Collecting the data from volatile memory in digital forensics -Khushank Raj Mahawan

Have you ever been so curious about how the forensics experts handle the digital evidences in the world of Cybersecurity? Then this is the article for you my friend, So what if there is a computer (Desktop/Laptop) found 'ON' at a crime scene? What would be their first step in this case? How do they do that? So, this article will surely answer all your

Starting off with the difference between Volatile and non-volatile memory,

Non volatile memory sustains the data even if the computer is turned off while in case of volatile memory data is only available untill the machine is not powered off.

Hence the forensics experts will try to get all the data in volatile memory first, There are many tools they use, we have used *FTK IMAGER*.

So what type of data will they look for in the volatile memory?

The following is the type of data they primarily look for:

1. <u>Log files</u>: A record that contain all the information about events, operations and errors occuring in a system including the communication between users at that time.

2. **Processes**: The processes running at that time

questions.

3. **<u>Registry files</u>**: The information database containing everything from setting, passwords and options of the windows only.

4. <u>Memory file</u> (.mem): This is basically the Dump of a RAM data which is again a volatile data. It is the data that is been processed or to be processed into kernel, which is present in RAM. It also includes following files:

A. <u>Swapfile</u>: Swapfile is a virtual memory file available in system drive as '*swapfile.sys*'. It stores the data that is not in use for that particular iinstance to swap of main memory and swap to, when in use.

B. <u>Hiberfil</u>: Hiberfil is a file storing the data if a main memory when the system is hibernated so that the state of system can be saved and sustained for the next use. This is again stored in system drive as '*hiberfil.sys*'.

C. Pagefile: Pagefile is a file storing the data in cases when the RAM is filled up, this is also stoed in a system drive as '*pagefile.sys*'.

Let's start on how to retrieve the data from volatile memory, We will be using the FTK IMAGER and windows 7 Professional OS so this article will also help you as a tutorial on How to use the FTK IMAGER as a beginner?

We will be starting from installing the FTK Imager in our USB that will be used for the data collection and investigation and for the rest of the steps, The complete Proof of Concept is given below.

1. Start by Capturing the Volatile memory, Navigate to Files and then select Capture memory.

Acc	essData FTK Imager 3.2.0.0				
Eile	<u>V</u> iew <u>M</u> ode <u>H</u> elp				
😰 A	dd Evidence Item	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	12 8		
A 🕼	dd All Attached Devices	File List			×
🖷 In	mage Mou <u>n</u> ting	Name	Size Type	Date Modified	
	emove Evidence Item				
🖄 R	emove All Evidence Items				
	reate Disk Image				
E	x <u>p</u> ort Disk Image				
E E	xport Logical Image (AD1)				
A 54	dd to Custom Content Image (AD <u>1</u>)				
🕮 Ci	reate Custom Content Image (AD1)				
D	ecrypt AD1 image				
<u> </u>	erify Drive/Image				
Ca	ap <u>t</u> ure Memory				
	btain Protected Files				
9 D	etect EFS Encryption				A
D B	xport <u>Fi</u> les				
E B	xport File <u>H</u> ash List				
E E	xport Directory Listing				
E	<u>x</u> it				
•	III. F				
New	Edit Remove All Create Image				
Pro	perties Hex Value Int Custom Conte	<u> </u>			Ψ
Capture	Memory				

2. Select the path of the USB and Enable dumping of pagefile and AD1 file.

Memory Capture	
Destination path:	
E:\	Browse
Destination filename:	
memdump.mem	
✓ Include pagefile	
pagefile.sys	
Create AD1 file	
memcapture.ad1	
Capture Memory	Cancel

3. Now this process of dumping will take time depending upon the RAM of that computer.

Destination:	E: \memdumpl.mem
Status:	Dumping RAM: 131MB/805MB [16%]
	Cancel
Memory Progr	ess
Destination:	E:\memcapture.ad1
Destination: Status:	E:\memcapture.ad1 Memory capture finished successfully
Destination: Status:	E:\memcapture.ad1 Memory capture finished successfully

Memory is captured, the data inside the RAM is now been with us.

