Collecting the data from volatile memory in digital forensics

-Khushank Raj Mahawan

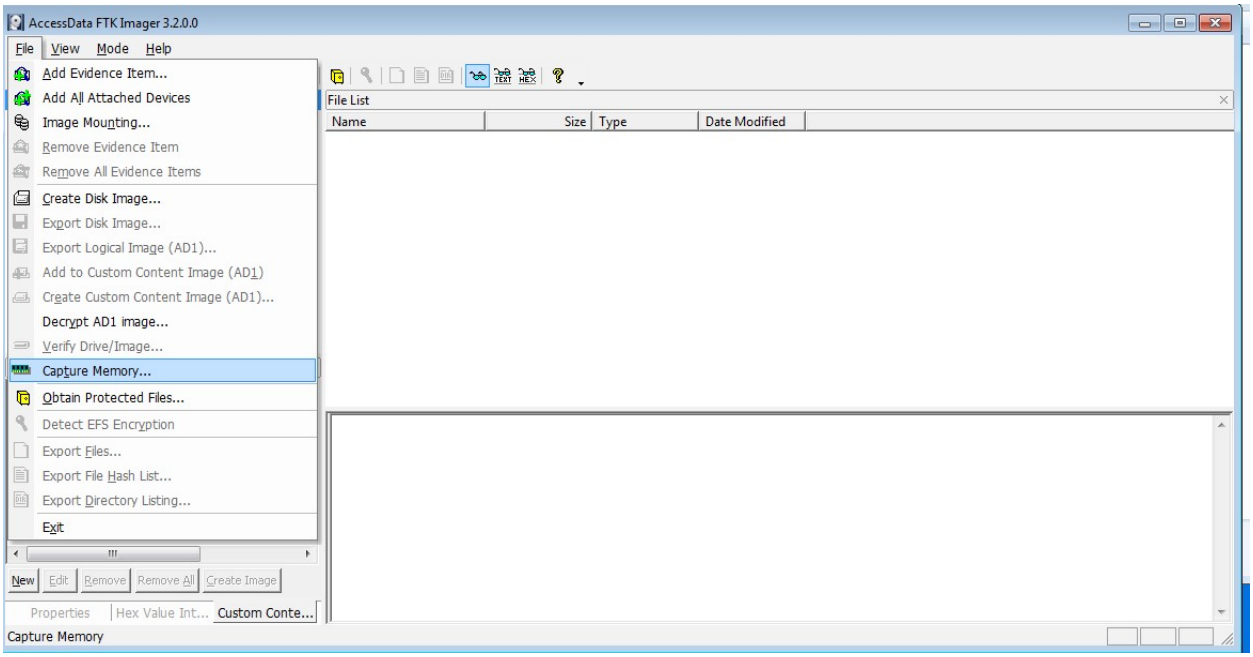
Have you ever been so curious about how the forensics experts handle the digital evidences in the world of Cybersecurity? Then this is the article for you my friend,
So what if there is a computer (Desktop/Laptop) found 'ON' at a crime scene? What would be their first step in this case? How do they do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

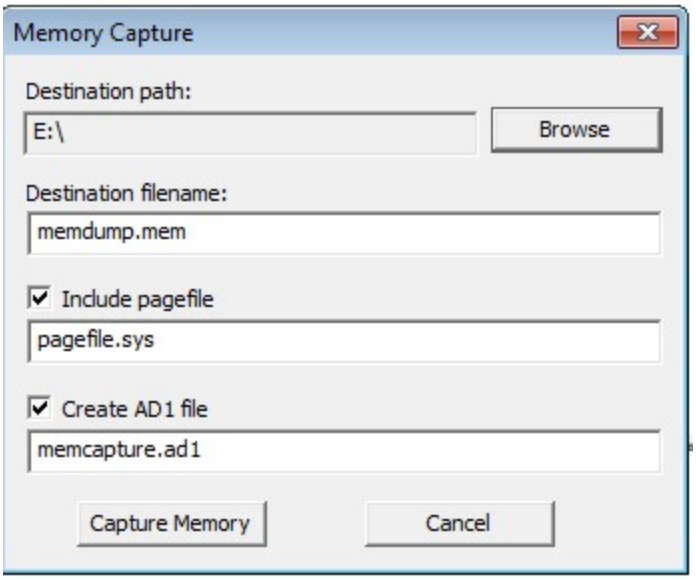
The following is the type of data they primarily look for:
1. **Log files**: A record that contain all the information about events, operations and errors occuring in a system including the communication between users at that time.
2. **Processes**: The processes running at that time
3. **Registry files**: The information database containing everything from setting, 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 is 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 iinstance 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 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.

