

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 questions.

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 until 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?

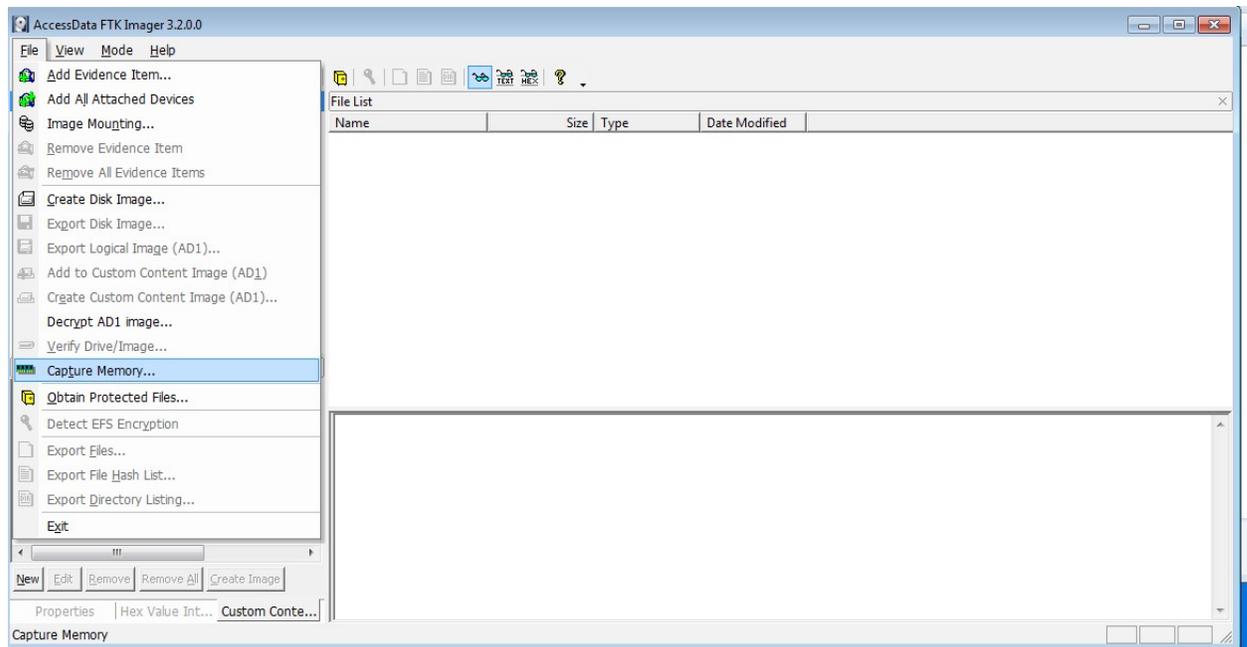
The following is the type of data they primarily look for:

1. **Log files**: A record that contains all the information about events, operations and errors occurring in a system including the communication between users at that time.
2. **Processes**: The processes running at that time
3. **Registry files**: The information database containing everything from settings, passwords and options of the windows only.
4. **Memory file** (.mem): This is basically the Dump of a RAM data which is again a volatile data. It is the data that has been processed or to be processed into kernel, which is present in RAM. It also includes following files:
 - A. **Swapfile**: 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 instance to swap of main memory and swap to, when in use.
 - B. **Hiberfil**: 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 stored in a system drive as '*pagefile.sys*'.

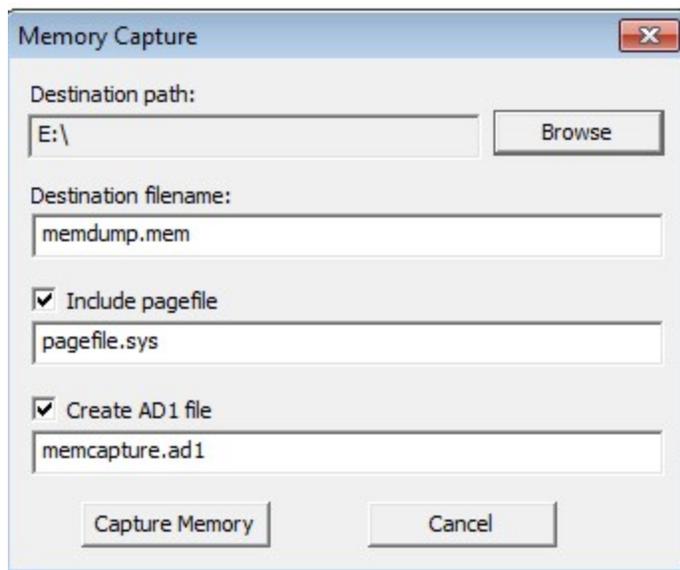
Let's start on how to retrieve the data from volatile memory, We will be using the FTK IMAGER and windows 7 Professional OS so this article will also help you as a tutorial on How to use the FTK IMAGER as a beginner?