4. Now, to collect the logs, navigate to files again

AccessData FTK Imager 3.2.0.0				
<u>File View M</u> ode <u>H</u> elp				
Add Evidence Item	📕 🖪 I S I D 🗎 🗎	🐱 रेसे सेटे 🦞 🖕		
Add All Attached Devices	File List			×
😫 Image Mou <u>n</u> ting	Name	Size Type	Date Modified	
Remove Evidence Item				
Remove All Evidence Items				
Greate Disk Image				
Export Disk Image				
Export Logical Image (AD1)				
Add to Custom Content Image (AD1)				
Create Custom Content Image (AD1)				
Decrypt AD1 image				
Verify Drive/Image				
Capture Memory	-			
Detain Protected Files				
S Detect EFS Encryption				*
Export Files				
Export File <u>H</u> ash List				
Export Directory Listing				
E <u>x</u> it				
•	P			
New Edit Remove Remove All Create Image				
Properties Hex Value Int Custom Conte	「			-
Adds evidence from disk, image file, or folder				

5. Since we don't know the actual physical memory location, we will go with the logical disk.



6. As OS is installed in C Drive, we will select the same.

Select Drive				×
- Source Dr Please s	ive Selection elect from the follo	wing available dr	ives:	
C:\- [N	ITFS]			•
-	< Back	Finish	Cancel	Help

7. Finishing off we get a screen with a tree explorer on the left, browse to the path: *C\Windows\System32\Winevt\Logs* for logs.

💽 AccessData FTK Imager 3.2.0.0					
<u>File View M</u> ode <u>H</u> elp					
🏩 🏩 🗣 🚔 🖆 🖬 🖬 🚛 🗷 🗢		🔁 👟 🖻 🗐 🕞 😹			
Evidence Tree	\times	File List			
🕀 🗀 WinBioPlugIns	*	Name	Size	Туре	Date Modified
WindowsPowerShell		\$130	28	NTFS Index All	1/21/2020 5:07:
		Application.evtx	1,092	Regular File	1/21/2020 5:46:
		HardwareEvents.evtx	68	Regular File	1/21/2020 6:21:
		Internet Explorer.evtx	68	Regular File	1/21/2020 6:21:
zh-CN		Key Management Serv	68	Regular File	1/21/2020 6:21:
zh-HK		Media Center.evtx	68	Regular File	1/21/2020 6:21:
zh-TW		Microsoft-Windows-A	68	Regular File	1/21/2020 6:21:
⊞ · 🛅 SysWOW64		Microsoft-Windows-A	68	Regular File	1/21/2020 6:21:
TAPI		Microsoft-Windows-A	68	Regular File	1/21/2020 6:21:
	- 218	Microsoft-Windows-A	68	Regular File	1/21/2020 6:21:
	-	Microsoft-Windows-A	68	Regular File	1/21/2020 6:21:
۲ <u> </u>	•	Microsoft-Windows-B	68	Regular File	1/21/2020 5:48:
Custom Content Sources	×	Microsoft-Windows-B	68	Regular File	1/21/2020 5:46:
Evidence:File System Path File Options		Microsoft-Windows-D	08	Regular File	1/21/2020 0:21:
		Interosoft-windows-D	08	Regular File	1/21/2020 3:46:
		00 30 00 00 00 01 00 00 0	00-00 10 00	00 01 00 00 0	0 0 • • • • • • • • • • • • • • • • • •
				00 01 00 00 0	10((
			00-18 00 00	00 03 00 00 0	
<	•				
New Edit Remove Remove All Create Image	5				