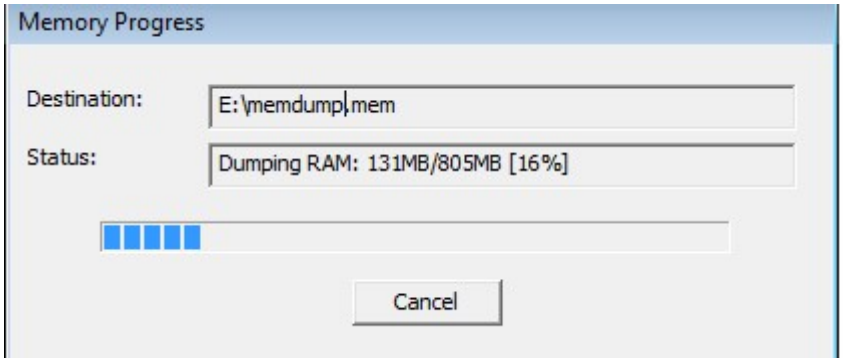
1. Start by Capturing the Volatile memory, Navigate to Files and then select Capture memory.

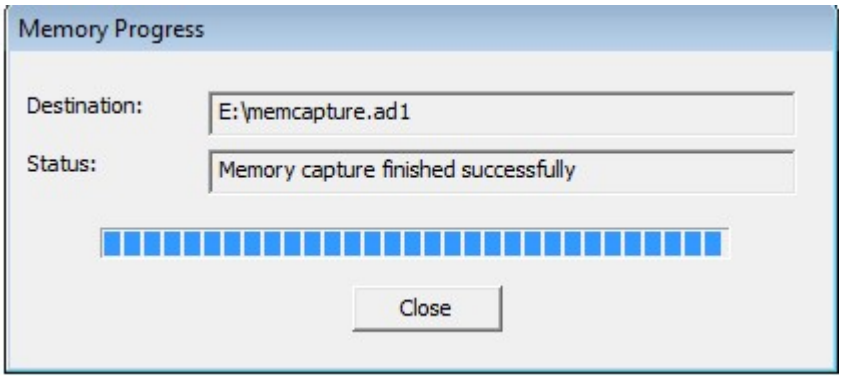


2. Select the path of the USB and Enable dumping of pagefile and AD1 file.



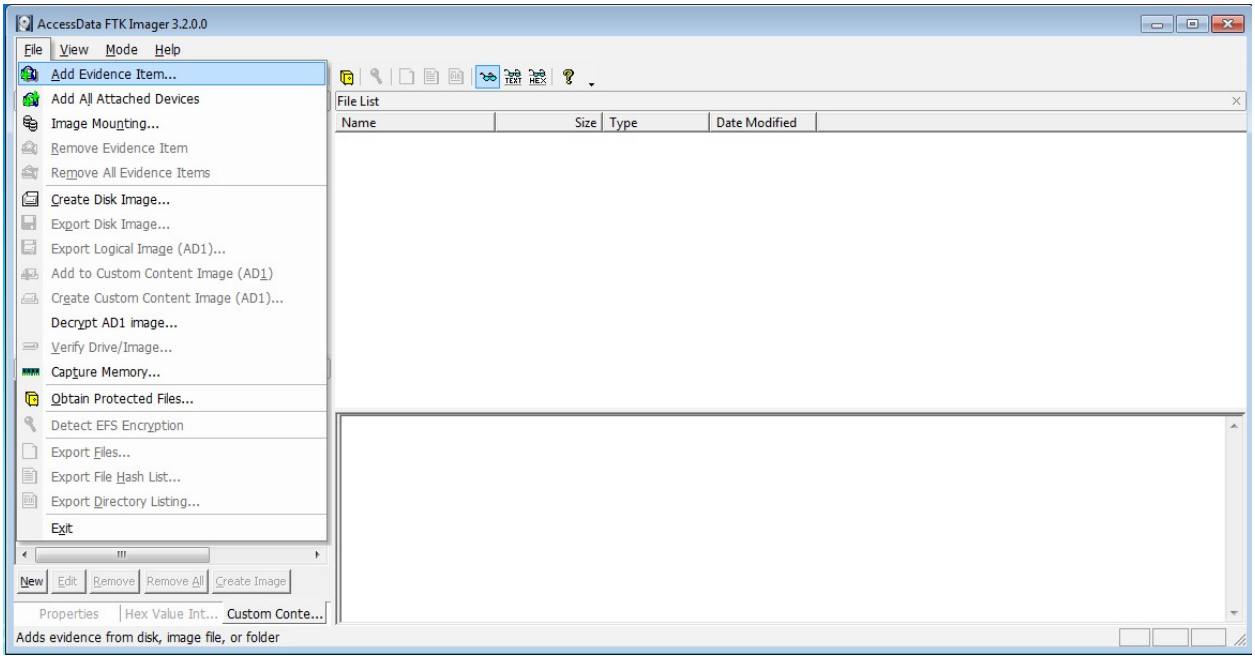
3. Now this process of dumping will take time depending upon the RAM of that computer.