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.

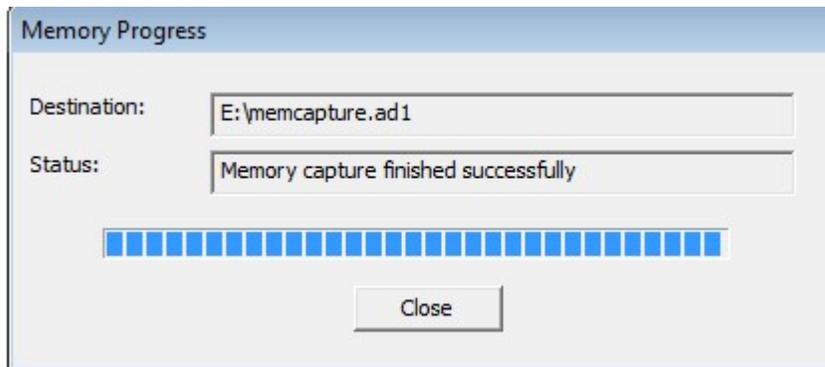
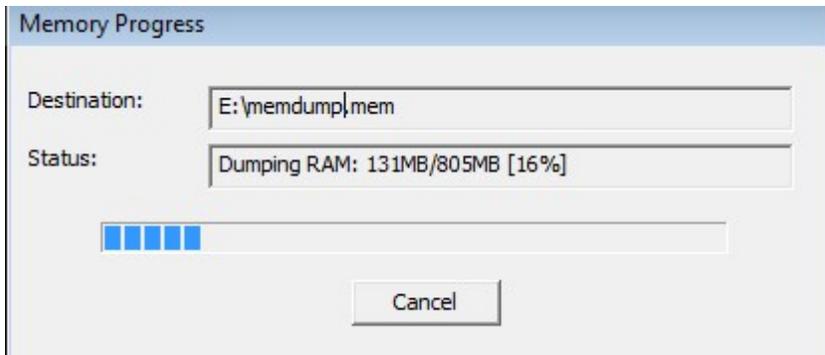
1. Start by Capturing the Volatile memory, Navigate to Files and then select Capture memory.