8. Export the log files to the path of your USB or the desired path.

AccessData FTK Imager 3.2.0.0	
File View Mode Help	
▲▲▲▲ ▲ □ □ □ □ = = = =	🔋 🍕 🗋 🗃 🔤 🐱 🐮 💡 🖕
Evidence Tree X	File List
🕀 🗀 WinBioPlugIns 🔺	Name Size Type Date Modified
E WindowsPowerShell	SI30 28 NTFS Index All 1/21/2020 5:07:
	Application.evtx 1,092 Regular File 1/21/2020 5:46:
Export Files	68 Regular File 1/21/2020 6:21:
	x 68 Regular File 1/21/2020 6:21:
	rv 68 Regular File 1/21/2020 6:21:
	(AD1) 68 Regular File 1/21/2020 6:21:
🛁 🗖 zh 🚌 🛛 Add to Custom Conte	ent Image (AD <u>1</u>) -A 68 Regular File 1/21/2020 6:21:
E GysWOw64	68 Regular File 1/21/2020 6:21:
	Microsoft-Windows-A 08 Regular File 1/21/2020 0:21:
	Microsoft-Windows-A 68 Regular File 1/21/2020 0:21:
Temp	Microsoft-Windows-A 68 Regular File 1/21/2020 0:21:
	Microsoft-Windows-B 68 Regular File 1/21/2020 5:46:
Custom Content Sources	Microsoft-Windows-D. 68 Regular File 1/21/2020 6:21:
Evidence:File System Path File Options	Microsoft-Windows-D 68 Regular File 1/21/2020 5:46:
	20 00 00 00 00 00 00 00 00-18 00 00 03 00 00 00 00
	30 04 00 00 00 00 00 00 00-
New Edit Remove All Create Image	
Properties Hex Value Int Custom Conte	Cursor pos = 0
Exports files from the image to a local folder	

☆ Favorites ■ Desktop	Documents library			
Downloads	Name	Date modified	Туре	Size
🔠 Recent Places	SI30	1/21/2020 10:37 AM	File	28 KB
Libraries	Application	1/21/2020 11:16 AM	Event Log	1,092 KB
Documents	HardwareEvents	1/21/2020 11:51 PM	Event Log	68 KB
Music	🛃 Internet Explorer	1/21/2020 11:51 PM	Event Log	68 KB
Pictures	🛃 Key Management Service	1/21/2020 11:51 PM	Event Log	68 KB
Videos	🛃 Media Center	1/21/2020 11:51 PM	Event Log	68 KB
La videos	Microsoft-Windows-Application-Experie	1/21/2020 11:51 PM	Event Log	68 KB
Computer	Microsoft-Windows-Application-Experie	1/21/2020 11:51 PM	Event Log	68 KB
- compater	Microsoft-Windows-Application-Experie	1/21/2020 11:51 PM	Event Log	68 KB
Network	Microsoft-Windows-Application-Experie	1/21/2020 11:51 PM	Event Log	68 KB
THEWOIR	Microsoft Microsoft Mindows Application	1 /01 /0000 11.51 DM	Front Lang	68 KB
	Microsof Type: Event Log	68 KB		
	Microsof Size: 68.0 KB	68 KB		
	Microsoft minutes onep circulation	M 1/21/2020 11.91 W	eveneed	68 KB
	Microsoft-Windows-Dhcpv6-Client%4Ad	1/21/2020 11:16 AM	Event Log	68 KB
	Microsoft-Windows-Diagnosis-DPS%4O	1/21/2020 11:16 AM	Event Log	68 KB
	Microsoft-Windows-Diagnosis-Schedule	1/21/2020 11:15 AM	Event Log	68 KB

9. Coming to registry files, Locate to 'Obtain Protected Files'.

AccessData FTK Imager 3.2.0.0					
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp					
🕼 🏟 🗣 🗠 🚖 🗇 🖬 🖬 🗸 🚙 😑 🛚	📵 🔍 🗋 🗎 🖬 🐱 😹	8.			
Evidence Tree	File List				
🕀 🖓 🗁 WinBioPlugIns		Size	Туре	Date Modified	
🕀 🧰 WindowsPowerShell	SIB0	28	NTFS Index All	1/21/2020 5:07:	
	Application.evtx	1,092	Regular File	1/21/2020 5:46:	
	HardwareEvents.evtx	68	Regular File	1/21/2020 6:21:	
	Internet Explorer.evtx	68	Regular File	1/21/2020 6:21:	
- zh-CN	🛃 Key Management Serv	68	Regular File	1/21/2020 6:21:	
	Media Center.evtx	68	Regular File	1/21/2020 6:21:	
🛁 🔂 zh-TW	Microsoft-Windows-A	68	Regular File	1/21/2020 6:21:	

