023-06-29 08:0	06:55	2023-06-29 0.	20	923-06
		C:\Cases\F\Windows\prefetch\AM_DELTA.EXE-B7261F		2023-06-29 08:0	07:23	2023-06-29 0.	20	923-06
		C:\Cases\F\Windows\prefetch\AM_ENGINE.EXE-69ACF		2023-06-29 08:	06:22	2023-06-29 0.	20	923-06
		C:\Cases\F\Windows\prefetch\APPLICATIONFRAMEHOS		2023-06-28 16:	24:19	2023-06-29 0.	20	923-06
		C:\Cases\F\Windows\prefetch\AUDIODG.EXE-BDFD302		2023-06-28 16:	14:35	2023-06-29 0.	20	923-06
		C:\Cases\F\Windows\prefetch\BACKGROUNDTASKHOST		2023-06-28 16:2	20:20	2023-06-28 1.	20	923-06
		C:\Cases\F\Windows\prefetch\BACKGROUNDTASKHOST		2023-06-28 16:	21:51	2023-06-29 0.	20	923-06
		C:\Cases\F\Windows\prefetch\BACKGROUNDTRANSFERH		2023-06-28 16:4	46:00	2023-06-28 1.	20	923-06
		C:\Cases\F\Windows\prefetch\BACKGROUNDTRANSFERH		2023-06-28 16:	24:21	2023-06-28 1.	20	923-06
		C:\Cases\F\Windows\prefetch\BACKGROUNDTRANSFERH		2023-06-28 16:	52:04	2023-06-28 1.	20	923-06
		C:\Cases\F\Windows\prefetch\BYTECODEGENERATOR.E		2023-06-28 16:	10:07	2023-06-29 0.	20	923-06
		C:\Cases\F\Windows\prefetch\CLOUDEXPERIENCEHOST		2023-06-28 16:	14:15	2023-06-28 1.	20	923-06
		C:\Cases\F\Windows\prefetch\CMD.EXE-4A81B364.pf		2023-06-28 16:	32:49	2023-06-28 1.	20	923-06
		C:\Cases\F\Windows\prefetch\COMPATTELRUNNER.EXE		2023-06-28 17:	13:24	2023-06-28 1.	20	923-06
		C:\Cases\F\Windows\prefetch\CONHOST.EXE-1F3E9D7		2023-06-28 16:	13:22	2023-06-29 0.	20	923-06
		C:\Cases\F\Windows\prefetch\CONSENT.EXE-531BD9E		2023-06-28 16:	20:43	2023-06-29 0.	20	923-06
		C:\Cases\F\Windows\prefetch\CSC.EXE-67679278.pf		2023-06-28 16:4	42:40	2023-06-28 1.	20	923-06
		C:\Cases\F\Windows\prefetch\CSRSS.EXE-3FE41F7E		2023-06-28 16:	20:38	2023-06-28 1.	20	923-06
		C:\Cases\F\Windows\prefetch\CVTRES.EXE-F2B7602E		2023-06-28 16:4	42:40	2023-06-28 1.	20	923-06

•

_

 \times

Auto run keys Analysis

Autorun and run keys are registry entries that allow programs to execute automatically when a device is connected or a user logs on. Malicious actors can use them to launch malware, bypass security controls, and maintain persistence on compromised hosts.

|--|

	4	Registry Expl	orer v	1.6.0.0			
	Fil	e Tools Optic	ons Bo	okmarks (29/0)	View	Help	
	Re	egistry hives (2)	Availa	ble bookmarks (59	9/0)		
	6	run					Find
		Key name					
	9		\ A -		TUCED	DAT	
			s (Analy	sis (Registry (N	IUSER.	DAT	
			Tever bior				
		E RunM	RU				
		E RunOi	nce				
		🕨 🚞 Shell					
		⊿ 👑 C:\Cases	Analy	sis\Registry\S	OFTWA	RE	
	<	l Chanr	iels				>
	— Bo	ookmark informatio	n				
	Hi	ve		C:\Cases\Analys	is (Regis	try\SOFT	WARE
	Ci	ategory		Autoruns			
	Na	ame		Run			
	Key path Short description		Microsoft\Windo	ws\Curre	entVersio	n\Run	
			Run key				
	Lo	ong description		Used to automat	ically sta	art progra	ams
		1					

1	/alues							
D	Drag a column header here to group by that column							
	Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated		
9	RBC	RBC	RBC	RBC				
►	SecurityHealth	RegExpandSz	%windir%\syste	00-00-00-00				
	VBoxTray	RegExpandSz	%SystemRoot%	00-00-1D-00-00-00				

You can insert the NTUSER hives in Registry Explorer and then search run.

Hive	C:\Cases\Analysis\Registry\SOFTWARE						
Category	Autoruns						
Name	Run						
Key path	Microsoft\Windows\CurrentVersion\Run						
Short description	Run key						
Long description	description Used to automatically start programs		Slack viewer Bi	nary viewer			
		Value name	SecurityHealth				
		Value type	RegExpandSz				
Key: Microsoft\	Vindows\CurrentVersion\Run				Value:	SecurityHealth	Collapse all hives
Selected hive: NTUSER.DA	Last write: 29-06-2023 08:01:53 +00:0	0 2 of 2 value	s shown (100.00%)			F	lidden keys: 0 1
H A H	🥭 🚍 🧉				^	🗐 🏗 🔩 1	05:49 6-07-2023

Registry Explorer v1.6.0.0

Fil	File Tools Options Bookmarks (29/0) View Help								
Re	egistry hiv	/es (2)	Available	bookmarks (59,	/0)				
	run 🕲 🔻 Find								
	Key name								
۴	RBC					^			
	C:\Cases\Analysis\Registry\NTUSER.DAT								
	C:\Cases\Analysis\Registry\SOFTWARE								
	▶ 🗖	Chann	nels						
	▶ □	Curre	entVersion	1					
		Curre	ntVersion						
		Image	File Execut	tion Options					
		Intern	et Explorer			-			
<		Run			>	~			
— В	ookmark ir	nformatio	n						
Hi	ive		C:	\Cases\Analysi	s\Registry\SOFTWARE				
Ci	ategory		Au	utoruns					
Na	ame		Ru	un					
Ke	ey path		Mi	crosoft\Windov	vs\CurrentVersion\Run				
Sł	hort descr	iption	Ru	un key					
Lo	ong descri	ption	Us	sed to automati	cally start programs		Γ		
	Key:	Mic	rosoft\Win	dows\Current	Version\Run		I L		
Se	lected hi	ve: NTU	SER.DAT	Last write:	29-06-2023 08:01:53 +	00:	00		

V	alues							
Drag a column header here to group by that column								
	Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated		
9	RBC	RBC	RBC	RBC				
•	SecurityHealth	RegExpandSz	%windir%\syste	00-00-00-00				
	VBoxTray	RegExpandSz	%SystemRoot%	00-00-1D-00-00-00				

þ

 \times

You can insert the Software hive in Registry Explorer and search run and show the autorun activities.

l	Cr (Cabes y maryon	offeed by portionite							
[Autoruns								
[Run								
[Microsoft\Window	vs\CurrentVersion\Run							
on [Run key								
on (Used to automatic	cally start programs	Type viewer	Slack viewer Bin	ary viewer				
			Value name	SecurityHealth					
			Value type	RegExpandSz					
Microsoft\W	/indows\Current	Version\Run				Value:	SecurityHealt	th Collapse	all hives
NTUSER.DAT	Last write:	29-06-2023 08:01:53 +00:00	0 2 of 2 value	s shown (100.00%)				Hidden keys	a 0 1
äŧ	<i>e</i> =	ڬ 😨				~	🛐 🏗 🕼	05:49 16-07-2023	5

📙 🛛 🛃 🚽 🛛 Registry								_	o ×	
File Home Share	View								~ 🕐	
\leftarrow \rightarrow \checkmark \uparrow \square \Rightarrow This F	~ Ū	Search Registry	Q							
A	Name	~	Date modifi	ed	Туре	Size				
Cuick access	UsrClass.dat		01-07-2023 1	10:55	Text Document	15 KB				
Desktop 🖈	UsrClass.dat		29-06-2023 (09:07	DAT File	3,328 KB				
🔶 Downloads 🖈	SYSTEM		01-07-2023 1	10:55	Text Document	373 KB				
🖆 Documents 🖈	SYSTEM		29-06-2023 (9:08	File	11,008 KB				
📰 Pictures 🛛 🖈	SOFTWARE		01-07-2023 1	10:55	Text Document	2,476 KB				
Evidence	SOFTWARE		29-06-2023 (09:08	File	68,608 KB				
Execution	SECURITY		01-07-2023 1	10:55	Text Document	4 KB				
NTFS			29-06-2023 (09:08	File	32 KB				
Registry	SAM	Open		0:55	Text Document	8 KB				
registry	SAM	Print		9:08	File	64 KB				
This PC	NTUSER.DA	Edit		1:02	Text Document	39 KB				
🗊 3D Objects	NTUSER.DA	Y Edit with Notepad++		9:07	DAT File	1,024 KB				
Desktop	DEFAULT	Share		0:55	Text Document	16 KB				
Documents	DEFAULT	Open with	>	9:08	File	512 KB				
🖶 Downloads		Restore previous versions								
👌 Music		Send to	>							
Pictures	-	Cut				• . •	1			
Videos		Сору		NTUSER hives open with						
SDT_x64FREE_EN	-			Notepad++.						
👸 CD Drive (D:) Vir		Delete			-					
🛖 Downloads (\\VI		Rename								
v	_	Kendille								
14 items 1 item selected 38	3.6 KB	Properties								
🕂 🔎 🛱 🧲) 📄 📫							へ 🚳 貯 🕼 16-07-	49 -2023 🕤	

	a la strand a la base	an a bhainn bha - Chùrachtail Mar a chuan an		i di Lini Stati Billi Di-		
🖹 C:\Ca	ases\Analysis\Registry\NTUS	ER.DAT.txt - Notepad++ [Administrator]			- 0	\times
File Ed	lit Search View Encodir	ng Language Settings Tools Macro Run Plugi	ins Window ?		+	• 🔻 🗙
🕞 📥 I	😑 🖻 🕞 🕞 📥 🛛 🚜 🗉	n n l d c l m 🐜 l 🤏 🤜 🖬 🖬 🛼 1	I 厓 🥃 📓 🕼 🖉	🛐 💼 💌 💌 🔳 🕨 🔤		
🔚 all 🛛	DEFAULT.txt 🛛 🔚 N		.txt 🛛 🔚 SAM.txt	🛪 🔚 UsrClass.dat.txt 🛛 🔚 SVS	STEM.txt	
776	2 = Resources					
777	0 = The Internet	5				<u> </u>
778		-				
779		Find		>	<	
780	run v.20200511	Find Replace Find in Files Find in Projects Mark				
781	(Software, NTUSER.					
783	Software\Microsoft	Eind what: run	\sim	Find Next		
784	LastWrite Time 202			Count		
785	MicrosoftEdgeAut			Coun <u>t</u>	t\Edge\Application\m	sedge
786	OneDrive - "C:\U	2	In selection	Find All in Current		
787				Document		
788	Software\Microsoft	Backward direction		Find All in All Opened		
789	Software Wow6432No	Match whole word only		Documents	Fine the run	
791	5010Wale (#0#045210	Match <u>c</u> ase		Close	command in All	
792	Software\Microsoft	Wrap around				
793	LastWrite Time 202	Search Mode		Transparency	current document	ts.
794	Software\Microsoft	Normal				
795	Software\Microsoft					
796	Software Migrosoft			Always		
798	Soltware (Microsolt	Regular expression <u>.</u> matches newline			A A	
799	Software\Microsoft					
800						
801	Software\Microsoft	t\Windows NT\CurrentVersion\Terminal S	Server\Install\	Software\Microsoft\Win	dows\CurrentVersion\Ru	n not
802			·····			
803	Software (Microsoft	t/Windows NI/Currentversion/lerminal :	berver\install\	Soltware (Microsolt (Win	dows(Currentversion(Ru	nonce
805	Software\Microsoft	\Windows\CurrentVersion\Policies\Expl	lorer\Run not f	ound.		
<						>
Normal te	ext file	length : 39,529 lines : 1,000 Lr	n:780 Col:15 Sel:	:8 1 Window	vs (CR LF) ANSI	INS
	o 🗄 🥖	🛏 📫 📫 🔜			∧ (과 ♥) 1= 05:51	P
					16-07-2023	0

📔 C:\Ca	ses\Analysis\F	Registry\NTUSER	R.DAT.txt - Not	tepad++ [Ad	dministr	ator]										- 0	×	<
File Edi	t Search \	/iew Encoding	Language	Settings	Tools	Macro	Run Plu	ugins V	Vindow	?						+	. 🔻	×
🕞 占 I	3 🖻 🔒 🛛	🕯 📥 🗟	n 🛍 🔁 🛛	2 🛍 🎭	. 🔍 🤇	🔫 ा	FR F ,	1 IF	<i>چ</i> 📡	u 🔊) 🔚 💌 🛛							
🔡 all 🗵	DEFAULT	.txt 🗵 🔚 NT	USER.DAT.txt	🔀 🔚 SEC	URITY.to	d 🗵 🔡	SOFTWA	RE.txt 🗵	B 🔚 SAN	M.txt 🗵	🔡 UsrClass.dat	t.txt 🗵	I 🔡 SYST	EM.txt 🗵	3			
776	2 = Re	sources																^
777	0 = Th	e Internet																
778																		
779																		
780	run v.20	200511			-													
781	(Softwar	e, NTUSER.I	DAT) [Auto	ostart] (Set au	itostar	t key	conten	nts fro	om Soft	tware hive							
782	Software	\Microsoft)	Windows	urrentV	argior	N Dum												
784	LastWrit	e Time 2023	R=06=28 17	7.52.557	19101	I \Kull												
785	Micros	oftEdgeAuto	Launch 1E	D6AFCC1	913946	652DA0C	4ECFC7	33304	- "C:\	Progra	am Files (x	86) \N	licroso	ft\Edge	=\Appli	cation/m	seda	-
786	OneDri	ve - "C:\Us	sers\Denis	sha\AppDa	ata\Lo	cal\Mi	crosof	t\OneL	Drive\0	DneDri	ve.exe" /ba	ckgro	ound					
787												-						
788	Software	\Microsoft	Windows\0	CurrentVe	ersion	n∖ <mark>Run</mark> h	as no	subkey	/s.									
789																		
790	Software	\Wow6432Noc	le\Microso	oft\Windo	ows/Cu	urrentV	Version	\Run n	not fou	und.								
791																		
792	Software	\Microsoft	Windows\0	CurrentVe	ersion	n\RunOn	ice											
793	LastWrit	e Time 2023	8-06-28 16	5:32:46Z														
794	Software	\Microsoft	Windows\0	CurrentVe	ersion	n\RunOn	ice has	no va	alues.									~
<																	>	
Search res	ults - (25 hits)																	×
Searc	h "run" (25 hits in	1 file of	f 1 sear	ched)													^
– C:\	Cases\Ana	lysis\Regi	stry\NTUS	ER.DAT.t	xt (2	5 hits))											
	ine 465:	(NTUSER.D	AT) Autos	tart – g	et Co	mmand H	Process	sor\Au	to <mark>Run</mark> '	value	from NTUSER	R.DAT	hive					
	ine 564:	(NTUSER.D.	AT) Gets .	load and	run	values	from u	iser h	ive									
	ine 5/1:	run value	not round	α.														
	ine 783.	Software	UUSII Migrogoft	Windowe	Curr	entVerd	aion\ Pr	110										
	ine 788.	Software	Microsoft'	Windows	Curr	entVers	sion\P	in has	no sui	bkeve	_							
T	ine 790:	Software	Wow6432No	de\Micro	soft\	Windows	s\Curre	entVer	sion\R	un not	found.							
Т	ine 792.	Software	Microsoft	Windows	Curr	entVer	eion\ Du	inOnce										~
Normal te	xt file		len	ngth : 39,529	lines :	1,000		Ln : 783	Col : 46	5 Sel:3	1		Windows	(CR LF)	ANSI		INS	
	р H	e		-	07									^ 3	투 1 1	05:51		
																16-07-2023	E.	2

C:\Cases	\Analysis\Registry\SOFTWARE.txt - Notepad+ + [Administrator] —	đ	\times									
File Edit	Search View Encoding Language Settings Tools Macro Run Plugins Window ?	+	• ×									
🕞 占 🗎	n n n n n n n n n n n n n n n n n n n											
🔚 all 🗵 📔	🖥 DEFAULT.txt 🗵 🔚 NTUSER.DAT.txt 🗵 🔚 SECURITY.txt 🗵 🔚 SOFTWARE.txt 🗵 🔚 SAM.txt 🗵 🔚 UsrClass.dat.txt 🗵 🔚 SYSTEM.txt 🗵											
40290	Software\Policies\Microsoft\Windows\PowerShell not found.		^									
40291	Policies\Microsoft\Windows\PowerShell not found.											
40292												
40293												
40294	294 run v.20200511											
40295	295 (Software, NTUSER.DAT) [Autostart] Get autostart key contents from Software hive											
40296												
40297	Microsoft/Windows/CurrentVersion/Run											
40298	Lastwrite lime 2023-06-29 08:01:532											
40299	VBOXITAY - SystemRoots(System32(VBOXITAY.exe											
40300	Securitynearth - swindris(SystemS2(SecuritynearthSystray.exe											
40302	Microsoft\Windows\CurrentVersion\Run has no subkeys Find the run command in											
40303	Find the Full command in											
40304	Microsoft\Windows\CurrentVersion\BunOnce software hives in current all											
40305	LastWrite Time 2019-12-07 09:17:27Z											
40306	Microsoft\Windows\CurrentVersion\RunOnce has no values. documents.											
40307	Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.											
40308	· · ·											
40309	Microsoft\Windows\CurrentVersion\RunServices not found.											
40310												
40311	Wow6432Node\Microsoft\Windows\CurrentVersion\Run											
40312	LastWrite Time 2019-12-07 09:17:27Z											
40313	Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no values.											
40314	Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no subkeys.											
40315												
40316	Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce											
40317	LastWrite Time 2019-12-07 09:17:27Z											
40318	Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.											
40319	Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.		\sim									
<			>									
Normal text f	file Ln: 40,297 Col: 1 Sel: 36 1 Windows (CR LF) UTF-8		INS									
- >	이 片· 🤶 📄 🍅 🧊 📝 🛛 💦 🖓 🖓 🖓	:52 7-2023	R.									

Startup Folder Analysis

Two location mention for startup folder.

- 1. C:\Cases\F\ProgramData\Microsoft\Windows\Start Menu
- 2. C:\Cases\F\Users\Denisha\AppData\Roaming\Microsoft\Windows

Open the given file location with ubuntu linux and use mnt directory, show mnt.csv file and using grep command show startup folders and scripts.

 Select forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/NTFS
 −
 □
 ×

forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases\$ cd ../../..
forensic@WIN-AJDB7GOIQEJ:/\$ cd /mnt/c/Cases/Analysis/NTFS
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/NTFS\$ ls -1

total 58904

-rwxrwxrwx 1 forensic forensic 60316000 Jul 1 16:42 <u>MFT.csv</u>

forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/NTFS\$ grep startup MFT.csv

14800,1, True,5280,1,.\Windows\WinSxS,amd64_microsoft_windows_s__32_kf_comm/nstartup_31bf3856ad364e35_10.0.19041.1_none_b2014b 56ea660ec9,,0,1,,True,False,False,True,False,False,None,Windows,2019-12-07 09:09:10.0828868,2023-06-29 05:03:11.0746274,2019-12-07 09:09:10.0828868,2023-06-29 05:03:11.0746274,2023-06-29 05:32:49.9658981,2023-06-29 05:03:11.0746274,2019-12-07 09:09:1 0.0828868,2023-06-29 05:03:11.0746274,0,185351776,551,,\$DSC,

14985,1,True,5280,1,.\Windows\WinSxS,amd64_microsoft-windows-s..estartup-change-pin_31bf3856ad364e35_10.0.19041.1237_none_665 f7346099d6350,,0,1,,True,False,False,True,False,False,None,Windows,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,20 21-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2023-06-29 05:32:50.0439843,2023-06-29 05:03:11.2621355,2021-10-06 13:5 4:23.7551351,2023-06-29 05:03:11.2621355,0,185379446,551,,\$DSC,

14986,1,True,14985,1,.\Windows\WinSxS\amd64_microsoft-windows-s..estartup-change-pin_31bf3856ad364e35_10.0.19041.1237_none_66 5f7346099d6350,f,,0,1,,True,False,False,True,False,False,None,DosWindows,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621 355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2023-06-29 05:32:50.0439843,2023-06-29 05:03:11.2621355,2021-10-0 6 13:54:23.7551351,2023-06-29 05:03:11.2621355,0,185379176,551,,\$DSC,

14987,1,True,14985,1,.\Windows\WinSxS\amd64_microsoft-windows-s..estartup-change-pin_31bf3856ad364e35_10.0.19041.1237_none_66 5f7346099d6350,r,,0,1,,True,False,False,True,False,False,None,DosWindows,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621 355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2023-06-29 05:32:50.0439843,2023-06-29 05:03:11.2621355,2021-10-0 6 13:54:23.7551351,2023-06-29 05:03:11.2621355,0,185379310,551,,\$DSC,

15238,1,True,5280,1,.\Windows\WinSxS,amd64_microsoft-windows-s..ngshandlers-startup_31bf3856ad364e35_10.0.19041.746_none_5227
01f930d0ca36,,0,1,,True,False,False,True,False,False,None,Windows,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,202
1-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,2023-06-29 05:32:50.1371573,2023-06-29 05:03:11.4972405,2021-10-06 13:52
:12.3431456,2023-06-29 05:03:11.4972405,0,185417952,551,,\$DSC,

15239,1,True,15238,1,.\Windows\WinSxS\amd64_microsoft-windows-s..ngshandlers-startup_31bf3856ad364e35_10.0.19041.746_none_522
701f930d0ca36,f,,0,1,,True,False,False,True,False,False,None,DosWindows,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.49724
05,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,2023-06-29 05:32:50.1371573,2023-06-29 05:03:11.4972405,2021-10-06
13:52:12.3431456,2023-06-29 05:03:11.4972405,0,185417687,551,,\$DSC,

15240,1,True,15238,1,.\Windows\WinSxS\amd64_microsoft-windows-s..ngshandlers-startup_31bf3856ad364e35_10.0.19041.746_none_522
701f930d0ca36,r,,0,1,,True,False,False,True,False,False,None,DosWindows,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.49724
05,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,2023-06-29 05:32:50.1371573,2023-06-29 05:03:11.4972405,2021-10-06
13:52:12.3431456,2023-06-29 05:03:11.4972405,0,185417829,551,,\$DSC,

15365,1,True,5280,1,.\Windows\WinSxS,amd64_microsoft-windows-s..restartup-baaupdate_31bf3856ad364e35_10.0.19041.1_none_ec3fd4 10728598b3,,0,1,,True,False,False,True,False,False,None,Windows,2019-12-07 09:10:43.7738833,2023-06-29 05:03:11.6235335,2019-12-07 09:51:57.4131230,2023-06-29 05:03:11.6235335,2023-06-29 05:32:50.1684200,2023-06-29 05:03:11.6235335,2019-12-07 09:51:5




Select forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/NTFS

06-29 05:31:49.2620434,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.2620434,2023-06-29 05:31:49.2620434,,2021-10-06 13:54: ^
19.8017226,2023-06-29 05:31:49.2620434,0,174624611,587,,\$DSC,

95546,1,True,24202,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c 1adbb3de92\r,fveapibase.dll,.dll,9395,1,,False,False,False,True,False,False,Archive,Windows,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.2620434,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.2620434,2023-06-29 05:31:49.2620434,,2021-10-06 13:54: 19.8017226,2023-06-29 05:31:49.2620434,0,174624639,587,,\$DSC,

95547,1,True,24201,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c 1adbb3de92\f,fveapibase.dll,.dll,16379,1,,False,False,False,True,False,False,Archive,Windows,2021-10-06 13:54:19.7861032,2023 -06-29 05:31:49.2620434,2021-10-06 13:54:19.7861032,2023-06-29 05:31:49.2620434,2023-06-29 05:31:49.2620434,,2021-10-06 13:54 :19.7861032,2023-06-29 05:31:49.2620434,0,174624723,587,,\$DSC,

95550,1,True,24202,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c 1adbb3de92\r,fveapi.dll,.dll,28304,1,,False,False,False,True,False,False,Archive,DosWindows,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.3104659,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.3104659,2023-06-29 05:31:49.3104659,,2021-10-06 13:54: 19.8017226,2023-06-29 05:31:49.3104659,0,174624787,587,,\$DSC,

105628,9,True,105627,9,.\AtomicRedTeam\atomics\T1547.001\src,bat<mark>startup</mark>.bat,.bat,34,1,,False,False,False,False,True,True,Arch ive,Windows,2023-06-28 17:57:10.9778236,,2022-04-27 12:44:48.0000000,2023-06-28 17:57:10.9778236,2023-06-28 17:57:10.9911164, 2023-06-28 17:57:10.9778236,2023-06-28 17:57:10.9778236,,17383848,374819591,2307,,,

105629,9,True,105627,9,.\AtomicRedTeam\atomics\T1547.001\src,jse<mark>startup</mark>.jse,.jse,44,1,,False,False,False,False,True,True,Arch ive,Windows,2023-06-28 17:57:10.9911164,,2022-04-27 12:44:48.0000000,2023-06-28 17:57:10.9911164,2023-06-28 17:57 ,2023-06-28 17:57:10.9911164,,17384288,374820360,2307,,,

105630,9,True,105627,9,.\AtomicRedTeam\atomics\T1547.001\src,vbs<mark>startup</mark>.vbs,.vbs,44,1,,False,False,False,False,True,True,Arch ive,Windows,2023-06-28 17:57:10.9911164,,2022-04-27 12:44:48.0000000,2023-06-28 17:57:10.9911164,2023-06-28 17:57:10.9911164, ,2023-06-28 17:57:10.9911164,,17384728,374821123,2307,,,

30028,2,False,601,1,.\PathUnknown\Directory with ID 0x00000259-00000001,startup_background.png,.png,175574,1,,False,False,Fal se,True,False,False,Archive|RecallOnOpen,Windows,2019-12-07 09:52:31.7251271,2023-06-29 05:04:24.6937921,2019-12-07 09:52:31. 7251271,2023-06-29 05:04:24.6937921,2023-06-28 16<mark>:07:58.5868695,2023-06-29 05:04:24.6937921,2023-06-28 16:07:58.5700946,2023-</mark> 06-29 05:04:24.6937921,2333896,437919618,1266,,,

forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/NTFS\$ _

Show the bat script in target

system





- **D**

 \times

Windows Services

Windows Server 2019 Datacenter Evaluation

^ □ 탓 ◁≈

Windows License valid for 161 days Build 17763.rs5_release.180914-1434

16-07-2023

A Windows service is an application that usually serves a core operating system function running in the background and has no user interface.

FTK Processes Performance Harry	Detaile	Services		
Processes Performance Users	Details	Services		
Name	PID	Description	Status	Group
AJRouter		AllJoyn Router Service	Stopped	LocalServiceN
🔍 ALG		Application Layer Gateway Service	Stopped	
AppIDSvc		Application Identity	Stopped	LocalServiceN
Appinfo		Application Information	Stopped	netsvcs
🔐 AppMgmt		Application Management	Stopped	netsvcs
AppReadiness		App Readiness	Stopped	AppReadiness
AppVClient		Microsoft App-V Client	Stopped	
AppXSvc		AppX Deployment Service (AppXSVC)	Stopped	wsappx
🔍 AudioEndpointBuilder		Windows Audio Endpoint Builder	Stopped	LocalSystemN.
Audiosrv 🔍		Windows Audio	Stopped	LocalServiceN
AxInstSV		ActiveX Installer (AxInstSV)	Stopped	AxInstSVGroup
See BFE	1468	Base Filtering Engine	Running	LocalServiceN
See BITS		Background Intelligent Transfer Servi	Stopped	netsvcs
See BrokerInfrastructure	740	Background Tasks Infrastructure Ser	Running	DcomLaunch
Contract BTAGService		Bluetooth Audio Gateway Service	Stopped	LocalServiceN
SthAvctpSvc		AVCTP service	Stopped	LocalService
See bthserv		Bluetooth Support Service	Stopped	LocalService
amsvc		Capability Access Manager Service	Stopped	appmodel
CaptureService		CaptureService	Stopped	LocalService
CaptureService_3dae8		CaptureService_3dae8	Stopped	LocalService
🔐 cbdhsvc		Clipboard User Service	Stopped	ClipboardSvc

🔿 Fewer details 🛛 🧠 Open Services

accounts_V...

ρ

Πi

e

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (29/0) View Help

Re	egistry hiv	/es (1)	Availal	ble bookmarks (29/0)				
[Find		
	Key nam	e						
۴	R B C						^	
	File	Safe	Boot					
•	🔹 🔺 🧧	= Serv	ices					
) 🚞 I	NET CLR D	Data				
	1) 🚞 J	NET CLR N	Networking				
) 🚞 J	NET CLR N	Networking 4.0.0.0				
) 🚞 J	NET Data	Provider for Oracle				
		• 🚞 ·	NET Data	Provider for SqlServer				
	1	· 🚍 .	NET Memo	ory Cache 4.0				
		• 🚞 .	NETFrame	work				
		1	394ohci				~	÷
<		. 3	Mara			>		
		-						
- B0	ookmark ir	nformati	on					
Hi	ve			C: \Cases \Analysis \Reg	istry\SYSTE	M		
Ci	ategory			Operating system				
Na	ame			Services				
Ke	ey path			ControlSet001\Services	s			
Sł	nort descr	iption		Service definitions and	parameter	s		
Lo	ong descri	ption						

e

As

3

⊟i

Type viewer

Dra	ag a colum	n header h	ere to grou	up by that	column							ρ
	Name	Descri	Display	Start	Servic	Name	Param	Group	Image	Servic	Require	
۴	RBC	A B C	A B C	=	=	=	=	A B C	A B C	A B C	R B C	^
	3ware			Boot	Kernel	2023-0	2019-1	SCSI miniport	System3 2\drivers \3ware.s ys			
	AarSvc	@%Syst emRoot %\syste m32\Aar Svc.dll,- 101	@%Syst emRoot %\syste m32\Aar Svc.dll,- 100	Manual	96	2019-1	2019-1		%Syste mRoot% \system 32\svch ost.exe -k AarSvcG roup -p	%Syste mRoot% \System 32\AarS vc.dll	SeImpers onatePrivil ege	
	ACPI		@acpi.in f,%ACPI .SvcDes c%;Micr osoft ACPI Driver	Boot	Kernel	2023-0	2023-0	Core	System3 2\drivers \ACPI.sy s			
	AcpiDev		@acpide v.inf,% AcpiDev.	Manual	Kernel	2019-1		Extende d Base	\System Root\Sy stem32\			~
Т	otal rows:	691									Export	?