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

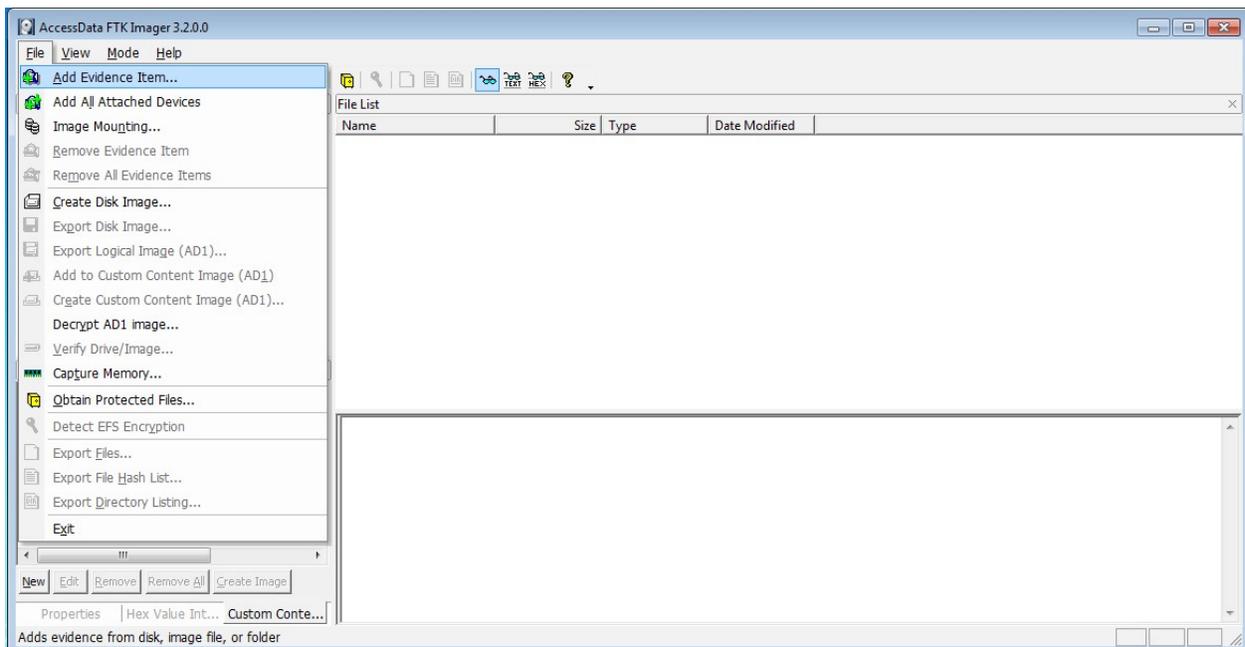


3. Now this process of dumping will take time depending upon the RAM of that computer.

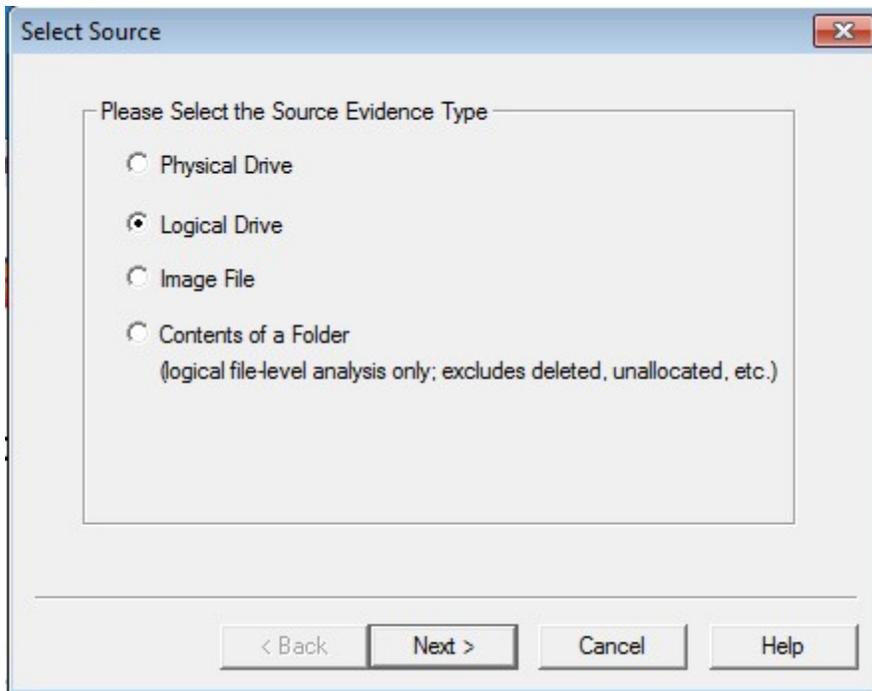


Memory is captured, the data inside the RAM is now been with us.

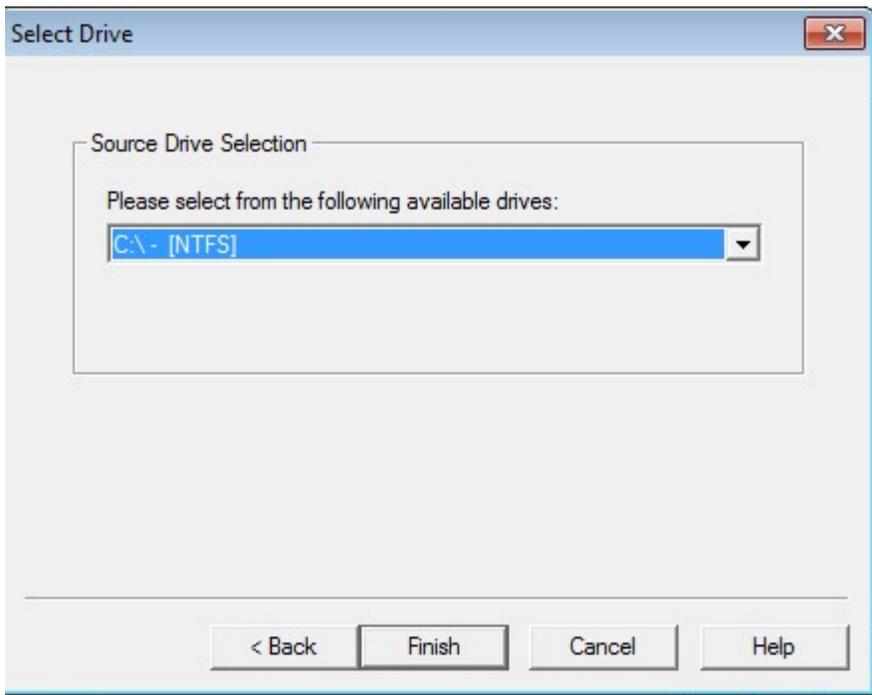
4. Now, to collect the logs, navigate to files again