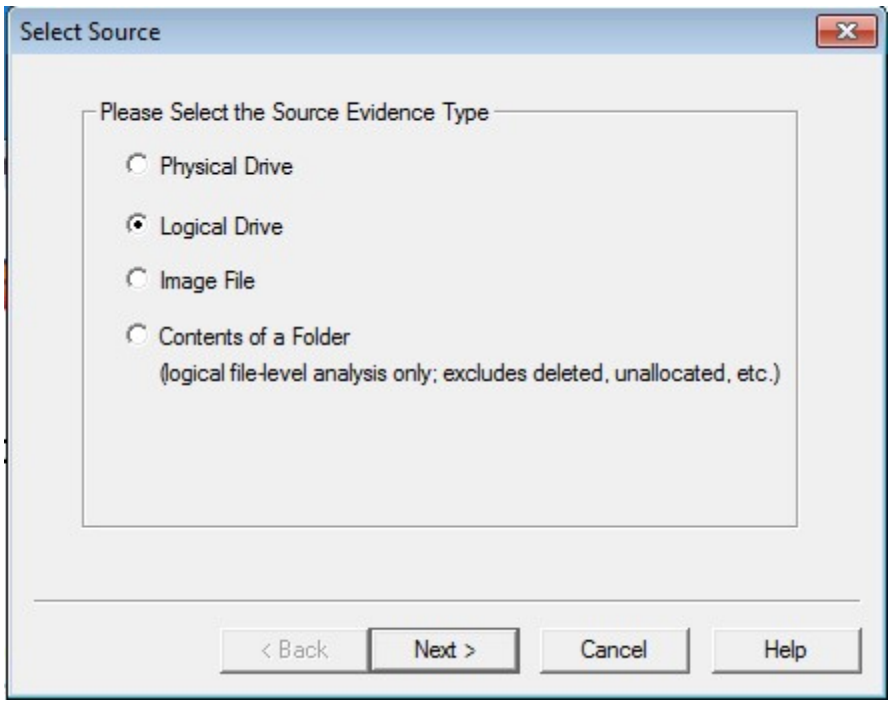


Memory is captured, the data inside the RAM is now been with us.

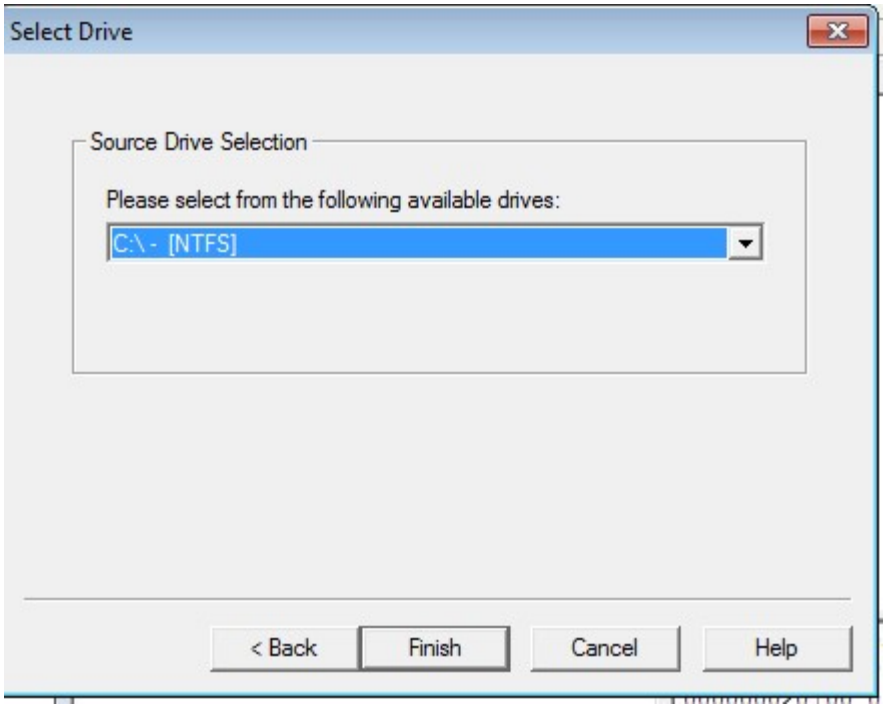
4. Now, to collect the logs, navigate to files again



