**1. Student Name:** G Shalom Shreyan

**2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in

**3. Program/Experiment Number:** 1

**4. Title of the Program/Experiment:** Memory Forensics

**5. Date Program/Experiment Performed:** 10/08/2022

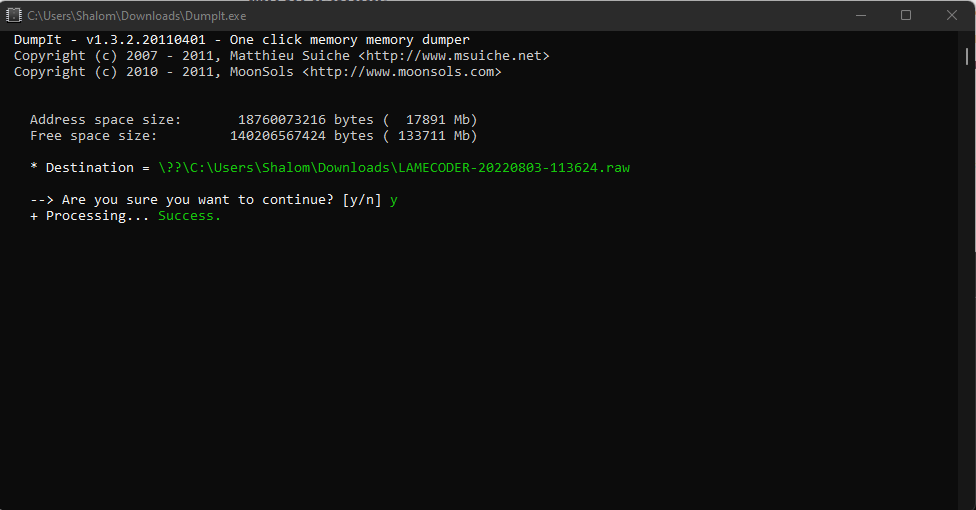
**6. Date Report Submitted:**

**7. Objective:** To analyze memory dump files using volatility tool

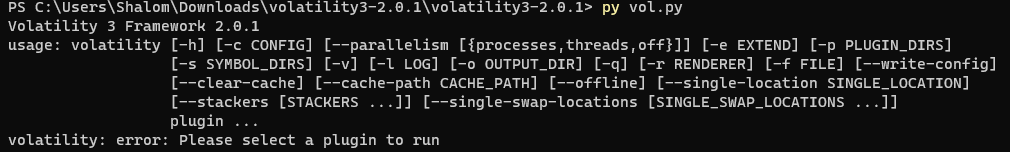
**8. Description:** We have to analyze memory dump files to do memory forensics. The system requirements were minimal, which included DumpIt, Python & Volatility, Only configuration needed is that Python needs to be installed to use Volatilty tool. No algorithms were used