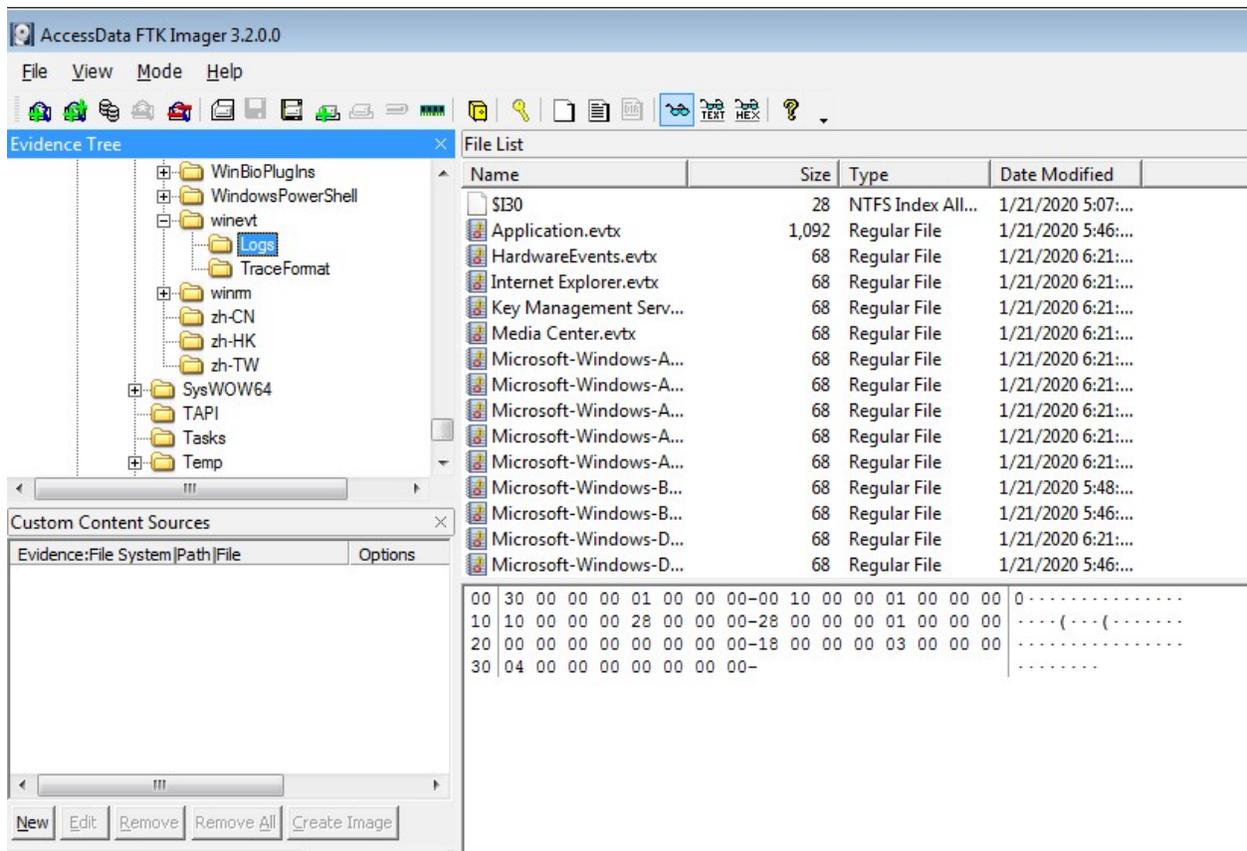
5. Since we don't know the actual physical memory location, we will go with the logical disk.



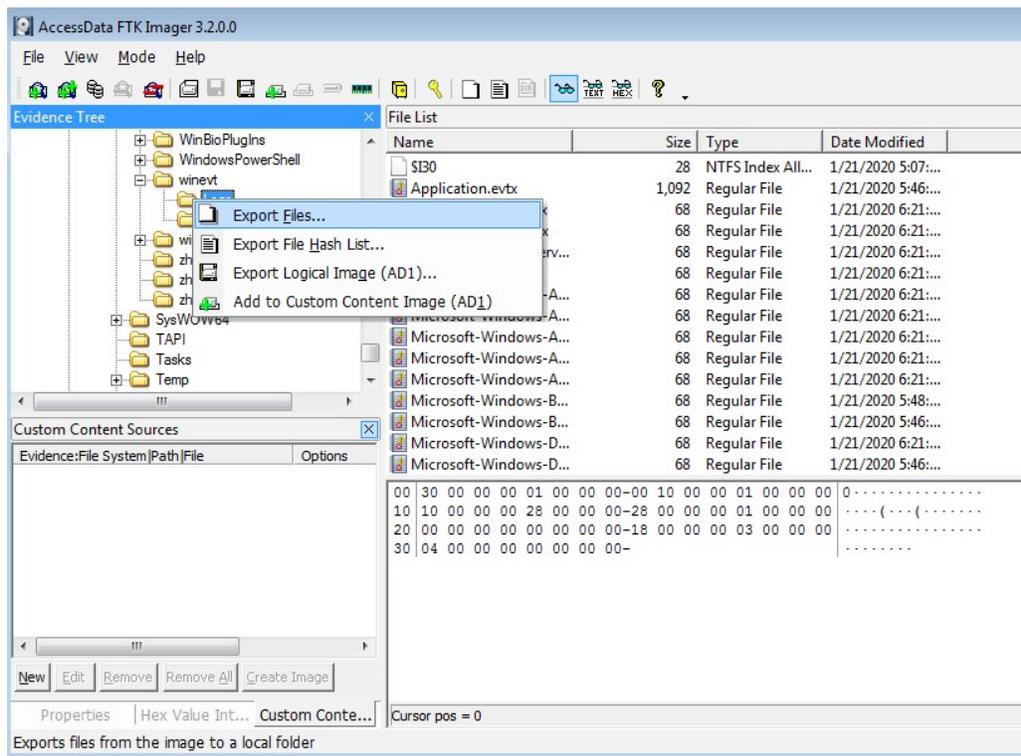
6. As OS is installed in C Drive, we will select the same.