10. Select the path to collect registry files along with password recovery and all registry files ticked.

Warning: Please be awar system files from the live	e that FTK Imager is system and not the	obtaining the acquired image
Destination for obtained f	iles:	Browse
C: \Users \PGDCSL \Docum	nentsWew folder	
Options C Minimum files for lo Password recovery	gin password recove and all registry files	ery
	ОК	Cancel

11. Verify the path for all the files including SAM file.

-

Documents library New folder			
Name	Date modified	Туре	Size
🍌 Logs	1/21/2020 12:40 PM	File folder	
🐌 Users	1/21/2020 12:46 PM	File folder	
default	1/21/2020 12:41 PM	File	256 KB
SAM	1/21/2020 11:16 AM	File	256 KB
SECURITY	1/21/2020 11:26 AM	File	256 KB
software	1/21/2020 12:46 PM	File	37,376 KB
system	1/21/2020 12:43 PM	File	12,288 KB

12. For the process and event details, you need to utilities, either locate them if available in your OS or just get them from google, The utilities are Autorun and Process Explorer. Open the autorun

🖄 KnownDLLs 🛛 🔮 Wi	nlogon 🌒 🌒 Winsock Providers	Print Monitors	😻 LSA Providers	Network	k Providers	🗃 wmi	📑 Sidebar Gadgets	1 Office
🖾 Everything 🛛 🏄 Logon	📃 🛃 Explorer 🛛 🥭 Internet I	Explorer 🙆 Scheduled Tasks	Services	Drivers	Codecs	Boot Execute	Image Hijacks	👌 AppInit
Autorun Entry	Description	Publisher	Image Path		Timestamp		VirusTotal	
HKLM\SYSTEM\CurrentControlS	et\Control\SafeBoot\AlternateShell				7/14/2009 10:19 AM	1		
Cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cr	md.exe	11/20/2010 3:16 PM	1		
HKLM\SOFTWARE\Microsoft\W	/indows\CurrentVersion\Run				1/21/2020 10:24 AM	1		
VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	c:\program files\vmware`	vmware tool	9/1/2019 2:08 PM			
VMware VM3DService		(Verified) VMware, Inc.	c:\windows\system32\vr	m3dservice	7/26/2019 9:14 AM			
HKLM\SOFTWARE\Microsoft\A	ctive Setup Installed Components				7/14/2009 10:19 AM	1		
🗹 🚳 n/a	Microsoft .NET IE SECURITY REGIS	(Verified) Microsoft Corporation	c:\windows\system32\m	scories.dll	6/4/2009 9:29 AM			
Themes Setup	Microsoft(C) Register Server	(Verified) Microsoft Windows	c:\windows\system32\re	egsvr32.exe	7/14/2009 5:44 AM			
Windows Desktop Update	Microsoft(C) Register Server	(Verified) Microsoft Windows	c:\windows\system32\re	egsvr32.exe	7/14/2009 5:44 AM			
HKLM\SOFTWARE\Wow6432N	lode\Microsoft\Active Setup\Installed Co	mponents			7/14/2009 10:19 AM	1		
🗹 🚳 n/a	Microsoft .NET IE SECURITY REGIS	. (Verified) Microsoft Corporation	c:\windows\syswow64\r	mscories.dll	9/29/2010 9:23 AM			
Themes Setup	Microsoft(C) Register Server	(Verified) Microsoft Windows	c:\windows\syswow64\r	regsvr32.exe	7/14/2009 5:28 AM			
Windows Desktop Update	Microsoft(C) Register Server	(Verified) Microsoft Windows	c:\windows\syswow64\r	regsvr32.exe	7/14/2009 5:28 AM			
HKLM\SOFTWARE\Classes\Pro	tocols\Filter				7/14/2009 10:23 AM	1		
application/octet-stream	Microsoft .NET Runtime Execution E	(Verified) Microsoft Corporation	c:\windows\system32\m	iscoree.dll	3/5/2010 8:35 AM			
application/x-complus	Microsoft .NET Runtime Execution E	(Verified) Microsoft Corporation	c:\windows\system32\m	iscoree.dll	3/5/2010 8:35 AM			
application/x-msdownload	Microsoft .NET Runtime Execution E	(Verified) Microsoft Corporation	c:\windows\system32\m	scoree.dll	3/5/2010 8:35 AM			
HKLM\System\CurrentControlSet	Services				1/21/2020 12:43 PM	1		
clr_optimization_v2.0.50	Microsoft .NET Framework NGEN v2	(Verified) Microsoft Corporation	c:\windows\microsoft.ne	t\framework	6/4/2009 10:55 AM			
clr_optimization_v2.0.50	Microsoft .NET Framework NGEN v2	(Verified) Microsoft Corporation	c:\windows\microsoft.ne	t\framework	6/4/2009 9:29 AM			
FontCache3.0.0.0	Windows Presentation Foundation Fo	(Verified) Microsoft Corporation	c:\windows\microsoft.net	t framework	9/29/2010 1:06 PM			
idsvc	Windows CardSpace: Securely enabl	(Verified) Microsoft Corporation	c:\windows\microsoft.ne	t framework	9/29/2010 12:55 PM	1		
Mozilla Maintenance	Mozilla Maintenance Service: The M	(Verified) Mozilla Corporation	c:\program files (x86)\mo	zilla mainten	1/18/2020 2:01 AM			
VGAuthService	VMware Alias Manager and Ticket S	(Verified) VMware, Inc.	c:\program files\vmware'	vmware tool	8/31/2019 12:49 PM	1		
VMTools	VMware Tools: Provides support for s	(Verified) VMware, Inc.	c:\program files\vmware	vmware tool	9/1/2019 2:08 PM			
mscories.dll	Size: 78 K							
Microsoft .NET IE SECURI	TY REGIST Time: 9/29/2010 9:23 A	м						
Microsoft Corporation	Version: 2.0 50727 5420							
Microsoft Corporation	version: 2.0.30727.3420							