07:54

5

へ 臣 d<mark>×</mark> 16-07-2023

 \times

Loaded the system hives in Registry Explorer



Q



Detecting and Analyzing scheduled tasks

Registry Explorer v1.6.0.0

– o ×

File Tools Options Bookmarks (29/0) View Help

Registry hives (2) Available bookmarks (59/0)	y	Values T	askCache										
Enter text to search Find	D	rag a colum	n header he	re to group	by that co	lumn							Q
		Version	Key Na	Path	Create	Last St	Last Stop	Task St	Last Ac	Source	Descrip	Author	
Key name	9	=	RBC	R B C	=	=	=	=	=	RBC	RBC	R B C	^
• • • • • • • • • • • • • • •	•	3	{001680 9F-CFDA -4F5B-A7 0B-84A7 5599B89 B} } {00446C F1-8668- 472D-BE DD-D0BB	Wicrosof t\Window s\Device Directory Client\Ha ndleWns Comman d \Microsof t\Window s\Registr y\RegIdl	2023-0			0	0	\$(@%sy stemroot %\syste m32\regi	\$(@%sy stemroot %\syste m32\regi	\$(@%sys temroot %\syste m32\regi	5
Bookmark information Hive		3	88DBA00 9} \$ {008539 BF-83F9- 4483-9E0 A-EEEE6	VMicrosof t\Window s\Shell\U pdateUse	2023-0			0	0	dle.dll,-6 01)	dle.dll,-6 02)	dle.dll,-6 00)	
Name Key path Load the Software hive on Registry Editor and click		3	EAC0A08 } } {02579F B1-5050-	rPictureT ask Microsof t\Window	2023-0			0	0			Furnat	~
Short description Itegistry Editor and energy Long description taskcache then click task	1	otai rows:										Ехроп	ſ
Key: Microsoft\Windows NT\CurrentVersion\Schedule\Task	Cach	e\Tasks							Va	lue: No	one Coll	apse all hi	ves
Selected hive: SYSTEM Last write: 29-06-2023 08:25:03 +00:00	Key	contains n	o values								Hidden	keys: 0	1
🚛 🔎 🛱 🤶 📻 崎 🗐 📝									-	~ 貯 🔩	08:44 16-07-2	023	

Administrator: Command Prompt

Folder: \	Nout Due Time	Ctature
1askname ====================================	Next Run Time	Status
User_Feed_Synchronization-{6C5B0DEF-65CE	16-07-2023 11:05:14	Ready
Folder: \Microsoft		
TaskName	Next Run Time	Status
INFO: There are no scheduled tasks prese	ntly available at yo	our access level.
Folder: \Microsoft\Windows		
TaskName INFO: There are no scheduled tasks prese Colder: \Microsoft\Windows\.NET Framewor TaskName	Next Run Time ====================================	Status
TaskName INFO: There are no scheduled tasks prese Folder: \Microsoft\Windows\.NET Framewor TaskName	Next Run Time 	Status
TaskName INFO: There are no scheduled tasks prese Folder: \Microsoft\Windows\.NET Framewor TaskName .NET Framework NGEN v4.0.30319	Next Run Time 	Status our access level. Status Ready
TaskName INFO: There are no scheduled tasks prese Folder: \Microsoft\Windows\.NET Framewor TaskName .NET Framework NGEN v4.0.30319 .NET Framework NGEN v4.0.30319 64	Next Run Time ====================================	Status our access level. Status Ready Ready
TaskName INFO: There are no scheduled tasks prese Folder: \Microsoft\Windows\.NET Framewor TaskName .NET Framework NGEN v4.0.30319 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 64 Critic	Next Run Time ====================================	Status our access level. Status Ready Ready Disabled Disabled
TaskName INFO: There are no scheduled tasks prese Folder: \Microsoft\Windows\.NET Framewor TaskName .NET Framework NGEN v4.0.30319 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 Critical	Next Run Time ====================================	Status our access level. Status Ready Ready Disabled Disabled
TaskName INFO: There are no scheduled tasks prese Folder: \Microsoft\Windows\.NET Framewor TaskName .NET Framework NGEN v4.0.30319 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 Critical Folder: \Microsoft\Windows\Active Direct	Next Run Time ntly available at yo k Next Run Time ====================================	Status our access level. Status Ready Ready Disabled Disabled
TaskName INFO: There are no scheduled tasks prese Folder: \Microsoft\Windows\.NET Framewor TaskName .NET Framework NGEN v4.0.30319 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 Critical Folder: \Microsoft\Windows\Active Direct TaskName	Next Run Time ====================================	Status our access level. Status Ready Ready Disabled Disabled ot Services Client Status
TaskName INFO: There are no scheduled tasks prese Folder: \Microsoft\Windows\.NET Framewor TaskName .NET Framework NGEN v4.0.30319 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 Critical Folder: \Microsoft\Windows\Active Direct TaskName AD RMS Rights Policy Template Management	Next Run Time ====================================	Status our access level. Status Ready Disabled Disabled Disabled Disabled Disabled
TaskName INFO: There are no scheduled tasks prese Folder: \Microsoft\Windows\.NET Framewor TaskName .NET Framework NGEN v4.0.30319 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 Critical Folder: \Microsoft\Windows\Active Direct TaskName AD RMS Rights Policy Template Management AD RMS Rights Policy Template Management	Next Run Time 	Status our access level. Status Ready Disabled Disabled Disabled Status Disabled Ready Disabled Ready
TaskName INFO: There are no scheduled tasks prese Folder: \Microsoft\Windows\.NET Framewor TaskName .NET Framework NGEN v4.0.30319 .NET Framework NGEN v4.0.30319 64 .NET Framework NGEN v4.0.30319 64 Critic .NET Framework NGEN v4.0.30319 Critical Folder: \Microsoft\Windows\Active Direct TaskName AD RMS Rights Policy Template Management AD RMS Rights Policy Template Management Eolder: \Microsoft\Windows\AppTD	Next Run Time ====================================	Status our access level. Status Ready Disabled Disabled Disabled Status Disabled Ready Disabled Ready

Open cmd as a Administrator and type this command.



þ

_

 \times

 $\hat{}$

~

1

C:\Cases\Analysis\Registry\SOFTWARE.txt - Notepad++ [Administrator]	– 0 ×
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window	+ 🔻 🗙
🕞 😑 🗄 👒 🕞 🦾 🖕 🖌 🐚 節 📮 🗲 🖬 🍇 🔍 🔍 🖼 🖼 🚍 💷 🛯	3 🂫 🖆 👁 💿 🗈 🕨 🃴
🔚 all 🗵 🔚 DEFAULT.txt 🗵 🔚 NTUSER.DAT.txt 🗵 🔚 SECURITY.txt 🗵 🔚 SOFTWARE.txt 🗵 🔚 SAM.	xt 🗷 🔚 UsrClass.dat.txt 🗷 🔚 SYSTEM.txt 🗵 🔚 SYSTEM 🗵
40484	^
40485 9 - LastWrite time: 2023-06-28 16:32:41Z	
40486 Path: file:///C:\[af17ba98-35d5-43f9-a08a-ffba85076e9d]\Users\	
40487	
40488	
40489 taskcache v.20200427	
40490 (Software) Checks laskcache (free root keys (hot subkeys)	
40492 MicrosoftEdgeUpdateTaskMachineCore	
40493 LastWrite: 2023-06-28 16:05:57Z	
40494 Id: {C32E8E08-558A-4F92-BAE5-3BEFEFE1827B}	Open the software hives with
40495 Task Reg Time: 2023-06-28 16:05:57Z	Open the software myes with
40496 Task Last Run: 2023-06-29 08:08:14Z	Notepad++ and search
40497 Task Completed: 2023-06-29 08:08:192	
40498	taskcache and show this
40499 MicrosoftEdgeUpdateTaskMachineUA	Result
40500 LastWrite: 2023-06-28 16:05:572	ixeouit.
40501 1d: {D30B1923-95AE-4E/C-9FFD-E4D3569602/C}	
40502 Task Reg Time: 2023-06-20 10:05:572	
40504 Task Completed: 2023-06-29 08:12:327	
40505	
40506 OneDrive Reporting Task-S-1-5-21-3331464962-214784631-3394824829	-1001
40507 LastWrite: 2023-06-28 16:25:12Z	
40508 Id: {FB7019CD-AADF-4803-AE0C-148AD2A4DDF1}	×
<	>
Search results - (3 hits)	×
Line 40489: taskcache v.20200427	<u>^</u>
Line 40490: (Software) Checks TaskCache\Tree root keys (not subkeys	
Line 40520: (Software) Checks TaskCache\Tasks subkeys	
Search "task cache" (0 hits in 0 files of 9 searched)	
Normal text file Iength : 25,34,532 lines : 41,650 Ln : 40,489 Col : 1	U Sel : 9 1 Windows (CR LF) UTF-8 INS
- Fi Cê <u>Ei</u> 😂 🔛 🔤	ヘ E 4 <mark>× 16-07-2023</mark> ●

Analysis with Sysinternals Autorun tool

Autoruns for Windows - Sysinternals | Microsoft Learn

	Usage Autorun tools use for detect and Analyze the aut
Filter by title	Autorunse Usage file like malware and virus Affected file run file
lome	Download hoot time etc
ownloads	
Downloads	By Mark Russinovich
File and Disk Utilities	Published: June 27, 2023 Download the too
Networking Utilities	from microsoft
Process Utilities	
Process Utilities	Run now from Sysinternals Live ☞.
AutoRups	
racontanto	
Handle	Z Autoruns - Sysintemals: www.sysinternals.com (Administrator) (REDMOND/marioh) - C
Handle	Autorums - Sysinternals: www.sysinternals.com (Administrator) (REDMOND/umarioh) - C File Search Entry User Options Category Help Ch I O O O O O I III III III O O O O O O
Handle ListDLLs	Autoruns - Sysintemals: www.sysintemals.com (Administrator) (REDMOND/marioh) File Search Entry User Options Category Help C Applnit Known DLLs & WinLogon Winsock Providers Print Monitors S LSA Providers Network Providers WM4
Handle ListDLLs Portmon	Autorums - Sysinternals: www.sysinternals.com (Administrator) (REDMOND/umarioh) - C File Search Entry User Options Category Help C Applnit & Known DLls & WinLogon © Winsock Providers @ Print Monitors © LSA Providers © Network Providers © WM4 C File Search Entry & Codecs © Boot Execute © Image Path
Handle ListDLLs Portmon ProcDump	Autorums - Sysintemals: www.sysintemals.com (Administrator) (REDMOND/marioh) File Search Entry User Options Category Help Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path Image: Path
Handle ListDLLs Portmon ProcDump Process Explorer	Autoruns - Sysintemals www.sysintemals.com (Administrator) (REDMOND/marioh) - C File Search Entry User Options Category Help
Handle ListDLLs Portmon ProcDump Process Explorer	Autoruns - Sysintemals.com (Administrator) (REDMOND/marioh) He Search Entry Use Options Category Help Description Applnit Microsoft Segion Microsoft Segion Microsoft Segie Microsof
Handle ListDLLs Portmon ProcDump Process Explorer Process Monitor	Autoruns - Sysinternals: www.sysinternals.com (Administrator) (REDMOND/marioh) File Search Entry User Options Category Help Compared Provides Category Help HELMSOFTWARE/HerosoftWeindows/CamentVersion/Run Compared Provides Category Help HELMSOFTWARE/MicrosoftCategory Category Help HELMSOFTWARE/MicrosoftCategory Provides Category Help HELMSOFTWARE/MicrosoftWindows/CamentVersion/Run HELMSOFTWARE/MicrosoftCategory Provides Category Provides HELMSOFTWARE/MicrosoftWindows/CamentVersion/Run HELMSOFTWARE/MicrosoftWindows/CamentVersion/Run HelpHSOFTWARE/MicrosoftWindows/CamentVersion/Run HelpHSOFTWARE/MicrosoftWindows/CamentVersion/Run HelpHSOFTWARE/MicrosoftWindows/CamentVersion/Run HelpHSOFTWARE/MicrosoftWindow
Handle ListDLLs Portmon ProcDump Process Explorer Process Monitor PsExec	Autorums - Sysinternals: www.sysinternals.com (Administrator) (REDMOND/marioh) - File Search Entry User Options Category Help File Search Entry User Options Category Help File Search Entry User Options Category Help File Search Entry
Handle ListDLLs Portmon ProcDump Process Explorer Process Monitor PsExec	Autorum - Sysintemals www.sysintemals.com (Administrator) (REDMOND/marioh) - File Search Entry Use Options Catagory Help Image: Delta Image: Delta<
Handle ListDLLs Portmon ProcDump Process Explorer Process Monitor PsExec PsGetSid	Autorums - Sysintemals.com (Administrator) (REDMOND/marioh) - File Search Entry User Options Category Help File Search Entry User Options Category Help File Search Entry User Options Category Help File Search Entry User Options Entry Windows Providers Print Monitors ElsA Providers Network Providers While Mine File Search Entry Entr
Handle ListDLLs Portmon ProcDump Process Explorer Process Monitor PsExec PsGetSid PsKill	Autorum - Sysintemals.com (Administrator) (REDMOND/marich) - File Search Entry User Options Catagory Help File Search Explore Unitscope Winloogon Winloogon Winloogon Search Distry Description Publisher Image Path File Hattonums Entry Description Publisher Image Path Colorest/manch/AgpDatal_Joca/APA Colorest/manch/AgpDatal_Joca/APA File Colorest/Marcold/Teld Microsoft Telenes Microsoft Corporation C/Hosers/manch/AgpDatal_Joca/APA File Colorest/Marcold/Teld Microsoft OneDrive Winfield/ Microsoft Corporation C/Hosers/manch/AgpDatal_Joca/APA File Microsoft/Microsoft/Microsoft/Microsoft/Microsoft/Microsoft/Microsoft/Microsoft/Microsoft/M
Handle ListDLLs Portmon ProcDump Process Explorer Process Monitor PsExec PsGetSid PsKill PsList	Autoruss - Sysietemists www.sysietemist.com (Administrator) (REDMOND/unarioh) Pare Sarch Entry User Options Category Help Pare Sarch Entry User Options Category Pare Sarch Explore Pare Options Category Pare Sarch Entry Description Pare Sarch Entry User Options Variation Options Pare Sarch Entry User Options Variation Option Pare Sarch Entry User Options Pare Sarch Entry User Option Pare Sarch Entry Entry Entry User Categor

J/

2019

ᄟ

リッ

16-07-2023

<mark> </mark> 🛃 🔄 🛨			Manage	Autoruns						_	ð	×
File Home Share	View	1	Application Tools									~ 🕐
\leftarrow \rightarrow \checkmark \uparrow \square \Rightarrow This	s PC ≯ Do	wnlo	oads > Autoruns						~ Ū	Search Autoruns		2
📃 Desktop 🛛 🖈 ^	Name		^		Date	modified	Туре	Size				
🕂 Downloads 🖈	😰 autor	runs			27-06	-2023 16:55	Compiled HTML	25 KB				
🔮 Documents 🖈	🔤 Auto	runs	5		27-06	-2023 16:55	Application	1,742 KB				
📰 Pictures 🛛 🖈	🚾 Auto	rune	-64		27-06	2023 16:55	Application	1,934 KB				
Evidence	🔤 Aut		Open			2023 16:55	Application	2,040 KB				
Execution	🖅 aut	•	Run as administra	tor		2023 16:55	Application	702 KB				
NTES	🖅 aut	2	Edit with Notepad	++		2023 16:55	Application	785 KB				
Registry	🖅 aut		Troubleshoot com	patibility		2023 16:55	Application	808 KB				
Registry	Eul		Pin to Start			2023 16:54	Text Document	8 KB				
💻 This PC		Ē	Share									
3D Objects			Give access to		>							
Cesktop			Pin to taskbar									
Documents			Restore previous v	ersions								
🕂 Downloads			Send to		>		Open the to	ol as run	Admir	nistrator		
b Music			Cut									
Pictures			Cut									
Videos			сору									
SDT x64FREE EN			Create shortcut									
CD Drive (D:) Vir			Delete									
Downloads (\)\\			Rename									
			Properties									
💣 Network												
~												
8 items 1 item selected 1	.88 MB											:==
🖬 🔿 🖬 🌔	6 🖡		6	<u> </u>						ヘ 및 4 00 00 00 00 00 00 00 00 00 00 00 00 0	9:16 17-2023	₽n

🚾 Autoruns - Sysinternals: www.s	sysinternals.com (4	Administrator) [WIN-AJ[DB7GOIQEJ\Adr	ministrator]						_	ð	\times
File Search Entry User O	ptions Category	/ Help										
Open Ctrl+O Save Ctrl+S			• Quick Filter									
Analyse Offline System	ecute	Image Hijacks	AppInit	🔒 Known DLLs	P_	Winlogon	🔍 Wi	nsock Provi	ders	🖶 Р	rint Moni	itors
Analyze Offline System	_	🖵 Net	work Providers			🖻 WMI			0	Office	2	
Compare	Logon	🐂 Explorer	🥭 Inte	ernet Explorer		Scheduled Task	s	🔍 Sen	ices	0	Drive	rs
C Refresh F5	_		Description			Publisher			Image Pa	ath		^
	-											
Cancel ESC	Set\Control\Safe	Boot\AlternateShell										
Exit	Harris NTV Criment	·//	Windows Com	mand Processor		(Verified) Micro	osoft Wind	ows	C:\Wind	ows\sys	stem32\c	md.e
30000	adows INT (Current	tversion\winiogon\Aite	Windows Com	mapleshells		(Verified) Micro	osoft Wind	OWE	C:\Wind		tem32\c	md e
HKLM\SOFTWARE\Microsoft\	Active Setup\Insta	lled Components	Windows com	internet roccasor		(venned) where		0113	C. (Willia	5 vv 3 (3y.	seemsz (e	mane
✓ N/a			Microsoft .NET	I IE SECURITY REGIS	TRATION	(Verified) Micro	osoft Corp	oration	C:\Wind	ows\Sy	stem32\n	nscor
HKLM\SOFTWARE\Wow6432N	lode\Microsoft\Ad	tive Setup\Installed Cor	mponents									
🗹 🗟 n/a			Microsoft .NET	FIE SECURITY REGIS	TRATION	(Verified) Micro	osoft Corp	oration	C:\Wind	ows\Sy	stem32\n	nscor
🐂 Explorer												
C Internet Explorer												
Scheduled Tasks												
lask Scheduler		01.10				04 - 15 - 15 A - 1	6 M.C. 1					
Microsoft/Windows/Sei	rver Manager\Clea	nupOldPerfLogs	Microsoft ® C	onsole Based Script	Host	(Verified) Micro	osoft Wind	ows	C:\Winde	ows\sys	stem32\c	script
	rtware inventory L	ogging\Collection	windows Com	imand Processor		(verified) Micro	osort wind	ows	C:\Wind	ows\sys	stem32\C	ma.e 🗸
												-





	Autoruns - S	ysinternals: www.sysinternals.com (Administrator) [WI	N-AJDB7GOIQEJ\/	Administrator]					- 6	1 ×	
(Offline Systen	n	×								
1	Select the dire	ectories of the offline system:									
	System Root:	F:\Windows		🚯 Known DLLs	🍫 Winlogon	🔍 🖉 V	Vinsock Provid	ders	🔓 Print I	Monitors	
	Line Des film			rs	🖶 WMI			0	Office		
	User Profile:	F: Users (Denisna		nternet Explorer	Scheduled Ta	sks	i Serv	ices	<u> </u>	Drivers	
					Publisher			Image Pat	th		^
4		ок	Cancel								
	Micros	softEdgeAutoLaunch_1ED6AFCC191394652DA0C4ECFC	.73 Microsoft E	dge	(Verified) Mi	crosoft Cor	poration	C:\Progra	m Files (x8	δ)\Micros	1
	🗹 📄 OneDr	rive	Microsoft O	neDrive	(Verified) Mi	crosoft Cor	poration	C:\Users\I	Denisha\Ap	opData\Lo	:
Ш°	HKLM\Syste	m\CurrentControlSet\Control\Terminal Server\Wds\rd	lpwd\StartupProgr	rams							
	🗹 💷 rdpclir	ρ	RDP Clipbo	ard Monitor	(Not Verified) Microsoft	Corporati	C:\Windo	ws\system	32\rdpclip	
Ľ	HKLM\SOFT	WARE\Microsoft\Windows\CurrentVersion\Run									
	Securi	/tyHealth	Windows Se	acurity notification icon	(Not Verified) Microsoft	Corporati	C:\Windo	ws\system	32\Securi	
	🗹 🧐 VBoxT	ray	VirtualBox @	Suest Additions Tray Applicati	(Not Verified) Oracle an	d/or its aff	C:\Windo	ws\system	32\VBoxT	
Ľ	HKLM\SOFT	WARE\Microsoft\Windows NT\CurrentVersion\Winlog	jon\Shell								
	🗹 📻 explor	/er.exe	Windows Ex	kplorer	(Not Verified) Microsoft	Corporati	C:\Windo	ws\explore	r.exe	
Ľ	HKLM\SYST	EM\CurrentControlSet\Control\SafeBoot\AlternateShe	All I								
	🗹 🔤 cmd.e	xe	Windows C	ommand Processor	(Not Verified) Microsoft	Corporati	C:\Windo	ws\system	32\cmd.e	
Ľ	HKLM\Softv	vare\Microsoft\Windows NT\CurrentVersion\Winlogor	n\UserInit								
	🗹 🔳 C:\Wir	ndows\system32\userinit.exe	Userinit Log	jon Application	(Not Verified) Microsoft	Corporati	C:\Windo	ws\system	32\userin	>
<										>	

OneDrive	Size:	2,311 K
Microsoft OneDrive	Time:	28-06-2023 16:25
(Verified) Microsoft Corporation	Version:	21.220.1024.0005

🥭 🥅 🍅

"C: \Users \Denisha \AppData \Local \Microsoft \OneDrive \OneDrive.exe" /background

<u>...</u>

01**%**____

9



ρ

Ц





🔤 Autoru	ıns - Sysinternals: wwv	v.sysinternals.com (Administrator) [WIN	AJDB7GOIQEJ\Ad	ministrator]						—	ð ×	<
File Se	arch Entry User	Options Categor	y Help										
	ひ 🗅 ク [<u></u>		P Quick Filter									
G C	odecs 🔅 Boot	t Execute	lmage Hijacks	C AppInit	🚯 Known DLL	s 🍫	Winlogon	🔍 Wi	insock Provi	ders	🖶 Prin	t Monitors	
	🕀 LSA Provide	ers	₽	Network Providers	;		🖶 WMI			0	Office		
6	Everything	🖺 Logon	🐂 Explorer	🥭 Int	ernet Explorer		Scheduled Task	cs	🔍 Serv	vices	Q	Drivers	
Autoruns	Entry			Description			Publisher			Image P	ath		^
Logon	-									2			
🔐 нкси	SOFTWARE\Microsoft	t\Windows\Current	Version\Run										
	MicrosoftEdgeAutoLa	unch_1ED6AFCC191	394652DA0C4ECFC7	Microsoft Edg	e		(Verified) Micr	osoft Corp	oration	C:\Progr	am Files ()	(86)\Micros	s
	OneDrive			Microsoft One	eDrive		(Verified) Micr	osoft Corp	oration	C:\Users	\Denisha\	AppData\L	¢
HKLM	\System\CurrentContr	rolSet\Control\Term	inal Server\Wds\rdp	vd\StartupProgram	ns								
	rdpclip			RDP Clipboard	d Monitor		(Not Verified)	Microsoft (Corporati	C:\Wind	ows\syste	m32\rdpcli	F I
	\SOFTWARE\Microsof	t\Windows\Current	Version\Run										
	SecurityHealth			Windows Sect	urity notification ico	on 	(Not Verified)	Microsoft (Corporati	C:\Wind	ows\syste	m32\Securi	r
	VBoxTray		· · · · · · · · · · · · · · · · · · ·	VirtualBox Gu	est Additions Tray A	Applicati	(Not Verified)	Oracle and	/or its aff	C:\Wind	ows\syste	m32\VBox1	
	SOF I WARE WICTOSOF	t/windows ivi /Cun	rentversion\winlogo	Windows Evol	orer		(Not Verified)	Microsoft (Corporati	C:\Wind	ows\evolo	rer eve	
	SYSTEM\CurrentCont	trolSet\Control\Safe	Boot\AlternateShell	Windows Expi	orei		(Not venned)	WIICIOSOTE C	corporati	C. (Willia	ows (explo	Tenexe	
	cmd.exe			Windows Con	nmand Processor		(Not Verified)	Microsoft (Corporati	C:\Wind	ows\svste	m32\cmd.e	e
	\Software\Microsoft\W	Windows NT\Curren	tVersion\Winlogon\l	JserInit									
	C:\Windows\system32	\userinit.exe	-	Userinit Logor	n Application		(Not Verified)	Microsoft (Corporati	C:\Wind	ows\syste	m32\userin	i 🗸
<												>	
							Show a	11 autor	runs fil	e like			
	OneDrive	Size:	2,311 K								1		
	Microsoft OneDrive	Time:	28-06-2023 16:25				malwar	e, viri	is file,	boot le	oad		
	(Verified) Microsoft Cor	rporation Versio	n: 21.220.1024.0005				file.						
	"C: (Users (Denisha (App	Data (Local (Microsoft)	(OneDrive (OneDrive.e)	e ⁻ /background									







へ 〒 ⊄<mark>≥</mark> 09:23 16-07-2023 🖣

Event log Analysis

The main purpose of the event logs is to provide information to administrators and users. They are structured in five levels (information, warning, error, critical, and success/failure audit). In terms of forensic analysis, this is a valuable source to understand the course of actions on a system.

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

\bigcirc what is mean windows $\leftarrow \rightarrow \mathbf{C}$ \square ulti	s × G english to gujarati tran: × G event log analysis in di × 🖗 W	Vindows Security Log ×	+ ~ - 0 ×		
Security Log Windows Webinars Training Encyclopedia	SharePoint SQL Server Exchange Training Tools News Encyclopedia Quick Reference Book Image: Comparison of the server of the s	sletter Webinars Blog	-		
Event IDsAll Event IDsAudit Policy	4624: An account was successfully logged on On this page	Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022		
Go To Event ID:	 Description of this event Field level details Examples Discuss this event 	Category • Subcategory Type	Logon/Logoff • Logon Success		
Security Log Quick Reference Chart	 Discuss this event Mini-seminars on this event This is a highly valuable event since it documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. You can tie this event 	Corresponding events in Windows 2003 and before nt to logoff events 4634 at	528 , 540		
	Win2012 adds the Impersonation Level field as shown in the example. Win2016/10 add further fields explained below.	nple.			
	Free Security Log Resources by Randy	Enter the eve	nt ID and show the		
Download now!	 Free Security Log Quick Reference Chart Windows Event Collection: Supercharger Free Edition Free Active Directory Change Auditing Solution Free Course: Security Log Secrets 	detail.			
	Description Fields in 4624				
Cookies help u	s deliver the best experience on our website. By using our webs	ite, you agree to the ι	Ise of cookies. Accept		
O Type here to	o search 📮 📮 📋 🍅	🗘 🎇 🚫	▲ 小 記 d ³¹ 16:31 16:07-2023		

Analyzing Windows event logs with EventLogExplorer and EvtxCmd

📙 🌛 📙 🖛 logs					_	ð	\times
File Home Share	View						~ 🕐
← → × ↑ 📙 C:\Ca	ses\F\Windows\System32\winevt\logs				✓ ひ Search logs		Q
^	Name	Date modified	Type	Size			^
📌 Quick access			.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	0.22			
🔜 Desktop 🛛 🖈	Application	29-06-2023 09:07	Event Log	1,092 KB			
🚽 Downloads 🖈	Microsoft-Client-Licensing-Platform%4A	29-06-2023 09:07	Event Log	1,028 KB			
🖾 Documents 🖈	Microsoft-Windows-AAD%4Operational	28-06-2023 16:31	Event Log	68 KB			
	Microsoft-Windows-Application-Experie	29-06-2023 09:07	Event Log	68 KB			
Pictures 💉	Microsoft-Windows-AppModel-Runtime	29-06-2023 09:07	Event Log	1,028 KB			
Evidence	Microsoft-Windows-AppReadiness%4Ad	28-06-2023 18:13	Event Log	1,092 KB	Show The All		
Execution	Microsoft-Windows-AppReadiness%4Op	28-06-2023 18:13	Event Log	68 KB	Event Log Of		
NTFS	Microsoft-Windows-AppXDeployment%	29-06-2023 09:07	Event Log	1,028 KB			
Registry	Microsoft-Windows-AppXDeploymentSe	29-06-2023 09:07	Event Log	5,124 KB	Target system.		
	Microsoft-Windows-AppxPackaging%40	29-06-2023 09:07	Event Log	1,028 KB			
💻 This PC	Microsoft-Windows-Audio%4CaptureM	28-06-2023 16:05	Event Log	68 KB			
3D Objects	🛃 Microsoft-Windows-Audio%4Operational	28-06-2023 16:05	Event Log	68 KB			
Desktop	🛃 Microsoft-Windows-Authentication User	28-06-2023 16:31	Event Log	68 KB			
Bocuments	🛃 Microsoft-Windows-BackgroundTaskInfr	28-06-2023 18:13	Event Log	68 KB			
Develanda	😹 Microsoft-Windows-Biometrics%40pera	29-06-2023 09:07	Event Log	68 KB			
Downloads	🛃 Microsoft-Windows-BitLocker%4BitLock	29-06-2023 09:07	Event Log	68 KB			
Music	🔠 Microsoft-Windows-Bits-Client%40perat	29-06-2023 09:07	Event Log	1,028 KB			
Pictures	Microsoft-Windows-CloudStore%40pera	29-06-2023 09:07	Event Log	68 KB			
🗃 Videos	Microsoft-Windows-CodeIntegrity%4Op	29-06-2023 09:07	Event Log	68 KB			
SDT_x64FREE_EN	😹 Microsoft-Windows-Containers-BindFlt	29-06-2023 09:07	Event Log	68 KB			
CD Drive (D:) Vir	Microsoft-Windows-Containers-Wcifs%4	29-06-2023 09:07	Event Log	68 KB			
System Perer us	Microsoft-Windows-CoreSystem-SmsRo	29-06-2023 09:07	Event Log	68 KB			
System Reserved	Microsoft-Windows-Crypto-DPAPI%4Op	29-06-2023 09:07	Event Log	68 KB			
Local Disk (F:) 101 items							

1-7

01**5**-

10:34 16-07-2023

^ 🛐 🖫 🗤



e

3

Ц

😥 Untitled.ELX - Event Lo	og Explorer							— C) ×			
<u>F</u> ile <u>D</u> atabase <u>T</u> ree <u>L</u> o	og <u>V</u> iew <u>E</u> vent	<u>A</u> dvanced <u>W</u> ir	ndow <u>H</u> elp									
📪 🐺 🔒 — 🖻	- 🗄 🍸	<load filter=""></load>	- 😿	े 🗟 🔊 🚪	🛉 🖻 🚔							
Objects tree X	Application.evt	x ×							-			
Search	₩ 4 > >>	Ju 291	√ 1			UTC						
> ····· 🖵 WIN-AJDB7GOIQ		Date	Time	Event	Source	Category	User	Computer	^			
> ····· 🛅 Log Files	tion	29-06-2023	08:14:51	16384	Microsoft-Windows	None	N/A	DESKTOP-MD2HC	CP T			
> ····· 😁 Task templates	tion	29-06-2023	08:13:57	15	SecurityCenter	None	N/A	DESKTOP-MD2HC	CPT			
	tion	29-06-2023	08:13:25	15	SecurityCenter	None	N/A	DESKTOP-MD2HC	СРТ			
	tion	29-06-2023	08:12:33	16394	Microsoft-Windows	None	N/A	DESKTOP-MD2HC	CPT			
	tion	29-06-2023	08:12:32	0	edgeupdate	None	N/A	DESKTOP-MD2HC	CPT			
	tion	29-06-2023	08:11:49	16384	Microsoft-Windows	None	N/A	DESKTOP-MD2HC	CPT			
Open the	tion	29-06-2023	08:09:53	16394	Microsoft-Windows	None	N/A	DESKTOP-MD2HC	CPT			
Errort log	tion	29-06-2023	08:09:45	16384	Microsoft-Windows	None	N/A	DESKTOP-MD2HC	CPT			
Event log	tion	29-06-2023	08:08:16	16394	Microsoft-Windows	None	N/A	DESKTOP-MD2HC	CP T			
explorer	tion	29-06-2023	08:08:11	15	SecurityCenter	None	N/A	DESKTOP-MD2HC	PT			
andlaad	tion	29-06-2023	08:08:08	15	SecurityCenter	None	N/A	DESKTOP-MD2H0	СРТ			
and Ioau	tion	29-06-2023	08:06:55	16384	Microsoft-Windows	None	N/A	DESKTOP-MD2HC	CPT			
the first	tion	29-06-2023	08:06:07	16394	Microsoft-Windows	None	N/A	DESKTOP-MD2HC	CPT			
orrorat	tion	29-06-2023	08:05:42	16384	Microsoft-Windows	None	N/A	DESKTOP-MD2HC	CPT			
event.									~			
	<								>			
	Description								×			
< >	Description The description for Event ID (15) in Source (SecurityCenter) could not be found. Either the component that raises this event is not installed on the computer or the installation is corrupted. You can install or repair the component or try to change Description Server. The following information was included with the event: Windows Defender Description Description											
								11.10)			
	e 📄		ie 😥	>			^ 🚳	記 4× 16-07-2	, 023 🖓			

~

File

Share View Home

л.