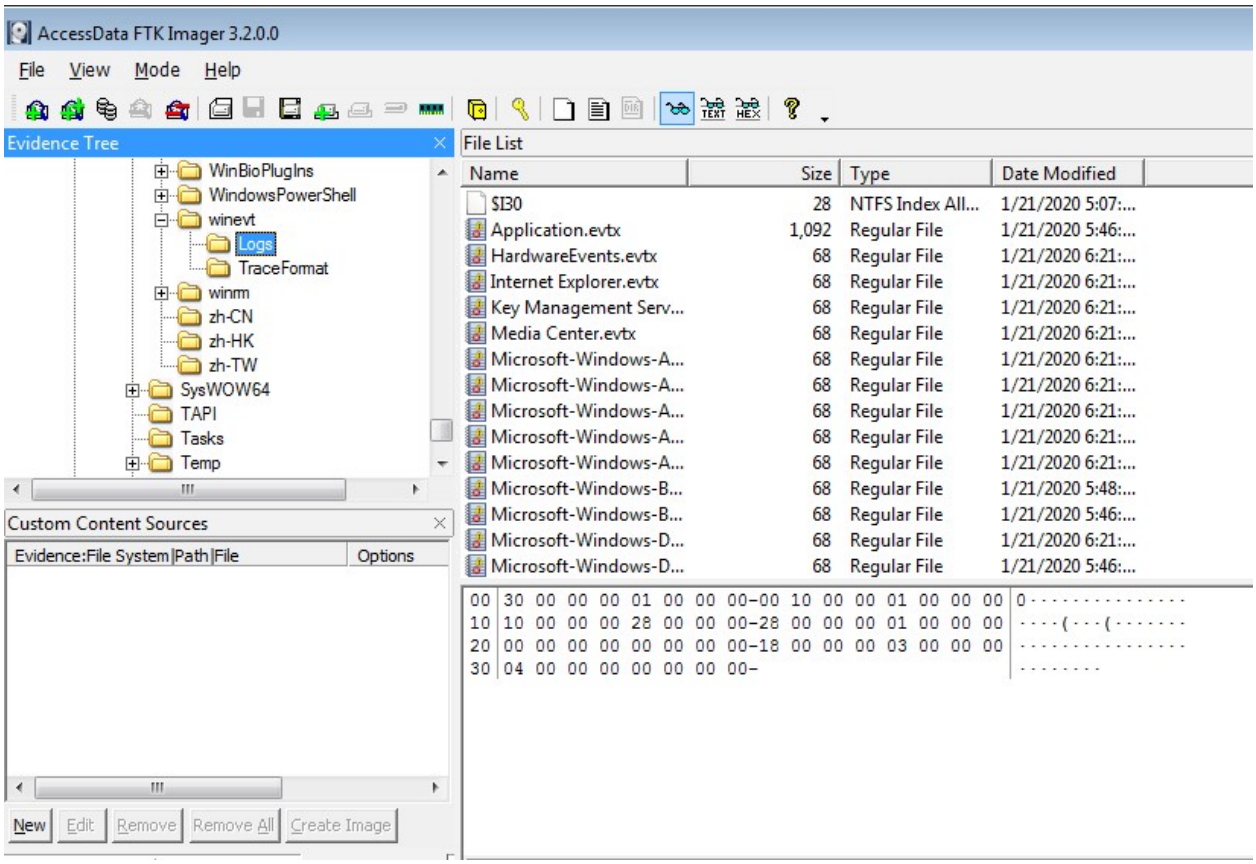
5. Since we don't know the actual physical memory location, we will go with the logical disk.



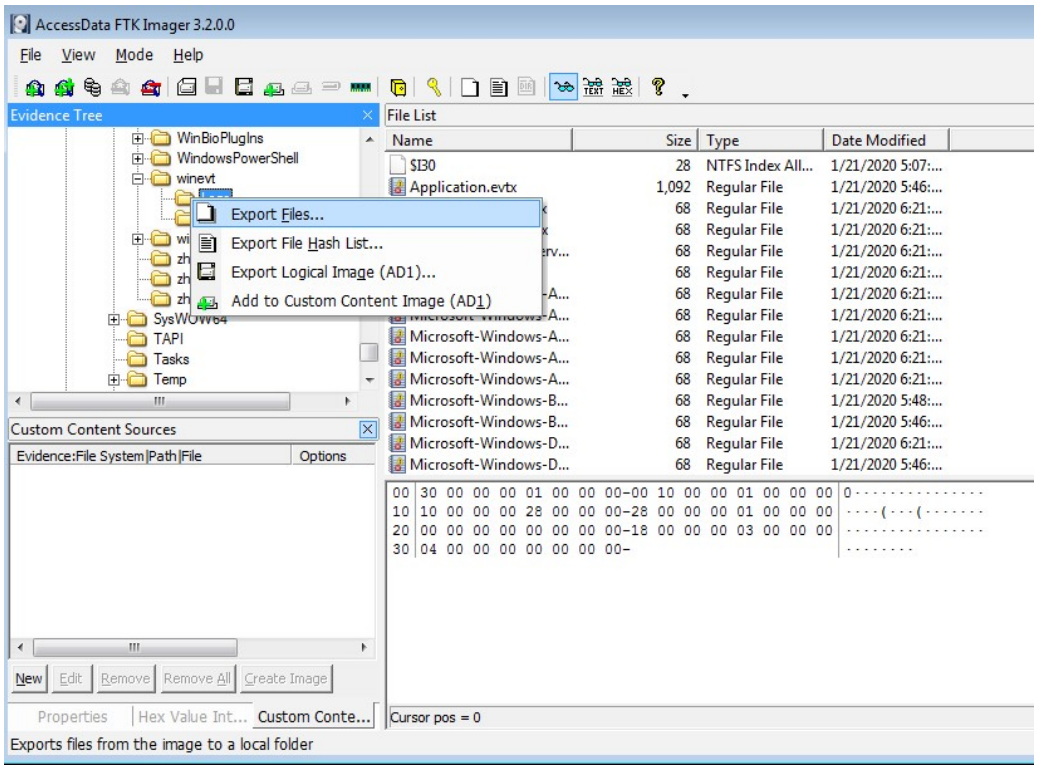
6. As OS is installed in C Drive, we will select the same.