You can export them in your USB by clicking on file and saving them either by Ctrl+S.

13. Now Open the Process Explorer

ile Options View Process Fin	nd Use	rs Help					
🛃 🛛 🖉 🗮 🖻 🚍 🚳 🛛 😭	* 4	۰			mill		
rocess	CPU	Private Bytes	Working Set	PID Desc	cription	Company Name	
Registry		6,724 K	28,580 K	120			
System Idle Process	92.60	60 K	8 K	0			
3 III System	0.75	220 K	14,552 K	4			
Interrupts	0.35	0 K	0 K	n/a Hardv	ware Interrupts and DPCs		
smss.exe		1,152 K	380 K	484			
Memory Compression	< 0.01	196 K	9,104 K	2292			
CSrss.exe	< 0.01	1,780 K	2,208 K	708			
🛛 💽 wininit.exe		1,396 K	1,036 K	796			
services.exe	0.02	5,084 K	7.272 K	868			
svchost.exe		924 K	1,140 K	640 Host	Process for Windows S	Microsoft Corporation	
svchost.exe		11,084 K	16,612 K	656 Host	Process for Windows S	Microsoft Corporation	
rundli32.exe		2,204 K	4,704 K	5772 Winde	ows host process (Run	Microsoft Corporation	
StartMenuExperience		37,364 K	37,228 K	6020			
EF Runtime Broker.exe		6,008 K	7,088 K	6260 Runtin	me Broker	Microsoft Corporation	
dllhost.exe		2,220 K	9,600 K	6276 COM	Surrogate	Microsoft Corporation	
SearchUI.exe	Susp	158,184 K	189,128 K	6448 Searc	ch and Cortana applicati	Microsoft Corporation	
SecurityHealthHost.exe		2,524 K	3,156 K	6652 Wind	ows Security Health Host	Microsoft Corporation	
Runtime Broker.exe		18,980 K	34,120 K	6836 Runtin	me Broker	Microsoft Corporation	
SkypeBackgroundHo	Susp	2,040 K	1,300 K	7136 Micro	soft Skype	Microsoft Corporation	
Runtime Broker.exe		6,140 K	15,956 K	7100 Runti	me Broker	Microsoft Corporation	
ShellExperienceHost	Susp	27,420 K	46,404 K	7776 Wind	ows Shell Experience H	Microsoft Corporation	
Runtime Broker.exe		4.648 K	13.124 K	8060 Runti	me Broker	Microsoft Corporation	
Application Frame Host		27.412 K	12,280 K	8624 Applic	cation Frame Host	Microsoft Corporation	
WinStore Ann exe	Susp	40.308 K	640 K	8648 Store		Microsoft Comporation	
Runtime Broker, exe		3.064 K	3.428 K	8872 Runti	me Broker	Microsoft Corporation	
SystemSettings exe	Susp	31.644 K	668 K	9076 Settin	nas	Microsoft Comporation	
MicrosoftEdge exe	Susp	30 528 K	680 K	2708 Micro	soft Edge	Microsoft Comoration	
= browser broker exe		1.732 K	2 316 K	5108 Brows	ser Broker	Microsoft Comoration	
BuntimeBroker exe	< 0.01	1.624 K	2 200 K	7244 Runtin	me Broker	Microsoft Comoration	