**9. Implementation Details:** No programming was done.

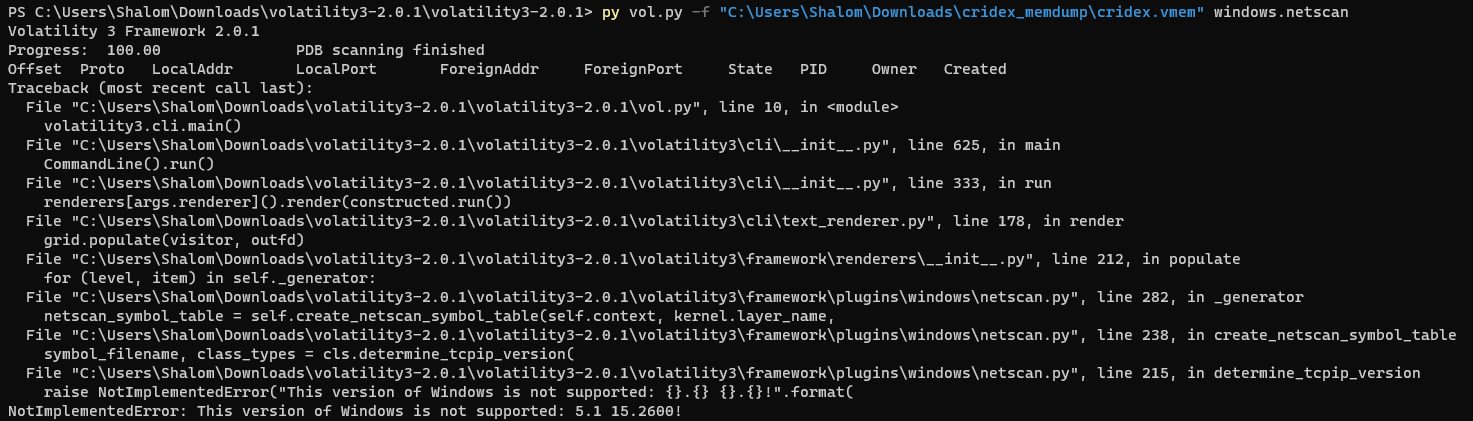
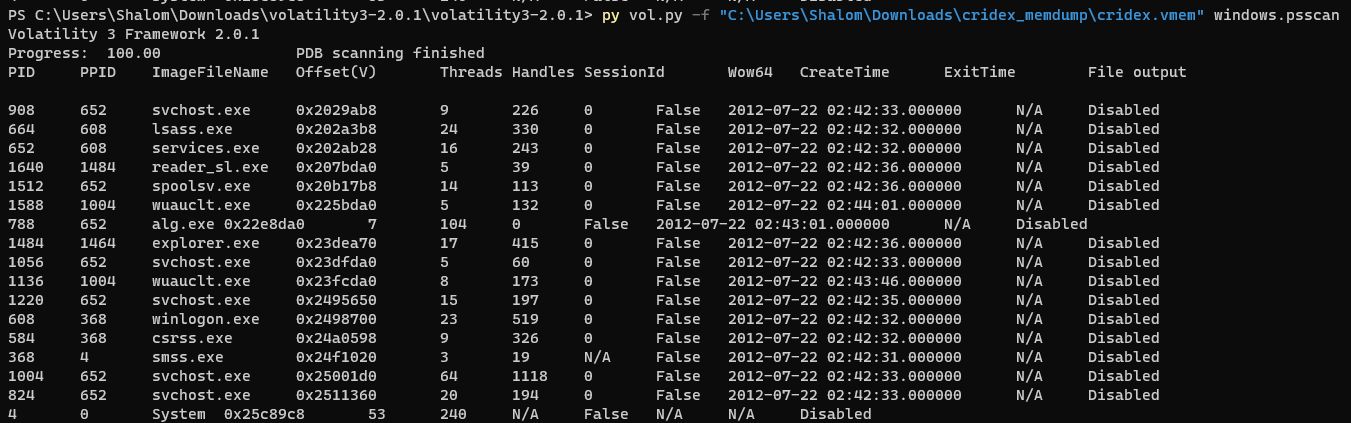
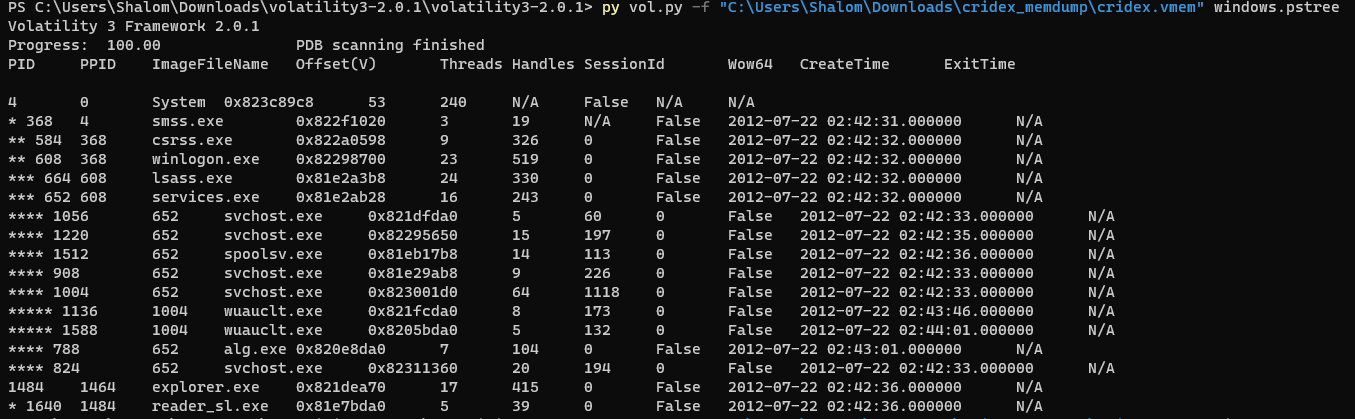
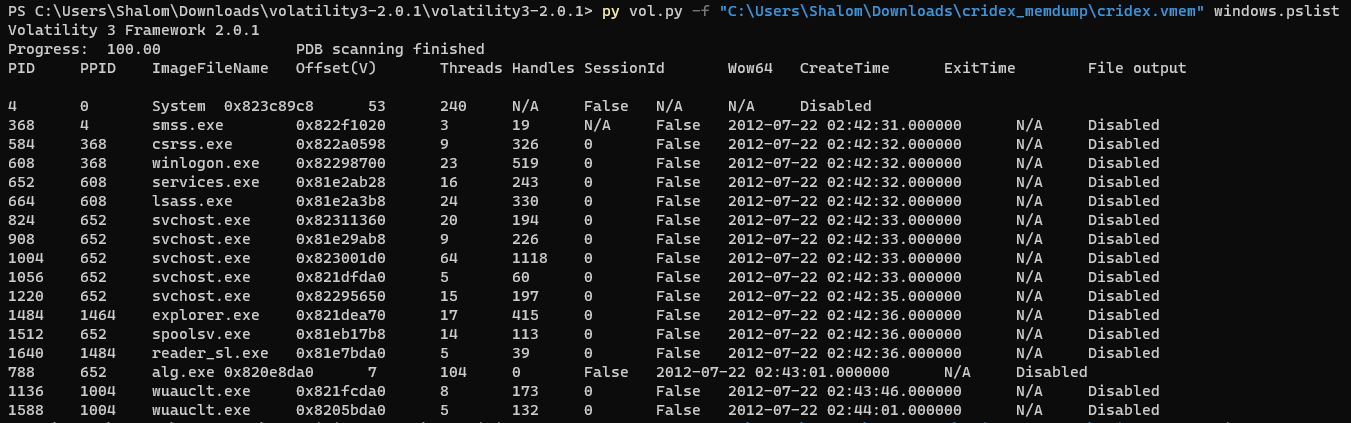
DumpIt tool (from <https://github.com/thimbleweed/All-In-USB/tree/master/utilities/DumpIt)> was downloaded to create a raw memory dump. The tool was run and a physical memory dump of the Windows machine was generated.