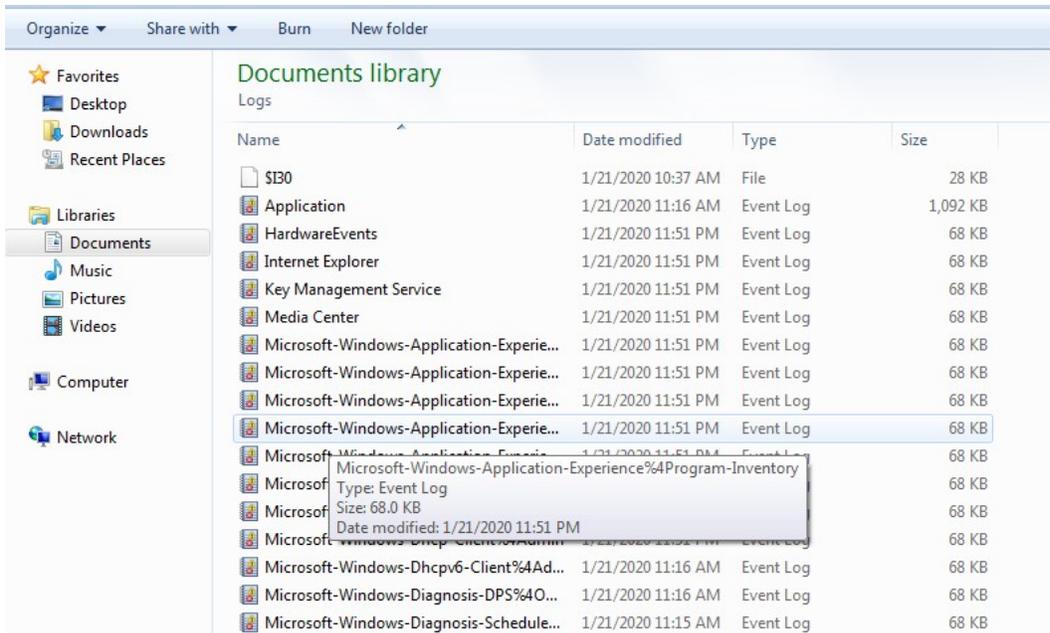


7. Finishing off we get a screen with a tree explorer on the left, browse to the path: *C\Windows\System32\Winevt\Logs* for logs.