MicrosoftEdgeSH	Susp	3.876 K	1.108 K	7872 Micro	soft Edge Web Platform	Microsoft Corporation	
MicrosoftEdgeCP exe	Susp	5 936 K	4 188 K	7192 Micro	soft Edge Content Proc	Microsoft Comporation	
YourPhone exe	Susp	21.488 K	7,500 K	3756	-	2	
Runtime Broker, exe		1.532 K	2.284 K	7968 Runti	me Broker	Microsoft Corporation	
GameBar.exe	< 0.01	27,468 K	19.092 K	6060			
Runtime Broker.exe	< 0.01	3.428 K	3,780 K	10020 Runti	me Broker	Microsoft Corporation	
GameBarFT.exe		2.920 K	3.656 K	2516			
WindowsInternal.Com		19.244 K	13.292 K	5632 Winde	owsInternal.Composabl	Microsoft Corporation	
SkypeApp.exe	Susp	22,596 K	1,376 K	6684 Skype	еАрр	Microsoft Corporation	
Runtime Broker.exe		2,696 K	3,404 K	5328 Runti	me Broker	Microsoft Corporation	
dllhost.exe		3,812 K	6,496 K	2760 COM	Surrogate	Microsoft Corporation	
Microsoft.Photos.exe	Susp	39,056 K	16,468 K	2572			
RuntimeBroker.exe		2,992 K	3,836 K	10100 Runtin	me Broker	Microsoft Corporation	
smartscreen.exe		7,888 K	22,120 K	7352 Winde	ows Defender SmartScr	Microsoft Corporation	
svchost.exe	0.15	8,672 K	12,012 K	1052 Host	Process for Windows S	Microsoft Corporation	
svchost.exe	0.03	2,692 K	4,028 K	1100 Host	Process for Windows S	Microsoft Corporation	
svchost.exe		5,780 K	8,792 K	1304 Host	Process for Windows S	Microsoft Corporation	
taskhostw.exe	0.02	7,596 K	11,976 K	5408 Host	Process for Windows T	Microsoft Corporation	
svchost.exe		2,740 K	5,392 K	1340 Host	Process for Windows S	Microsoft Corporation	
svchost.exe		2,688 K	5,268 K	1348 Host	Process for Windows S	Microsoft Corporation	
svchost.exe		1,504 K	1,644 K	1452 Host	Process for Windows S	Microsoft Corporation	
svchost.exe		1,636 K	1,780 K	1560 Host	Process for Windows S	Microsoft Corporation	
svchost.exe		12,700 K	11,996 K	1568 Host	Process for Windows S	Microsoft Corporation	
svchost.exe		1,900 K	4,432 K	1572 Host	Process for Windows S	Microsoft Corporation	
svchost.exe		1,536 K	2,224 K	1688 Host	Process for Windows S	Microsoft Corporation	
svchost.exe		4,228 K	4,944 K	1732 Host	Process for Windows S	Microsoft Corporation	
svchost.exe		1.552 K	2.164 K	1816 Host	Process for Windows S	Microsoft Corporation	
svchost.exe		2,700 K	4,284 K	1924 Host	Process for Windows S	Microsoft Corporation	
svchost.exe	0.09	2.812 K	5.228 K	1932 Host	Process for Windows S.	Microsoft Corporation	
DILLIAN 7 40% Commit Change	24.039/	Dec 165					