Volatility tool (https://github.com/volatilityfoundation/volatility3) was downaloaded . Run vol.py to check if it is working fine or not.

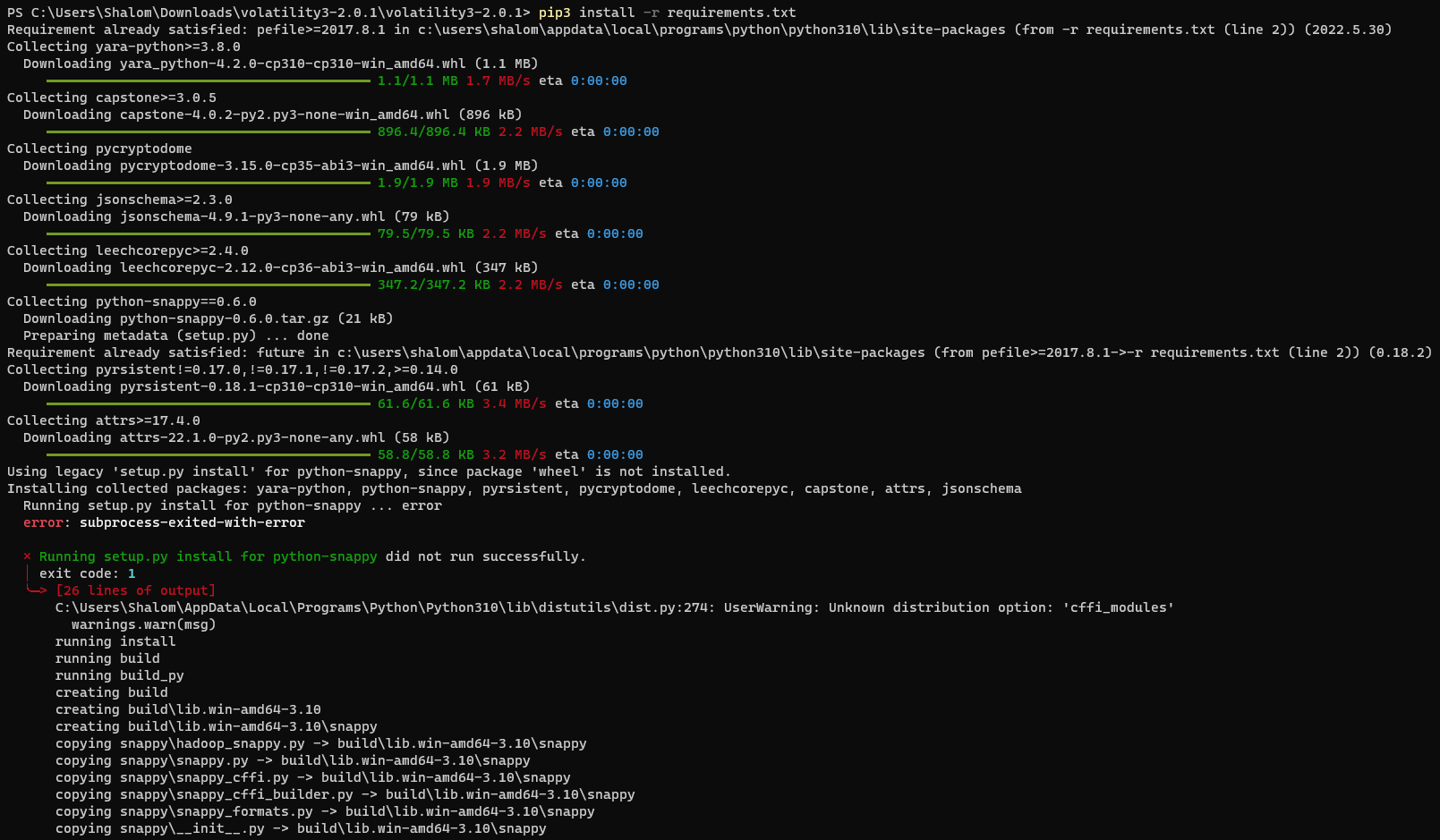


Run various commands to gain intel.