ρ

e

đ

 \times

~ 🕐

 \mathbf{A}

 \checkmark :==

 \square

Q

_

← → × ↑ 📙 C:\Too	ls\Get-ZimmermanTools				~ 0	Search Get-ZimmermanTools
📰 Pictures 🛛 🖈 ^	Name	Date modified	Туре	Size		
Evidence	EvtxECmd	28-06-2023 13:40	File folder			
Execution	EZViewer	28-06-2023 13:40	File folder			
NTFS		28-06-2023 13:41	File folder			
Registry	iisGeolocate	28-06-2023 13:44	File folder			
	JumpListExplorer	28-06-2023 13:41	File folder			Open the
This PC	MFTExplorer	28-06-2023 13:41	File folder			command hase
3D Objects	RECmd	28-06-2023 13:41	File folder			
📃 Desktop	RegistryExplorer	28-06-2023 13:42	File folder			EvtxECmd.
🔮 Documents	SDBExplorer	28-06-2023 13:42	File folder			
🖶 Downloads	ShellBagsExplorer	01-07-2023 10:36	File folder			
b Music	SQLECmd	28-06-2023 13:43	File folder			
Dictures	📊 TimelineExplorer	01-07-2023 05:43	File folder			
Fictures	XWFIM	28-06-2023 13:44	File folder			
Videos	🗔 !!!RemoteFileDetails	28-06-2023 13:44	CSV File	5 KB		
SDT_x64FREE_EN	😚 AmcacheParser	21-05-2023 11:49	Application	4,661 KB		
🚳 CD Drive (D:) Vir	AppCompatCacheParser	07-03-2023 15:13	Application	4,523 KB		
🕳 System Reserved	m bstrings	20-05-2022 12:38	Application	3,997 KB		
Local Disk (F:)	ChangeLog	28-06-2023 13:44	Text Document	33 KB		
Local Disk (G:)	📓 Get-ZimmermanTools	18-05-2023 14:24	Windows PowerS	24 KB		
Downloads (\\\/	💰 JLECmd	13-03-2023 17:06	Application	4,792 KB		
E Downloads (((v)	🕎 LECmd	04-03-2023 10:30	Application	5,063 KB		
💣 Network	MFTECmd	20-10-2022 13:37	Application	4,409 KB		
~	PECmd	28-01-2022 12:08	Application	3,885 KB		
32 items 1 item selected	—					

ia 😓

(2)



🗿 Untitled ELX - Event Log Explorer Administrator: C:\Windows\System32\cmd.exe \times File Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. Ob C:\Tools\Get-ZimmermanTools\EvtxECmd>EvtxECmd.exe SeDescription: EvtxECmd version 1.5.0.0 Author: Eric Zimmerman (saericzimmerman@gmail.com) https://github.com/EricZimmerman/evtx Examples: EvtxECmd.exe -f "C:\Temp\Application.evtx" --csv "c:\temp\out" --csvf MyOutputFile.csv EvtxECmd.exe -f "C:\Temp\Application.evtx" --csv "c:\temp\out" EvtxECmd.exe -f "C:\Temp\Application.evtx" --json "c:\temp\jsonout" Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes Usage: EvtxECmd [options] Options: -f <f> File to process. This or -d is required Directory to process that contains evtx files. This or -f is required -d <d> Directory to save CSV formatted results to --csv <csv> File name to save CSV formatted results to. When present, overrides default name --csvf <csvf> Directory to save JSON formatted results to --json <json> --jsonf <jsonf> File name to save JSON formatted results to. When present, overrides default name Directory to save XML formatted results to --xml <xml> --xmlf <xmlf> File name to save XML formatted results to. When present, overrides default name --dt <dt> The custom date/time format to use when displaying time stamps [default: yyyy-MM-dd HH:mm:ss.ffffff]] List of Event IDs to process. All others are ignored. Overrides --exc Format is 4624,4625,5410 --inc <inc> or try to change Description Server. The following information was included with the event: Windows Defender Description / Data > Juliu 17703.133 Telease, 100314 🔨 🚮 🖫 ላ 🗙 ρ e

😥 Untitled ELX - Event Log Explorer

<u>F</u>il

Ob

ρ

Administrator: C:\Windows\System32\cmd.exe

	Nations (Systems): (entailede		- ^
fj tdt <tdt></tdt>	When true, export all available data when usingjson [defau The number of seconds to use for time discrepancy detection	ult: False] [default: 1]	
met)b maps <maps></maps>	When true, show metrics about processed event log [default:] The path where event maps are located. Defaults to 'Maps' fol	[rue] lder where program was executed	
Sevss	<pre>[default: C:\Tools\Get-ZimmermanTools\EvtxECmd\Maps] Process all Volume Shadow Copies that exist on drive specifie</pre>	ed by -f or -d [default: False]	
>dedupe >sync	Deduplicate -f or -d & VSCs based on SHA-1. First file found If true, the latest maps from https://github.com/EricZimmerma downloaded and local maps updated [default: False]	wins [default: True] an/evtx/tree/master/evtx/Maps are	
debug trace	Show debug information during processing [default: False] Show trace information during processing [default: False]	Create the Event log folder	
version -?, -h,help	Show Version information Show help and usage information	in Analysis folder then After	
-f or -d is requi	red. Exiting	this command is execute.	
C:\Tools\Get-Zimm ntlogs EvtxECmd version :	ermanTools\EvtxECmd>EvtxECmd.exe -d C:\Cases\F\Windows\System32 1.5.0.0	2\winevt\logscsv C:\Cases\Analys	sis\Eve
Author: Eric Zimme https://github.com	erman (saericzimmerman@gmail.com) m/EricZimmerman/evtx		
Command line: -d	C:\Cases\F\Windows\System32\winevt\logscsv C:\Cases\Analysis	s\Eventlogs	
CSV output will be	e saved to C:\Cases\Analysis\Eventlogs\20230716112553_EvtxECmd	_Output.csv	

 $\langle \! \circ \! \rangle$

015-

Error loading map file C:\Tools\Get-ZimmermanTools\EvtxECmd\Maps\Microsoft-Windows-Storage-ClassPnP-Operational_Microsof V The following information was included with the event:

Windows Defender ____

公

Description / Data

>

Цi

e

Dullu 17703-153 Telease-100314-1434

 \sim

 \times





Timeline Explorer v1.3.0.0

File Tools Tabs View Help

20230716112553_EvtxECmd_Output.csv

Show the output

Dr	ag a co	lumn h	eader here to gr	Enter text to search	Find				
	Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level	Provider	
Ŧ	=		=	=	=	=	RBC	RBC	
	175		175	175	2023-06-28 16	15	Info	SecurityCenter	
	176		176	176	2023-06-28 16	16394	Info	Microsoft-Windows-Sec	urity-
	177		177	177	2023-06-28 16	15	Info	SecurityCenter	
	178		178	178	2023-06-28 16	15	Info	SecurityCenter	
	179		179	179	2023-06-28 16	15	Info	SecurityCenter	
	180		180	180	2023-06-28 16	16384	Info	Microsoft-Windows-Sec	urity-
	181		181	181	2023-06-28 16	16394	Info	Microsoft-Windows-Sec	urity-
	182		182	182	2023-06-28 16	16384	Info	Microsoft-Windows-Sec	urity-
	183		183	183	2023-06-28 16	8224	Info	VSS	
	184		184	184	2023-06-28 16	16394	Info	Microsoft-Windows-Sec	urity-
	185		185	185	2023-06-28 16	1034	Info	Microsoft-Windows-Sec	urity-
	186		186	186	2023-06-28 16	1033	Info	Microsoft-Windows-Sec	urity-
	187		187	187	2023-06-28 16	16384	Info	Microsoft-Windows-Sec	urity-
	188		188	188	2023-06-28 16	1001	Info	Windows Error Reportin	ng
	189		189	189	2023-06-28 16	15	Info	SecurityCenter	
	190		190	190	2023-06-28 17	16394	Info	Microsoft-Windows-Secu	urity-
	191		191	191	2023-06-28 17	16384	Info	Microsoft-Windows-Sec	urity-
	192		192	192	2023-06-28 17	1001	Info	Windows Error Reportio	ng
4	193		193	193	2023-06-28 17	1001	Info	Windows Error Reportin	ng •

 \times

1. Windows Event Logs Defender Analysis



O

12:40

16-07-2023

へ 🚮 🏪 🕼

⊟i

Ω

e

😥 Untitled.ELX - Event Log	g Explorer						_		×
<u>File Database Tree Log</u>	g <u>V</u> iew <u>E</u> vent <u>A</u> dvanced	Window Help							3
<mark>i:: </mark>	🚽 🔡 🍸 🔹 <load filt<="" td=""><td>er> 🔹 🏹</td><td>F 🗟 🔊</td><td># 🖻 🚔</td><td></td><td></td><td></td><td></td><td></td></load>	er> 🔹 🏹	F 🗟 🔊	# 🖻 🚔					
Objects tree ×	Microsoft-Windows-Windows	Defender %40pe	rational.evtx	~					
Search	₩ ◆ ▶ ₩ 🕹 57	√ 1			ι	лс			
> ····· 🖵 WIN-AJDB7GOIQ	Туре	Date	Time	Event	Source	Category	User	Computer	~
> ····· 🔁 Log Files	(i) Information	29-06-2023	08:15:09	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
> ····· 😁 Task templates	 Information 	29-06-2023	08:15:09	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
	 Information 	29-06-2023	08:15:09	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	5
	 Information 	29-06-2023	08:15:09	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
	 Information 	29-06-2023	08:15:09	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
Show the	 Information 	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
bilow the	 Information 	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
output of	 Information 	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
windows	 Information 	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
WIIIdows	 Information 	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
defender	 Information 	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
100	 Information 	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
10g.	 Information 	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
	 Information 	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
	 Information 	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
	 Information 	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1 -
	<							>	•
	Description								×
< >>	Microsoft Defender Antivirus malware. Old value: Default\F New value: HKLM\S Description Data	Configuration ha eatures\Tamper OFTWARE\Micro	as changed. If ProtectionSou osoft\Windows	this is an unexp rce = 0x0 Defender\Featu	ected event you sho ires\TamperProtecti	ould review the setting onSource = 0x5	gs as this may be the	result of	
								12:41	
	🥭 🥅 🍅 🖉	× 🙌	•				^ 🚳 ঢ় ଏ⊗ ₁₆	12:41 5-07-2023	\Box

O Untitled ELV - Event Log	Filter X	
S Ontried.EEX - Event Eog t	Apply filter to:	
<u>File Database Iree Log</u>	Active event log view (File: C:\Cases\F\Windows\System32\winevt\logs\Microsoft-Winde	
📴 🖙 🔒 🗕 🗁	O Event log view(s) on your choice	
Objects tree ×	Event types Source: Exclude	
Search	☐ Information Category:	
> ····· VIN-AJDB7GOIQ	Warning	Computer 🔨
> 🔁 Log Files 🛛 🗍 🤇	User: Exclude	DESKTOP-I
> E Task templates		DESKTOP-I
Ō	Computer:	DESKTOP-I
Č		DESKTOP-I
Č		DESKTOP-I
Č	Event ID(s):	DESKTOP-I
Filter the	5000,5001	DESKTOP-I
	Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)	DESKTOP-I
Particular	Text in description:	DESKTOP-I
109 as your	RegExp Exclude	DESKTOP-I
iog us your	Date Time Separately	DESKTOP-I
requiremet	From: 16-07-2023 🔍 00:00:00 🚔 To: 16-07-2023 🔍 00:00:00 🚔 Exclude	DESKTOP-I
		DESKTOP-I
	Display event for the last 0 A days 0 A bours Evolute	DESKTOP-I
		DESKTOP-I
	Custom columns Description params	DESKTOP-I 🗸
· · · · · · · · · · · · · · · · · · ·	Name Operator Value	>
	Custom column 1	×
	Custom column 2 Custom column 3	boy he the requit of
	Custom column 4	nay be the result of
	Custom column 5	
		· · ·
< >>	Clear Load Save OK Cancel	
		<u> </u>
		ᢪᠴ ਪੋ≊ 16-07-2023 └~┘

😥 Untitled.ELX - Event L	og Explorer						_		×
<u>F</u> ile <u>D</u> atabase <u>T</u> ree <u>L</u>	og <u>V</u> iew <u>E</u> vent <u>A</u> dvanced	<u>W</u> indow <u>H</u> elp	0						2
📑 🖷 🔒 — I	늘 🔡 🍸 👘 <load fi<="" td=""><td>ter> - 🏹</td><td>7 🗟 🔊</td><td>M 🖻 🚔</td><td></td><td></td><td></td><td></td><td></td></load>	ter> - 🏹	7 🗟 🔊	M 🖻 🚔					
Objects tree ×	Microsoft-Windows-Window	s Defender %40pe	erational.evtx	×					•
Search	📢 🔹 🕨 🔛 🕁 57 '	7 4 🗹 1			1	лс			
> ···· 📮 WIN-AJDB7GOIO	2 Туре	Date	Time	Event	Source	Category	User	Computer	^
> ····· 🔁 Log Files	(i) Information	29-06-2023	08:02:07	5000	Microsoft-Windows	None	\SYSTEM	DESKTOP-	1
> ······ 🖅 Task templates	(i) Information	28-06-2023	16:47:04	5001	Microsoft-Windows	None	\SYSTEM	DESKTOP-	•
	Information	28-06-2023	16:32:14	5000	Microsoft-Windows	None	\SYSTEM	DESKTOP-	8
	(i) Information	28-06-2023	16:28:01	5001	Microsoft-Windows	None	\SYSTEM	DESKTOP-	-Þ
	<							2	~
	Description								×
<	Microsoft Defender Antivirus Description Data	s Real-time Prote	ection scanning	for malware and	l other potentially u	nwanted software wa	s enabled.		
	🚍 📦		\Diamond				へ 强 🖫 🕼 10	12:46 5-07-2023	\Box

😥 Untitled.ELX - Event Lo	g Explorer						_		×
<u>F</u> ile <u>D</u> atabase <u>T</u> ree <u>L</u> o	g <u>V</u> iew <u>E</u> vent <u>A</u> dvanced	Window Help	0						2
📴 🐺 🔒 — 🖻	🚽 🔡 🍸 👘 <load filt<="" td=""><td>er> - 🏹</td><td>7 🗟 🔊</td><td>M 🖻 🚔</td><td></td><td></td><td></td><td></td><td></td></load>	er> - 🏹	7 🗟 🔊	M 🖻 🚔					
Objects tree ×	Microsoft-Windows-Windows	Defender%40pe	erational.evtx	×					-
Search	₩ 4 🕨 🖬 🕹 57 💐	74 🗹 1			l. l.	лс			
> ···· 📮 WIN-AJDB7GOIQ	Туре	Date	Time	Event	Source	Category	User	Computer	^
> ····· 🗁 Log Files	(i) Information	29-06-2023	08:02:07	5000	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
> ····· 📨 Task templates	(i) Information	28-06-2023	16:47:04	5001	Microsoft-Windows	None	\SYSTEM	DESKTOP	-1
	(i) Information	28-06-2023	16:32:14	5000	Microsoft-Windows	None	\SYSTEM	DESKTOP	-D
	 Information 	28-06-2023	16:28:01	5001	Microsoft-Windows	None	\SYSTEM	DESKTOP	8
									~
	<)	
	Description								×
	Microsoft Defender Antivirus	Real-time Prote	ection scanning	for malware and	l other potentially u	nwanted software was	disabled.		
< >	Description Data								~
								12:45	
	Ce 📃 😜 🐇		Q				^ ☞ ♥ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	6-07-2023	\Box

2. System log Analysis



13:06

16-07-2023

へ 强 🏪 🕼

101 items 1 item selected 1.06 MB

Ξi

e

ρ

😥 Untitled.ELX - Event Log	Explorer						- 0	\times
<u>F</u> ile <u>D</u> atabase <u>T</u> ree <u>L</u> o	g <u>V</u> iew <u>Event</u> <u>A</u> dvanced	Window Help						
📴 🐺 🔒 — 🖻	🚽 📑 💙 🛛 <load filt<="" td=""><td>er> - 🏹</td><td>🗟 🖗</td><td>M 🖻 🛔</td><td></td><td></td><td></td><td></td></load>	er> - 🏹	🗟 🖗	M 🖻 🛔				
Objects tree ×	🖷 System.evtx 🛛 🗙							-
Search	₩ • >> <u>↓</u> 818	1				υтс		
> ····· VIN-AJDB7GOIQ	Туре	Date	Time	Event	Source	Category	User	^
> ····· 🔁 Log Files	 Information 	29-06-2023	09:07:51	50037	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE	
> ······ 🖅 Task templates	(i) Information	29-06-2023	09:07:51	50106	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE	
	(i) Information	29-06-2023	09:07:50	51057	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE	
	(i) Information	29-06-2023	09:07:50	51047	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE	
	(i) Information	29-06-2023	09:07:50	50105	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE	
Click	(i) Information	29-06-2023	09:07:50	50104	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE	
CIICK	(i) Information	29-06-2023	09:07:51	6006	EventLog	None	N/A	
this icon	(i) Information	29-06-2023	09:07:48	7002	Microsoft-Windows	(1102)	\SYSTEM	
	(i) Information	29-06-2023	09:07:41	1074	User32	None	\S-1-5-21-3331464962-214784631	-33
	(i) Information	29-06-2023	09:06:16	7040	Service Control Mar	None	\SYSTEM	
	(i) Information	29-06-2023	09:04:23	7040	Service Control Mar	None	\SYSTEM	
	(i) Information	29-06-2023	08:27:44	16	Microsoft-Windows	None	\SYSTEM	
	(i) Information	29-06-2023	08:27:08	19	Microsoft-Windows	Windows Update Age	\SYSTEM	
	(i) Information	29-06-2023	08:27:06	16	Microsoft-Windows	None	\S-1-5-21-3331464962-214784631	-33
	(i) Information	29-06-2023	08:27:06	43	Microsoft-Windows	Windows Update Age	\SYSTEM	
	(i) Information	29-06-2023	08:27:03	16	Microsoft-Windows	None	\SYSTEM	
								~
	<							>
	Description							×
	DHCPv4 client service is stop	ped. ShutDown	Flag value is	1				
< >>	Description Data							
■ へ 🛱	🥭 🚍 🍅 🔮		\odot				へ 🚮 🕼 13:02	\Box

😡 Untitled.ELX - Event Log E	xplorer					- 0	×
<u>File Database Tree Log</u>	View Event	t <u>A</u> dvanced	<u>W</u> indow <u>H</u> elp				
📴 🖙 🔒 — 🖿	7 💾 🔻	<load filte<="" th=""><th>n> 🚽 👗 💆</th><th>7 🖓 🥂 🍳 着</th><th></th><th></th><th></th></load>	n> 🚽 👗 💆	7 🖓 🥂 🍳 着			
Objects tree ×	🖷 System.evt	x ×					-
Search	H4 4 > 1	🛏 🕹 818 🏹	7 10 🗹 1		UTC		
> ····· 🖵 WIN-AJDB7GOIQ	Time	Event	Source	Category	User	Computer	~
> ····· 🗁 Log Files	16:58:13	7045	Service Control Mar	None	\S-1-5-21-3331464962-214784631-3394824829-1001	DESKTOP-MD2HCPT	
> ····· 📂 Task templates	16:58:13	7045	Service Control Mar	None	5-1-5-21-3331464962-214784631-3394824829-1001	DESKTOP-MD2HCPT	
	16:30:52	7045	Service Control Mar	None	\S-1-5-21-3331464962-214784631-3394824829-1001	DESKTOP-MD2HCPT	
	16:30:52	7045	Service Control Mar	None	\S-1-5-21-3331464962-214784631-3394824829-1001	DESKTOP-MD2HCPT	
	16:30:51	7045	Service Control Mar	None	\S-1-5-21-3331464962-214784631-3394824829-1001	DESKTOP-MD2HCPT	
	16:30:46	7045	Service Control Mar	None	\SYSTEM	DESKTOP-MD2HCPT	
	16:30:43	7045	Service Control Mar	None	\SYSTEM	DESKTOP-MD2HCPT	
	16:07:49	7045	Service Control Mar	None	\SYSTEM	WIN-SMB9MDN3Q04	
	16:06:25	7045	Service Control Mar	None	\SYSTEM	WIN-SMB9MDN3Q04	
	16:05:21	7045	Service Control Mar	None	\SYSTEM	WIN-SMB9MDN3Q04	
	<						>
	Description						×
	A service was Service Name: Service File Na Service Type: Service Start Service Accou	installed in the s Sysmon ame: C:\Window user mode sen Type: auto star int: LocalSyster	system. ws\Sysmon.exe vice t n	Descriptio script.	on about the attack		
< >>	Description	Data					
	ê 📄	🖕 🖉	s 😥 😥		^ 🚳	13:05 仁 4 <mark>8</mark> 16-07-2023	\Box

3. Security and Authentication Event logs



Ω

⊟i

e

😥 Untitled.ELX - Event Log	Explorer						-	- 0	\times
<u>File Database Tree Lo</u>	g <u>V</u> iew <u>Event</u> <u>A</u> dvanced	Window Help	•						
📴 🐺 🔒 — 🖻	- Load filt	er> - 🏹	R 🗟 🖓	M 🖻 🛔					
Objects tree X	🖷 Security.evtx 🛛 🗙								-
Search	H I I161	√ 1				итс			
> ····· VIN-AJDB7GOIQ	Туре	Date	Time	Event	Source	Category	User	Computer	~
> ····· 🗁 Log Files	🔍 Audit Success	29-06-2023	09:07:51	1100	Microsoft-Windows	Service shutdown	N/A	DESKTOP-MD2	2H
> ····· 📂 Task templates	🔍 Audit Success	29-06-2023	09:07:48	4798	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	09:07:48	4798	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	09:07:48	4798	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	09:07:48	4798	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
Click this	🔍 Audit Success	29-06-2023	09:07:48	4798	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
icon for filton	🔍 Audit Success	29-06-2023	09:07:46	4647	Microsoft-Windows	Logoff	N/A	DESKTOP-MD2	2H
1con for litter	🔍 Audit Success	29-06-2023	09:04:27	4799	Microsoft-Windows	Security Group Manag	N/A	DESKTOP-MD2	2H
the event id	🔍 Audit Success	29-06-2023	09:04:27	4799	Microsoft-Windows	Security Group Manag	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	09:03:19	4672	Microsoft-Windows	Special Logon	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	09:03:19	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	08:46:45	4672	Microsoft-Windows	Special Logon	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	08:46:45	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	08:32:32	4672	Microsoft-Windows	Special Logon	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	08:32:32	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	08:27:36	4672	Microsoft-Windows	Special Logon	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	08:27:36	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	08:16:45	4672	Microsoft-Windows	Special Logon	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	29-06-2023	08:16:45	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2	2Н 🧅
	<								>
	Description								×
	An account was successfully	logged on.							^
	Subject:								
< >	Jubject.								*
	🤶 📄 🍅 🖪						へ む 🗤	05:10	\neg

😥 Untitled.ELX - Event Log	Filter Ex	×	– 0 X
<u>File Database Tree Log</u>	g Apply filter to:		
늘 🗖 🖨 🗕 🖻	● Active event log view (File: C:\Cases\F\Windows\System32\winevt\logs\Security.evtx)		
	Event log view(s) on your choice		
Objects tree ×	Event types		
Search	Verbose Exclude		
WIN-AIDB7GOIO	· ☐ Information Category: Exclude		Computer
> ····· 🗁 Log Files	Warning		DESKTOP-MD2H
> 🗁 Task templates	✓ Error User: Exclude		DESKTOP-MD2H
	Computer:		DESKTOP-MD2H
	Audit Success		DESKTOP-MD2H
Fill the event			DESKTOP-MD2H
	Vert ID(s):		DESKTOP-MD2H
ia and	Exclude		>
description	D Text in description:		×
asper	Denisha Exclude		^
roquiromont			
requirement			
	Prom: [1/-0/-2023] 00:00:00] 10: [1/-0/-2023] 00:00:00]		
	Display event for the last 0 ays 0 hours Exclude		
	Custom columns Description params		
	Name Operator Value		
	Custom column 1		
	Custom column 2		
	Custom column 4		
	T Custom column 5		s the Server service, or a
			✓
< >	Clear Load Save OK Cano	el	
III ク Lit	🤅 🚍 🧉 😥 🔼	^	05:40 ℡ ⊄ <mark>≋</mark> 17-07-2023 🕤

😥 Untitled.ELX - Event Log Explorer								- 0	\times
<u>File Database Tree Log</u>	Log <u>V</u> iew <u>E</u> vent <u>A</u> dvanced <u>W</u> indow <u>H</u> elp								
	🚽 📑 🍸 👘 <load filt<="" td=""><td>ter> - 🏹</td><td>र 🗟 🖓</td><td>) 💾 🖻 🛔</td><td></td><td></td><td></td><td></td><td></td></load>	ter> - 🏹	र 🗟 🖓) 💾 🖻 🛔					
Objects tree ×	🖷 Security.evtx 🛛 🗙								-
Search	₩ • • • ₩ 🕁 1161	₹ 170 🗹 0				υтс			
> ····· 🖵 WIN-AJDB7GOIQ	Туре	Date	Time	Event	Source	Category	User	Computer	^
> ····· 🔁 Log Files	🔍 Audit Success	29-06-2023	09:03:19	4624	Microsoft-Windows	Logon	N/A	DESKTOP-M	D2H
> ····· E Task templates	🔍 Audit Success	29-06-2023	08:46:45	4624	Microsoft-Windows	Logon	N/A	DESKTOP-M	D2H
	🔍 Audit Success	29-06-2023	08:32:32	4624	Microsoft-Windows	Logon	N/A	DESKTOP-M	D2H
	🔍 Audit Success	29-06-2023	08:27:36	4624	Microsoft-Windows	Logon	N/A	DESKTOP-M	D2H
	🔍 Audit Success	29-06-2023	08:16:45	4624	Microsoft-Windows	Logon	N/A	DESKTOP-M	D2H
	🔍 Audit Success	29-06-2023	08:14:34	4624	Microsoft-Windows	Logon	N/A	DESKTOP-M	D2H
	1								```
	Description								×
		Is a set of the							
	An account was successfully	loggea on.							
	Subject:			Sho	w the all deta				
	Security ID:	S-1-5-18							
	Account Name: Account Domain:	WORKGE		ever	nt log.				
	Logon ID:	0x3e7			_				
	Logon Informations								
	Logon Type:	5							
	Restricted Admin M	ode: -							
	Virtual Account:	No							
	Elevated Token:	res							
	Impersonation Level:	Impersor	nation						
	New Logon:								
	Security ID:	S-1-5-18							
	Account Name:	SYSTEM							
< >	Description								
		\$						05:12	
		2					^ ┞┙ ◁⊗	17-07-2023	

4. Authentication & Logon IDs logs

4624 event id use for login detail which by filtering we can see all login details same but same time same login details have different login id. If the event log is viewed by filtering the login ID, it will show any Malicious activity like user joined a Administrator group, Any user is created, Any other user change the credential details etc.

😥 Untitled.ELX - Event Log I	Ext					×	_	Ō	\times
<u>File Database Tree Log</u>	Apply filter to:								
	Active event log view (File: C	:\Cases\F\Windows\Syste	em32\wine∨t\log	gs\Security.evtx)					
	 Event log view(s) on your che 	pice							
Objects tree ×	Event types	Sources			Evdude				-
Search	Verbose	Source.							
> ····· WIN-AJDB7GOIO	□ □ Information	Category:			Exclude	-	Co	mputer	^
> Eog Files	Warning	User:			Exclude		DE	SKTOP-M	D2H
> 🔁 Task templates							DE	SKTOP-M	D2H
		Computer:			Exclude		DE	SKTOP-M	D2H
							DE	SKTOP-M	D2H
	Event ID(c):						DE	SKTOP-M	D2H
D'1 (Evdude	-	DE	SKTOP-M	D2H
Filter with	Enter ID numbers and/or ID range	jes, separated by comas,	use exclamatio	n mark to exclude criteria (e	e.g. 1-19,100,250-450!10,255)	-	DE	SKTOP-M	D2H
login ID	Text in description:						DE	SKTOP-M	D2H
	(0x20c75				RegExp Exclude		DE	SKTOP-M	D2H
	Date Time Sep	arately					DE	SKTOP-M	D2H
	Erom: 17-07-2023	00.00.00	To: 17-07-2	023	Exclude		DE	SKTOP-M	D2H
			17 07 2	00.00.00	₽ Exclude		DE	SKTOP-M	D2H 🗸
	Display event for the last	🛉 days 🛛 🖡	hours	Exclude					×
	Custom columns Description pa	rams							•
	Name	Ope	erator	Value					
	N Custom column 1								
	Custom column 2 Custom column 3								
	Custom column 4								
	Custom column 5								
									~
<	Clear Load	Save			OK Car	ncel			
H へ Hi	🥭 🖬 🧉 🧔	A				~ •	に 日 ↓ 17-	06:37 07-2023	5

😥 Untitled.ELX - Event Log	Explorer						-	_ D	\times
<u>File Database Tree Log</u>	g <u>V</u> iew <u>E</u> vent <u>A</u> dvanced	Window Help							
📴 🐺 🔒 — 🖿	🚽 📑 💙 👘 <load filt<="" td=""><td>er> 🛛 🕶 🍸</td><td>🗑 🖓</td><td>M 🖻 🛔</td><td></td><td></td><td></td><td></td><td></td></load>	er> 🛛 🕶 🍸	🗑 🖓	M 🖻 🛔					
Objects tree ×	🖷 Security.evtx 🛛 🛛								-
Search	H · · · · · · · · · · · · · · · · · · ·	7 19 🗹 1				υтс			
> ····· WIN-AJDB7GOIQ	Туре	Date	Time	Event	Source	Category	User	Computer	~
> ····· 🛅 Log Files	🔍 Audit Success	28-06-2023	16:19:55	4648	Microsoft-Windows	Logon	N/A	DESKTOP-MD2	2H
> ····· 🗁 Task templates	🔍 Audit Success	28-06-2023	16:19:22	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	28-06-2023	16:19:22	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	28-06-2023	16:19:22	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	28-06-2023	16:19:22	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
Same login ID	🔍 Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
and details	🔍 Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
show different	🔍 Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	28-06-2023	16:18:43	5059	Microsoft-Windows	Other System Events	N/A	DESKTOP-MD2	2H
	🔍 Audit Success	28-06-2023	16:18:43	5061	Microsoft-Windows	System Integrity	N/A	DESKTOP-MD2	2Н 🗸
	<								>
	Description								×
	Credential Manager credentia	ais were read.							~
	Subject: Security ID: S-1-5-21-3331464962-214784631-3394824829-1000 Account Name: defaultuser0 Account Domain: DESKTOP-MD2HCPT Logon ID: 0x20c75 Read Operation: Enumerate Credentials								
	This event occurs when a us	er performs a re	ead operation	n on stored crea	dentials in Credential	Manager.			\sim
<	Description Data								
II A Ei	🥭 🚍 🍅 🍕	>					∧ ঢ়_ 4≥	06:21 17-07-2023	
D Untitled.ELX - Event Log Explorer

Eile Database Iree Log View Event Advanced Window Help

0 \times -

Computer

MSEDGEWIN10

User

N/A

Security Group Management

•

~

×

Objects tree	× BANCrosoft-Windows-V	🖷 Microsoft-Windows-Windows Defender%-(Operational.evtx:							
Search	H4 4 P PH L	4528 🖓 11 🗹 1			UTC				
> - 📮 WIN-8K1Q9542K3L (local)	Туре	Date	Time	Event	Source	Category			
Y - 📴 Log Files	Audit Success	3/18/2022	12:24:47 AM	4732	Microsoft-Windows-Security-Auditing	Security (
Microsoft-Windows-Windows Defender%4Operational (C:\Cases\E\W	Audit Success	3/18/2022	12:24:47 AM	4724	Microsoft-Windows-Security-Auditing	User Acco			
System (C:\Cases\E\Windows\System32\Winevt\logs\System.evtx)	Audit Success	3/18/2022	12:24:47 AM	4738	Microsoft-Windows-Security-Auditing	User Acco			
> - Task templates	Audit Success	3/18/2022	12:24:47 AM	4798	Microsoft-Windows-Security-Auditing	User Acco			
	Audit Success	3/18/2022	12:24:47 AM	4732	Microsoft-Windows-Security-Auditing	Security (
	Audit Success	3/18/2022	12:24:47 AM	4738	Microsoft-Windows-Security-Auditing	User Acco			
	Audit Success	3/18/2022	12:24:47 AM	4722	Microsoft-Windows-Security-Auditing	User Acco			
	Audit Success	3/18/2022	12:24:47 AM	4720	Microsoft-Windows-Security-Auditing	User Accs			
	Audit Success	3/18/2022	12:24:47 AM	4728	Microsoft-Windows-Security-Auditing	Security (
	Audit Success	3/18/2022	12:10:38 AM	4672	Microsoft-Windows-Security-Auditing	Special Lo			
Same login	Audit Success	3/18/2022	12:10:38 AM	4624	Microsoft-Windows-Security-Auditing	Logon			

ID and details show different

Ξī

-

1

۲

19

						2200	
Audit Success 3/1	18/2022	12:24:47 AM	4724	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success 3/3	18/2022	12:24:47 AM	4738	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success 3/3	18/2022	12:24:47 AM	4798	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success 3/1	18/2022	12:24:47 AM	4732	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEDGEWIN10
Audit Success 3/1	18/2022	12:24:47 AM	4738	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success 3/3	18/2022	12:24:47 AM	4722	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success 3/1	18/2022	12:24:47 AM	4720	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success 3/1	18/2022	12:24:47 AM	4728	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEDGEWIN10
Audit Success 3/1	18/2022	12:10:38 AM	4672	Microsoft-Windows-Security-Auditing	Special Logon	N/A	MSEDGEWIN10
Audit Success 3/1	18/2022	12:10:38 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	MSEDGEWIN10
user account was created.							
ibject: Secunty ID: Account Name: Account Domain:	5-1-5-2 IEUser MSEDGE	1-3461203602-409630 EWIN10	04019-226908	00 69 -1000			
Logon ID: w Account: Security ID: Account Name: Account Domain:	S-1-5-2 art-test MSEDGE	1-3461203602-409630 EWIN10	04019-226908	0069-1003			
tributes: SAM Account Name: Display Name: User Principal Name: Home Drive: Script Path: Profile Path: User Workstations: Password Last Set: Account Expires: Primary Group ID: Alowed To Delegate Ti Old UAC Value: User Account Control: Account Control: Account Disabi 'Password Not 'Normal Accour User Parameters: «valu SID History: Loogn Hours:	art-test <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <value <val< th=""><th>not set> not set> not set> not set> not set> > ></th><th></th><th></th><th></th><th></th><th></th></val<></value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value </value 	not set> not set> not set> not set> not set> > >					
iditional Information: Privileges	•						Activate Windows Go to Settings to activate Windows
Description Data	•						Go to Setti



5. Windows Event logs Power shell overview, Analyse Malicious Activity.

Source Windows PowerShell Event IDsDescription400Engine state is changed from None to Available

Windows Power shell stored all logs about the command base execution like run the any script, install the any applications, etc.