14. Navigate to Options and click on verify image signatures.

e Opt	ions View Process Fir	nd Use	rs Help					
2	Run At Logon		@					
e	Verify Image Signatures		Private Bytes	Working Set	PID	Description		Company Name
	VirusTotal.com	•	6,524 K	28,804 K	120			
i —			60 K	8 K	0	1		
	Always On Top		220 K	14,552 K	4			
	Replace Task Manager		0 K	0 K	n/a	Hardware Intern	pts and DPCs	
- T	Hide When Minimized		1,152 K	380 K	484			
	Allow Only One Instance		196 K	9,064 K	2292			
	Allow Only One instance		1,780 K	2,212 K	708			
-	Confirm Kill		1,396 K	1,036 K	796			
	Travicons		5,084 K	7,272 K	868			
	indy icons		924 K	1,140 K	640	Host Process fo	Windows S	Microsoft Corporation
	Configure Symbols		11,296 K	16,720 K	656	Host Process fo	Windows S	Microsoft Corporation
	Configure Colors		2,204 K	4,704 K	5772	Windows host p	rocess (Run	Microsoft Corporation
	Difference Uighlight Dur	tion	37,292 K	37,188 K	6020			
			5,940 K	7,076 K	6260	Runtime Broker		Microsoft Corporation
	Font		2,248 K	9,640 K	6276	COM Surrogate		Microsoft Corporation
_	SearchUI.exe	Susp	158,312 K	190,260 K	6448	Search and Cort	ana applicati	Microsoft Corporation
	SecurityHealthHost.exe		2,524 K	3,156 K	6652	Windows Secur	ty Health Host	Microsoft Corporation
	RuntimeBroker.exe		19,736 K	35,928 K	6836	Runtime Broker		Microsoft Corporation
	SkypeBackgroundHo	Susp	2,040 K	1,300 K	7136	Microsoft Skype		Microsoft Corporation
	RuntimeBroker.exe		7,832 K	18,516 K	7100	Runtime Broker		Microsoft Corporation
	ShellExperienceHost	Susp	27,420 K	46,404 K	7776	Windows Shell I	Experience H	Microsoft Corporation
	RuntimeBroker.exe		4,648 K	13,124 K	8060	Runtime Broker		Microsoft Corporation
	Application Frame Host		27,412 K	12,280 K	8624	Application Fram	e Host	Microsoft Corporation
	WinStore.App.exe	Susp	40,308 K	640 K	8648	Store		Microsoft Corporation
	RuntimeBroker.exe		3,064 K	3,428 K	8872	Runtime Broker		Microsoft Corporation
	Sustam Sattinga ava	Sugar	21 644 K	CC0 K	0070	Cattingan		Microsoft Comparation