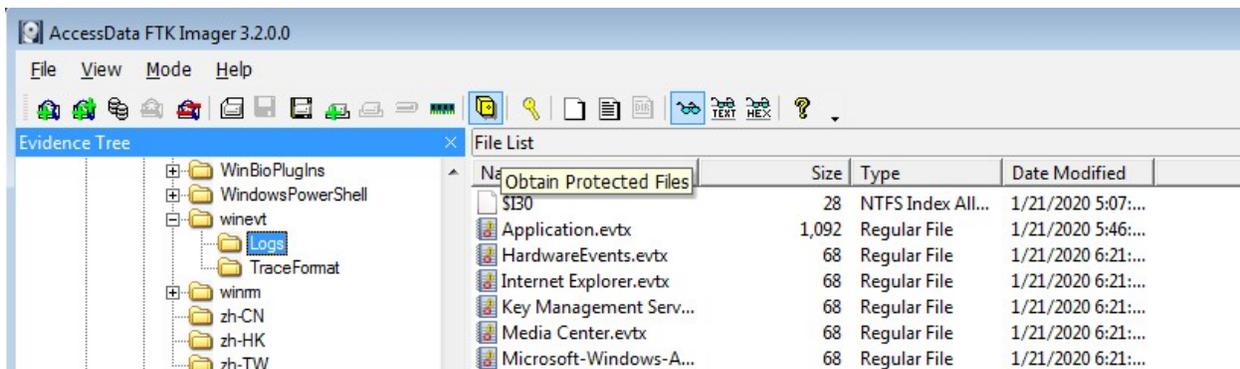


8. Export the log files to the path of your USB or the desired path.





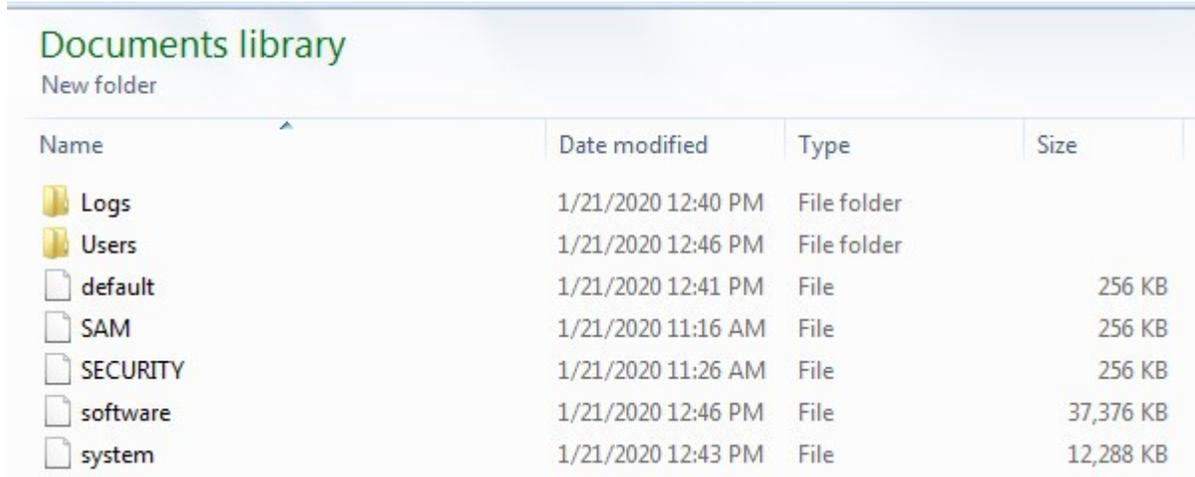
9. Coming to registry files, Locate to '*Obtain Protected Files*'.