📙 🔄 🔄 🚽 🗌 logs							- O	\times
File Home Share	View							^ ?
Pin to Quick Copy Paste access	Cut Copy path Paste shortcut	love Copy to T	ne New folder	v item • y access • Proper	B Open ▼ Edit ties	Select all Select none Invert selection		
Clipboard		Organize	New		Open	Select		
\leftarrow \rightarrow \checkmark \uparrow \square \Rightarrow This	s PC > SDT_x64FREE_I	EN-US_VHD (C:) > Cases >	$F \Rightarrow$ Windows \Rightarrow	System32 → wine	evt → logs	✓ Ö Sear	ch logs	,c
Evidence	Name	^	Date modified	Type	Size			^
Execution	Microsoft-Wind	ows-VolumeSpanshot-Dr	20-06-2023 00:07	EventLog	68 KI	3		
NTES	Microsoft-Wind	lows-Wemsve%40peratio	29-06-2023 09:07	Event Log	68 KI	3		
Registry	Microsoft-Wind	lows-WebAuthN%4Opera	29-06-2023 09:07	Event Log	68 KI	3		
Registry	Microsoft-Wind	ows-WER-PayloadHealth	28-06-2023 18:13	Event Log	68 KI	3		
💻 This PC	Microsoft-Wind	lows-WFP%4Operational	28-06-2023 16:17	Event Log	68 KI	3		
🗊 3D Objects	🛃 Microsoft-Wind	lows-Windows Defender	29-06-2023 09:07	Event Log	68 KI	3 -	4.4 • 4	
E Desktop	🔠 Microsoft-Wind	lows-Windows Defender	28-06-2023 16:18	Event Log	68 KI	B Loa	d the windows	
Documents	🛃 Microsoft-Wind	lows-Windows Firewall W	29-06-2023 09:07	Event Log	1,028 KI	³ pow	er shell logs on	
🖶 Downloads	🛃 Microsoft-Wind	lows-Windows Firewall W	28-06-2023 16:17	Event Log	68 KI	exnl	orer	
Music	Microsoft-Wind	lows-WindowsBackup%4	28-06-2023 16:31	Event Log	68 KI		0101	
Pictures	Microsoft-Wind	lows-WindowsUpdateClie	29-06-2023 09:07	Event Log	68 KI	3		
Videos	Microsoft-Wind	lows-WinlNet-Config%4P	28-06-2023 16:31	Event Log	68 KI	3		
SDT v64EREE EN	Microsoft-Wind	lows-Winlogon%40perati	29-06-2023 09:07	Event Log	1,028 KI	3		
CD Drive (Dr) Vir	Microsoft-Wind	lows-winkivi%40peratio	29-06-2023 09:07	Event Log	08 KI	5		
Devertise de 0.) VII	Security	lows-wivil-Activity‰40p	29-06-2023 09:07	Event Log	1,028 Ki	2		
	E Setup		28-06-2023 16:17	Event Log	68 KI	3		
Network	Svstem		29-06-2023 09:07	Event Log	1.092 Ki	3		
~	Windows Power	rShell	29-06-2023 09:07	Event Log	1,092 Ki	3		~
101 items 1 item selected	1.06 MB						[





😥 Untitled.ELX - Event Log	Explorer						-	- 0	\times
<u>F</u> ile <u>D</u> atabase <u>T</u> ree <u>Log</u>	g <u>V</u> iew <u>E</u> vent <u>A</u> dvanced	Window Help							
📴 🐺 🔒 🗕 🖻	🚽 📑 🍸 👘 <load filt<="" td=""><td>er> 🛛 🕇 🏹</td><td>- TT 🔎</td><td>M 🖣</td><td></td><td></td><td></td><td></td><td></td></load>	er> 🛛 🕇 🏹	- TT 🔎	M 🖣					
Objects tree ×	Windows PowerShell.evtx	×							-
Search	₩ • • • ↓ 188	1				итс			
> ····· WIN-AJDB7GOIQ	Туре	Date	Time	Event	Source	Category	User	Computer	^
> ·····🗁 Log Files	(i) Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MI	D2H
> ····· 🛅 Task templates	i Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MI	D2H
	i Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MI	D2H
	 Information 	29-06-2023	08:03:35	400	PowerShell	Engine Lifecycle	N/A	DESKTOP-MI	D2H
	(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-M	D2H
	(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MI	D2H
	(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MI	D2H
	(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MI	D2H
	(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MI	D2H
	(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MI	D2H
	(i) Information	28-06-2023	18:02:00	800	PowerShell	Pipeline Execution De	N/A	DESKTOP-MI	D2H
	(i) Information	28-06-2023	18:02:00	800	PowerShell	Pipeline Execution De	N/A	DESKTOP-MD	D2H
	(i) Information	28-06-2023	18:01:44	400	PowerShell	Engine Lifecycle	N/A	DESKTOP-M)2Н 🗸
	<								>
	Description								×
	HostName=Console HostVersion=5.1.19 HostId=1cb3bb2b-1 HostApplication=C:\ \Desktop\PWF-main\PWF-main Engineversion=5.1. RunspaceId=34b13 PipelineId= CommandName= CommandType= Description Data	Host 041.1237 850-4cf4-32b7 Windows\Syste ain\AtomicRedTe 19041.1237 4b3-9b15-4196-	0362cf07c54 m32\Windov aam' 839a-39236	vsPowerShell\v1 e79bd83	.0\powershell.exe	-noexit -command Set-	Location -literalPath 'C	::\Users\Denisl	ha V
								08:06	
	C 🗖 🧉 🖉						^ 腔 ੍≈	17-07-2023	

🔘 Untitled.ELX - Event Log	Explorer						-	- 0	\times
<u>F</u> ile <u>D</u> atabase <u>T</u> ree <u>Log</u>	g <u>V</u> iew <u>E</u> vent <u>A</u> dvanced	<u>W</u> indow <u>H</u> elp							
🕞 🖶 🔒 — 🖻	🖢 📑 🍸 🔹 <load filte<="" td=""><td>er> - 🏹</td><td>F 🗟 🔊</td><td>M 🖻 🛔</td><td></td><td></td><td></td><td></td><td></td></load>	er> - 🏹	F 🗟 🔊	M 🖻 🛔					
Objects tree ×	Windows PowerShell.evtx	×							-
Search	H I I88	1				итс			
> ····· WIN-AJDB7GOIQ	Туре	Date	Time	Event	Source	Category	User	Computer	^
> ····· 🗁 Log Files	 Information 	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD)2H
> ····· 🗁 Task templates	(i) Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD	2H
	(i) Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD	2H
	(i) Information	29-06-2023	08:03:35	400	PowerShell	Engine Lifecycle	N/A	DESKTOP-MD	02H
	(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD	02H
	(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD	02H
	(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD	02H
	(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD	02H
	(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD	2H
	 Information 	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD	02H
	() Information	28-06-2023	18:02:00	800	PowerShell	Pipeline Execution De	N/A	DESKTOP-MD)2H
	(i) Information	28-06-2023	18:02:00	800	PowerShell	Pipeline Execution De	N/A	DESKTOP-MD	2H
	(i) Information	28-06-2023	18:01:44	400	PowerShell	Engine Lifecycle	N/A	DESKTOP-MD	2Н 🗸
	<								>
	Description								×
<	UserId=DESKTOP-M HostName=Consolet HostVersion=5.1.19 HostId=c8d3a583-8 HostApplication=C:\ \Desktop\PWF-main\PWF-mai EngineVersion=5.1.3 RunspaceId=50a379 PipelineId=14 ScriptName=C:\Wind Description Data	D2HCP I \Denish lost 041.1237 72c-4d21-hf69- Windows\Syste in\Install-Sysmo 19041.1237 9e5-2c5a-426e-4 dows\system32	a 5 <u>e941e11b7</u> m32\Window n' 83f6-209ad2 \WindowsPo	d6 vsPowerShell\v1 331f12 werShell\v1.0\N	.0\powershell.exe 1odules\Microsoft.P	-noexit -command Set- owerShell.Archive\Micro	Location -literalPath 'C psoft.PowerShell.Archi	C:\Users\Denish	na v
I P H	🥭 🖿 🍯 🛛	\mathbf{O}					^ 탓 ੍∞	08:07 17-07-2023	



Setting up volatility3 in Ubuntu

Setting up the Volatility3 in the Ubuntu that open the link <u>https://bluecapesecurity.com/build-your-forensic-workstation/</u> Show the instruction linux based tools.



ρ

Цi

e

Recyc

O forensic@WIN-AJDB7GOIQEJ: ~

– 🗆 🗆

Try: sudo apt install <deb name> \sim forensic@WIN-AJDB7GOIQEJ:~\$ sudo apt-get update [sudo] password for forensic: FireGet:1 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB] Hit:2 http://archive.ubuntu.com/ubuntu focal InRelease Get:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB] Get:4 http://archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB] [Get:5 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [2304 kB] Get:6 http://archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8628 kB] EvenGet:7 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [367 kB] FxpGet:8 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [13.0 kB] Get:9 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [1987 kB] Get:10 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [277 kB] Get:11 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f Metadata [576 B] Get:12 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [858 kB] Get:13 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [179 kB] Get:14 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [18.8 kB] Get:15 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [23.6 kB] Get:16 http://security.ubuntu.com/ubuntu focal-security/multiverse Translation-en [5504 B] Get:17 http://archive.ubuntu.com/ubuntu focal/universe Translation-en [5124 kB] Get:18 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f Metadata [548 B] Get:19 http://archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadata [265 kB] ^{po}Get:20 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [144 kB] Get:21 http://archive.ubuntu.com/ubuntu focal/multiverse Translation-en [104 kB] Get:22 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 c-n-f Metadata [9136 B] Get:23 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [2687 kB] Get:24 http://archive.ubuntu.com/ubuntu focal-updates/main Translation-en [449 kB] Get:25 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [16.9 kB] U^gGet:26 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [2092 kB] accounts_V...

Windows Server 2019 Datacenter Evaluation Windows License valid for 156 days Build 17763.rs5_release.180914-1434





Recyc

Even

Expl

Noter

🧿 forensic@WIN-AJDB7GOIQEJ: ~

 \Box \times

Fetched 27.7 MB in 22s (1269 kB/s)

Reading package lists... Done forensic@WIN-AJDB7GOIQEJ:~\$ sudo apt install python3-pip

Reading package lists... Dor

FireBuilding dependency tree

Reading state information... Done

The following additional packages will be installed:

binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-9 dpkg-dev fakeroot g++ g++-9 gcc gcc-9
gcc-9-base libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan5 libatomic1 libbinutils
libc-dev-bin libc6 libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libdpkg-perl libexpat1 libexpat1-dev
libfakeroot libfile-fcntllock-perl libgcc-9-dev libgomp1 libisl22 libitm1 liblsan0 libmpc3 libpython3-dev
libpython3.8 libpython3.8-dev libpython3.8-minimal libpython3.8-stdlib libquadmath0 libstdc++-9-dev libtsan0
libubsan1 linux-libc-dev make manpages-dev python-pip-whl python3-dev python3-wheel python3.8 python3.8-dev
python3.8-minimal zlib1g zlib1g-dev

Suggested packages:

binutils-doc cpp-doc gcc-9-locales debian-keyring g++-multilib g++-9-multilib gcc-9-doc gcc-multilib autoconf automake libtool flex bison gdb gcc-doc gcc-9-multilib glibc-doc bzr libstdc++-9-doc make-doc python3.8-venv python3.8-doc binfmt-support

The following NEW packages will be installed:

binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-9 dpkg-dev fakeroot g++ g++-9 gcc gcc-9 gcc-9-base libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan5 libatomic1 libbinutils libc-dev-bin libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libdpkg-perl libexpat1-dev libfakeroot libfile-fcntllock-perl libgcc-9-dev libgomp1 libisl22 libitm1 liblsan0 libmpc3 libpython3-dev libpython3.8-dev

bo libquadmath0 libstdc++-9-dev libtsan0 libubsan1 linux-libc-dev make manpages-dev python-pip-whl python3-dev python3-pip python3-wheel python3.8-dev zlib1g-dev

The following packages will be upgraded:

libc6 libexpat1 libpython3.8 libpython3.8-minimal libpython3.8-stdlib python3.8 python3.8-minimal zlib1g 8 upgraded, 50 newly installed, 0 to remove and 251 not upgraded.

Need to get 61.4 MB of archives.

U!After this operation, 228 MB of additional disk space will be used. accounts_V...

Windows Server 2019 Datacenter Evaluation Windows License valid for 156 days Build 17763.rs5_release.180914-1434









e ρ Цi



Build 17763.rs5_release.180914-1434



ρ

e





🧿 forensic@WIN-AJDB7GOIQEJ: ~

forensic@WIN-AJDB7GOIQEJ:~\$ vol -h

Command 'vol' not found, did you mean:

```
command 'gol' from deb growl-for-linux (0.8.5-5)
command 'vl' from deb atfs (1.4pl6-14)
command 'hvol' from deb hfsutils (3.2.6-14)
command 'sol' from deb aisleriot (1:3.22.9-1)
command 'vor' from deb vor (0.5.7-3)
command 'vos' from deb openafs-client (1.8.4~pre1-1ubuntu2.4)
command 'col' from deb bsdmainutils (11.1.2ubuntu3)
```

Try: sudo apt install <deb name>

forensic@WIN-AJDB7GOIQEJ:~\$ ls -la

```
total 8
drwxr-xr-x 1 forensic forensic 512 Jul 21 17:48 .
                               512 Jun 28 05:44 ..
drwxr-xr-x 1 root
                     root
-rw----- 1 forensic forensic 140 Jul 16 06:27 .bash history
-rw-r--r-- 1 forensic forensic 220 Jun 28 05:44 .bash logout
-rw-r--r-- 1 forensic forensic 3771 Jun 28 05:44 .bashrc
drwxrwxrwx 1 forensic forensic 512 Jul 21 17:48 cache
drwxr-xr-x 1 forensic forensic 512 Jun 28 05:45 .landscape
drwx----- 1 forensic forensic 512 Jul 21 17:48 .local
-rw-rw-rw- 1 forensic forensic 0 Jul 21 17:32 .motd shown
-rw-r--r-- 1 forensic forensic 807 Jun 28 05:44 .profile
-rw-r--r-- 1 forensic forensic
                                 0 Jul 21 17:37 .sudo as admin successful
forensic@WIN-AJDB7G0I0EJ:~$ source .profile
forensic@WIN-AJDB7GOIOEJ:~$ vol -h
Volatility 3 Framework 2.4.1
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN DIRS]
                  [-s SYMBOL DIRS] [-v] [-1 LOG] [-o OUTPUT DIR] [-q] [-r RENDERER] [-f FILE] [--write-config]
                  [--save-config SAVE CONFIG] [--clear-cache] [--cache-path CACHE PATH] [--offline]
                  [--single-location SINGLE_LOCATION] [--stackers [STACKERS [STACKERS ...]]]
                  [--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]]
                 plugin ...
```

Б

17:51

^ 🏷 🕼

 \times

~



What is memory Analysis

Memory forensics (sometimes referred to as memory analysis) refers to the analysis of volatile data in a computer's memory dump. Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data.

Copy the target machine memory image from host system and paste the memory in cases > Analysis > memory folder create > paste Here.

Open the Ubuntu linux. Go to the path on memory image file did paste.

Of forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory	- 6	\times t
<pre>* Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage</pre>		î
System information as of Sat Jul 22 07:54:56 DST 2023		
System load:0.52Processes:7Usage of /home:unknownUsers logged in:0Memory usage:43%IPv4 address for eth0:10.0.2.15Swap usage:1%		
259 updates can be applied immediately. 188 of these updates are standard security updates. To see these additional updates run: apt listupgradable		
This message is shown once a day. To disable it please create the /home/forensic/.hushlogin file. forensic@WIN-AJDB7GOIQEJ:~\$ pwd /home/forensic forensic@WIN-AJDB7GOIQEJ:~\$ cd /mnt forensic@WIN-AJDB7GOIQEJ:/mnt\$ ls		
<pre>forensic@WIN-AJDB7GOIQEJ:/mnt\$ cd forensic@WIN-AJDB7GOIQEJ:/\$ ls bin dev home lib lib64 media opt root sbin srv tmp var boot etc init lib32 lib32 mnt proc run snap sys usr forensic@WIN-AJDB7GOIQEJ:/\$ cd /mnt/c/Cases/Analysis/Memory/ forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory\$ pwd /mnt/c/Cases/Analysis/Memory forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory\$ ls -la total 2234248 drwxrwxrwx 1 forensic forensic 512 Jul 22 07:49 -rwxrwxrwx 1 forensic forensic 512 Jul 22 07:49 -rwxrwxrwx 1 forensic forensic 2287868348 Jul 22 06:38 win10-memory.raw forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory\$</pre>		
	07:57	. 5

Gathering Windows system information with Volatility3

 \times

^ 門 ◁≈

^

Select forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory _ П forensic@WIN-AJDB7G0I0EJ:/mnt/c/Cases/Analysis/Memory\$ vol -h Volatility 3 Framework 2.4.1 usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-1 LOG] [-0 OUTPUT DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline] [--single-location SINGLE LOCATION] [--stackers [STACKERS [STACKERS ...]]] [--single-swap-locations [SINGLE SWAP LOCATIONS [SINGLE SWAP LOCATIONS ...]]] plugin ... An open-source memory forensics framework optional arguments: -h, --help Show this help message and exit, for specific plugin options use 'volatility <pluginname> --help' -c CONFIG, --config CONFIG Load the configuration from a json file --parallelism [{processes,threads,off}] Enables parallelism (defaults to off if no argument given) -e EXTEND, --extend EXTEND Type the command Extend the configuration with a new (or changed) setting for volatility help -p PLUGIN DIRS, --plugin-dirs PLUGIN DIRS Semi-colon separated list of paths to find plugins -s SYMBOL DIRS, --symbol-dirs SYMBOL DIRS and show all plugins Semi-colon separated list of paths to find symbols for different -v, --verbosity Increase output verbosity -1 LOG, --log LOG Log output to a file as well as the console operating system. -o OUTPUT DIR, --output-dir OUTPUT DIR Directory in which to output any generated files Remove progress feedback -q, --quiet -r RENDERER, --renderer RENDERER Determines how to render the output (quick, none, csv, pretty, json, jsonl) -f FILE, --file FILE Shorthand for --single-location=file:// if single-location is not defined Write configuration JSON file out to config.json --write-config --save-config SAVE CONFIG Save configuration JSON file to a file Clears out all short-term cached items --clear-cache --cache-path CACHE PATH Change the default path (/home/forensic/.cache/volatility3) used to store the cache

Цi

Ω

e

Checks for malicious trustedbsd modules mac.vfsevents.VFSevents Lists processes that are filtering file system events timeliner.Timeliner Runs all relevant plugins that provide time related information and orders the results by time. windows.bigpools.BigPools List big page pools. windows.callbacks.Callbacks Lists kernel callbacks and notification routines. windows.cmdline.CmdLine Lists process command line arguments. windows.crashinfo.Crashinfo windows.devicetree.DeviceTree Listing tree based on drivers and attached devices in a particular windows memory image. windows.dlllist.DllList Lists the loaded modules in a particular windows memory image. windows.driverirp.DriverIrp List IRPs for drivers in a particular windows memory image. windows.drivermodule.DriverModule Determines if any loaded drivers were hidden by a rootkit windows.driverscan.DriverScan Scans for drivers present in a particular windows memory image. windows.dumpfiles.DumpFiles Dumps cached file contents from Windows memory samples. windows.envars.Envars Display process environment variables windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.getservicesids.GetServiceSIDs Lists process token sids. windows.getsids.GetSIDs Print the SIDs owning each process we have use windows.handles.Handles windows info Lists process open handles. windows.info.Info Show OS & kernel details of the memory sample being analyzed. plugins. windows.joblinks.JobLinks Print process job link information

오 H: 🥭 🚍 🍅 🧕

Б

 \times

forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Ana	alysis/Memory	— r	J X
Progress: 99.98 Rea	ading Symbol layer		^
Progress: 99.98 Rea	ading Symbol layer		
Progress: 99.99 Rea	ading Symbol layer		
Progress: 99.99 Rea	ading Symbol layer		
Progress: 99.99 Rea	ading Symbol layer		
Progress: 99.99 Rea	ading Symbol layer		
Progress: 99.99 Rea	ading Symbol layer		
Drogness: 100.00 Rea	ading Symbol layer		
Progress: 100.00 Rea	ading Symbol layer		
Progress: 100.00 PDB	B scanning finished		
100100 100			
Variable Value			
Kernel Base Øxf8063d41d000			
DTB 0x1aa000			
Symbols file:///home/forensic/.loca	al/lib/python3.8/site-packages/volatility3/symbols/windows/ntkrnlmp.pdb/CA8E	2FØ1B822E	DE6357
898BFBF862997-1.json.xz			
IS64Bit True			
ISPAE Faise			
memory layer 1 Elf64 aver			
hase laver 2 Filelaver			
KdVersionBlock 0xf8063e02c368			
Major/Minor 15.19041	Type this command how the		
MachineType 34404	rogult		
KeNumberProcessors 2	165011.		
SystemTime 2023-07-22 06:37:29	9		
NtSystemRoot C:\Windows			
NtProductType NtProductWinNt			
NtMajorVersion 10			
NtMinorVersion 0			
PE MajorOperatingSystemVersion 10			
PE MinorOperatingSystemVersion 0			
PE Machine 34404			
PE limeDateStamp Wed Jan 4	04:2/:11 1995		
TOPENSIC@WIN-AJDB/GOLQEJ:/mnt/c/Cas	ses/Analysis/Memory\$ vol -+ win10-memory.raw windows.in+o		~
		, 08:29	
		22-07-20	023 1

memory_	layer	1 Elf64Layer											
base_la	yer	2 FileLayer											
KdVersi	onBlock	0xf8063e02c368		T Tain a t			a list and	+10 a 10-					
Major/M	inor	15.19041		Using t	ne pstre	e plugit	n list out	the nc	ow many	y services	are		
Machine	Туре	34404		running	T								
KeNumbe	rProcess	ors 2											
SystemT	ime	2023-07-22 06:3	7:29										
NtSyste	mRoot	C:\Windows											
NtProdu	ctType	NtProductWinNt											
NtMajor	Version	10											
NtMinor	Version	0											
PE Majo	r0perati	ngSystemVersion	10										
PE Mino	rOperati	ngSystemVersion	0										
PE Mach	ine	34404											
PE Time	DateStam	ip Wed Jan	4 04:27:11 199	5									
forensi	C@WIN-AJ	DB7GOIQEJ:/mnt/c	/Cases/Analysis/	Memory\$	vol -f w	in10-mem	ory.raw	windows.	pstree				
Volatil	ity 3 Fr	amework 2.4.1		_	•								
^Z^Cres	s: 11.	38	Scanning memory	_layer u	sing Byt	esScanne	r						
[1]+ S	topped	v	ol -† win10-memo	ry.raw w	indows.p	stree							
forensi	C@WIN-AJ	DB7GOIQEJ:/mnt/c	/Cases/Analysis/	Memory\$	vol -t w	in10-mem	ory.raw	windows.	pstree >	pstree.tx	.t		
torensi	C@WIN-AJ	DB/GOIQEJ:/mnt/c	/Cases/Analysis/	Memory\$	VOI -+ W	in10-mem	ory.raw	windows.	pstree				
Volatil	1ty 3 Fr	amework 2.4.1		المحاجة م									
Progres	S: 100.	June	PDB scanning fi	nisnea	llandlar.	Constan	Tal	Linu C 4	CreateT				
PID	PPID	ImageriieName	OffSet(V)	inreaus	Handles	Session	IIU	W0W04	creater.	Twe E	XICIIME	Ê	
4	9	Sustem Avera68	7674080 124	-	NZA	False	2023-07	-22 06.3	3.00 000	999 N	1/ ^		
* 1494	4	MemCompression	AXCC068e308040	14	-	N/A	False	2023-07	-22 06:34	4.20 0000	10	N/A	
* 92	4	Registry	0xcc06877b6040	4	_	N/A	False	2023-07	-22 00:3	A:52 00000	ie ie	N/A	
* 348	4	Smss_exe	0xcc0687c6c040	2		N/A	False	2023-07	-22 06:3	3:09.00000	ด้	N/A	
532	512	CSPSS-exe	0xcc068d369080	12		1	False	2023-07	-22 06:3	3:37.00000	ด	N/A	
596	512	winlogon.exe	0xcc068a750240	6		1	False	2023-07	-22 06:3	3:37.00000	00	N/A	
* 800	596	fontdrvhost.ex	0xcc068d3f6080	5		1	False	2023-07	-22 06:3	3:40.00000	00	N/A	
* 2180	596	userinit.exe	0xcc068eaaf080	0		1	False	2023-07	-22 06:3	6:41.00000	00	2023-07-22	0
:36:56.	000000												
** 2488	2180	explorer.exe	0xcc068ec78080	49		1	False	2023-07	-22 06:3	6:43.00000	90	N/A	
* 976	596	dwm.exe 0xcc068	e14a300 16		1	False	2023-07	-22 06:3	3:42.000	000 N	I/A		
forensi	c@WIN-AJ	DB7GOIQEJ:/mnt/c	/Cases/Analysis/	Memory\$									
	Q E	i: 🥖 🗀								,	^ 1⊡ ປ.	08:48	
												22-07-2023	K

þ \times

 $\mathbf{\wedge}$

¥

α.