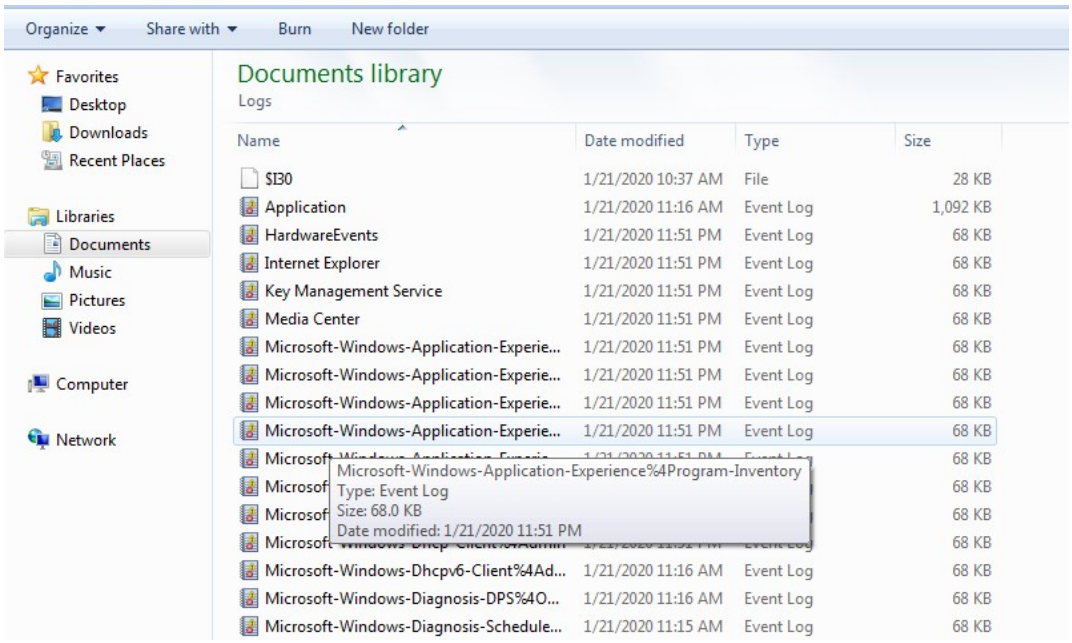


7. Finishing off we get a screen with a tree explorer on the left, browse to the path: ***C\Windows\System32\Winevt\Logs*** for logs.