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

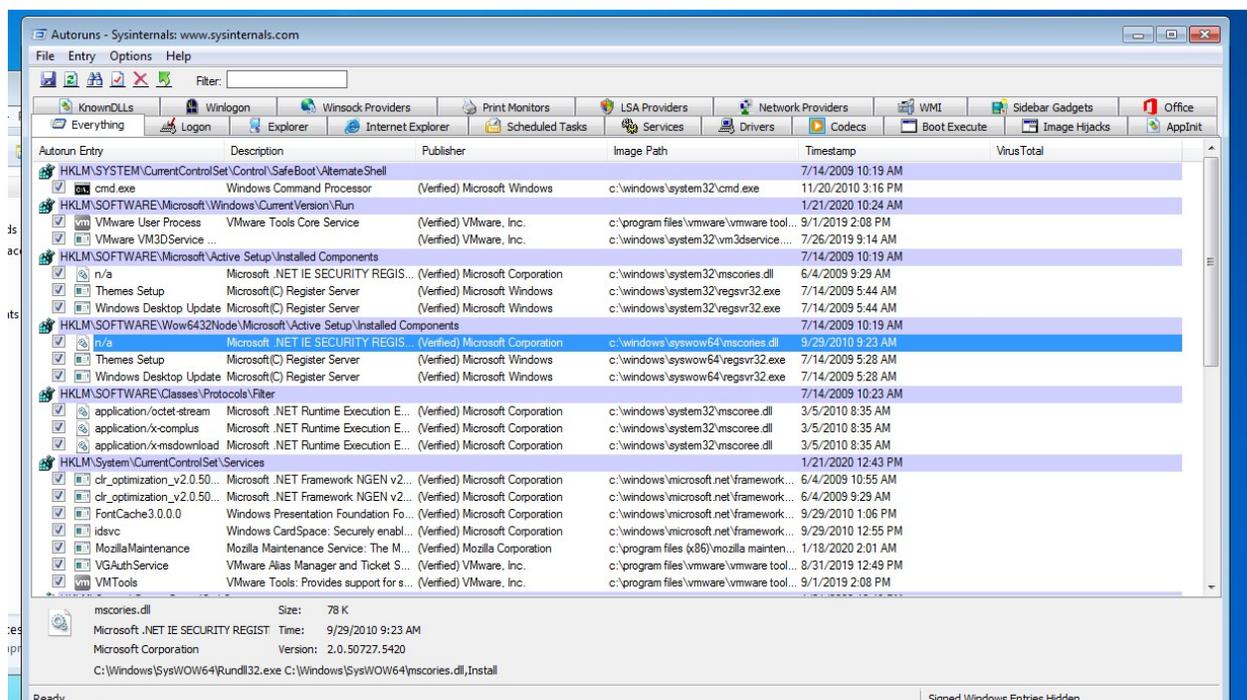


11. Verify the path for all the files including SAM file.



Name	Date modified	Type	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



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

13. Now Open the Process Explorer

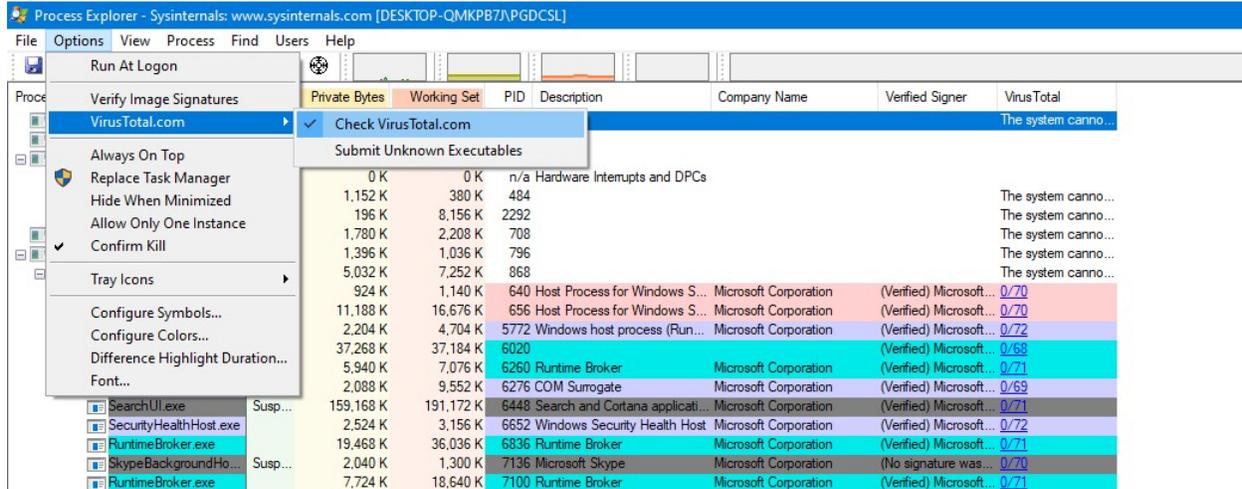
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		6,724 K	28,580 K	120		
System Idle Process	92.60	60 K	8 K	0		
System	0.75	220 K	14,552 K	4		
Interrupts	0.35	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,152 K	380 K	484		
Memory Compression	< 0.01	196 K	9,104 K	2292		
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
rundll32.exe		2,204 K	4,704 K	5772	Windows host process (Run...	Microsoft Corporation
StartMenuExperience...		37,364 K	37,228 K	6020		
RuntimeBroker.exe		6,008 K	7,088 K	6260	Runtime Broker	Microsoft Corporation
dlhost.exe		2,220 K	9,500 K	6276	COM Surrogate	Microsoft Corporation
SearchUI.exe	Susp...	158,184 K	189,128 K	6448	Search and Cortana applicati...	Microsoft Corporation
SecurityHealthHost.exe		2,524 K	3,156 K	6652	Windows Security Health Host	Microsoft Corporation
RuntimeBroker.exe		18,980 K	34,120 K	6836	Runtime Broker	Microsoft Corporation
SkypeBackgroundHo...	Susp...	2,040 K	1,300 K	7136	Microsoft Skype	Microsoft Corporation
RuntimeBroker.exe		6,140 K	15,956 K	7100	Runtime Broker	Microsoft Corporation
ShellExperienceHost...	Susp...	27,420 K	46,404 K	7776	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		4,648 K	13,124 K	8060	Runtime Broker	Microsoft Corporation
ApplicationFrameHost...		27,412 K	12,280 K	8624	Application Frame 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
SystemSettings.exe	Susp...	31,644 K	668 K	9076	Settings	Microsoft Corporation
MicrosoftEdge.exe	Susp...	30,528 K	680 K	2708	Microsoft Edge	Microsoft Corporation
browser_broker.exe		1,732 K	2,316 K	5108	Browser_Broker	Microsoft Corporation
RuntimeBroker.exe	< 0.01	1,624 K	2,200 K	7244	Runtime Broker	Microsoft Corporation
MicrosoftEdgeSH...	Susp...	3,876 K	1,108 K	7872	Microsoft Edge Web Platform	Microsoft Corporation
MicrosoftEdgeCP.exe	Susp...	5,936 K	4,188 K	7192	Microsoft Edge Content Proc...	Microsoft Corporation
YourPhone.exe	Susp...	21,488 K	7,500 K	3756		
RuntimeBroker.exe		1,532 K	2,284 K	7968	Runtime Broker	Microsoft Corporation
GameBar.exe	< 0.01	27,468 K	19,092 K	6060		
RuntimeBroker.exe	< 0.01	3,428 K	3,780 K	10020	Runtime Broker	Microsoft Corporation
GameBarFT.exe		2,920 K	3,656 K	2516		
WindowsInternal Com...		19,244 K	13,292 K	5632	WindowsInternal Composabi...	Microsoft Corporation
SkypeApp.exe	Susp...	22,596 K	1,376 K	6684	SkypeApp	Microsoft Corporation
RuntimeApp.exe		2,696 K	3,404 K	5328	Runtime Broker	Microsoft Corporation
dlhost.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	Runtime Broker	Microsoft Corporation
smartscreen.exe		7,888 K	22,120 K	7352	Windows 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	4,828 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