_





ð X

🧿 forensi	@WIN-AJD	B7GOIQEJ: /mnt/c/Case	s/Analysis/Memory							—	o ×	(
* 92	4	Registry	0xcc06877b6040	4		N/A	False	2023-07-22	06:30:52.000000	N/A		,
* 348	4	smss.exe	0xcc0687c6c040	2		N/A	False	2023-07-22	06:33:09.000000	N/A		
532	512	csrss.exe	0xcc068d369080	12		1	False	2023-07-22	06:33:37.000000	N/A		
596	512	winlogon.exe	0xcc068a750240	6		1	False	2023-07-22	06:33:37.000000	N/A		
* 800	596	fontdrvhost.ex	0xcc068d3f6080	5		1	False	2023-07-22	06:33:40.000000	N/A		
* 2180	596	userinit.exe	0xcc068eaaf080	0		1	False	2023-07-22	06:36:41.000000	2023-0	7-22 06	
:36:56.0	00000											
** 2488	2180	explorer.exe	0xcc068ec78080	49		1	False	2023-07-22	06:36:43.000000	N/A		
* 976	596	dwm.exe 0xcc068e	≥14a300 16		1	False	2023-07-	-22 06:33:42	2.000000 N/A			
forensio	@WIN-AJD	B7GOIQEJ:/mnt/c/	/Cases/Analysis/N	Memory\$ \	vol -f w	in10-memo	ory.raw w	windows.dll	listpid 596			
Volatili	lty 3 Fra	mework 2.4.1										
^CTraceb	ack (mos	t recent call la	ast):									
File "	/home/fo	prensic/.local/bi	in/vol", line 8,	in <modu< td=""><td>ule></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></modu<>	ule>							
sys.	exit(mai	.n())										
File "	/home/fo	rensic/.local/li	ib/python3.8/sit	e-package	es/volat:	ility3/c]	li/init	tpy", lin	ne 797, in main			
Comn	nandLine().run()										
File "	/home/fo	prensic/.local/li	ib/python3.8/site	e-package	es/volat:	ility3/c]	li/init	tpy", lin	ne 302, in run			
auto	magics =	 automagic.avai] 	lable(ctx)									
File "	/home/fo	prensic/.local/li	ib/python3.8/site	e-package	es/volat:	ility3/fr	ramework/	/automagic/_	initpy", line 37	, in av	ailable	
impo	ort_files	(sys.modules[r	name])									
File "	/home/fo	prensic/.local/li	ib/python3.8/site	e-package	es/volat:	ility3/fr	ramework/	/initpy	y", line 152, in impo	rt_file	s	
fail	ures +=	<pre>import_file(</pre>										
File "	/home/fo	prensic/.local/li	ib/python3.8/site	e-package	es/volat:	ility3/fr	ramework/	/initpy	y", line 184, in impo	rt_file		
impo	ortlib.im	port_module(modu	ule)									
File "	'/usr/lib	/python3.8/impor	<pre>rtlib/initpy</pre>	y", line	127, in	import_n	nodule					
retu	ırn _boot	strapgcd_impor	<pre>rt(name[level:],</pre>	package	, level)							
File "	' <frozen< td=""><td><pre>importlibboots</pre></td><td>strap>", line 10</td><td>14, in _į</td><td>gcd_impo</td><td>rt</td><td></td><td></td><td></td><td></td><td></td><td></td></frozen<>	<pre>importlibboots</pre>	strap>", line 10	14, in _į	gcd_impo	rt						
File "	' <frozen< td=""><td><pre>importlibboots</pre></td><td>strap>", line 99:</td><td>1, in _fi</td><td>ind_and_</td><td>load</td><td></td><td>Search</td><td>other files run on r</td><td>hid no</td><td>596</td><td></td></frozen<>	<pre>importlibboots</pre>	strap>", line 99:	1, in _fi	ind_and_	load		Search	other files run on r	hid no	596	
File " <frozen importlibbootstrap="">", line 975, in _find_and_load_unlocked Scaren onler mestan on pid no 570</frozen>												
File "	' <frozen< td=""><td><pre>importlibboots</pre></td><td>strap>", line 67:</td><td>1, in _l(</td><td>oad_unlo</td><td>cked</td><td></td><td>using a</td><td>dll list</td><td></td><td></td><td></td></frozen<>	<pre>importlibboots</pre>	strap>", line 67:	1, in _l(oad_unlo	cked		using a	dll list			
File "	' <frozen< td=""><td><pre>importlibboots</pre></td><td>strap_external>"</td><td>, line 84</td><td>44, in e</td><td>xec_modul</td><td>le</td><td>00</td><td></td><td></td><td></td><td></td></frozen<>	<pre>importlibboots</pre>	strap_external>"	, line 84	44, in e	xec_modul	le	00				
File "	<frozen< td=""><td><pre>importlibboots</pre></td><td>strap_external>"</td><td>, line 93</td><td>39, in g</td><td>et_code</td><td></td><td></td><td></td><td></td><td></td><td></td></frozen<>	<pre>importlibboots</pre>	strap_external>"	, line 93	39, in g	et_code						
File "	<frozen< td=""><td><pre>importlibboots</pre></td><td>strap_external>"</td><td>, line 10</td><td>038, in</td><td>get_data</td><td></td><td></td><td></td><td></td><td></td><td></td></frozen<>	<pre>importlibboots</pre>	strap_external>"	, line 10	038, in	get_data						
Keyboard	eyboardInterrupt											

forensic@WIN-AJDB7G0IQEJ:/mnt/c/Cases/Analysis/Memory\$ vol -f win10-memory.raw windows.dlllist --pid 596 > dll.txt
forensic@WIN-AJDB7G0IQEJ:/mnt/c/Cases/Analysis/Memory\$ _



へ EP 4<mark>8 22-07-2023</mark>

 \mathbf{v}



G)	Select forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Anal	ysis/Memory	r
----	--	-------------	---

KeyboardInterrupt

forensio	@WIN-AJDB7GOIQE]:/mnt/c/	/Cases/An	nalysis/Me	mory\$ vol -f	win10-memo	ory.raw windows.dl	llistpid 5	96 > dll.txt	
forensio	@WIN-AJDB7GOIQE]:/mnt/c/	/Cases/An	nalysis/Me	mory\$ vol -f	win10-memo	ory.raw windows.dl	llistpid 5	96dump	
Volatili	ity 3 Framework 2	2.4.1			-					
Progress	5: 100.00		PDB scan	ning fini	shed			Ext	ract the files a	ind give
PID	Process Base	Size	Name	Path Lo	oadTime	File out	tput			
								moi	e information]
596	winlogon.exe	0x7++674	4bb0000	0xec000 w	inlogon.exe	C:\Windo	ows\system32\winlo	gon.exe	2023-07-22 0	6:33:37.0
00000	pid.596.winlogo	n.exe.0x1	la † 71 † 81e	290.0x7++6	74bb0000.dmp					
596	winlogon.exe	0x7++942	2430000	0x1+5000	ntdll.	dll	C:\Windows\SYSTEM	32\ntdll.dll	2023-07-22 0	6:33:37.0
00000	pid.596.ntdl1.d	ll.0x1af7	71 f 81d00.	0x7ff9424	30000.dmp					
596	winlogon.exe	0x7ff941	LF10000	0xbe000 K	ERNEL32.DLL	C:\Windo	ows\System32\KERNE	L32.DLL	2023-07-22 0	6:33:37.0
00000	pid.596.KERNEL3	2.DLL.0x1	Laf71f824	130.0x7ff9	41f10000.dmp					
596	winlogon.exe	0x7ff93f	Fe70000	0x2c9000	KERNEL	BASE.dll	C:\Windows\System	32\KERNELBASE	.dll 2023	-07-22 06
:33:37.0	000000 pid.596	.KERNELBA	ASE.dll.e	0x1af71f82	a40.0x7ff93fe	70000.dmp				
596	winlogon.exe	0x7ff941	Le70000	0x9e000 m	svcrt.dll	C:\Windo	ows\System32\msvcr	t.dll 2023-0	7-22 06:33:37.	000000 p
id.596.n	nsvcrt.dll.0x1af	71f83c50.	.0x7ff941	Le70000.dm	p					
596	winlogon.exe	0x7ff942	2350000	0x9b000 s	echost.dll	C:\Windo	ows\System32\secho	st.dll 2023-0	7-22 06:33:37.	000000 p
id.596.9	sechost.dll.0x1a	f71f83fd0	0.0x7ff94	12350000.di	mp					
596	winlogon.exe	0x7ff941	1480000	0x12a000	RPCRT4	.dll	C:\Windows\System	32\RPCRT4.dll	2023-07-22 0	6:33:37.0
00000	pid.596.RPCRT4.0	dll.0x1af	F71f843c0	0.0x7ff941	480000.dmp					
596	winlogon.exe	0x7ff940	9630000	0x355000	combas	e.dll	C:\Windows\System	32\combase.dl	1 2023-07-22 0	6:33:37.0
00000	pid.596.combase	.dll.0x1a	af71f8480	0.0x7ff94	0630000.dmp					
596	winlogon.exe	0x7ff940	9210000	0x100000	ucrtba	se.dll	C:\Windows\System	32\ucrtbase.d	11 2023	-07-22 06
:33:37.0	000000 pid.596	.ucrtbase	e.dll.0x1	laf71f84cc	0.0x7ff940210	000.dmp				
596	winlogon.exe	0x7ff941	12f0000	0xac000 a	dvapi32.dll	C:\Windo	ows\System32\advap	i32.dll	2023-07-22 0	6:33:37.0
00000	pid.596.advapi32	2.dll.0x1	laf71f856	580.0x7ff94	412f0000.dmp					
596	winlogon.exe	0x7ff93f	F9c0000	0x4b000 p	owrprof.dll	C:\Windo	ows\SYSTEM32\powrp	rof.dll	2023-07-22 0	6:33:37.0
00000	pid.596.powrpro	f.dll.0x1	laf71f850	0e0.0x7ff9	3f9c0000.dmp					
596	winlogon.exe	0x7ff93f	F9a0000	0x12000 U	MPDC.dll	C:\Windo	ows\system32\UMPDC	.dll 2023-0	7-22 06:33:37.	000000 p
id.596.U	JMPDC.dll.0x1af7:	1f91ac0.0	0x7ff93f9	a0000.dmp						
596	winlogon.exe	0x7ff93f	Fa90000	0x1f000 p	rofapi.dll	C:\Windo	ows\system32\profa	pi.dll 2023-0	7-22 06:33:37.	000000 p
id.596.p	profapi.dll.0x1a	f71f849e0	0.0x7ff93	3fa90000.d	mp					
596	winlogon.exe	0x7ff940	9480000	0x1a1000	user32	.dll	C:\Windows\System	32\user32.dll	2023-07-22 0	6:33:37.0
00000	pid.596.user32.0	dll.0x1af	F71f96e90	0.0x7ff940	480000.dmp					
596	winlogon.exe	0x7ff93f	Fb50000	0x22000 w	in32u.dll	C:\Windo	ows\System32\win32	u.dll 2023-0	7-22 06:33:37.	000000 p
	р Ц: 🥖		(1)						へ 町 d。 ¹²	2:45
				<u> </u>					22-0	7-2023





 \frown

 \mathbf{v}

📊 🛃 📕 🖛 Mer	mory										đ	\times
File Home	Share	View										~ 🕐
Pin to Quick Copy access	Daste Paste	✓ Cut ✓ Copy path Paste shortcut	Move Copy to •	Delete Renar	me New folder	ew item ▼ sy access ▼	Properties	Open ▼ Edit	Select all Select nor Invert sele	ection		
Clip	oboard		Org	anize	New	1	Ор	en	Select			
$\leftarrow \rightarrow \checkmark \land $	> Th	is PC > SDT_x64FR	EE_EN-US_VHD (C:) > Cases >	Analysis > Mem	ory			~ Ū	Search Memory		م ر
- Evidence	^	Name	^		Date modified	Туре		Size				^
- Execution		dll			22-07-2023 12:36	Text Do	cument	6 KB	Í.			
Memory		pid.596.adva	pi32.dll.0x1af71f8	5680.0x7ff9	22-07-2023 12:44	DMP Fil	e	688 KB				
Registry		pid.596.appł	nelp.dll.0x1af71fa9	ac0.0x7ff93	22-07-2023 12:45	DMP Fil	e	576 KB		01	1	
This DC	- 10	pid.596.Bcry	pt.dll.0x1af71f98d	70.0x7ff940	22-07-2023 12:44	DMP Fil	e	156 KB		Show the all	aump	
		pid.596.bcry	ptprimitives.dll.0x	1af71f98ea	22-07-2023 12:44	DMP Fil	e	524 KB	1	file in memor	y fold	er
3D Objects		📄 pid.596.com	base.dll.0x1af71f8	4800.0x7ff9	22-07-2023 12:44	DMP Fil	e	3,412 KB			•	
📃 Desktop		pid.596.CRY	PT32.dll.0x1af71fa	9860.0x7ff9	22-07-2023 12:45	DMP Fil	e	1,368 KB				
🔮 Documents		pid.596.CRY	PTBASE.dll.0x1af7	1fa8db0.0x	22-07-2023 12:45	DMP Fil	e	48 KB				
👆 Downloads		pid.596.cryp	tsp.dll.0x1af71fa87	7c0.0x7ff93f	22-07-2023 12:45	DMP Fil	e	96 KB				
👌 Music		pid.596.DNS	API.dll.0x1af71f98	780.0x7ff93	22-07-2023 12:44	DMP Fil	e	816 KB				
Pictures		pid.596.DPA	PI.dll.0x1af71fa999	0.0x7ff93f8	22-07-2023 12:45	DMP Fil	e	40 KB				
Videos		pid.596.dsre	g.dll.0x1af71fa88f(0.0x7ff93c6	22-07-2023 12:45	DMP Fil	e	1,276 KB				
	EN	jpid.596.dwm	napi.dll.0x1af71fa9	4d0.0x7ff93	22-07-2023 12:45	DMP Fil	e	188 KB				
		pid.596.dwm	hinit.dll.0x1af71fa9	0600.0x7ff93	22-07-2023 12:45	DMP Fil	e	80 KB				
to Drive (D:)	VIE	pid.596.firew	allapi.dll.0x1af71f	99100.0x7ff	22-07-2023 12:44	DMP Fil	e	636 KB				
🛫 Downloads (\	(\VE	pid.596.fwba	se.dll.0x1af71fa84	30.0x7ff93e	22-07-2023 12:44	DMP Fil	e	188 KB				
💣 Network		pid.596.GDI3	2.dll.0x1af71f9827	0.0x7ff9417	22-07-2023 12:44	DMP Fil	e	172 KB				
		pid.596.gdi3	2tull.dll.0x1at/1f9	8860.0x/ft9	22-07-2023 12:44	DMP Fil	e	1,068 KB				
50 items 1 item s	▼	5 66 KB	52.DEL.0x1at71f98	sstu.ux/tt94	22-07-2023 12:44	DIVIP FI	e	192 KB				
Joittems Tittem s	elected	2.00 KD										

^ ₽ 4<mark>×</mark> 22-07-2023 ₽

오 H 🤶 🗔 🍅 <u> (</u>

Select forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory	-	- 0	\times
96.MPR.dll.0x1af71faa0b0.0x7ff939b60000.dmp			^
<pre>torensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory\$ LThis program connet be rup in DOS mode</pre>	strings pid.596.dsreg.dll.0x1a+71+a88+0.0x7++93c680000.dmp		
Picho			
text			
` rdata			
0. data			
pdata			
0.didat			
rsrc	Gathering deep information using		
@.reloc			
L\$0H	particular dmp file.		
L\$xH			
L\$(H			
D\$0H			
D\$ H			
L\$0H3			
\\$XH			
t\$`H			
T\$xL			
D\$0A			
D\$41			
19580 £A9790			
fA9<@u			
D\$`H			
D\$PH			
D\$0L			
D\$pE3			
L\$xI			
\$ H			
M@H3			
A^_]			
t\$ UWAWH			~
🚛 🔎 🛱 🧀 🦳	へ む 4× 。	12:47	5

Identify process owners and associated SIDs

~

22-07-2023

Windows.getsids.GetSIDs plugin use for print SIDs owning each process.

🧿 fore	ensic@WIN-AJDB7GOIQE	J: /mnt/c/Cases/Analys	is/Memory	
TTBL				
TEMP				
TEMPP				
H7^A				
TEMP\$				
TEMP				
TEMP				
TEMP				
TEMPO				
B=7=				
foren	sic@WTN-ADB7GOTC	DEl:/mpt/c/Cases	/Analysis/Memory\$ vol _f win10-	memory raw windows getsids _h
Volat	ility 3 Eramework	2.4.1	/Analysis/Hemoryp voi -1 winite-	memory.raw windows.getsids -n
usage	· volatility wind	dows_getsids_Get	STDs [-h] [pid [PTD [PTD]	11
asage	· ····································	ions.Becords.dec	5105 [II] [P14 [I15 [I15 III]	11
optio	nal arguments:			
'-h,	help	show this hel	p message and exit	
p	id [PID [PID]	11		
		Filter on spe	cific process IDs	
foren	sic@WIN-AJDB7GOIQ	QEJ:/mnt/c/Cases	/Analysis/Memory\$ vol -f win10-	memory.raw windows.getsidspid 596 532
Volat	ility 3 Framework	< 2.4.1		
Progr	ess: 100.00	PDB s	canning finished	
PID	Process SID	Name		
532	CERES AVA	5-1-5-18	Local System	
532		5-1-5-32-544	Administrators	
532	CSrSS_exe	5-1-1-0 Every	one	Getsids plugin use for find the owner of
532	csrss.exe	5-1-5-11	Authenticated Users	
532	csrss.exe	5-1-16-16384	System Mandatory Level	the process show the output here
596	winlogon.exe	S-1-5-18	Local System	the process show the output here.
596	winlogon.exe	S-1-5-32-544	Administrators	
596	winlogon.exe	S-1-1-0 Every	one	
596	winlogon.exe	S-1-5-11	Authenticated Users	
596	winlogon.exe	5-1-16-16384	System Mandatory Level	
foren	sic@WIN-AJDB7GOIQ	QEJ:/mnt/c/Cases	/Analysis/Memory\$	
				13:10

Detecting and Analyzing malicious registry key entries from memory

Of forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory	- Ø	\times
<pre>forensic@WIN-AJDB7G0IQEJ:/mnt/c/Cases/Analysis/Memory\$ vol -f win10-memory.raw windows.registry.printke</pre>	y -h	
Volatility 3 Framework 2.4.1		
usage: volatility windows.registry.printkey.PrintKey [-h] [offset OFFSET] [key KEY] [recurse]		
<pre>optional arguments: -h,help show this help message and exit -offset OFFSET Hive Offset key KEY Key to start from recurse Recurses through keys forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory\$ vol -f win10-memory.raw windows.registry.hivelis Volatility 3 Framework 2.4.1 Progress: 100.00 PDB scanning finished</pre>	t	
Offset FileFullPath File output		
0xa3030e855000Disabled0xa3030e895000\REGISTRY\MACHINE\SYSTEMDisabled0xa3030e898000\REGISTRY\MACHINE\SYSTEMDisabled0xa30310551000\SystemRoot\System32\Config\SAMDisabled0xa30310551000\SystemRoot\System32\Config\SECURITYDisabled0xa3031051000\SystemRoot\System32\Config\SECURITYDisabled0xa3031051000\SystemRoot\System32\Config\SECURITYDisabled0xa3031051000\SystemRoot\System32\Config\SOFTWAREDisabled0xa303124b0000\Device\HarddiskVolume1\Boot\BCDDisabled0xa3031224b0000\??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DATDisabled0xa30312247000\??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DATDisabled0xa3031223e000\??\C:\Windows\AppCompat\Programs\Amcache.hveDisabled0xa30314219000\??\C:\Windows\AppCompat\Programs\Amcache.hveDisabled0xa30314219000\??\C:\Users\Denisha\ntuser.datDisabled	sistry print key try hive list find on specific key	
<pre>0xa30314774000 \??\C:\Users\Denisha\AppData\Local\Microsoft\Windows\UsrClass.dat Disabled</pre>		
0xa30316deb000 \SystemRoot\System32\config\DRIVERS Disabled		
<pre>0xa30317618000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Search_1.</pre>	14.2.19041_neutral_ne	au
tral_cw5n1h2txyewy\ActivationStore.dat Disabled		
<pre>0xa30317586000 \??\C:\Users\Denisha\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\Sett</pre>	ings\settings.dat	D
isabled		
0xa3031//b6000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.StartMenu	ExperienceHost_10.0.1	.9
forensic@WIN-AJDB7G0I0EJ:/mnt/c/Cases/Analysis/Memory\$ vol -f win10-memory.raw windows.registry.printke	voffset 0xa3031477	14
000key AtomicRedTeam		
	へ に	1

forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory\$ vol -f win10-memory.raw windows.registry.printkey --offset 0xa30314774 ^ 000 --key AtomicRedTeam

> Using this command find the detail about Atomic RedTeam key value(any key enter).





 \mathbf{v}

 \times

D

Super Timeline Analysis

A detailed timeline of everything that occurred on a system, also known as a Super Timeline, can be extremely beneficial in determining what took place in a digital investigation.

1. Prepare Tools

Volatility3 Plaso Log2Timeline QEMU

2. Prepare Evidence

Disk image(RAW!) Memory image

3. Run Tools

Memory-generate bodyfile Disk-generate plaso file Merge files Generate super timeline with psort

4. Timeline Analysis EZ Timeline Explorer

Prepare tools and Converting the disk image with QEMU

Use the link for install the Tools

forensic@WIN-AJDB7GOIQEJ: ~	—	þ	\times
<pre>forensic@WIN-AJDB7GOIQEJ:~\$ sudo add-apt-repository ppa:gift/stable [sudo] password for forensic: Periodic releases, contains periodic releases intended for non-development use More info: https://launchpad.net/~gift/+archive/ubuntu/stable Press [ENTER] to continue or Ctrl-c to cancel adding it.</pre>			^
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease Hit:2 http://archive.ubuntu.com/ubuntu focal-updates InRelease Hit:3 http://security.ubuntu.com/ubuntu focal-security InRelease Get:4 http://ppa.launchpad.net/gift/stable/ubuntu focal InRelease [18.0 kB] Hit:5 http://archive.ubuntu.com/ubuntu focal-backports InRelease			

Add the plaso GIFT repository for this command.





forensic@WIN-AJDB7GOIQEJ: ~	—	ð
Get:4 http://ppa.launchpad.net/gift/stable/ubuntu focal InRelease [18.0 kB]		
Hit:5 http://archive.ubuntu.com/ubuntu focal-backports InRelease		
0% [Working] Satu Subtra (/ana lawashand ant/aist/atable/whysia) Satu Subtrain and St. Dashanna [SD. O. HD]		
Get:6 http://ppa.launcnpad.net/gift/stable/ubuntu focal/main amd64 Packages [63.0 kB]		
Get:/ http://ppa.iaunchpad.net/gitt/stable/ubuntu tocal/main Translation-en [1/.1 kB]		
Reading package lists Done		
forensic@WIN_AIDB7GOTOFI\$		
forensic@WIN_AJDB7GOTOF1:~\$ sudo apt install gemu-utils		
Reading package lists Done		
Building dependency tree		
Reading state information Done		
The following additional packages will be installed:		
ibverbs-providers libboost-iostreams1.71.0 libboost-thread1.71.0 libibverbs1 libiscsi7 libnl-3-200 libnl-route	-3-200	9
librados2 librbd1 librdmacm1 qemu-block-extra sharutils		
Suggested packages:		
debootstrap sharutils-doc bsd-mailx mailx		
The following NEW packages will be installed:		
ibverbs-providers libboost-iostreams1.71.0 libboost-thread1.71.0 libibverbs1 libiscsi7 libnl-3-200 libnl-route	-3-200	9
librados2 librbd1 librdmacm1 qemu-block-extra qemu-utils sharutils		
0 upgraded, 13 newly installed, 0 to remove and 261 not upgraded.		
Need to get 7133 kB of archives.		
After this operation, 33.7 MB of additional disk space will be used.		
Do you want to continue? [Y/n] Y Catua https://anchive.whwntw.com/whwntw.facel.wndates/main.and64_libel_2_200_and64_2_4_0_awhwntw0_4_[F4_4_kD]		
Get:1 http://archive.ubuntu.com/ubuntu focal-updates/main amdo4 libni-3-200 amdo4 3.4.0-lubuntu0.1 [54.4 KB] Got:2 http://archive.ubuntu.com/ubuntu focal updates/main amd64 libni pouto 2 200 amd64 2 4 0 lubuntu0 1 [151 kB	1	
Get:3 http://archive.ubuntu.com/ubuntu focal/main amd64 libibyerbs1 amd64 28 0-1ubuntu1 [53 6 kB]	J	
Get:4 http://archive.ubuntu.com/ubuntu focal/main amd64 ibverbs-providers amd64 28.0-1ubuntu1 [232 kB]		
Get:5 http://archive.ubuntu.com/ubuntu focal/main amd64 libboost-iostreams1.71.0 amd64 1.71.0-6ubuntu6 [237 kB]		
Get:6 http://archive.ubuntu.com/ubuntu focal/main amd64 libboost-thread1.71.0 amd64 1.71.0-6ubuntu6 [249 kB]		
Get:7 http://archive.ubuntu.com/ubuntu focal/main amd64 librdmacm1 amd64 28.0-1ubuntu1 [64.9 kB]		
Get:8 http://archive.ubuntu.com/ubuntu focal/main amd64 libiscsi7 amd64 1.18.0-2 [63.9 kB]		
Get:9 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 librados2 amd64 15.2.17-0ubuntu0.20.04.4 [3227 k	В]	
Get:10 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 librbd1 amd64 15.2.17-0ubuntu0.20.04.4 [1625 kB]	
Get:11 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 qemu-block-extra amd64 1:4.2-3ubuntu6.27 [53.4	kB]	
Get:12 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 qemu-utils amd64 1:4.2-3ubuntu6.27 [969 kB]		
87% [12 qemu-utils 273 kB/969 kB 28%]	1010	kB/s (
	06:	23
	24-07-	-2023

)s_____

1

 \times

^

SVirtualBox VM Machine View Input Devices Window Help

×

Windows2019-FOR (after VOL memory analysis) [Running]



Recycle Bin





Ø



Arsenalima.

) 🛱 📄 🔤 🚳

forensics@WIN-BK1Q9542K3L: ~ - 0 Get:11 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f Metadata [520 8] Get:12 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [706 kB] Get:13 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [126 kB Get:14 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [14.5 kB] Get:15 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [22.2 kB] Get:16 http://security.ubuntu.com/ubuntu focal-security/multiverse Translation-en [5376 8] Get:17 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f Metadata [512 B] Get:18 http://ppa.launchpad.net/gift/stable/ubuntu focal/main amd64 Packages [62.9 kB] Get:19 http://ppa.launchpad.net/gift/stable/ubuntu focal/main Translation-en [17.1 kB] Get:20 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1874 kB] Get:21 http://archive.ubuntu.com/ubuntu focal-updates/main Translation-en [343 kB] Get:22 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [15.4 kB] Get:23 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [1842 k8] Get:24 http://archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [148 k8] Get:25 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 c-n-f Metadata [520 B] Get:26 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [927 kB] Get:27 http://archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [208 kB] Get:28 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [20.7 kB] Get:29 http://archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 c-n-f Metadata [596 8] Get:30 http://archive.ubuntu.com/ubuntu focal-backports/main amd64 Packages [44.5 k8] Get:31 http://archive.ubuntu.com/ubuntu focal-backports/main Translation-en [10.9 k8] Get:32 http://archive.ubuntu.com/ubuntu focal-backports/main amd64 c-n-f Metadata [980 B] Get:33 http://archive.ubuntu.com/ubuntu focal-backports/universe amd64 Packages [23.7 kB] Get:34 http://archive.ubuntu.com/ubuntu focal-backports/universe Translation-en [15.9 kB] Get:35 http://archive.ubuntu.com/ubuntu focal-backports/universe amd64 c-n-f Metadata [860 B] Fetched BB28 kB in 20s (434 kB/s) Reading package lists... Done

Forensics@WIN-BK109542K3L:-\$
forensics@WIN-BK109542K3L:-\$
sudo apt-get install plaso-tools
Building dependency tree... 0%

Install plaso tool





📙 🛃 📙 🖛 Cas	ses										_	đ	\times
File Home	Share	e View											~ 😨
Pin to Quick Copy access	Paste	 从 Cut ∞ Copy path Paste shortcut 	Move Copy to *	ename	New New folder	item • access •	Properties	Gpen → ZEdit	Select all	ne ection			
Clì	ipboaro	Ŀ	Organize		New		Ope	en	Select				
← → • ↑ 📘	r > Ti	his PC > SDT_x64FR	`EE_EN-US_VHD (C:) → Cas	es >					~ Ū	Search	Cases		Q
Evidence	^	Name	^	Da	ite modified	Туре		Size					
Execution		Analysis		16	-07-2023 11-24	File fold	er						
NTFS		F		30	-06-2023 08:31	File fold	er						
Registry		🕳 {0926ccea-dt	^s d7-4e08-bd93-7a85bd79797	7 29	-06-2023 15:38	Hard Dis	sk Image F	1,40,05,697	·				
		2023-06-30T	08_30_13_5798095_ConsoleL	og 30	-06-2023 08:31	Text Doo	cument	4 K	(B				
		2023-06-30T	08_30_13_5798095_CopyLog	30	-06-2023 08:31	CSV File	ř.	189 k	(B				
3D Objects		2023-06-30T	08_30_13_5798095_SkipLog.c	t sv 30)-06-2023 08:31	CSV File	ź	9 k	KB				
Desktop													
Documents													
👆 Downloads				-	. .	4							
🁌 Music			Pası	te hei	re the hard	disk.							
Pictures													
Videos													
L SDT_x64FREE	E_EN												
🥳 CD Drive (D:)) Vir												
🛖 Downloads ((\\VE												
💣 Network													
	~	1											
6 items													
	∃ †	🥭 🚍 🚺	۵							~ ^t	타 4× ~	17:42	易

오 H 🤶 📃







-

Notepad++

Q

Event Log Explorer

2

Arsenalima. - Shortcut

G forensics@WIN-8K1Q9542K3L: /mnt/c/Cases forensics@WIN-BK1Q9542K3L:~\$ cd /mnt/c/Cases/ forensics@WIN-BK109542K3L:/mnt/c/Cases\$ 1s -1 total 15433700 -rwxrwxrwx 1 forensics forensics 3760 Mar 23 22:40 2022-03-23T223835 ConsoleLog.txt -rwxrwxrwx 1 forensics forensics 195855 Mar 23 22:40 2022-03-23T223835_CopyLog.csv -rwxrwxrwx 1 forensics forensics 9630 Mar 23 22:40 2022-03-23T223835_SkipLog.csv 512 Jun 7 17:51 drwxrwxrwx 1 forensics forensics drwxrwxrwx 1 forensics forensics 512 Mar 23 22:40 -rwxrwxrwx 1 forensics forensics 7374 May 18 04:37 Notes.docx -rwxrwxrwx 1 forensics forensics 15803884544 Mar 19 00:13 win10-disk.vhd

forensics@WIN-BK109542K3L:/mnt/c/Cases\$ gemu-img convert -0 raw win10-disk.vhd win10-disk.raw
forensics@WIN-BK109542K3L:/mnt/c/Cases\$ _

\$

qemu-ing convert –O raw win10disk.vhd win10-disk.raw

- 0

×

This PC

Using the Following Command converting the disk image.

Videos
Local Disk (C:)
CD Drive (D:) VirtualBox Guest Additions
Commant: (1) VBoxGue) (7:)
I0 items 1 item selected





Firefox



Event Log Explorer



Arsenalima... - Shortcut









Memory timeline creation with Volatility3

Create a folder Timeline . Go to the folder path in ubuntu linux.
















-

6



Using vol –h show all plugins in detail.