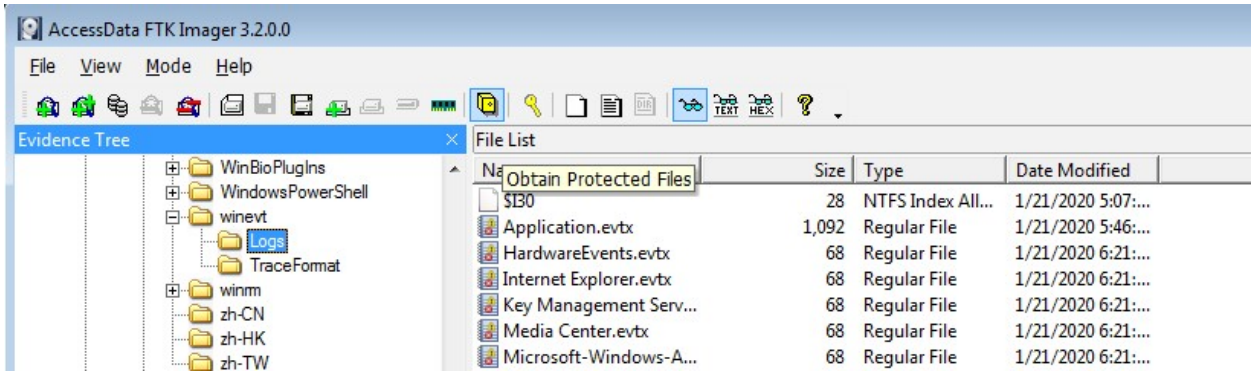


8. Export the log files to the path of your USB or the desired path.

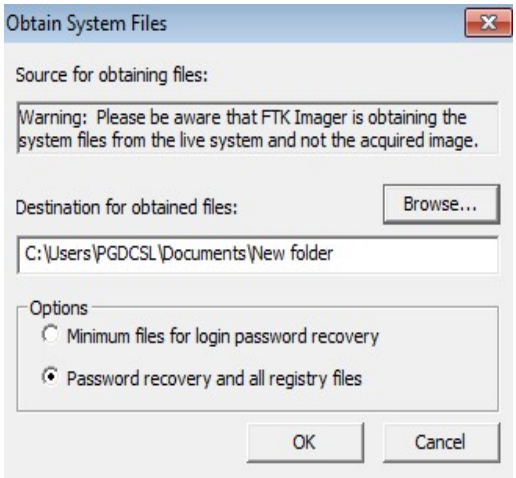




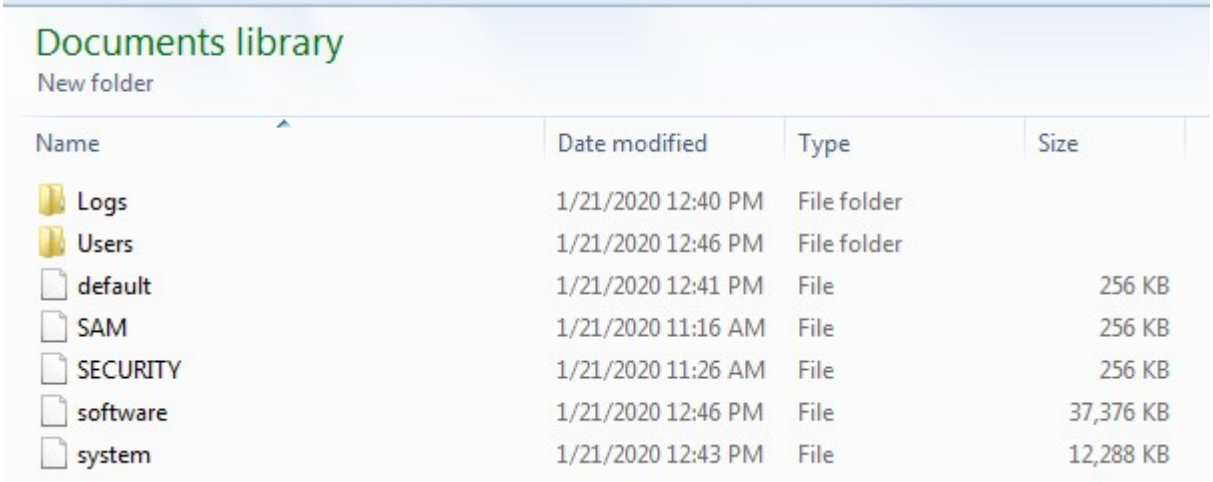
9. Coming to registry files, Locate to '***Obtain Protected Files***'.



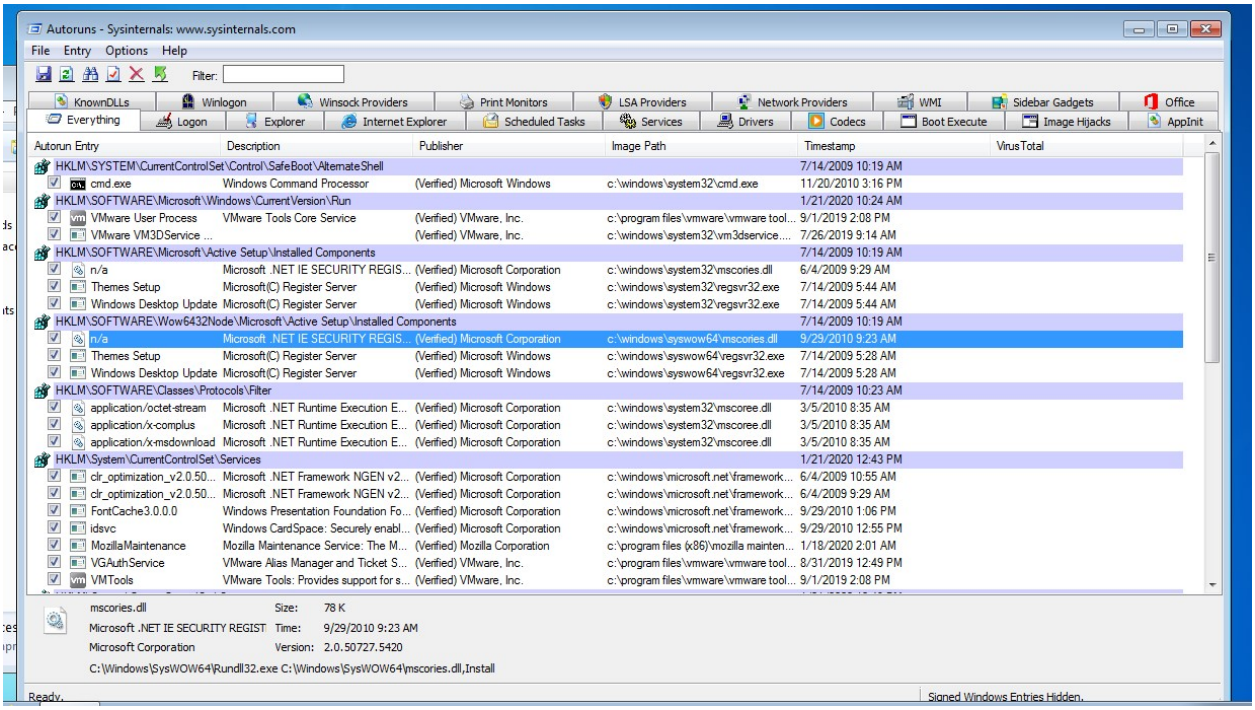
10. Select the path to collect registry files along with password recovery and all registry files ticked.