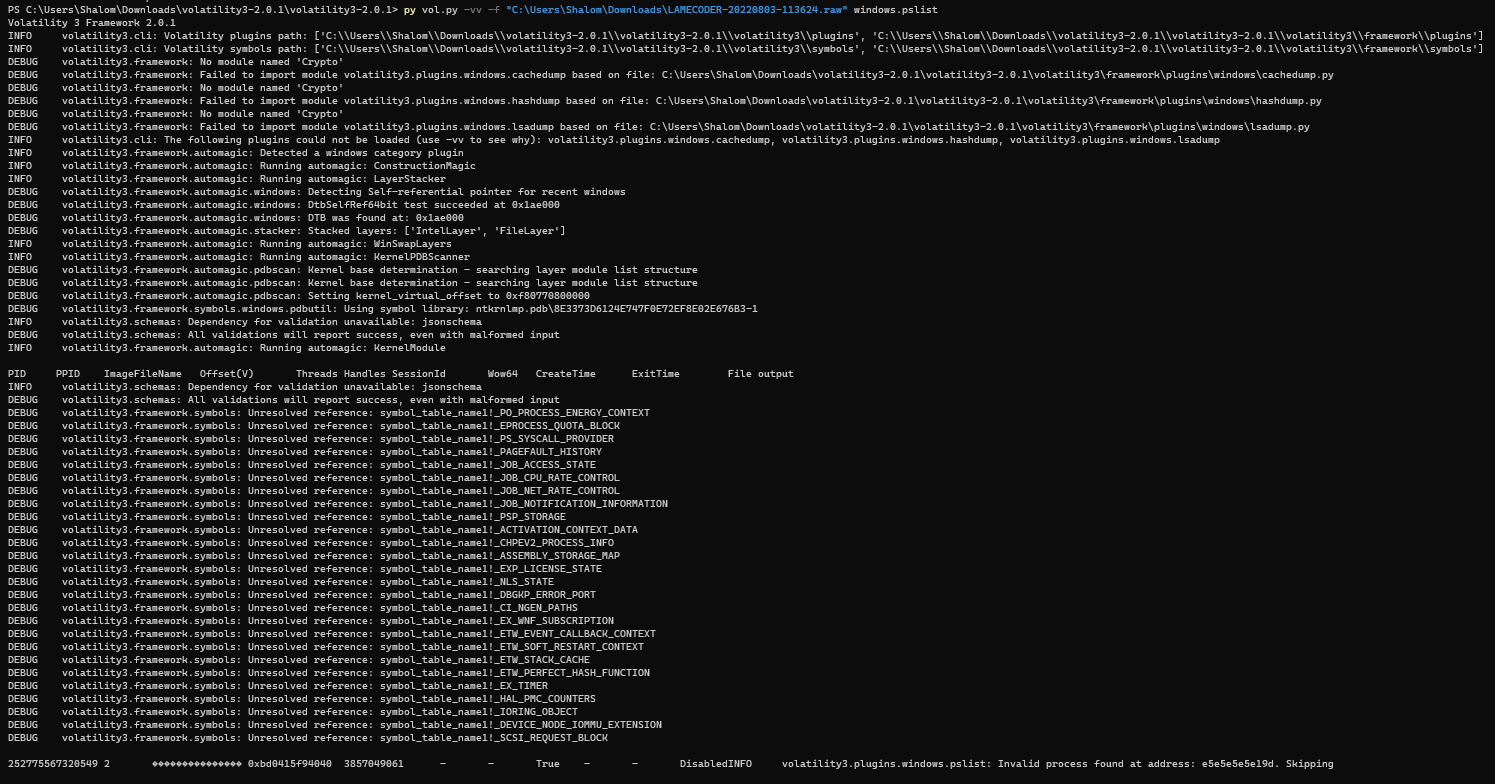


**10. Error Description:**

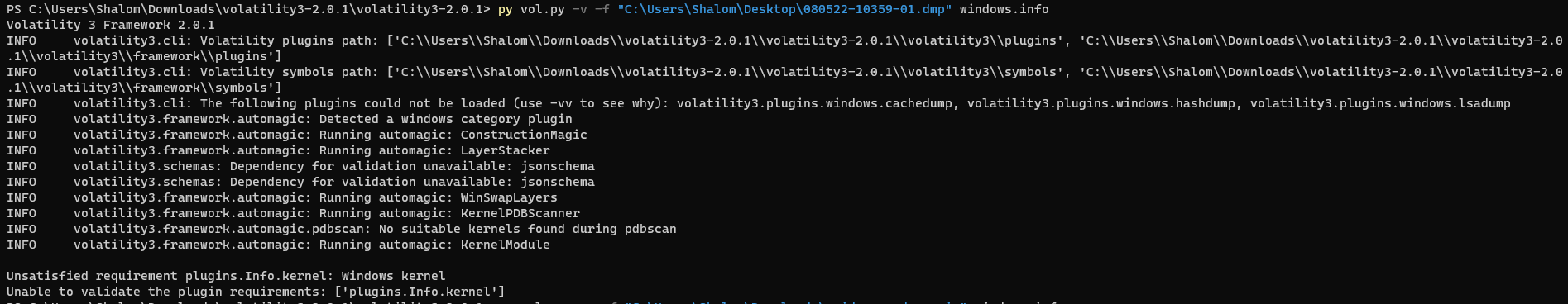
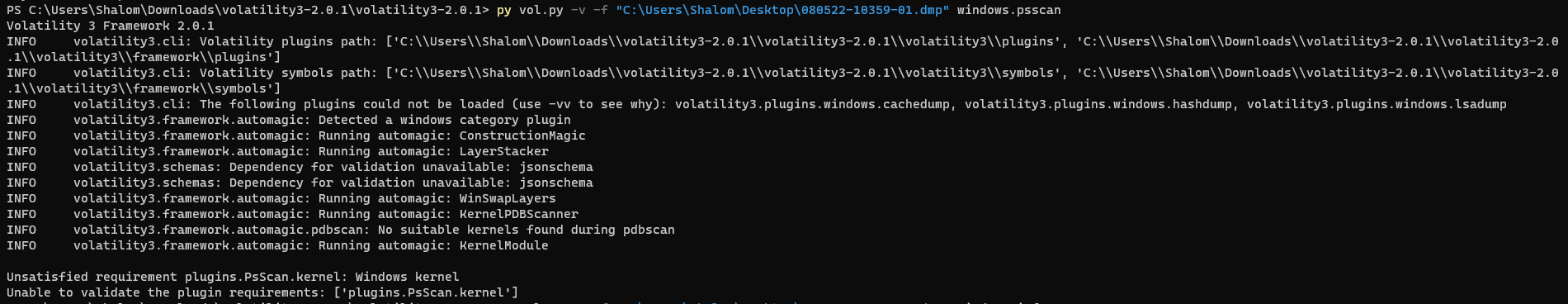
1. Getting all required libraries wasn’t possible due to errors in installing snappy library. Also found a link for possible fix (https://stackoverflow.com/questions/42979544/how-to-install-snappy-c-libraries-on-windows-10-for-use-with-python-snappy-in-an) but it resulted in another error, which wasn’t fixable.



1. Invalid process detected in the memory dump created of Windows 11, possible system issue as Windows XP dump ran fine.



1. Windows Kernel error when tried to analyze memory dumps created automatically by WindowsTried getting a profile but was not able to detect kernel



**11. Conclusion:** Memory analysis has been successfully done

**12. Reference:**

<https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples>

<https://neoslab.com/2020/04/28/how-to-extract-data-from-windows-memory-dump-using-volatility-cUNHMlhCTmxtTGdENEhRek1NWTlOdz09>

<https://blog.cyberhacktics.com/memory-forensics-on-windows-10-with-volatility/>

<https://github.com/volatilityfoundation/volatility3>

<https://infosecwriteups.com/forensics-memory-analysis-with-volatility-6f2b9e859765>

<https://www.youtube.com/watch?v=gHbejxlPbRQ>

<https://www.hackingarticles.in/multiple-ways-to-capture-memory-for-analysis/>