0

~



0





Select forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline









- Shortcut

Π

-

0

<pre>lists all network connections for all processes. mac.proce.maps.phys Lists process memory ranges that potentially contain injected code. mac.porce.maps.phys Lists processes programe command line arguments. mac.pslist.Plists Lists the processes present in a particular mac memory image. mac.stree.PsTree Plugin for listing processes in a tree based on their parent process ID. mac.stree.PsTree Plugin for listing processes in a tree based on their parent process ID. mac.stree.PsTree Plugin for listing processes in a tree based on their parent process ID. mac.stree.PsTree Plugin for listing processes in a tree based on their parent process ID. mac.stree.PsTree Plugin for listing processes in a tree based on their parent process ID. mac.trutedbid.Trustedbid mac.trutedbid.Trustedbid mac.trutedbid.Trustedbid mac.visevents.VFSevents infections_listing processes that are filtering file system events if inclines_listing processes that are filtering file system events if inclines_listing processes command line arguments. windows.cellbacks.Cellbacks (lists kernel callbacks and notification routines. windows.cellbacks.Cellbacks cellbacks.Cellbacks it ists process command line arguments. windows.cellbacks.Cellbacks if the source.provering uindows.defiles_DougFiles December 2. windows.defiles_DougFiles December 2. windows.files.Dup process environment variables windows.files.Stand itsts process token sids. windows.entifiescing files files process token sids. windows.matind.Halfund windows.fore file for modules present in a particular windows memory</pre>		mac.netstat.Netstat		
<pre>mac.proc.sups.Mps Lists process memory ranges that potentially contain injected code. mac.psaux.Paux Recover program command line arguments. mac.pstree.Pstree Plugin for listing processes in a particular mac memory image. mac.stet.filters.Socket_filters. mac.timers.Timers (theck for malicious kernel timers. mac.timers.Timers (theck for malicious kernel timers. mac.timers.Timers (theck for malicious kernel timers. mac.timers.Timers (theck for malicious trustedbsd modules mac.vfsevents.Wfsevents Lists processes that are filtering file system events timelineimeline</pre>			Lists all network connections for all processes.	
<pre>mac.psux.Psax Recovers program command line arguments. mac.pslist.Psix L hists the processes present in a particular mac memory image. mac.pslist.Psix Lines.Socket filters. Fundementes kernel socket filters. mac.titers.Fire Plugin for listing processes in a tree based on their parent process ID. mac.tocket.filters.Socket.filters. mac.trustedbsd.Trustedbsd modules mac.vfsevents.VFsevents Lists processes that are filtering file system events Lists process command line arguments. windows.callbacks. windows.callbacks. windows.callbacks List big page pools. windows.callbacks. windows.callbacks for drivers in a particular windows memory image. windows.drivers. Dusp cached file contents from Windows memory image. windows.files.can.FileScan Dusp cached file contents from Windows memory image. windows.files.can.FileScan Scans for file objects present in a particular windows memory image. windows.files.can.FileScan Display process environment variables windows.santind.Austinu windows.malfied.Namdles. windows.info.Info the SiDS owning each process windows.malfied.Namdles. w</pre>		mac.proc_maps.Maps	Lists process memory ranges that potentially contain injected code.	
<pre>mac.pslist.Pslist Lists the processes present in a particular mac memory image. mac.storee.Pslist.Pslist [lists the processes in a true based on their parent process ID. mac.stockt_filters.Scoket_filters mac.tarkstedbasch_Trustedbas mac.trustedbasch_Trustedbas mac.trustedbasch_Trustedbas mac.trustedbasch_Trustedbas mac.storee.Pslist lists process schat are filtering file system events lists process schat are filtering file system events lists process schat are filtering file system events list big page pols. windows.callbacks lists big page pols. windows.callbacks lists kernel callbacks and notification routines. windows.callbacks lists the loaded modules in a particular windows memory image. windows.driverinp.Drivering lists the loaded modules in a particular windows memory image. windows.driverinp.Drivering list IDPs for drivers in a particular windows memory image. windows.drivers.an.DriverScan Scans for drivers present in a particular windows memory image. windows.drivers.frwars lists process cenvironment variables windows.getservicesids.detForwiceSDs lists process environment variables windows.info.Info Show 05 & kernel details of the memory samples height and gathering windows.info.Info Show 05 & kernel details of the memory sample being analyzed. windows.info.Info Show 05 & kernel details of the memory sample being analyzed. windows.info.Info Show 05 & kernel details of the memory sample being analyzed. windows.info.Info Show 05 & kernel details of the memory sample being analyzed. windows.info.Info Show 05 & kernel details of the memory sample being analyzed. windows.info.Info Show 05 & kernel details of the memory sample being analyzed. windows.info.Info Show 05 & kernel details of the memory sample being analyzed. windows.info.Info Show 05 & kernel details of the memory sample being analyzed. windows.info.Info Show 05 & kernel details of the memory image. windows.memory.temmory windows.memory.temmory using windows.memory.temmory using windows.heb Modules</pre>		mac.psaux.Psaux	Recovers program command line arguments.	
<pre>mac.pstree_Pirree_Plugin for listing processes in a tree based on their parent process ID. mac.stocket_filters.Stocket_filters. mac.timers.Filters.Stocket_filters. mac.timers.Filters.Stocket_filters. mac.timers.Filters.Stocket_filters. mac.timers.Filters.Stocket_filters. mac.timers.Filter</pre>		mac.pslist.PsList	Lists the processes present in a particular mac memory image.	
<pre>mac.socket_filters Enumerates kernel socket filters. mac.timers.Timers Check for malicious kernel timers. mac.trustebdd Checks for malicious trustedbsd modules mac.vfsevents Lists processes that are filtering file system events timeliner Runs all relevant plugins that provide time related information and orders the results by time. Windows.fileplore Runs all relevant plugins that provide time related information and orders the results by time. Windows.calks.Callbacks Lists big page pools. Windows.caddine Lists kernel callbacks and notification routines. Windows.cdfiles.Common Lists the loaded modules in a particular windows memory image. Windows.driverirp.DriveFirp List TBPs for drivers in a particular windows memory image. Windows.drivers.can DriverScan Scans for file objects present in a particular windows memory image. Windows.drivers.Envors Dumps cached file contents from Windows memory samples. Windows.equestids.detServiceSiDs Windows.ifies.on.FileScan Kindows.getsrvicesids.detServiceSiDs Windows.info.Info Show OS & Kernel details of the memory sample being analyzed. Windows.info.Info Show OS & Kernel details of the memory sample being analyzed. Windows.info.Info Show OS & Kernel details of the memory sample being analyzed. Windows.info.Info Show OS & Kernel details of the memory sample being analyzed. Windows.info.Info Show OS & Kernel details of the memory sample being analyzed. Windows.info.Info Show OS & Kernel details of the memory sample being analyzed. Windows.info.Info Show OS & Kernel details of the memory sample being analyzed. Windows.memory.Memang Windows.me</pre>		mac.pstree.PsTree	Plugin for listing processes in a tree based on their parent process	ID.
Enumerates kernel socket filters. mac.timers.Check for malicious kernel timers. mac.timers.Times Check for malicious trustedbad modules mac.vfsevents.VFSevents Lists processes that are filtering file system events timeliner_lineliner Runs all relevant plugins that provide time related information and orders the results by time. windows.callbacks.Callbacks windows.callbacks.Callbacks and notification routines. windows.calline.CadLine Lists process command line arguments. windows.crashinfo.Crashinfo windows.crashinfo.Crashinfo windows.driverinp.DriverIrp Lists the loaded modules in a particular windows memory image. windows.drivers.an DriverScan Scans for file objects present in a particular windows memory image. windows.getServicesids.GetServiceSIDS windows.getServicesids.GetServiceSIDS windows.getServicesids.GetServiceSIDS windows.getServicesids.GetServiceSIDS windows.getServicesids.GetServiceSIDS windows.getServicesids.GetServiceSIDS windows.malfind.Nalfind Lists process kolen sids. windows.malfind.Nalfind Lists process memory mage that potentially contain injected code. windows.malfind.Nalfind Checks for mules present in a particular windows memory using timeline plugins. Mindows.malfind.Nalfind Checks for modules present in a particular windows memory using timeline plugins. Mindows.malfind.Nalfind Checks process memory mage that potentially contain injected code. Windows.memory.Memory Windows.memory.Memory Windows.memory.Memory Windows.memory.Memory Windows.memory.Memory Windows.memory.Memory Manfind Kens for modules present in a particular windows memory image. Windows.memory.Memory Windows.memory.Memory Manfind Windows.memory.Memory Manfind Kens for modules present in a particular windows memory image. Windows.memory.Memory Manfind Windows.memory.Memory Manfind Kens for modules present in a particular windows memory image. Windows.memory.Memory Manfind Windows.memory.Memory Manfind Windows.memory.Memory Manfind Windows.Memory Manfind Windows.memory.Memo		<pre>mac.socket_filters.</pre>	Socket_filters	
<pre>mac.timers.Timers Check for multicious kernel timers. mac.trustedbod Checks for multicious trustedbsd modules mac.trustedbsd.Trustedbsd Lists processes that are filtering file system events timeliner.Timeliner Runs all relevant plugins that provide time related information and orders the results by time. windows.digools.BigPools List big page pools. windows.callbacks.List big page pools. windows.callbacks.List kernel callbacks and notification routines. windows.crashinfo.Crashinfo Lists process command line arguments. windows.crashinfo.Crashinfo Lists the loaded modules in a particular windows memory image. windows.driverinp.Driverinp List TRPs for drivers in a particular windows memory image. windows.diles.Doumpiles Dumps cached file contents from Windows memory image. windows.getservicesids.GetServiceSIDS Lists process token sids. windows.handles.Hundles Lists process token sids. windows.handles.Hundles Lists process token sids. windows.handles.Hundles Lists process token sids. windows.handles.Hundles Lists process token sids. windows.network.The SIDs owning each process windows.handles.Hundles Lists process token sids. windows.memop.Memmap Prints the memory map windows.memop.Memmap Membus Modules present in a particular windows memory image. windows.memop.Memmap Memdows.memop.Memmap Memdows.memop.Memmap Memdows.memop.Memmap Memdows.Memmap Membus Modules present in a particular windows memory image. Windows.memop.Memmap Memdows.memop.Memmap Memdows.Memmap Membus Modules Memory map Membus Memory Memmap Memory Memory Memmap Memory Memory M</pre>			Enumerates kernel socket filters.	
<pre>mac.trustedbsd.Trustedbsd Checks for malicious trustedbsd modules mac.vfsevents.VFSevents Lists processes that are filtering file system events timeliner Timeliner Runs all relevant plugins that provide time related information and orders the results by time. windows.chigpools.BigPools List big page pools. windows.callbacks.Callbacks Lists kernel callbacks and notification routines. windows.calline.GetLine Lists process command line arguments. windows.crashinfo windows.drivering.Drivering Lists the loaded modules in a particular windows memory image. windows.driverscan.DriverScan Scans for drivers present in a particular windows memory image. windows.filescan.FileScan windows.filescan.FileScan Lists process token sids. windows.getervicesids.GetServiceSIDS windows.newmap.temson Lists process token sids. windows.nemmap.temson Lists process token sids. windows.nemmap.temson Lists process token sids. windows.memmap.temson Lists process token sids. windows.memmap.temson Lists process token sids. windows.memmap.temson Lists process token sids. windows.memmap.temson Lists process memory ranges that potentially contain injected code windows.memmap.temson Prints the memory map windows.memiles.Modules Scans for modules present in a particular windows memory image. windows.memmap.temson Prints the memory map windows.memory.temson Scans for modules present in a particular windows memory image. windows.memory.temson Scans for modules present in a particular windows memory image. windows.memory.temson Scans for modules present in a particular windows memory image. windows.memory.temson Scans for modules present in a particular windows memory image. windows.memory.temson Scans for modules present in a particular windows memory image. windows.memory.temson Scans for modules present in a particular windows memory image. windows.memory.temson Scans for modules present in a particular windows memory image. windows methols to bottow scans for modules present in a particular windows memory image. windows.methols.temson scans f</pre>		mac.timers.Timers	Check for malicious kernel timers.	
Checks for malicious trustedbsd modules Lists processes that are filtering file system events Lists processes that are filtering file system events The line The Nums all relevant plugins that provide time related information and orders the results by time. List big page pools. List big page pools. Lists big page pools. Windows.callbacks. Callbacks Lists kernel callbacks and notification routines. Windows.calline.Calline Lists process command line arguments. Windows.crashinfo.Crashinfo Lists the loaded modules in a particular windows memory image. Windows.drivering.Drivering List TRPs for drivers present in a particular windows memory image. Windows.diles.Dumpfiles Dumps cached file contents from Windows memory image. Windows.getservicesids.GetservicesIDS Windows.getservicesids.GetservicesIDS Windows.handles.Handles Lists process token sids. Windows.handles.Handles Lists process coken sids. Windows.handles.Handles Lists process coken sids. Windows.memory.Bemmang Lists process coken sids. Windows.memory.Bemmang Mindows.Memory ang Mindows.memory.Bemmang Mindows.Memory ang Mindows.Memory ang Mindows.Memor		mac.trustedbsd.Trus	tedbsd	
<pre>mac.vfsevents.vFsevents Lists processes that are filtering file system events timeliner_fimeliner Runs all relevant plugins that provide time related information and orders the results by time. windows.bigpools.BigPools Lists to big page pools. windows.callbacks.callbacks Lists thereal callbacks and notification routines. windows.cmaline.cmdline Lists thereal callbacks and notification routines. windows.cashinfo.Crashinfo Windows.dliist.Dllist Lists the loaded modules in a particular windows memory image. windows.driverscan.DriverScan Scans for drivers present in a particular windows memory image. windows.flescan.FileScan Scans for file objects present in a particular windows memory image. windows.flescan.FileScan Scans for file objects present in a particular windows memory image. windows.getserviceids.detStDs Windows.handles.Handles Lists process token sids. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.amamap. Prints the memory mag windows.amamap. Prints the memory mag windows.memory. Scans for modules present in a particular windows memory image. windows.amamap. Prints the memory mag windows.amamap. Scans for modules present in a particular windows memory image. Windows.memory using timeline plugin.</pre>			Checks for malicious trustedbsd modules	
Lists processes that are filtering file system events Runs all relevant plugins that provide time related information and orders the results by time. windows.bigpools.BigPools List big page pools. Windows.callbacks.Callbacks Lists kernel callbacks and notification routines. Windows.calline.Gudline Lists process command line arguments. Windows.crashinfo.crashinfo Windows.diverirp.DriverIp List RPS for drivers in a particular windows memory image. Windows.driverirp.DriverIp List IRPS for drivers in a particular windows memory image. Windows.drivers.cnn.DriverScan Scans for drivers present in a particular windows memory image. Windows.files.can.FileScan Display process environment variables Windows.getserviceids.GetSTOS Mindows.getserviceids.GetSTOS Mindows.info.Info Show OS & kernel details of the memory sample being analyzed. Windows.info.Show OS & kernel details of the memory sample being analyzed. Windows.info.Info Show OS & kernel details of the memory sample being analyzed. Windows.info.Info Show OS & kernel details of the memory sample being analyzed. Windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. Windows.mamage.Memmag Prints the memory mage Windows.memage.Memmag Cans for modules present in a particular windows memory image. Windows.manalfind.Malfind Cases for file objects present in a particular windows memory image. Windows.manalfind.Malfind Cases for modules present in a particular windows memory image. Windows.mamage.Memmag Cases for modules present in a particular windows memory image. Windows.mamage.Memmag Cases for modules present in a particular windows memory image. Windows.mamage.Memmag Cases for modules present in a particular windows memory image. Windows.mamage.Memmag		<pre>mac.vfsevents.VFSev</pre>	ents	
Runs all relevant plugins that provide time related information and orders the results by time. Windows.bigpools. Windows.callbacks. Windows.callbacks. Windows.callbacks. Windows.cashinfo. Windows.crashinfo. Windows.driverizep. Lists the loaded modules in a particular windows memory image. Windows.driverizep. Uist RPs for drivers present in a particular windows memory image. Windows.driverizep. Windows.driverizep. Windows.driverscan. Scans for drivers present in a particular windows memory image. Windows.driverscan. Scans for file objects present in a particular windows memory image. Windows.driverscan. Scans for file objects present in a particular windows memory image. Windows.driverscan. Scans for file objects present in a particular windows memory image. Windows.driverscan. Scans for file objects present in a particular windows memory image. Windows.getserviceids.GetServiceSIDS Windows.andles.Handles. Windows.info.Info. Show 05 & kernel details of the memory sample being analyzed. Windows.andles.Handles Lists process open handles. Windows.memory.Memorg Prints the memory mage Windows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memory Mape Windows.methes.the memory mape Windows.memory.Memorg Mindows.memory.Memorg Mindows.memory.Memory Mape Mindows.memory.Memory Mape Mindows.Mem			Lists processes that are filtering file system events	
<pre>kuns all relevant plugins that provide time related information and orders the results by time. List big page pools. Windows.callbacks (allbacks Lists kernel callbacks and notification routines. Windows.cmdline.fmdline Lists process command line arguments. Windows.cmshinfo.Crashinfo Lists the loaded modules in a particular windows memory image. Windows.driverscon.DriverScon Scans for drivers present in a particular windows memory image. Windows.driverscan.DriverScon Scans for drivers present in a particular windows memory image. Windows.driverscan.DriverScon Display process environment variables Windows.getservicesids.GetServiceSIDS Lists process token sids. Windows.andies.Handles Windows.andies.Handles Lists process open hanles. Windows.analfind.Halfind Lists process memory mage that potentially contain injected code. Windows.modscan.ModScan Scans for modules present in a particular windows memory image. Windows.analfind.Halfind Lists process memory mage Windows.modscan.ModScan Scans for modules present in a particular windows memory image. Windows.modscan.ModScan Scans for for modules present in a particular windows memory image. Windows.modscan.ModScan Scans for modules present in a particular windows memory image. Windows.modscan.ModScan Scans for modules present in a particular windows memory image. Windows.modscan.ModScan Scans for modules present in a particular windows memory image. Windows.modscan.ModScan Scans for modules present in a particular windows memory image.</pre>		timeliner		
<pre>windows.bigpools. List big page pools. windows.callbacks.callbacks Lists kernel callbacks and notification routines. windows.cmdline.CmdLine Lists process command line arguments. windows.crashinfo.CrcAshinfo windows.dllist.Dllist Lists the loaded modules in a particular windows memory image. windows.driverscan.DriverScan Scans for drivers present in a particular windows memory image. windows.dumpfiles.Dumpfiles Dumps cached file contents from Windows memory image. windows.dumpfiles.Dumpfiles Dumps cached file contents from Windows memory image. windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.getservicesids.detSprviceSIDs Lists process open handles. Lists process open handles. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows.modscan.WodScan Scans for modules present in a particular windows memory image. windows memory. Hemmory Scans for modules present in a particular windows memory image. Windows memory. Is the memory map windows memory. Memory Scans for modules present in a particular windows memory image. Windows memory. Is the memory map windows memory memory. Is the memory map windows memor</pre>			Runs all relevant plugins that provide time related information and o	rders the results by time.
List big page pools. windows.callbacks Lists kernel callbacks windows.cashinfo.Crashinfo windows.crashinfo.Crashinfo windows.dllist.Dllist Lists the loaded modules in a particular windows memory image. windows.dllist.Dllist Lists the loaded modules in a particular windows memory image. windows.drivericp.DriverFrp List IRPs for drivers in a particular windows memory image. windows.driverscan.DriverScan windows.driverscan.DriverScan Display process environment variables windows.getservicesids.GetServiceSIDs Lists process token sids. windows.sinfo.Info Show 05 & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows.for Show 05 & kernel details of the memory sample being analyzed. windows.memmap.Memmap Scans for modules present in a particular windows memory image. windows.memmap.Memmap Scans for modules present in a particular windows memory image. windows.memmap.Memmap Scans for modules present in a particular windows memory image. windows.memmap.Memmap		windows.bigpools.Bi	gPools	
<pre>windows.callbacks Lists kernel callbacks and notification routines. windows.cmdline.CmdLine Lists process command line arguments. windows.crashinfo.Crashinfo windows.dlllist.Dlllist Lists the loaded modules in a particular windows memory image. windows.diverscan.DriverSran Scans for drivers present in a particular windows memory image. windows.dumpfiles.Dumpfiles Dumps cached file contents from Windows memory samples. windows.envars.Envars Display process environment variables windows.filescan.fileScan Lists process token sids. windows.getservicesids.GetSTDs windows.handles.Handles Lists process open handles. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows.memmap.Memmap Scans for modules present in a particular windows memory image. windows.memmap.Memmap Scans for modules present in a particular windows memory image. windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows for modules present in a particular windows memory image.</pre>			List big page pools.	
Lists kernel callbacks and notification routines. windows.cmdline.dine Lists process command line arguments. windows.dllist.Dllist Lists the loaded modules in a particular windows memory image. windows.dllist.Dllist Lists the loaded modules in a particular windows memory image. windows.driverscan.DriverScan Scans for drivers present in a particular windows memory image. windows.dumpfiles.Dumpfiles Dumps cached file contents from Windows memory samples. windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.adlis.detSIDs windows.info.Info Show 05 & kernel details of the memory sample being analyzed. windows.malfind.Nalfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modiscan.Modiscan Scans for modules present in a particular windows memory image.		windows.callbacks.C	allbacks	
<pre>windows.cmdline.cmdline Lists process command line arguments. windows.crashinfo.Crashinfo windows.dlllist.DllList List the loaded modules in a particular windows memory image. windows.driverspr.DriverTrp List IRPs for drivers in a particular windows memory image. windows.driverscan.DriverScan Scans for drivers present in a particular windows memory image. windows.dumpfiles.DumpFiles Dumps cached file contents from Windows memory samples. windows.envars.Envars Display process environment variables windows.getservicesIDS Lists process token sids. windows.getsids.GetSTDs windows.getsids.GetSTDs Lists process open handles. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.medifind.Malfind Lists process memory ranges that potentially contain injected code. windows.memap.Memmap Prints the memory map windows.modscan.ModesAn Scans for modules present in a particular windows memory image. windows.modscan.Wolkes</pre>			Lists kernel callbacks and notification routines.	
 Lists process command line arguments. windows.crashinfo.Crashinfo Lists the loaded modules in a particular windows memory image. windows.drivericp.DriverTrp List IRPs for drivers in a particular windows memory image. windows.driverscan.DriverScan Scans for drivers present in a particular windows memory image. windows.dumpfiles.Dumpfiles Dumps cached file contents from Windows memory samples. windows.filescan.fileScan Scans for file objects present in a particular windows memory image. windows.getservicesiOS windows.getservicesiOS windows.handles.Handles Lists process open handles. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.medifind. Lists process memory ranges that potentially contain injected code. windows.memap.Memmap Prints the memory map windows.modscan.Modles. 		windows.cmdline.Cmd	Line	
<pre>windows.crashinto.transhinto windows.dllist.Dlllist Lists the loaded modules in a particular windows memory image. windows.driverscan.DriverScan Scans for drivers present in a particular windows memory image. windows.dumpfiles.Dumpfiles Dumps cached file contents from Windows memory samples. windows.envars.Envars Display process environment variables windows.getservicesids.GetServiceSIDs Lists process token sids. windows.getsids.GetServiceSIDs Lists process token sids. windows.standles.Handles Windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image.</pre>		44	Lists process command line arguments.	
<pre>windows.dilist.billist Lists the loaded modules in a particular windows memory image. windows.drivers.DriverScan Scans for drivers present in a particular windows memory image. windows.dumpfiles Dumps cached file contents from Windows memory samples. windows.envars.Envars Display process environment variables windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.getservicesids.GetServiceSIDs Lists process token sids. windows.getsids.GetSIDs Print the SIDs owning each process windows.handles.Handles Lists process open handles. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows.modscan.ModScan Scans for modules present in a particular windows memory image.</pre>		windows.crashinto.c	rashinto	
<pre>windows.driverip.DriverTop List TRPs for drivers in a particular windows memory image. windows.driverscan.DriverScan Scans for drivers present in a particular windows memory image. windows.dumpfiles.Dumpfiles Dumps cached file contents from Windows memory samples. windows.envars.Envars Display process environment variables windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.getservicesids.GetServiceSIDs Lists process token sids. windows.getsids.GetStor Lists process token sids. windows.handles.Handles Lists process open handles. windows.info.Info Show 0S & kernel details of the memory sample being analyzed. windows.memmap.Memmap windows.memmap.Memmap windows.modscan.ModScan Scans for modules Present in a particular windows memory image. windows.modscan.ModScan Scans for modules present in a particular windows memory image.</pre>		windows.dlllist.Dll	LISU PROVIDE AND THE REPORT OF T	
 List TRPs for drivers in a particular windows memory image. windows.driverscan.DriverScan Scans for drivers present in a particular windows memory image. windows.dumpfiles.Dumpfiles Dumps cached file contents from Windows memory samples. windows.envars.Envars Display process environment variables windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.getserviceSIDs Print the SIDs owning each process windows.info.Info Show 05 & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap windows.modscan.ModScan Scans for modules present in a particular windows memory image. 		windows detunction D	Lists the loaded modules in a particular windows memory image.	
<pre>windows.driverscan.Driverscan Scans for drivers present in a particular windows memory image. windows.dumpfiles.Dumps cached file contents from Windows memory samples. windows.envars.Envars Display process environment variables windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.getservicesids.GetServiceSIDs Lists process token sids. windows.getsids.GetSIDs Lists process token sids. windows.handles.Handles Lists process open handles. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap windows.modscan.ModScan Scans for modules present in a particular windows memory image.</pre>		windows.driverirp.u	list TRDs fon drivens in a nanticular windows memory image	
 Scans for drivers present in a particular windows memory image. windows.dumpfiles.DumpFiles Dumps cached file contents from Windows memory samples. windows.envars.Envars Display process environment variables windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.getservicesids.GetServiceSIDs Lists process token sids. windows.getsids.GetSIDs Print the SIDs owning each process windows.handles.Handles Lists process open handles. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap windows.modscan.ModScan Scans for modules present in a particular windows memory image. 		windows drivenscen	DeiverScan	
windows.dumpfiles.Dumpfiles Dumps cached file contents from Windows memory samples. windows.envars.Envars Display process environment variables windows.filescan.FileScan Scans for file objects present in a particular windows memory image. Windows.getservicesids.GetServiceSIDS Lists process token sids. windows.getsids.GetSIDS Print the SIDs owning each process windows.handles.Handles Lists process open handles. Windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image.		windows.uriverscan.	Scans for drivers present in a particular windows memory image	
Dumps cached file contents from Windows memory samples. windows.envars.Envars Display process environment variables windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.getservicesids.GetServiceSIDs Lists process token sids. windows.getsids.GetSIDs Print the SIDs owning each process windows.handles.Handles Lists process open handles. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.melfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows medules Modules		windows dumpfiles D	umoFiles	
windows.envars.Envars Display process environment variables windows.filescan.FileScan Scans for file objects present in a particular windows memory image. windows.getservicesids.GetSIDS Lists process token sids. windows.handles.Handles Lists process open handles. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap memory Memmap windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows.modules		Hillions to amprilies to	Dumps cached file contents from Windows memory samples	
Display process environment variables windows.filescan.FileScan Scans for file objects present in a particular windows memory image. Windows.getserviceSiDs Lists process token sids. Windows.getsids.GetServiceSiDs Print the SIDs owning each process Windows.handles.Handles Lists process open handles. Windows.info.Info Show OS & kernel details of the memory sample being analyzed. Windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. Windows.memmap.Memmap Prints the memory map Windows.modScan.ModScan Scans for modules present in a particular windows memory image.		windows.envars.Enva	P5	
<pre>windows.filescan.FileScan Scans for file objects present in a particular windows memory image. Windows.getservicesids.GetServiceSIDS Lists process token sids. Windows.getsids.GetSIDS Print the SIDs owning each process windows.handles.Handles Lists process open handles. Windows.info.Info Show OS & kernel details of the memory sample being analyzed. Windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. Windows.memmap.Memmap Prints the memory map Windows.modscan.ModScan Scans for modules present in a particular windows memory image.</pre>			Display process environment variables	
Scans for file objects present in a particular windows memory image. windows.getservicesids.GetServiceSIDs Lists process token sids. windows.getsids.GetSIDs Print the SIDs owning each process windows.handles.Handles Lists process open handles. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image. Windows modules Modules		windows.filescan.Fi	leScan	
windows.getservicesids.GetServiceSIDs Lists process token sids. windows.getsids.GetSIDs Print the SIDs owning each process windows.handles.Handles Lists process open handles. windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows modules			Scans for file objects present in a particular windows memory image.	
Lists process token sids. windows.getsids.GetSIDs Print the SIDs owning each process windows.handles.Handles Lists process open handles. windows.info.Info Show 0S & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. Windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows modules Modules		windows.getservices	ids.GetServiceSIDs	Charry the timeline
windows.getsids.GetSIDs Print the SIDs owning each process windows.handles.Handles Lists process open handles. Windows.info.Info Show OS & kernel details of the memory sample being analyzed. Windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. Windows.memmap.Memmap Prints the memory map Windows.modscan.ModScan Scans for modules present in a particular windows memory image. Windows modules			Lists process token sids.	Show the unlenne
Print the SIDs owning each process windows.handles.Handles Lists process open handles. windows.info.Info Show 0S & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image.		windows.getsids.Get	SIDs	
windows.handles.Handles Lists process open handles. windows.info.Info Show 0S & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows modules Modules			Print the SIDs owning each process	plugins and gathering
Lists process open handles. windows.info.Info Show 0S & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows modules Modules		windows.handles.Han	dles	
windows.info.Info Show OS & kernel details of the memory sample being analyzed. windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows modules Modules			Lists process open handles.	the all detail about
windows.malfind.Malfind Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image.		windows.info.Info	Show OS & kernel details of the memory sample being analyzed.	1 1
Lists process memory ranges that potentially contain injected code. windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image.		windows.malfind.Mal	find	target memory using
windows.memmap.Memmap Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image.			Lists process memory ranges that potentially contain injected code.	
Prints the memory map windows.modscan.ModScan Scans for modules present in a particular windows memory image.		windows.memmap.Memm	ap	timeline plugin.
windows.modscan.ModScan Scans for modules present in a particular windows memory image. windows modules Modules		. N. S	Prints the memory map	1 0
scans for modules present in a particular windows memory image.		windows.modscan.Mod	Scan	
		indexing model in the	scans for modules present in a particular windows memory image.	
The second		windows.modules.Mod	lists the leaded keepel medules	
windows mutantscan MutantScan		windows mutants can	MutantScan	
withows mutants can inveation		withdows mutantistan.	In concocont	
	-	(a)		

^ 🛃 🛥 🖅 🖓 💏 CIQud

- 0

×













The following plugins could not be loaded (use -vv to see why): volatility3.plugins.windows.cachedump, volatility3.plugins.windows.hashdump, volatility3.plugins.windows.lsadump forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline\$ forensics@WIN-BK109542K3L:/mnt/c/Cases/Analysis/Timeline\$ vol timeliner -h Volatility 3 Framework 2.0.1 usage: volatility timeliner.Timeliner [-h] [--plugins PLUGINS] [--record-config] [--plugin-filter [PLUGIN-FILTER [PLUGIN-FILTER ...]]] [--create-bodyfile]

optional arguments:

-h, --help show this help message and exit --plugins PLUGINS Comma separated list of plugins to run --record-config Whether to record the state of all the plugins once complete --plugin-filter [PLUGIN-FILTER [PLUGIN-FILTER ...]] Only run plugins featuring this substring --create-bodyfile Whether to create a body file whilst producing results forensics@WIN-BK109542K3L:/mnt/c/Cases/Analysis/Timeline\$ vol -f /mnt/c/Cases/Analysis/Memory/ dlls/ dlls.txt win10-memory.raw forensics@WIN-BK109542K3L:/mnt/c/Cases/Analysis/Timeline\$ vol -f /mnt/c/Cases/Analysis/Memory/win1}-memory.raw timeliner --create-bodyfil



	forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline					-	
	Dillist DLL Load: Process 5108 svchost.exe Loaded sec	host.dll (C:\Windows\System32\sechost.dll) Size 647168 Offset 140718923317248 202	22-03-18 00:28:27.00	0000 N/A	N/A	N/A	
cle Bin	DIILIST DLL Load: Process 5108 svchost.exe Loaded RPC	KI4.dll (C:\Windows\System32\RPCRI4.dll) Size 118/840 Offset 140/1889/233920 202	22-03-18 00:28:27.00	9000 N/A	N/A	N/A	
	Dillist DLL Load: Process 5108 sychost eve Loaded our	Loase.dll (C:\Windows\System32\combase.dll) Size 3330048 Offset 140718886037364 202	22-03-18 00:28:27.00	0000 N/A	N/A	N/A	
	Dillist DLL Load: Process 5108 sychost eve Loaded for	untPrimitives dll (C:\Windows\System32\bcryntPrimitives dll) Size 516096 Offset 140718	RR66235392 2022-	03-18 00·28·27 00	0000	N/A	N/A
0	N/A		1 X	/3 10 00:20:27:00	0000	11/17	10.7
and out	Dillist DLL Load: Prov		022-03-18 00	:28:27.000000	N/A	N/A	N/A
reruit	DILList DLL Load: Prot File Home Share View		00:28:27.00	0000 N/A	N/A	N/A	
	DllList DLL Load: Proc 🌛 🖻 🎽 Cut	📜 🙀 🎽 🌇 New Item 🔹 🎲 🕢 Open 🔹 🔠 Select all	00:28:27.00	0000 N/A	N/A	N/A	
5/	DllList DLL Load: Prot	💌 🧰 🔨 🚟 🦰 Easy access + 🔛 📝 Edit 🔡 Select none	00:28:27.00	0000 N/A	N/A	N/A	
	DIIList DLL Load: Prot access Paste Paste shortcut	o* to* * folder *	00:28:27.00	0000 N/A	N/A	N/A	
rpad++	DIIList DLL Load: Prot Clipboard	Organize New Open Select	00:28:27.00	0000 N/A	N/A	N/A	
	DIIList DLL Load: Prot	> Cases > Analysis > Timeline V D Search Timeline	00:28:27.00	3000 N/A	N/A	N/A	CALLER !!
	DIILIST DLL Load: Pro		140/1865/3/	2160 2022-0	3-18 00:2	8:27.000	000
	N/A N/A N/A Dillist Dilliond: Deprint Purcharcess	Name Date modified Type Size	00-29-27 00	0000 N/A	NZA	N/A	
2	Dillist Dil Load: Proc	volatility.body 6/7/2022 10:20 PM BODV File 1,147 KB	00.28.27.00	0000 N/A	NIA	N/A	
nt Log	Dillist DLL Load: Pro	N	00:28:27.00	0000 N/A	N/A	N/A	
piorei	Dillist DLL Load: Pro	h	00:28:27.00	0000 N/A	N/A	N/A	
1	DllList DLL Load: Proc		00:28:27.00	0000 N/A	N/A	N/A	
	DIIList DLL Load: Proc 🕹 Downloads		22880 Offset	140718267760640	2022-03	-18 00:2	8:27.00
nallma	0000 N/A N/A 🗄 Documents 💉						
ortcut	DIIList DLL Load: Prov 🔄 Pictures 🖈		00:28:27.00	0000 N/A	N/A	N/A	
	PsScan Process: 5108 Analysis_temp	Show the file in timeline folder					
	PsScan Process: 5108				Same in a	THE REAL PROPERTY OF	ALL SALES
	DIILIST DLL Load: Pro		9632 Offset	140718717272064	2022-03	-18 00:2	8:28.00
	Dillist Dilliond: Depu		032-02-10-00	- 29 - 29 - 000000	NZA	N/A	NZA
	Dillist Dil Load: Proc		022-03-18 00	0000 N/A	NIA	N/A	TH/PA
	Dillist Dil Load: Proc		022-03-18 00	-28-28,000000	N/A	N/A	N/A
	DllList DLL Load: Prog ID Objects		00:28:28.00	0000 N/A	N/A	N/A	10100
	DIILIST DLL Load: Prog Desktop		00:28:28.00	0000 N/A	N/A	N/A	
	DllList DLL Load: Proc 🔂 Documents		00:28:28.00	0000 N/A	N/A	N/A	
	DllList DLL Load: Prov 🤳 Downloads		4 2022-	03-18 00:28:28.00	0000	N/A	N/A
	N/A Music						
	DIILIST DLL Load: Prot		00:28:40.00	0000 N/A	N/A	N/A	
	NetScan Network conner		N/A	N/A N/A			
	NetScan Network connet		N/A				
	NetScan Network conner		N/A				
	NetScan Network conner		N/A	N/A N/A			
	NetScan Network connet 1 item 1 item selected 1.11 MB		N/A	N/A N/A			
	NetScan Network connection: Process 2812 sychost.exe	Local Address :::0 Remote Address *:0 State Protocol UDPv6 2022-03-18 00:29:05.	.000000 N/A	N/A N/A			
	NetScan Network connection: Process 2812 svchost.exe	Local Address 0.0.0.0:0 Remote Address *:0 State Protocol UDPv4 2022-03-18 00:29:07.	.000000 N/A	N/A N/A			
	NetScan Network connection: Process 2812 svchost.exe	Local Address 0.0.0.0:0 Remote Address *:0 State Protocol UDPv4 2022-03-18 00:29:07.	.000000 N/A	N/A N/A			
	NetScan Network connection: Process 2812 svchost.exe	Local Address :::0 Remote Address *:0 State Protocol UDPv6 2022-03-18 00:29:07.	.000000 N/A	N/A N/A			
	NetScan Network connection: Process 2812 sychost.exe	Local Address 0.0.0.0:0 Remote Address *:0 State Protocol UDPv4 2022-03-18 00:29:07.	.000000 N/A	N/A N/A			
	NetScan Network connection: Process 2812 sychost.exe	Local Address :::0 Remote Address *:0 State Protocol UDPv6 2022-03-18 00:29:07.	.000000 N/A	N/A N/A			
	NetScan Network connection: Process 2812 sychost.exe	Local Address 0.0.0.0.0 Remote Address 10 State Protocol UDPV4 2022-03-18 00:29:07.	.000000 N/A				
	netscan network connection: Process 2012 Svchost.exe	Local Address 0 Remote Address .0 State Protocol 00PV0 2022-03-18 00:29:07.	1000000 N/A	N/A N/A			