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

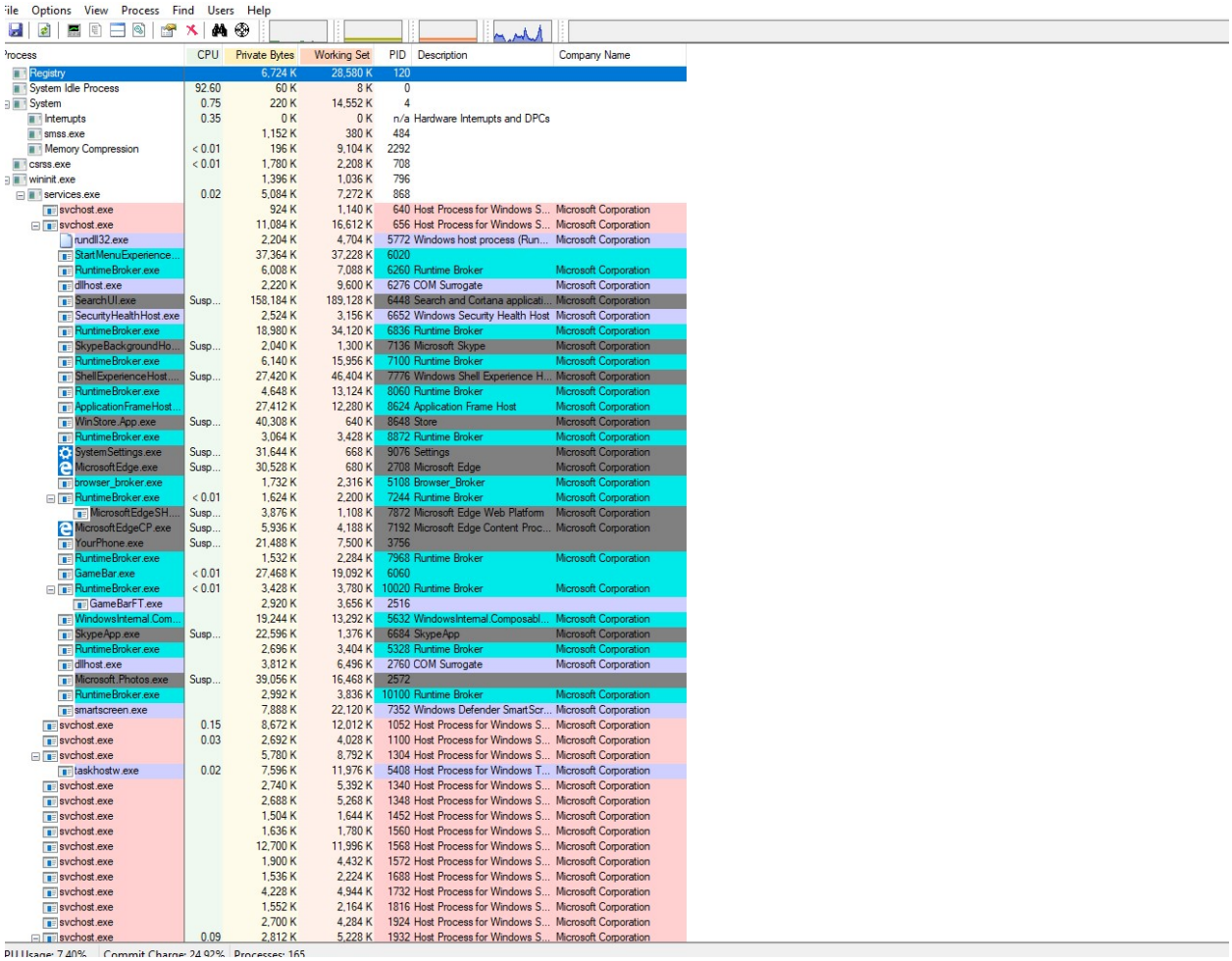


12. For the process and event details, you need to utilities, either locate them if available in your OS or just get them from google, The utilities are Autorun and Process Explorer. Open the autorun