DllCache: 7.40% | Commit Charge: 24.92% | Processes: 165

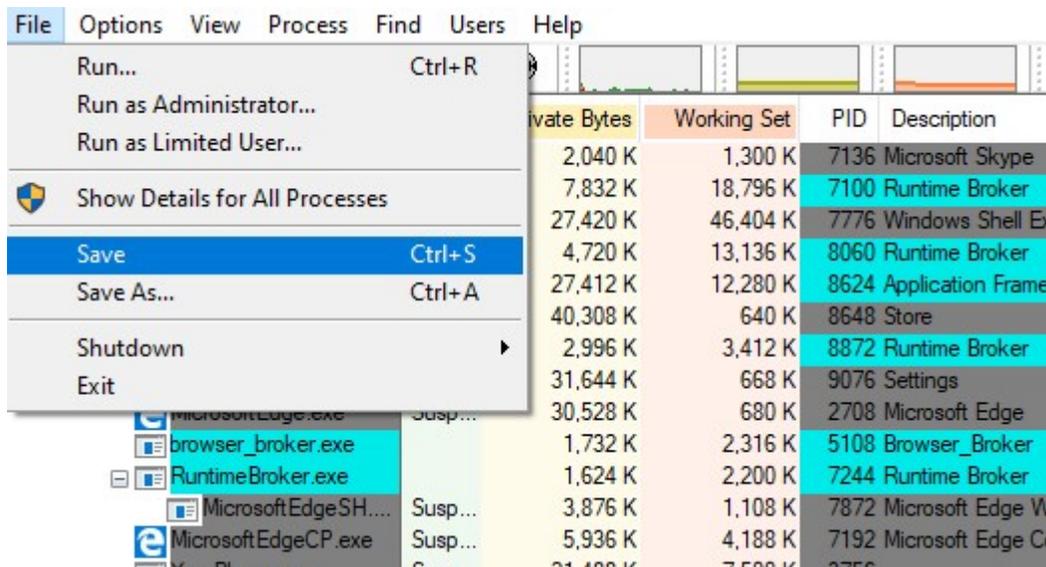
14. Navigate to Options and click on verify image signatures.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Verify Image Signatures		6,524 K	28,804 K	120		
VirusTotal.com		60 K	8 K	0		
Always On Top		220 K	14,552 K	4		
Replace Task Manager		0 K	0 K	n/a	Hardware Interrupts and DPCs	
Hide When Minimized		1,152 K	380 K	484		
Allow Only One Instance		196 K	9,064 K	2292		
Confirm Kill		1,780 K	2,212 K	708		
Tray Icons		1,396 K	1,036 K	796		
Tray Icons		5,084 K	7,272 K	868		
Configure Symbols...		924 K	1,140 K	640	Host Process for Windows S...	Microsoft Corporation
Configure Colors...		11,296 K	16,720 K	656	Host Process for Windows S...	Microsoft Corporation
Difference Highlight Duration...		2,204 K	4,704 K	5772	Windows host process (Run...	Microsoft Corporation
Font...		37,292 K	37,188 K	6020		
SearchUI.exe	Susp...	158,312 K	190,260 K	6448	Search and Cortana applicati...	Microsoft Corporation
SecurityHealthHost.exe		2,524 K	3,156 K	6652	Windows Security 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 Experience H...	Microsoft Corporation
RuntimeBroker.exe		4,648 K	13,124 K	8060	Runtime Broker	Microsoft Corporation
ApplicationFrameHost...		27,412 K	12,280 K	8624	Application Frame 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
SystemSettings.exe	Susp...	31,644 K	668 K	9076	Settings	Microsoft Corporation

15. Also verify the signatures using the Virus Total



16. Save by clicking on file and then save.



17. Verify the path