🖶 ର 🛱 🔚 🛅 👹

0

^ 🔄 🖙 🖅 🖓 🗍 1044 PM CIQud

	forensics@WIN-BK1Q9542K3L:	/mnt/c/Cases/Analysis/Timeline														
e	DllList DLL Load: Pro	cess 5108 svchost.exe Loaded	sechost.dl	11 (C:\Windows	System32\secho	st.dll) Size	647168 Offset :	14071892	23317248 20	22-03-18	00:28:27.00	0000	N/A	N/A	N/A	^
ecycle Bin	DIIList DLL Load: Prod	cess 5108 svchost.exe Loaded	RPCRT4.dll	1 (C:\Windows\	System32\RPCRT4	.dll) Size 1	187840 Offset 14	40718897	7233920 20	22-03-18	00:28:27.00	0000	N/A	N/A	N/A	
	DllList DLL Load: Pro	cess 5108 svchost.exe Loaded	ucrtbase.d	dll (C:\Windows	s\System32\ucrt	base.dll) Si	ze 1024000 Offs	et 14071	18866956288 20	22-03-18	00:28:27.00	0000	N/A	N/A	N/A	
	DllList DLL Load: Proc	cess 5108 svchost.exe Loaded	combase.dl	ll (C:\Windows	\System32\comba	se.dll) Size	3330048 Offset	1407188	886027264 20	22-03-18	00:28:27.00	0000	N/A	N/A	N/A	100000
<i>6</i>	DIIList DLL Load: Pro	cess 5108 svchost.exe Loaded	bcryptPrim	mitives.dll (C	:\Windows\Syste	m32\bcryptPr:	imitives.dll) Si	ize 5160	096 Offset 14071	88662353	92 2022-	03-18 00	:28:27.000	000	N/A	N/A
	N/A	📙 🔄 🛄 🖛 Timeline							- 0	x c						10
Firefox	DllList DLL Load: Pro	File Home Share View								~ 0	022-03-18 00	:28:27.0	00000	N/A	N/A	N/A
	DIIList DLL Load: Pro				- Pastan tan a	Et Dave	- Pretest all				00:28:27.00	0000	N/A	N/A	N/A	
1 A 1	DIILIST DLL Load: Pro	× =	4 4	X 🗐	TE New nem *	✓ Open	Select an				00:28:27.00	0000	N/A	N/A	N/A	
42	Dillist DLL Load: Pro	Pin to Quick Copy Paste	Move Copy	Delete Rename	New Lasy access *	Properties	and select none				00:28:27.00	0000	N/A	N/PA	N/A	
A REAL	Dillist DLL Load: Pro	access Paste shortcut	to - to -	•	older	•	m invert selection				00:28:27.00	0000	N/A	NZA	N/A	
lotepad++	Dillist DLL Load: Pro	Clipboard	01	rganize	New	Open	Select				00.28.27.00	0000 0000	N/A	N/A	M/A	
	Dillist Dil Load: Pro	🗧 🕂 👻 🛧 📘 > This PC > Local Dis	c (C:) → Cases	Analysis > Timelin	e			νõ	Search Timeline	P	14071865737	2160	2022-03	-18 00:2	8:27.00	3000
	N/A N/A N/A	and the second se	^ □ N+		Date	modified Typ	Size				21012003131					
0	DllList DLL Load: Pro	🖈 Quick access	(Paral a		195613	1.80	10000				00:28:27.00	0000	N/A	N/A	N/A	
Frent Log	DIIList DLL Load: Pro	Tools	*	volatility.bod	en with	and reserved BO	DY File 1,	147 KB			00:28:27.00	0000	N/A	N/A	N/A	
Explorer	DllList DLL Load: Pro	Cases	1	CY EN	it with Notenadu +						00:28:27.00	0000	N/A	N/A	N/A	
	DllList DLL Load: Pro	Desktop	2	12 54	i min notepadr +						00:28:27.00	0000	N/A	N/A	N/A	
AX.	DIIList DLL Load: Pro	- Downloads		P.	dare presions versions						00:28:27.00	0000	N/A	N/A	N/A	
-	DIIList DLL Load: Pro	Devenueds	3		store previous versions						22880 Offset	1407182	67760640	2022-03	-18 00:	28:27.00
senalima	0000 N/A N/A	Documents	1	Se	nd to	>					00.00.07.00	0000		11/10		
- Shortcut	DIILIST DLL Load; Pro	Pictures	×.	Cu	t						00:28:27.00	0000	N/A	N/A	N/A	
	PsScan Process: 5108	Analysis_temp		Co	РУ		Fi1	e on	en with							
	Dillist DLL Load: Pro	Evidence		Cr	nate shortcut		1 11	c op			9632 Offset	14071871	7272064	2022-03	-18 00:	28:28.00
	0000 N/A N/A	Execution		De	lete		No	ntena	A++					100104000-0000		
	DllList DLL Load: Pro	System32		Re	name			ncpe			022-03-18 00	:28:28.0	00000	N/A	N/A	N/A
	DIIList DLL Load: Pro	This PC			inginine.						00:28:28.00	0000	N/A	N/A	N/A	51 51
	DllList DLL Load: Pro			Pro	operties						022-03-18 00	:28:28.0	00000	N/A	N/A	N/A
	DllList DLL Load: Pro	ab objects									00:28:28.00	0000	N/A	N/A	N/A	
	DIIList DLL Load: Pro	Desktop									00:28:28.00	0000	N/A	N/A	N/A	
	DIIList DLL Load: Pro	Documents									00:28:28.00	0000	N/A	N/A	N/A	
	DIILIST DLL LOAD: PPO	Downloads								í	4 2022-	03-18 00	:28:28.000	1000	NZA	N/A
	Dillist DLL Load: Prov	J Music									00-78-10 00	aaaa	M/A	NZA	N/A	
	NetScan Network conner	Fictures									N/A	N/A	N/A	11/10	11/0	
	NetScan Network conner	Videos									N/A	N/A	N/A			
	NetScan Network conne	Local Disk (C:)									N/A	N/A	N/A			
	NetScan Network conner	CD Drive (D:) VirtualBox Guest Addition	s								N/A	N/A	N/A			
	NetScan Network conne	Documente (\\VErsSur) (7)	*							State 1	N/A	N/A	N/A			
	NetScan Network conne	1 item 1 item selected 1,11 MB									N/A	N/A	N/A			
	NetScan Network connec	ction: Process 2812 svchost.e	xe Local A	Address :::0 Re	emote Address *	:0 State Pro	otocol UDPv6	2022	2-03-18 00:29:05	.000000	N/A	N/A	N/A			
	NetScan Network connec	ction: Process 2812 svchost.e	ke Local A	Address 0.0.0.	0:0 Remote Addr	ess *:0 State	e Protocol UDP	v4 2022	2-03-18 00:29:07	.000000	N/A	N/A	N/A			
	NetScan Network connec	ction: Process 2812 sychost.e	xe Local A	Address 0.0.0.0	3:0 Remote Addr	ess *:0 State	Protocol UDP	v4 2022	2-03-18 00:29:07	.0000000	N/A	N/A	N/A			
	NetScan Network connec	ction: Process 2812 sychost.e	ke Local A	Address 2.0 R	anote Address *	State Pro	Protocol UDPv6	2024	2-03-18 00:29:07	000000	N/A	N/A	N/A			
	NetScan Network conner	ction: Process 2812 sychost.e	xe Local A	Address A	mote Address *	-0 State Pe	atocol UDPv6	2022	2-03-18 00:29:07	000000	N/A	N/A	N/A			
	NetScan Network conner	ction: Process 2812 sychost e	ke Local A	Address 0 0 0 0	0 Remote Addr	ess *:0 State	Protocol UDP	v4 2022	2-03-18 00:29:07	000000	N/A	N/A	N/A			
	NetScan Network conner	ction: Process 2812 sychost.e	ke Local A	Address :::0 R	emote Address *	:0 State Pro	otocol UDPv6	2023	2-03-18 00:29:07	.000000	N/A	N/A	N/A			
			and the first states of the	An event bester i that and the second	ALL REAL PROPERTY AND A RE	A HALL SECONDERING CONTRACT	and and the ball of the ball.			never namen and	T-MARKAN	CACE OF T	The second s			×

📑 🔎 🛱 🦲 🔛 📦

0

^ 🗟 🖮 🗊 🕼 👘 Cloud

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window 7

🔚 NTUSER DAT tot 🔄 📑 SAM tot 🔄 📑 SECURITY tot 🕄 📑 SOFTWARE tot 🔄 📑 SYSTEM tot 🕃 📑 UorGass dat tot 🕃 🛏 volatility body 🖸 |PsList - Process: 4 System (221572833432000)|||||||||||||1647562205 |PsList - Process: 88 Registry (221572834857024)||||||||||1647562199 2 PsList - Process: 316 smss.exe (221572846485568) ||||||||||||1647562205 [PsList - Process: 408 csrss.exe (221572897677440)] |||||1647562214 [PsList - Process: 484 wininit.exe (221572905160832)]]]]]]]]]1647562214 PsList - Process: 492 csrss.exe (221572905239872)|||||||||||1647562214 6 Process: 544 winlogon.exe (221572905431168) |||||||||1647562214 |PsList PsList - Process: 624 services.exe (221572897637696)||||||||||||647562214 8 PsList - Process: 632 lsass.exe (221572897621120)|||||||||||647562214 [PsList - Process: 732 sychost.exe (221572904571648)]]]]]]11111111647562215 10 PsList - Process: 744 fontdrvhost.ex (221572892942464)||||||||||1647562215 11 [PsList - Process: 752 fontdryhost.ex (221572892955136)]]]]]]11111111647562215 12 PsList - Process: 824 sychost.exe (221572905198336) |||||||||||647562215 13 PsList - Process: 872 sychost.exe (221572905870208)||||||||||1647562215 14 [PsList - Process: 920 sychost.exe (221572906251008)] 15 ||||1647562215 [PsList - Process: 996 dwm.exe (221572912832704)]]]]]]111111647562215 16 17 [PsList - Process: 360 svchost.exe (221572913124224)] 1111111647562216 18 PsList - Process: 480 sychost.exe (221572913214400)||||||||||||647562216 PsList - Process: 688 svchost.exe (221572913365824) 19 11111647562216 PSList - Process: 620 svchost.exe (221572913378240) |||||||||||647562216 21 [PsList - Process: 1088 svchost.exe (221572833669312)]]]]]]1647562216 IPsList - Process: 1124 sychost.exe (221572834099328) |||||||||1647562216 23 PsList - Process: 1148 svchost.exe (221572834119808) |||||||||||1647562216 24 PsList - Process: 1284 svchost.exe (221572833927296) ||||||||||1647562216 [PsList - Process: 1296 VBoxService.ex (221572833902720) |||||||||||647562216 26 PSList - Process: 1316 svchost.exe (221572913996544) |||||||||||647562216 IPsList - Process: 1368 sychost.exe (221572914676608)||||||||||1647562216 27 PsList - Process: 1480 sychost.exe (221572915028736) |||||||||||647562217 28 29 [PsList - Process: 1500 svchost.exe (221572915286912)]]]]]]111111647562217 PsList - Process: 1520 svchost.exe (221572915315520) ||||||||||1647562217 PsList - Process: 1548 sychost.exe (221572915380992) ||||||||||1647562217 31 [PsList - Process: 1620 svchost.exe (221572915549056) || || || || 1647562217 [PsList - Process: 1684 MemCompression (221572915695680) |||||||||||1647562217 33 PsList - Process: 1724 sychost.exe (221572915921792) || 34 1111647562217 [PsList - Process: 1752 sychost.exe (221572915917568)]]]]]]111111647562217 PsList - Process: 1852 svchost.exe (221572916216640) 36 111647562217 PsList - Process: 1868 sychost.exe (221572915724416) | | | 37 111647562217 PsList - Process: 1984 svchost.exe (221572916556672) 39 PsList - Process: 1144 svchost.exe (221572933685376) 40 PsList - Process: 1904 svchost.exe (221572933673088) [PsList - Process: 1944 svchost.exe (221572933668992)]]]]]]]]111111647562217 41 42 IPsList - Process: 2120 sychost.exe (221572933656704) []]] 111647562218

0

Show the All Events.

Normal text file

-

~ 🖬

Creating a Timeline of the disk image with Plaso tools

Bin		
	Select forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline	- 🗆 ×
5	is 2147483648 (2 GiB). If a worker process exceeds this limit it is killed by the main (foreman) process.	
*	worker_timeout MINUTES,worker-timeout MINUTES Number of minutes before a worker process that is not providing status updates is considered inactive. The default timeout process exceeds this timeout it is killed by the main (foreman) process.	is 15.0 minutes. If a worker
	workers WORKERS Number of worker processes. The default is the number of available system CPUs minus one, for the main (foreman) process.	
1++	sigsegv_handler,sigsegv-handler Enables the SIGSEGV handler. WARNING this functionality is experimental and will a deadlock worker process if a real segfau SIGSEGV. This functionality is therefore primarily intended for debugging purposes	lt is caught, but not signal
	profiling arguments:	
	profilers PROFILERS_LIST	
/ 09	List of profilers to use by the tool. This is a comma separated list where each entry is the name of a profiler. Use "pro available profilers.	filers list" to list the
er	profiling_directory DIRECTORY,profiling-directory DIRECTORY	a support working directory
	profiling sample rate SAMPLE RATEprofiling-sample-rate SAMPLE RATE	e current working directory.
	Profiling sample rate (defaults to a sample every 1000 files).	
na :ut	storage arguments:	
	storage_file PATH,storage-file PATH	
	storage_format_FORMAT,storage_format_FORMAT	
	task storage format FORMAT task-storage-format FORMAT	
	Format for task storage, the default is: sqlite. Supported options: redis, sqlite	
	Example usage: Using t	he disk image
	Run the tool against a storage media image (full kitchen sink)	e this command
	log2timeline.py /cases/mycase/storage.plaso imynd.dd	cuits command
	Instead of answering questions, indicate some of the options on the and sto	re the output in
	command line (including data from particular VSS stores).	
	log2timeline.pyvss_stores 1,2 /cases/plaso_vss.plaso_image.E01 One file	with name
	And that is how you build a timeline using log2timeline	
	forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline\$	aso .
	forensics@WIN-BK109542K3L:/mnt/c/Cases/Analysis/Timeline\$ log2timeline.pystorage-file disk.plaso /mnt/c/Cases/	
	2022-03-23T223835_CopyLog.csv Analysis/ Notes.docx win10-disk.vhd	
	forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline\$ log2timeline.pystorage-file disk.plaso /mnt/c/Cases/win10-disk.raw	

Firef

Notep

Event Explo

Arsenal - Shor

-

0

6

- 1	2	8		۲.	
				L	
		3	۰		
Re	evi	1	6	Rı	•

.

Not

rsena

- Shortcut

	6 forensics@WIN-B	3K1Q9542K3L: /r	nnt/c/Cases/Analysis/Ti	meline			- 0
A	plaso - log2t	imeline ve	ersion 20220428	3			
refox	Source path Source type Processing tim	me	: /mnt/c/Case : storage med : 01:40:20	es/win10-disk.raw Jia image	I		
apad++	Tasks:	Queued 0	Processing 0	ы Merging 0	Abandoned 0	Total 158051	
	Identifier Main	PID 84	Status	Memory 622 5 MiB	Sources	Events 1451337 (0)	File
?	Worker_00 Edge\User\Defi	89 ault\Data	idle idre\Data\nous	415.6 MiB ser1\120712-0049\	59935 (0) DBStore\LogFiles	763754 (52)	NTFS:\Users\IEUser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\Micro
nt Log olorer	Worker_01 Edge\User\Def	91 ault\Data	idle tore\Data\nous	479.2 MiB	98115 (0) DBStore\LogFiles	687583 (36) s\edbres00002.irs	NTFS:\Users\IEUser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\Micro
20	Processing co	mpleted.					

"Number of warnings generated while extracting events: 9.

Use pinfo to inspect warnings in more detail.

forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline\$ _

Take a more time for finish the process.

Processing Time ~ 1:40

Activate Windows Go to Settings to activate Windows

×

osoft osoft





and the second second	

-

Q

🛱 🔚 🛅 🍏

0

	6 forensics@WIN-B	K1Q9542K3L: /r	mnt/c/Cases/Analysis/Ti	meline					- 0			
(11)	plaso - log2ti	imeline ve	ersion 20220428	3								
Firefox	Source path Source type Processing tim	ie	: /mnt/c/Case : storage med : 01:40:20	es/win10-disk.rav Ha image	4							
Notepad++	Tasks:	Queued Ø	Processing 0	Merging Ø	Abandoned Ø	Total 158051						
	Identifier	PID	Status	Memory	Sources	Events	File					
\odot	Main Worker_00	84 89	idle	622.5 M18 415.6 MiB	158051 (0) 59935 (0)	1451337 (0) 763754 (52)	NTFS:\Users\IEU	ser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\	AC\Microsof			
Event Log Explorer	Edge\User\Defa Worker_01 Edge\User\Defa	91 91 101t\Data	idle Store\Data\nous Store\Data\nous	er1\120712-0049 479.2 MiB ser1\120712-0049	DBStore\LogFiles 98115 (0) DBStore\LogFiles	\edbtmp.log 687583 (36) \edbres00002.jrs	NTFS:\Users\IEU	lser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\	AC\Microsof			
	Processing com	npleted.										
Arsenalima - Shortcut	Number of warr	per of warnings generated while extracting events: 9.										
	Use pinfo to inspect warnings in more detail.											
	forensics@WIN- total 684952	BK1Q9542	GL:/mnt/c/Case	es/Analysis/Time	line\$ ls -l							
	-rwxrwxrwx 1 f -rwxrwxrwx 1 f -rwxrwxrwx 1 f forensics@WIN-	Forensics Forensics Forensics -BK1Q9542	forensics 7001 forensics forensics 12 C3L:/mnt/c/Case	153856 Jun 8 02 394 Jun 8 02 235166 Jun 7 22 25/Analysis/Time	09 disk.plaso 09 log2timeline- 46 volatility.bo line\$ pinfo.py di	20220608T002923. dy sk.plaso	log,gz	Show the file in timeline folder and then after open the file				
	Fireformat v	ilename : version :	**** Plaso Stor disk.plaso 20211121	rage Information	*******	*****		and show the all event logs.				
	Serialization	format :	json									
	++++++++++++++++++++++++++++++++++++++	-4854-a69	a-248c7b326453	Sessions ******** : 2022-06-08T00	29:25.907642+00:	*****						

^ 🛃 🛥 🖅 🖓 🖓 🖓 CIQUd

~

×

Recycle Bin			
	Select forensics@WIN-BK1Q9542K3L: /mnt/c/Cas	es/Analysis/Timeline	
	**************************************	generated per parser ***	****************
	Parser (plugin) name	: Number of events	
Firefox	amcache	: 190	
	appcompatcache	: 344	
1	bagmru	: 21	
	bam	: 14	
	explorer mountpoints2	: 4	
otepad++	explorer programscache	: 1	
	filestat	: 632137	
	lnk	: 453	
0	mrulist string	- 1	
	mrulistex_string	: 2	
vent Log	mrulistex string and shell item	: 3	
apiorei	msie zone	: 36	
477	networks	: 4	A 11 arout the area in this file
	olecf automatic destinations	: 34	All event show in this me.
	olecf default	: 76	
Shortcut	olecf_document_summary	: 8	
2110111101	olecf summary	: 58	
	oxml	: 14	
	pe	: 48694	
	prefetch	: 965	
	setupapi	: 62	
	shell_items	: 414	
	userassist	: 26	
	usnjrnl	: 237652	
	windows_boot_execute	: 2	
	windows_run	: 9	
	windows_sam_users	: 13	
	windows_services	: 603	
	windows_shutdown	: 2	
	windows_task_cache	: 443	
	windows_timezone	: 1	
	windows_typed_urls	: 5	
	windows_version	: 4	
	winevtx	: 64170	
	winlogon	: 4	
	winreg_default	: 464868	
	Total	: 1451337	

0

H 🥅 🔤 🍪

Activate Windows Go to Settings to activate Windows.

~

- 🗆 X



Generating a Super Timeline with plaso tool

(a) forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline		-	o ×
<pre>83 : type: OS, location: /mnt/c/Cases/win10-disk.raw</pre>	Merging timelines with		
No analysis reports stored.	command.		
<pre>forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline\$ forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline\$ forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline\$ 1s -1 total 684952 -rwxrwxrwx 1 forensics forensics 700153856 Jun 8 02:09 disk.plaso -rwxrwxrwx 1 forensics forensics 394 Jun 8 02:09 log2timeline-20220608T002923.log.gz -rwxrwxrwx 1 forensics forensics 1235166 Jun 7 22:46 volatility.body forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline\$ log2timeline.pyparser=mactimestorage-file=disk.plaso volume volume</pre>	latility.body _		

Activate Windows Go to Settings to activate Windows

0	Select forensics@W	/IN-BK1Q9542K3L: /mrit/c	:/Cases/Analysis/Timeline						;	-	
pla	aso - psort v	version 2022042	8								
Sto Pro	orage file ocessing time	: dis : 00:0	k.plaso 06:36								
Eve	ents:	Filtered 1318514	In time slice Ø	Duplicates 24	MACB grouped 140077	Total 1458958					
Ide Mai	entifier in	PID 110	Status completed	Memory 315.0 MiB	Events 140444 (0)	Tags 0 (0)	Reports 0 (0)				
Pro	cessing comp rensics@WIN-E	leted. 3K109542K3L:/mn	t/c/Cases/Analysi	s/Timeline \$							

Activate Windows

@ forensics@WIN	V-BK1Q9542K3L:	/mnt/c/Cases/Analysis/T	imeline					×
plaso - log2	timeline	version 2022042	8					^
Source path Source type Processing t	ime	: /mnt/c/Case : single file : 00:00:02	es/Analysis/⊺ime e	line/volatility	.body			
Identifier Main	PID 106	Status completed	Memory 178.0 MiB	Sources 1 (0)	Events 7621 (1358)	File OS:/mnt/c/Cases/Analysis/Timeline/volatility.body		
Processing c	ompleted.							
forensics@WI total 688244 -rwxrwxrwx 1 -rwxrwxrwx 1 -rwxrwxrwx 1 forensics@WI	N-BK1Q9542 forensic forensic forensic forensic N-BK1Q954	2K3L:/mnt/c/Case s forensics 703 s forensics s forensics s forensics 1 2K3L:/mnt/c/Cas	es/Analysis/Time 524864 Jun 8 02 394 Jun 8 02 177 Jun 8 02 235166 Jun 7 22 es/Analysis/Time	<pre>line\$ ls -1 :46 disk.plaso :09 log2timelin :46 log2timelin :46 volatility. line\$ psort.py</pre>	e-20220608T002923. e-20220608T024654. body - o l2tcsv -w super	log.gz log.gz -timeline.csv disk.plaso "date > '2022-03-01 00:00:00'"		
_				A DAVING BUILTING THE TAX MICLAGE MIDDLE	NO MONTENERS W SERVICE			

Using this command plaso file convert to csv file. And also create super timeline.

> Activate Windows Go to Settings to activate Windows



Activate Windows Go to Settings to activate Windows

Super timeline Analysis

A detailed timeline of everything that occurred on a system, also known as a Super Timeline, can be extremely beneficial in determining what took place in a digital investigation.

Recycle Bin

Firefox

Notepad+

P

Event Log

Explore

AX.

.

Isenalima

Shortcut

e la

-



Activate Windows Go to Settings to activate Window



Timeline Explorer v1.3.0.0	1
----------------------------	---

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

Enter text to search... - | Find

Find

×

	Line	Tag	Timestamp	* Source Description	Source Name	macb	Inode	Long Description	
Ŧ	-		-	4 0 :	* O E	+Oc	-	10:	-
	915		0001-01-01 00:00:00	System - Network Co	LOG	.a	46357	7 SSID: Network Description: Network Connection Type: Wired Default Gateway Mac: 52:54:00:12:35:02 DNS Suffix: <none></none>	
2	1		2022-03-01 22:10:46	PE Event	PE	b	126961	1 PE Type: Dynamic Link Library (DLL)	
	2		2022-03-01 22:10:47	PE Event	PE	b	126963	3 PE Type: Dynamic Link Library (DLL)	
	3		2022-03-01 22:10:48	PE Event	PE	b	126965	5 PE Type: Dynamic Link Library (DLL) Chorry A 11 orrepto	
	4		2022-03-01 22:10:49	PE Event	PE	b	126967	7 PE Type: Dynamic Link Library (DLL) SHOW All EVEILS.	
	5		2022-03-01 22:10:49	PE Event	PE	b	126969	9 PE Type: Dynamic Link Library (DLL)	
	6		2022-03-01 22:10:50	PE Event	PE	b	126971	1 PE Type: Dynamic Link Library (DLL)	
	7		2022-03-01 22:10:51	PE Event	PE	b	126973	3 PE Type: Dynamic Link Library (DLL)	
	8		2022-03-01 22:10:52	PE Event	PE	b	126975	5 PE Type: Dynamic Link Library (DLL)	
	9		2022-03-01 22:10:53	PE Event	PE	b	126977	7 PE Type: Dynamic Link Library (DLL)	
	10		2022-03-01 22:11:00	PE Event	PE	b	126979	9 PE Type: Dynamic Link Library (DLL)	
	11		2022-03-01 22:11:13	PE Event	PE	b	126981	1 PE Type: Dynamic Link Library (DLL)	
	12		2022-03-01 22:11:25	PE Event	PE	b	126983	3 PE Type: Dynamic Link Library (DLL)	
	13		2022-03-01 22:11:50	PE Event	PE	b	126985	5 PE Type: Dynamic Link Library (DLL)	
	14		2022-03-01 22:12:13	PE Event	PE	b	126987	7 PE Type: Dynamic Link Library (DLL)	
	15		2022-03-01 22:12:39	PE Event	PE	b	126989	9 PE Type: Dynamic Link Library (DLL)	
	16		2022-03-01 22:12:52	PE Event	PE	b	126991	1 PE Type: Dynamic Link Library (DLL)	
	17		2022-03-01 22:13:07	PE Event	PE	b	126993	3 PE Type: Dynamic Link Library (DLL)	
	18		2022-03-01 22:13:21	PE Event	PE	b	126995	5 PE Type: Dynamic Link Library (DLL)	
	19		2022-03-01 22:13:26	PE Event	PE	b	126997	7 PE Type: Dynamic Link Library (DLL)	
	20		2022-03-01 22:13:30	PE Event	PE	b	126999	9 PE Type: Dynamic Link Library (DLL)	
	21		2022-03-01 22:13:35	PE Event	PE	b	127001	1 PE Type: Dynamic Link Library (DLL)	
	22		2022-03-01 22:13:43	PE Event	PE	b	127003	3 PE Type: Dynamic Link Library (DLL)	
	23		2022-03-01 22:13:47	PE Event	PE	b	127005	5 PE Type: Dynamic Link Library (DLL)	
	24		2022-03-01 22:13:53	PE Event	PE	b	127007	7 PE Type: Dynamic Link Library (DLL)	
	25		2022-03-01 22:13:57	PE Event	PE	b	127009	9 PE Type: Dynamic Link Library (DLL)	
	26		2022-03-01 22:13:59	PE Event	PE	b	127011	1 PE Type: Dynamic Link Library (DLL)	
	27		2022-03-01 22:14:00	PE Event	PE	b	127013	3 PE Type: Dynamic Link Library (DLL)	
	28		2022-03-01 22:14:02	PE Event	PE	b	127015	5 PE Type: Dynamic Link Library (DLL)	
	29		2022-03-01 22:14:05	PE Event	PE	b	127017	7 PE Type: Dynamic Link Library (DLL)	
	30		2022-03-01 22:14:06	PE Event	PE	b	127019	9 PE Type: Dynamic Link Library (DLL)	
	31		2022-03-01 22:14:08	PE Event	PE	b	127021	1 PE Type: Dynamic Link Library (DLL)	
	32		2022-03-01 22:14:10	PE Event	PE	b	127023	3 PE Type: Dynamic Link Library (DLL)	
	33		2022-03-01 22:14:11	PE Event	PE	b	127025	5 PE Type: Dynamic Link Library (DLL)	
	34		2022-03-01 22:14:12	PE Event	PE	b	127027	7 PE Type: Dynamic Link Library (DLL) Activate Windows	ç.
	35		2022-03-01 22:14:13	PE Event	PE	b	127029	9 PE Type: Dynamic Link Library (DLL) Go to Settings to active	ate Windows.
+1					1220	L.			