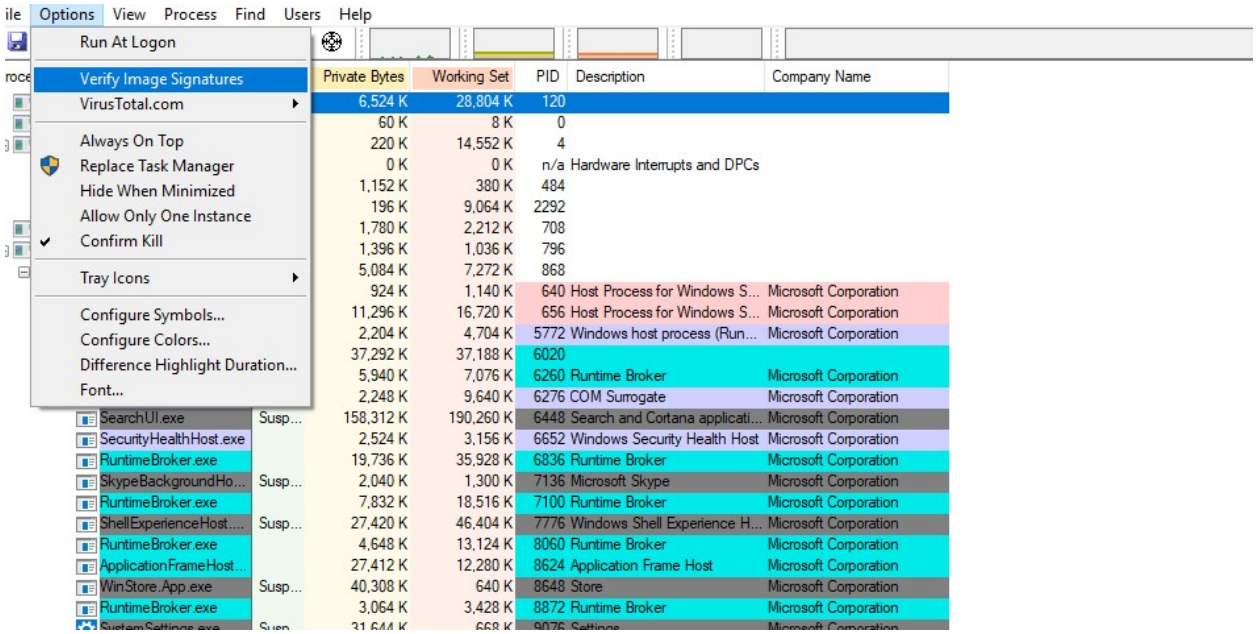


You can export them in your USB by clicking on file and saving them either by Ctrl+S.

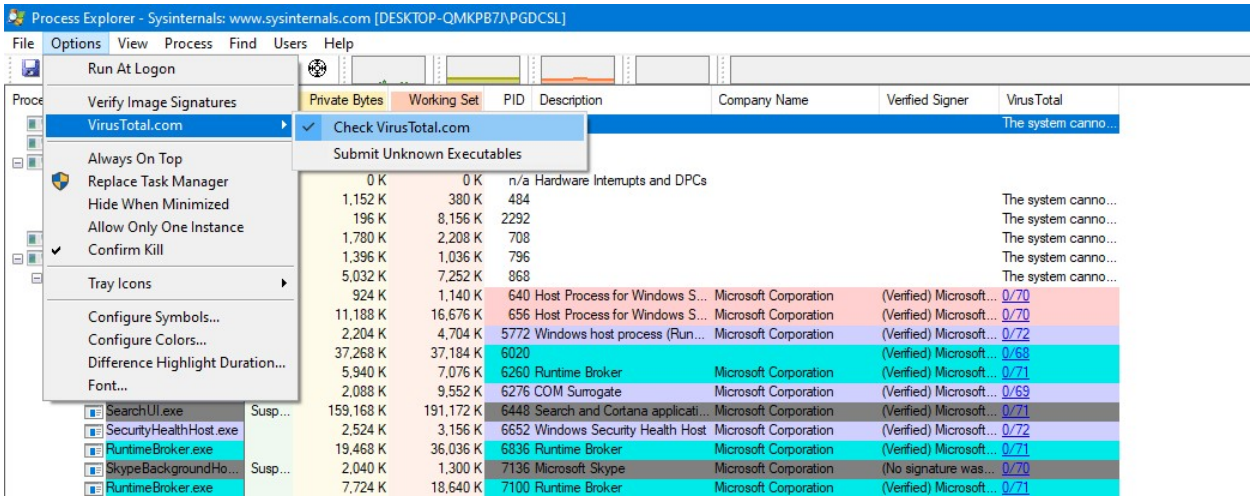
13. Now Open the Process Explorer



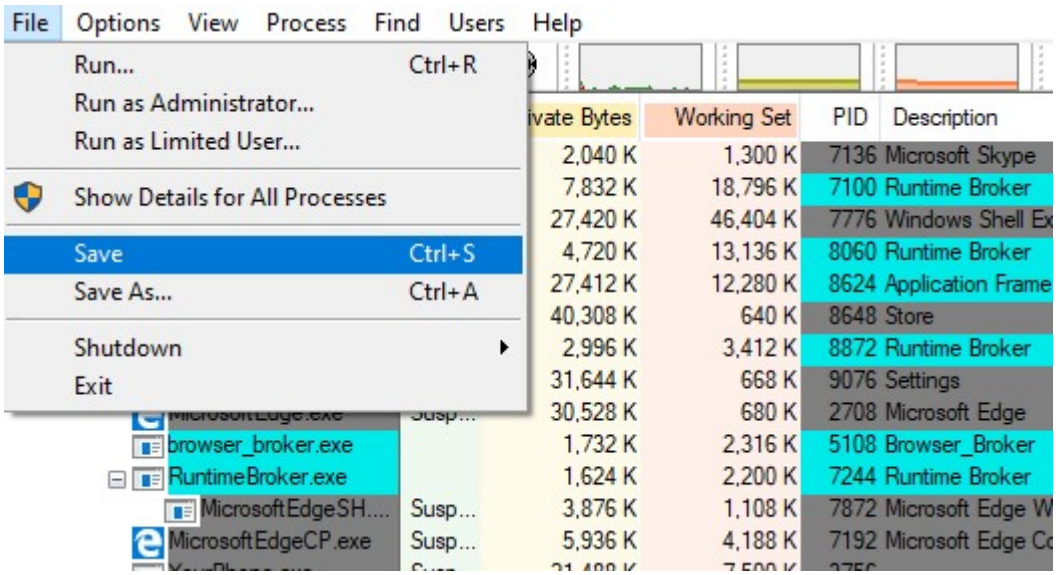
14. Navigate to Options and click on verify image signatures.



15. Also verify the signatures using the Virus Total



16. Save by clicking on file and then save.



17. Verify the path