15. Also verify the signatures using the Virus Total

🂐 P	roces	s Explorer - Sysinternals: www.	sysint	ernals.com [DES	SKTOP-QMKPE	7J\PG	DCSL]			
File	Opt	ions View Process Find	User	s Help						
		Run At Logon		@						
Proce		Verify Image Signatures		Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
		VirusTotal.com	•	 Check Viru 	IsTotal.com					The system canno
		Always On Top		Submit Un	known Execut	ables				
	•	Replace Task Manager	1	0 K	0 K	n/a	Hardware Interrupts and DPCs			
		Hide When Minimized	- 1	1,152 K	380 K	484				The system canno
		Allow Only One Instance	- 1	196 K	8,156 K	2292				The system canno
		Confirm Kill	- 1	1,780 K	2,208 K	708				The system canno
	× .	Confirm Kill		1,396 K	1,036 K	796				The system canno
		Travicons		5,032 K	7,252 K	868				The system canno
		nuy icons		924 K	1,140 K	640	Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	. <u>0/70</u>
		Configure Symbols	- 1	11,188 K	16,676 K	656	Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	. <u>0/70</u>
		Configure Colors	- 1	2,204 K	4,704 K	5772	Windows host process (Run	Microsoft Corporation	(Verified) Microsoft	. 0/72
		Difference Highlight Duratio		37,268 K	37,184 K	6020			(Verified) Microsoft	. <u>0/68</u>
		Difference Highlight Duratio	m	5,940 K	7,076 K	6260	Runtime Broker	Microsoft Corporation	(Verified) Microsoft	. <u>0/71</u>
		Font		2,088 K	9,552 K	6276	COM Surrogate	Microsoft Corporation	(Verified) Microsoft	. 0/69
	_	SearchUI.exe Su	ısp	159,168 K	191,172 K	6448	Search and Cortana applicati	. Microsoft Corporation	(Verified) Microsoft	. <u>0/71</u>
		SecurityHealthHost.exe		2,524 K	3,156 K	6652	Windows Security Health Host	Microsoft Corporation	(Verified) Microsoft	. 0/72
		RuntimeBroker.exe		19,468 K	36,036 K	6836	Runtime Broker	Microsoft Corporation	(Verified) Microsoft	. <u>0/71</u>
		SkypeBackgroundHo Su	ısp	2,040 K	1,300 K	7136	Microsoft Skype	Microsoft Corporation	(No signature was	0/70
		RuntimeBroker.exe		7,724 K	18,640 K	7100	Runtime Broker	Microsoft Corporation	(Verified) Microsoft	. <u>0/71</u>

16. Save by clicking on file and then save.

File	Options View Process Fil	nd Users	Help		
	Run	Ctrl+R			
	Run as Administrator		ivate Bytes	Working Set	PID Description
	Run as Limited User		2,040 K	1,300 K	7136 Microsoft Skype
	Show Details for All Processes		7,832 K	18,796 K	7100 Runtime Broker
·	Show Details for Air Frocesses		_ 27,420 K	46,404 K	7776 Windows Shell Ex
	Save	Ctrl+S	4,720 K	13,136 K	8060 Runtime Broker
	Save As	Ctrl+A	27,412 K	12,280 K	8624 Application Frame
			- 40,308 K	640 K	8648 Store
	Shutdown	•	2,996 K	3,412 K	8872 Runtime Broker
	Exit		31,644 K	668 K	9076 Settings
_	MICrosoft Luge.cxc	Juap	30,528 K	680 K	2708 Microsoft Edge
	browser_broker.exe		1,732 K	2,316 K	5108 Browser_Broker
	RuntimeBroker.exe		1,624 K	2,200 K	7244 Runtime Broker
	MicrosoftEdgeSH	Susp	3,876 K	1,108 K	7872 Microsoft Edge W
	MicrosoftEdgeCP.exe	Susp	5,936 K	4,188 K	7192 Microsoft Edge Co
	Vau Diana au	Curr	21 400 V	7 500 1/	2750

17. Verify the path

SECURITY	1/21/2020 11:26 AM	File	256 KB
SECURITY	1/11/11/11/11/16 0.04	File	756 K P
SAM	1/21/2020 11:16 AM	File	256 KB
	1/21/2020 12:41 PM	File	256 KB
📕 Users	1/21/2020 12:46 PM	File folder	
퉬 Logs	1/21/2020 12:40 PM	File folder	