C:\Cases\Analysis\Timeline\super-timeline.csv

101

Total lines 119,983 Visible lines 119,983 Open files: 1 👪 Search options



	100	Timeline	Explorer 1	1.3.0.0
--	-----	----------	------------	---------

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

		×
Enter text to search	-	Find

	Line	T	ag	Timestamp /	Source Description	Source Name	macb	Inode	Long Description	
Ŧ	-			-	•D:	+ O :	+Oc	-	-0:	7
		66		2022-03-01 22:14:48	PE Event	PE	b	127091	PE Type: Dynamic Link Library (DLL)	-
		67		2022-03-01 22:14:49	PE Event	PE	b	127093	PE Type: Dynamic Link Library (DLL)	
		68		2022-03-01 22:14:50	PE Event	PE	b	127095	PE Type: Dynamic Link Library (DLL)	
		69		2022-03-01 22:14:51	PE Event	PE	b	127097	PE Type: Dynamic Link Library (DLL)	
		70		2022-03-01 22:14:52	PE Event	PE	b	127099	PE Type: Dynamic Link Library (DLL)	
		71		2022-03-01 22:14:53	PE Event	PE	b	127101	PE Type: Dynamic Link Library (DLL)	
		72		2022-03-01 22:14:53	PE Event	PE	b	127103	PE Type: Dynamic Link Library (DLL)	
		73		2022-03-01 22:14:54	PE Event	PE	b	127105	PE Type: Dynamic Link Library (DLL)	
		74		2022-03-01 22:14:55	PE Event	PE	b	127107	PE Type: Dynamic Link Library (DLL)	
		75		2022-03-01 22:14:56	PE Event	PE	b	127109	PE Type: Dynamic Link Library (DLL)	
		76		2022-03-01 22:14:57	PE Event	PE	b	127111	PE Type: Dynamic Link Library (DLL)	
		77		2022-03-01 22:14:58	PE Event	PE	b	127113	PE Type: Dynamic Link Library (DLL)	
		78		2022-03-01 22:15:04	PE Event	PE	b	127115	PE Type: Dynamic Link Library (DLL)	
		79		2022-03-01 22:15:18	PE Event	PE	b	127117	PE Type: Dynamic Link Library (DLL)	
		80		2022-03-01 22:1 29	PE Event	PE	b	127119	PE Type: Dynamic Link Library (DLL)	
		81		2022-03-01 22:15:37	PE Event	PE	b	127121	PE Type: Dynamic Link Library (DLL)	
		82		2022-03-01 22:15:46	PE Event	PE	b	127123	PE Type: Dynamic Link Library (DLL)	
		83		2022-03-01 22:15:57	PE Event	PE	b	127125	PE Type: Dynamic Link Library (DLL)	
		84		2022-03-01 22:16:10	PE Event	PE	b	127127	PE Type: Dynamic Link Library (DLL)	
		85		2022-03-01 22:30:02	PE Event	PE	b	82809	PE Type: Executable (EXE) Import hash: c757b6532bf3304f2e1da07efe23042e	
		86		2022-03-01 22:30:02	PE Event	PE	b	89341	PE Type: Executable (EXE) Import hash: c757b6532bf3304f2e1da07efe23042e	
		87		2022-03-05 03:19:27	PE Event	PE	b	32865	PE Type: Executable (EXE) Import hash: 73effd46557538d5fa5561eee3ffc59c	
	3	88		2022-03-09 16:48:30	PE Event	PE	m	54463	PE Type: Dynamic Link Library (DLL) [DIRECTORY_ENTRY_EXPORT] DLL name: USERMGRCLI.dll Import hash: fd490a0262febd37990bdbdd445c01509	
		89		2022-03-09 16:48:30	PE Event	PE	m	54463	PE Type: Dynamic Link Library (DLL) [DIRECTORY_ENTRY_EXPORT] DLL name: USERMGRCLI.dll Import hash: fd490a0262febd37990bdbdd445c01509	
		90		2022-03-09 16:48:30	PE Event	PE	b	54463	PE Type: Dynamic Link Library (DLL) Import hash: fd490a0262febd37990bdbd445c01509	
		91		2022-03-09 16:48:30	PE Event	PE	b	54463	PE Type: Dynamic Link Library (DLL) Import hash: fd490a0262febd37990bdbd445c01509	
		92		2022-03-11 19:30:07	File stat	FILE	mb	0	NTFS:\Users\IEUser\AppData\Local\Temp\wctFD02.tmp Type: file	
		93		2022-03-11 19:33:44	File stat	FILE	mb	0	NTFS:\Users\IEUser\AppData\Local\Temp\wctF1F5.tmp Type: file	
		94		2022-03-14 18:18:04	PE Event	PE	b	82876	PE Type: Dynamic Link Library (DLL)	
		95		2022-03-14 18:18:04	PE Event	PE	b	82878	PE Type: Dynamic Link Library (DLL)	
		96		2022-03-14 18:53:38	File stat	FILE	ma.b	0	NTFS:\Users\IEUser\AppData\Local\Microsoft\Windows\Notifications\wpnidm\1c7f31e8.png Type: file	
		97		2022-03-14 19:14:17	PE Event	PE	b	32881	PE Type: Executable (EXE) Import hash: 73effd46557538d5fa5561eee3ffc59c	
		98		2022-03-14 19:14:17	PE Event	PE	b	32874	PE Type: Executable (EXE) Import hash: 73effd46557538d5fa5561eee3ffc59c	
		99		2022-03-15 16:56:35	PE Event	PE	m	40112	PE Type: Dynamic Link Library (DLL) [DIRECTORY_ENTRY_EXPORT] DLL name: Qdvd.dll Import hash: 4a828507e62d541bc643dd70e74340c8	
	1	00		2022-03-15 16:56:35	PE Event	PE	m	40112	PE Type: Dynamic Link Library (DLL) [DIRECTORY_ENTRY_EXPORT] DLL name: Qdvd.dll Import hash: 4a828507e62d541bc643dd70e74340c8	
	1	01		2022-03-15 16:56:35	PE Event	PE	b	40112	PE Type: Dynamic Link Library (DLL) Import hash: 4a828507e62d541bc643dd70e74340c8 Go to Settings to activate Windows	
4	12				(Lara)	122				

C:\Cases\Analysis\Timeline\super-timeline.csv

= , p 🖽 🥽 🛅 👹

0

Total lines 119,983 Visible lines 119,983 Open files: 1

^ 🗟 📾 🗊 🎧 👬 🖓 ClQud

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

super-timeline.csv

×

6	Tag	Timestamp	 Source Description 	T Course Mana anch	Tanda Lana Deceminitian	1	
		-	• D :	Values Text Filters			
42		2022-03-01 22:14:22	PE Event	(Protocological States)			
43		2022-03-01 22:14:23	PE Event	Enter text to search		4	
44		2022-03-01 22:14:24	PE Event	(All)			X 7 (°1, 1 'C' ,
45		2022-03-01 22:14:25	PE Event	AppCompatCache Registry	Entry		You can filter the specific events.
46		2022-03-01 22:14:26	PE Event	Backgroun Activity Moder	ator Registry Entry		•
47		2022-03-01 22:14:27	PE Event	File entry shell item			
48		2022-03-01 22:14:28	PE Event	File stat			
49		2022-03-01 22:14:29	PE Event	Mactime Bodyfie			
50		2022-03-01 22:14:30	PE Event	OLECF Dest list entry			
51		2022-03-01 22:14:30	PE Event	OLEO ^{II} Item			
52		2022-03-01 22:14:31	PE Event	PE Event			
53		2022-03-01 22:14:32	PE Event	Registry Key			
54		2022-03-01 22:14:35	PE Event	Registry Key - BagMRU			
55		2022-03-01 22:14:36	PE Event	Registry Key - Service			
56		2022-03-01 22:14:38	PE Event	Registry Key - Typed LIRLs			
57		2022-03-01 22:14:39	PE Event	Registry Key - User Account	t Information		
58		2022-03-01 22:14:40	PE Event	Registry Key - UserAssist			
59		2022-03-01 22:14:41	PE Event	Registry Key - Winlogon	19		
60		2022-03-01 22:14:42	PE Event	System	- X		
61		2022-03-01 22:14:43	PE Event	System - Network Connects	on		
62		2022-03-01 22:14:44	PE Event	Task Cache			
63		2022-03-01 22:14:45	PE Event	Windows Setupapi Log			
64		2022-03-01 22:14:46	PE Event	WeEVTX			
65		2022-03-01 22:14:47	PE Event	WnPrefetch			
66		2022-03-01 22:14:48	PE Event				
67		2022-03-01 22:14:49	PE Event	1			
68		2022-03-01 22:14:50	PE Event				
69		2022-03-01 22:14:51	PE Event				
70		2022-03-01 22:14:52	PE Event				
71		2022-03-01 22:14:53	PE Event				
72		2022-03-01 22:14:53	PE Event				
73		2022-03-01 22:14:54	PE Event	Clear Filter		Close	
74		2022-03-01 22:14:55	PE Event	FC0	12/10/ PC Type: Dynamic Link Li	many (ULL)	
75		2022-03-01 22:14:56	PE Event	PEb	127109 PE Type: Dynamic Link Li	orary (DLL)	
76		2022-03-01 22:14:57	PE Event	PEb	127111 PE Type: Dynamic Link Li	orary (DLL)	Activate Windows
77	ET.	2022-03-01 22:14:58	PE Event	PEb	127113 PE Type: Dynamic Link Li	many (DLL)	The Annual An

C:\Cases\Analysis\Timeline\super-timeline.csv

🔳 🖓 🛱 🧮 🛸

201

Total lines 119,983 Visible lines 119,983 Open files: 1 🖏 Search options

Super timeline Analysis Malicious Events

Timeline	Explorer	v1,3,0,	0						a ×
File Tools	Tab:	Vie	w Help					77 1 11	
super-timelin	e.csv							You can show all	
Drag a c	olumn	head	ler here to group by the	at column				ART-attack. [is 1]	x + Find
Line	1	Tag	Timestamp *	Source Description	Source Name	macb	Inode	e Long Description events artattadopsi	
т -			-	10:	+ O t	-0-	-		
	128		2022-03-17 01:04:57	NTFS USN change	FILE		5717	177 bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN REASON DATA OVERWRITE	
	129		2022-03-17 01:04:57	NTES USN change	FILE		5717	177 bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN REASON DATA OVERWRITE USN REASO	ON CLOSE
	130		2022-03-17 01:04:58	NTFS USN change	FILE	c.	5717	177 bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN REASON DATA OVERWRITE	
	131		2022-03-17 01:04:58	NTFS USN change	FILE		57177	177 bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN REASON DATA OVERWRITE USN REASO	ON CLOSE
	132		2022-03-17 01:04:58	NTES USN change	FILE		5717	177 bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN REASON DATA OVERWRITE	10 - 0.0020000
	133	n	2022-03-17 01:04:58	NTFS USN change	FILE		5717	177 bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN REASON DATA OVERWRITE USN REASON	ON CLOSE
	134		2022-03-17 01:05:03	NTFS USN change	FILE		5717	177 bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN REASON DATA OVERWRITE	lin n- cristian
	135		2022-03-17 01:05:03	NTFS USN change	FILE	c.	5717	177 bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN REASON DATA OVERWRITE USN REASO	ON CLOSE
	136		2022-03-17 01:05:03	NTES USN change	FILE		5717	177 bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN REASON DATA OVERWRITE	
	137		2022-03-17 01:05:03	NTES USN change	FILE		5717	177 bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN REASON DATA OVERWRITE USN REASO	ON CLOSE
	138		2022-03-17 01:05:03	NTES USN change	FILE		5717	177 EtwRTUBPM.etl File reference: 3495-4 Parent file reference: 4312-1 Update source: Update reason: USN REASON FILE CREATE	
	139	Ē	2022-03-17 01:05:03	NTES USN change	FILE		5717	177 EtwRTURPM.etl File reference: 3495-4 Parent file reference: 4312-1 Undate source: Undate reason: USN REASON DATA EXTEND USN REASON 1	THE CREAT
	149	n	2022-03-17 01:05:03	NTES USN change	FILE		5717	177 FtwRTDiaglog.etl File reference: 80516-3 Parent file reference: 4312-1 Undate source: Undate reason: USN REASON DATA OVERWRITE	
	141		2022-03-17 01:05:03	NTES USN change	FILE		5717	177 EtyRTDiaglog etl File reference: 88516-3 Parent file reference: 4312-1 Undate source: Undate reason: USN REASON DATA OVERWRITE USN I	REASON DAT
-	142		2022-03-17 01:05:03	NTES USN change	FTLF		5717	177 FtwRTFventlog-System etl File reference: 88517-3 Parent file reference: 4312-1 Undate source: Undate reason: USN REASON DATA OVERWET	(F
	143	Ē	2022-03-17 01:05:03	NTES USN change	FILE		5717	177 EtwRTEventlog-System etl File reference: 80517-3 Parent file reference: 4312-1 Undate source: Undate reason: USN REASON DATA OVERNET	E USN RE
	144	n	2022-03-17 01:05:03	NTES USN change	FILE		5717	177 BCD.LDG File reference: 80504-3 Parent file reference: 80374-3 Update source: Update reason: USN REASON DATA OVERWRITE	
	145	n.	2022-03-17 01:05:04	NTES USN change	FTLE		5717	177 BCD File reference: 80501-3 Parent file reference: 80174-3 Undate source: Undate reason: USN REASON DATA OVERWRITE	
	146	Ē	2022-03-17 01:05:04	NTES USN change	FTLE		5717	177 FtwRTHRPM at1 File reference: 3495-4 Parent file reference: 4312-1 Undate source: Undate reason: USN REASON DATA EXTEND USN REASON I	TIE CREAT
	147	n	2022-03-17 01-05-04	NTES USN change	ETLE		5717	177 FriedThiaglog et1 File reference: 88515.3 Parent file reference: 4312.1 Undate source: Undate reason: USN REASON DATA OVERWRITE USN	REASON DAT.
	148		2022-03-17 01:05:04	NTES USN change	FTLE		5717	177 FriedTreantion System et 1 File reference: 88517-3 Parent file reference: 4312-1 Undate course: Undate rescon: USA REASON DATA OVERNET	TE LISN RE.
	149		2022-03-17 01:05:04	NTES USN change	ETLE		5717	177 hontstat dat file peference' 81810.1 Perent file peference' 1883.1 Hodate source' Indate peacon USN REASON DATA OVERWRITE	e osn_ner
-	150	-	2022-03-17 01:05:04	NTES USN change	ETLE		5717	177 bootstat dat File reference: 81810-1 Parent File reference: 1803-1 Deduce Source: Undate reason: USA REASON DATA OVERWRITE USA REASO	IN CLOSE
	151	-	2022-03-17 01:05:04	NTES USN change	FUE		5717	177 BCD File reference: 80501.3 Parent file reference: 8072.3 Undate source: Undate reason: USN REASON DATA OVERWRITE USN REASON () OSE	AL CLOSE
	152	H	2022-03-17 01:05:04	NTES USN change	ETLE		5717	177 BCD LDG File reference: \$8584.3 Parent file reference: \$8374.3 Indate square: Indate reson: USN REASON DATA OVERWRITE LISN REASON	OSE
	153	H	2022-03-17 01:05:04	PF Event	DE		4164	648 PF Type: Dynamic Link Lincary (DLL) IDIRFCTORY ENTRY EXPORTI DLL name: NovGinRadioManager dll Import hach: 5d628e9abd82a55fa9d	Effeh2aa
-	154	-	2022-03-17 15:26:04	PE Event	PE		4164	648 PE Type: Oynamic Link Lincary (DLL) [DIRECTORY ENTRY EXPORT] DLL name: NorvingEdiaManager dll Tmoort hach: 54628a9abd82a65cfa9cdf996	F6eb2aa
	155	E.	2022-03-17 15:26:04	PE Event	PE	h	A16A	one is type: by manife link is the sty (bit) [praction_chine] and might be manife about programming in the import manife link is the style of the st	000200
	156	-	2022-03-17 15:26:04	DE Event	DE	h	41040	one it type, bynamic Link Library (bit) import hash, subcessburgsschasstarisstebsta	
	457	H	2022-03-17 15:20.04	PE Event	DE	W	9397	040 rt type, bynamic Link Library (DLT) import nash, subzessbudzabitasturssbreezaa	
	100	H	2022-03-17 10:10:41	PE Event	DE		0207	077 PE type, bynamic Link Library (DL)	
-	150	H	2022-03-17 10:10:41	DE Event	DE DE	b	12284	811 DE Tune: Dunamic Link Library (DLL)	
	160	-	2022-03-17 10:17:09	PE Event	DE		12701	922 DE Turne, Durnamie Link Library (DLL)	
	161	H	2022-03-17 10:17:40	AppCompatCacho Pard	PEC	***0	12/82	072 FC Type, bynamic cink cibrary (UCC) 071 [UKEY LOCAL MACUTMENS/Content/	007161-14
	101		2022-03-17 10:27:16	Appcompatcache Kegi	CTLE		4207	Intro _ controlsecontrolsecontrolsession manager/appcomparcatnej tathed entry: 7 Path: C:/Atomickedleam/atomics/11545	A/1110/ 600
141	10%		2055-02-11 10:51:10	FALC STAL	PALC	III + + +		o HIPS. Activate Vindexes (Actack Havigator-Lavers (art-havigator-laver-agers art-havigator-laver-agers) art have a constructed by the construction of the constructio	

X 📝 Timestamp Is same day 2022-03-17 00:00:00 2022-03-18 00:00:00 +

101

C:\Cases\Analysis\Timeline\super-timeline.csv

HI 📻 **F**1-8

Total lines 119,983 Visible lines 98,243 Open files: 1 🖏 Search options

Go to Settings to activate Windows

^ 🗟 📾 🗊 🎧 👬 📶 ClQud

Edit Filter

0	Timeline Explore	r v1.3.0.	.0							- 0	×
ile	Tools Ta	bs Vie	sw Help								
up	er-timeline.csv										
)ri	ag a colum	n head	der here to group by t	hat column					ART-attack.ps1	× -	Find
1	Line	Tag	Timestamp *	* Source Description	Source Name	macb	Inode	Long Description			
r	-		-	-0:	4 0 1	*Oc	-	0			
	920		2022-03-17 23:35:52	File stat	FILE	mb	0	NTFS:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\ <mark>ART-attack.ps1</mark> Type: file			
	32926		2022-03-18 00:17:31	NTFS USN change	FILE		57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASO	N_BASIC_INFO_CHANGE		
	32927		2022-03-18 00:17:31	NTFS USN change	FILE	c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASO	N_BASIC_INFO_CHANGE	USN_REASO	N_CI
	32928		2022-03-18 00:17:31	NTFS USN change	FILE	c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASO	N_FILE_CREATE		
	32929		2022-03-18 00:17:31	NTFS USN change	FILE	c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASO	N_DATA_EXTEND USN_R	EASON_FILE	_CR
	32930		2022-03-18 00:17:31	NTFS USN change	FILE	c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASO	N_DATA_EXTEND USN_R	EASON_FILE	CR
	32931		2022-03-18 00:17:31	NTFS USN change	FILE	c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASO	N_BASIC_INFO_CHANGE		
	32932		2022-03-18 00:17:31	NTFS USN change	FILE	c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASO	N_BASIC_INFO_CHANGE	USN_REASO	N_C
	32933		2022-03-18 00:17:31	File stat	FILE	c.	0	NTFS:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\ART-attack.ps1 Type: file			
	43962		2022-03-18 00:20:49	File stat	FILE		0	NTFS:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\ART-attack.os1 Type: file			

You can search specific events and show result.

2

× 🕑 Timestamp Is same day 2022-03-12 00:00:00 2022-03-18 00:00:00 -

C:\Cases\Analysis\Timeline\super-timeline.csv

-

EX-

1

0

Π



to activate Windows.

^ 🛐 📾 🖫 🎧 👬 🎆 CIĐud

Activate Windows

Total lines 119,983 Visible lines 10 Open files: 1 👪 Search options

Edit Filter

×

-	100			-			1.00		1.4	
100	1.100			- wrv	let		UT.	3.1	1.0	
2.00		100	-		100	÷.	7.44	211	P 1 W 1	

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

atomicservice.exe	× +	Find

-

	Line	Tag	Timestamp 🔺	Source Description	Source Name	macb	Inode	Long Description
Ŧ	-		-	-	10:	* D :	-	0:
	161		2022-03-17 16:27:16	AppCompatCache Regi.	REG		42071	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] Cached entry: 7 Path: C:\AtomicRedTeam\atomics\T1543.003\bin\
	679		2022-03-17 16:27:16	File stat	FILE	m	0	NTF5:\AtomicRedTeam\atomics\T1543.003\bin\ <mark>AtomicService.exe</mark> Type: file
	64767		2022-03-18 00:23:59	NTFS USN change	FILE	c.	57177	AtomicService.exe File reference: 126258-2 Parent file reference: 126257-2 Update source: Update reason: USN_REASON_FILE_CREATE
	64768		2022-03-18 00:23:59	NTFS USN change	FILE	c.	57177	AtomicService.exe File reference: 126258-2 Parent file reference: 126257-2 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_FILE
	64769		2022-03-18 00:23:59	NTFS USN change	FILE		57177	AtomicService.exe File reference: 126258-2 Parent file reference: 126257-2 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_FILE
	64770		2022-03-18 00:23:59	NTFS USN change	FILE	c.	57177	AtomicService.exe File reference: 126258-2 Parent file reference: 126257-2 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
	64771		2022-03-18 00:23:59	NTFS USN change	FILE	c.	57177	AtomicService.exe File reference: 126258-2 Parent file reference: 126257-2 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE USN_REASO
	64774		2022-03-18 00:23:59	File stat	FILE	cb	0	NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicServIce.exe Type: file
	64786		2022-03-18 00:23:59	WinEVTX	EVT	mb	89021	[11 / 0x000b] Source Name: Microsoft-Windows-Sysmon Strings: ['EXE' '2022-03-18 00:23:59.239' '{747F3D96-D020-6233-6801-000000001200}' '6988'
	76958		2022-03-18 00:25:36	Mactime Bodyfile	FILE	b	0	D11List - DLL Load: Process 6572 AtomicService. Loaded AtomicService.exe (C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe) Size 32768 Of
	76996		2022-03-18 00:25:36	WinE I and for success	et al time line formate	a	~ 7021	[1 / 0x0001] Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2022-03-18 00:25:36.418' '{747F3D96-D180-6233-FE01-000000001200}' '3760' 'C
	77000		2022-03-18 00:25:36	WinE WinE	itted timeline formats	0	021	[1 / 0x0001] Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2022-03-18 00:25:36.619' '{747F3D96-D180-6233-0002-000000001200}' '5176' 'C
	77001		2022-03-18 00:25:36	WINE FILE OPENING			799	[7045 / 0x1b85] Source Name: Service Control Manager Strings: ['AtomicTestService_CMD' 'C:\\AtomicRedTeam\\atomics\\T1543.003\\bin\\AtomicService
	77002		2022-03-18 00:25:36	Regi WEB HISTORY			2071	[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\AtomicTestService_CMD] Type: Service - Own Process (0x10) Start: Manual (3) Image path: C:\Atom
	77004		2022-03-18 00:25:36	WinE			021	[13 / 0x000d] Source Name: Microsoft-Windows-Sysmon Strings: ['T1031 T1050' 'SetValue' '2022-03-18 00:25:36.676' '{747F3D96-CDE6-6233-0800-000
	77006		2022-03-18 00:25:36	WinE			021	[1 / 0x0001] Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2022-03-18 00:25:36.704' '{747F3D96-D180-6233-0102-000000001200}' '2168' 'C
	77007		2022-03-18 00:25:36	WinP			1874	Prefetch [ATOMICSERVICE.EXE] was executed - run count 1 path hints: \ATOMICREDTEAM\IMP\ATOMIC-RED-TEAM-MASTER\ATOMICS\I1543.003\BIN\ATOMICSERVICE
	77008		2022-03-18 00:25:36	WinE Wine was			021	[1 ⁶ / 0x0001] Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2022-03-18 00:25:36.805' '{747F3D96-D180-6233-0202-000000001200}' '6572' 'C
۲	77383		2022-03-18 00:25:47	NTFS PLACE OPENING			1177	ATOMICSERVICE.EXE-CFFBD82A.pf File reference: 82874-5 Parent file reference: 80798-1 Update source: Update reason: USN_REASON_FILE_CREATE
	77384		2022-03-18 00:25:47	NTFS LOG FILE			177	ATOMICSERVICE.EXE-CFFBD82A.pf File reference: 82874-5 Parent file reference: 80798-1 Update source: Update reason: USN_REASON_DATA_EXTEND USN_R
	77385		2022-03-18 00:25:47	NTFS our change			_/177	ATOMICSERVICE.EXE-CFFBD82A.pf File reference: 82874-5 Parent file reference: 80798-1 Update source: Update reason: USN_REASON_DATA_EXTEND USN_R
	77386		2022-03-18 00:25:47	File stat	FILE	macb	0	NTFS:\Windows\Prefetch\ATOMICSERVICE.EXE-CFFBD82A.pf Type: file
	78073		2022-03-18 00:26:00	File stat	FILE	.0	0	NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe Type: file
	97024		2022-03-18 22:18:56	Registry Key	REG	m	46357	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\CIT\Module\Microsoft.NET/Framework64/v4.0.30319/clr.dll] \Device\
	97514		2022-03-18 22:18:58	NTFS USN change	FILE		57177	AtomicService.exe.log File reference: 32823-6 Parent file reference: 115206-3 Update source: Update reason: USN_REASON_FILE_CREATE
	97515		2022-03-18 22:18:58	NTFS USN change	FILE		57177	AtomicService.exe.log File reference: 32823-6 Parent file reference: 115206-3 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_F
	97516		2022-03-18 22:18:58	NTFS USN change	FILE		57177	AtomicService.exe.log File reference: 32823-6 Parent file reference: 115206-3 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_F
	97518		2022-03-18 22:18:58	File stat	FILE	macb	0	NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\ <mark>AtomicService.exe</mark> .log Type: file
	97522		2022-03-18 22:18:58	WinEVTX	EVI	mb	89021	[11 / 0x000b] Source Name: Microsoft-Windows-Sysmon Strings: ['ProcessHostingdotNETCode' '2022-03-18 22:18:58.353' '{747F3096-D180-6233-0202-00

Using colorcode you know about execution on events.

Activate Windows

C:\Cases\Analysis\Timeline\super-timeline.csv

X 🔽 Timestamp Is same day 2022-03-17 00:00:00 2022-03-18 00:00:00

-

2

Total lines 119,983 Visible lines 29 Open files: 1 📆 Search options

^ 🛃 📾 🖫 🎧 👘 🖓 Cloud

Edit Filter

page 1	-	-		1 2 4	
1.1	Imenne	: CXD	orer v	1,2,0,	<i>v</i>

File Tools Tabs View Help

super-timeline.csv

		HTC .					24.0	1
1	- X						Offset 140718688829440	
1	2022-03-18 00:25:52	Mactime Bo	Line #	77636	Version	2		ize 69632 Offset 140718863417344
-	2022-03-18 00:25:52	Mactime Bo	Timestamo	2022-03-18 00-25-52	Eile name	NTES:\Windows\System32\winevt\Loos\b		Offset 140718872854528
1	2022-03-18 00:25:52	Mactime Bo	Time anno		Toode	00004		t 140718929543168
1	2022-03-18 00:25:52	Mactime Bo	time zone	UTC -	mode	89021		set 140695128834048
	2022-03-18 00:25:52	Mactime Bo	macb	mb	Notes	•		140718930395136
	2022-03-18 00:25:52	Mactime Bo	Source name Source description	EVT	Extra	winevtx		set 140718847295488
	2022-03-18 00:25:52	Mactime Bo		WinEVTX		<pre>message_identifier: 1; provider_identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9}; * recovered: False; sha256_hash: d74145cbcc3e1afcb66f565df4b7bee523f8764edc76d97aecb256bbdb277439; user sid:</pre>	t 140718415282176	
	2022-03-18 00:25:52	Mactime Bo	Туре	Content Modification Time; Creation Time			Iffset 140718863745024	
	2022-03-18 00:25:52	Mactime Bo	User name			S-1-5-18; xml_string: <event< td=""><td>et es est training</td><td>set 140718863548416</td></event<>	et es est training	set 140718863548416
	2022-03-18 00:25:52	Mactime Bo	Host name	-		xmins="http://schemas.microsoft.com/win/2004/08/events/event"> < System>	3E0-8F4C-	set 140718923317248
	2022-03-18 00:25:52	Mactime Bo	Short description	[1 / 0x0001] Strings: ['-' '2022-03-18 00:25:52.204' '(747F3D96-D190-6233-0		06F5698FFBD9}"/>- <eventid>1</eventid> - <version>5</version>		t 140718883340288
	2022-03-18 00:25:52	Mactime Bo	Long description	[1 / 0x0001] Source Name: Microsoft-Windows-Sysmon Strings: [1-1 2022-03-18	-	<level>4</level> - <task>1</task> - <opcode>0</opcode> - <keywords>0x8000000000000000</keywords> - <timecreated< td=""><td></td><td>Size 2150400 Offset 140718838251520</td></timecreated<>		Size 2150400 Offset 140718838251520
	2022-03-18 00:25:52	Mactime Bo	a cong usacipiton	00:25:52.204' '(747F3D96-D190-6233-0A02-00000001200)' '6552' 'C:\		SystemTime="2022-03-18T00:25:52.2255829002"/>-		Offset 140718866956288
	2022-03-18 00:25:52	Mactime Bo		\Windows\\System32\\notepad.exe' '10.0.17763.1 (WinBuild.160101.0800)' 'Notepad' 'Microsoft'® Windows® Operation System' 'Microsoft Corporation'		<eventrecordid>496</eventrecordid> - <correlation></correlation> - <execution ProcessID="7468" ThreadID="3880"/>- <channel>Microsoft-Windows-</channel></execution 		et 140718691647488
	2022-03-18 00:25:52	Mactime Bo		"NOTEPAD.EXE' "C:\\Windows\\system32\\notepad.exe" ' C:\\Users\\IEUser\		Sysmon/Operational- <computer>MSEDGEWIN10</computer> - <security userd="S-1-5-18"></security> - - <eventdata>- <data Name="RuleName">-- <data name="UtcTime">2022-03-18 00:25:52.204</data>- <data name="ProcessGuid">(747F3D96-D190-6233-0A02-</data></data </eventdata>	ter>-	set 140718834384896
	2022-03-18 00:25:52	Mactime Bo		\AppData\Local\\Temp\\' 'MSEDGEWIN10\\IEUser' '{747F3D96-CDFE-6233-AA52- canonanananal' 'icononananana'saa' '1' 'Hisb'				t 140718874230784
	2022-03-18 00:25:52	Mactime Bo		'MD5=782877830735ABD1EAE241F13145F664			5233-0A02-	Size 7643136 Offset 140718874689536
	2022-03-18 00:25:52	Mactime Bo		SHA256=E46B3CA5A0EBB4A6979F852F50E22BD08C9F2D0206CC04383978BE0172A		00000001200}- <data name="Processid">6552</data> - <	Data	Offset 140718801420288
	2022-03-18 00:25:52	Mactime Bo		-0502-00000001200)' '6156' 'C:\\Windows\\System32\\WindowsPowerShell\		Name="mage">C:\Windows\System32\notepad.exe- <data Name="FileVersion">10.0.17763.1 (WinBuild.160101.0800)- <</data 	Data	
	2022-03-18 00:25:52	Mactime Bo		\v1.0\\powershell.exe' "powershell.exe" & {\$mypid = (Start Process notepad		Name="Description">Notepad- <data name="Product">Micros</data>	oft®	
	2022-03-18 00:25:52	WinEVTX	1	PassThru).id\nmavinject_Smypid_/J/UECTRUNNING_C:\\AtomicRedTeam\\atomics\ \T1055.001\\src\\x64\\T1055.001.dll}''MSEDGEWIN10\\IEUser']_Computer_Name:		Windows@ Operating System- <data name="Company">Micro Corporation</data> - <data name="OriginalFileName">NOTEPAD.EXE</data>	:/Data>-	-0A02-00000001200}' '6552' 'C:\\W1
	2022-03-18 00:25:52	WinPrefet		MSEDGEWIN10 Record Number: 496 Event Level: 4		<data name="CommandLine">"C:\Windows\system32\notepad.exe" <td>ata>-</td><td>me: 1 [serial number: 0x84A6FEC6 dev</td></data>	ata>-	me: 1 [serial number: 0x84A6FEC6 dev
	2022-03-18 00:25:53	Mactime Bo	2			<data name="CurrentDirectory">C:\Users\IEUser\AppData\Local\Temp\ <data name="User">MSEDCEWIN10\TEUser</data>- <data logonid"="" name="U</td><td>/Data>-</td><td>set 140718862237696</td></tr><tr><td></td><td>2022-03-18 00:25:53</td><td>Mactime Bo</td><td></td><td></td><td></td><td>{747F3D96-CDFE-6233-AA52-0400000000000}</br></td><td>and a second second</td><td>et 140718770028544</td></tr><tr><td></td><td>2022-03-18 00:25:53</td><td>Mactime Bo</td><td>9</td><td></td><td></td><td>Name=">0x0000000000452aa</data>- <data< td=""><td></td><td>55.001.d11) Size 118784 Offset 140718</td></data<></data>		55.001.d11) Size 118784 Offset 140718
	2022-03-18 00:26:02	NTFS USN	9	Show all events in long		Name="IntegrityLevel">High- <data< td=""><td></td><td>_REASON_DATA_TRUNCATION</td></data<>		_REASON_DATA_TRUNCATION
	2022-03-18 00:26:02	NTFS USN		Show all events in folig		Name="Hashes">MD5=782877830735A8D1EAE241F13145F664	00001734.00	_REASON_DATA_EXTEND USN_REASON_DATA_
	2022-03-18 00:26:02	NTES USN	Show formatted	description also		8EE IMPHASH=C89228E3DCDFE85994C9EEE7745DC22E < Cota	0000172000	_REASON_DATA_EXTEND USN_REASON_DATA_
	2022-03-18 00:26:02	File stat	Silver formation	ucscription also.		Name="ParentProcessGuid">{747F3D96-D184-6233-0502-00000001200	-	
	2022-03-18 22:18:39	Registry	Show raw		5	 Suata Name= ParentProcessio >0150- Suata Name="Parently IMindows/Custom23)MindowsBowsrChollout_Obacustcholl_overs/Data>- 	Anata -	terval: [REG_DWORD_LE] 20160 ETag: [R
	2022-03-18 22:18:45	File stat	Always on top (Previous rec	ord Next record	
	2022-03-18 22:18:45	File stat	FILE	.a., Ø NTFS:\Windows\WinSxS\amd64_microsoft	-windows-n	otepad_31bf3856ad364e35_10.0.17763.1_none_5fe07760c829	276f\notepad	exe Type: file
	2022-03-18 22:18:45	File stat	FILE	.a 0 NTFS:\Windows\notepad.exe Type: file	R.			
	2022-03-18 22:18:50	Registry H	Key REG	m 83610 [HKEY CURRENT USER\Software\Classes\	Local Sett	ings\MuiCache\8\52C6487E1 @"C:\Windows\system32\window	powershell\	v1.0\powershell.cexe.iu-108: [REG SZ] R

^ 🔄 🛥 💭 🖓 👘 🚧 CIQud

- 0 ×

×

Reporting types and consideration

Reporting Considerations

- 1. Establish expectations in the beginning!
- 2. Consider the audience that you are targeting.
- 3. Alternative Explanations.
- 4. Actionable Information.

Types of Reporting

Forensic Report - Legal Cases

High-level presentation – Executive debriefs, Q &A documents

System Timeline – Events listed in temporal order

Etc. – Resolving Tickets like some proof screen shorts

Thanks for Attending This Session