

**Assignment 03**

*by*

Md. Fardous Al Masum

Reg No: 11904043

Roll: 47

Section: KE058

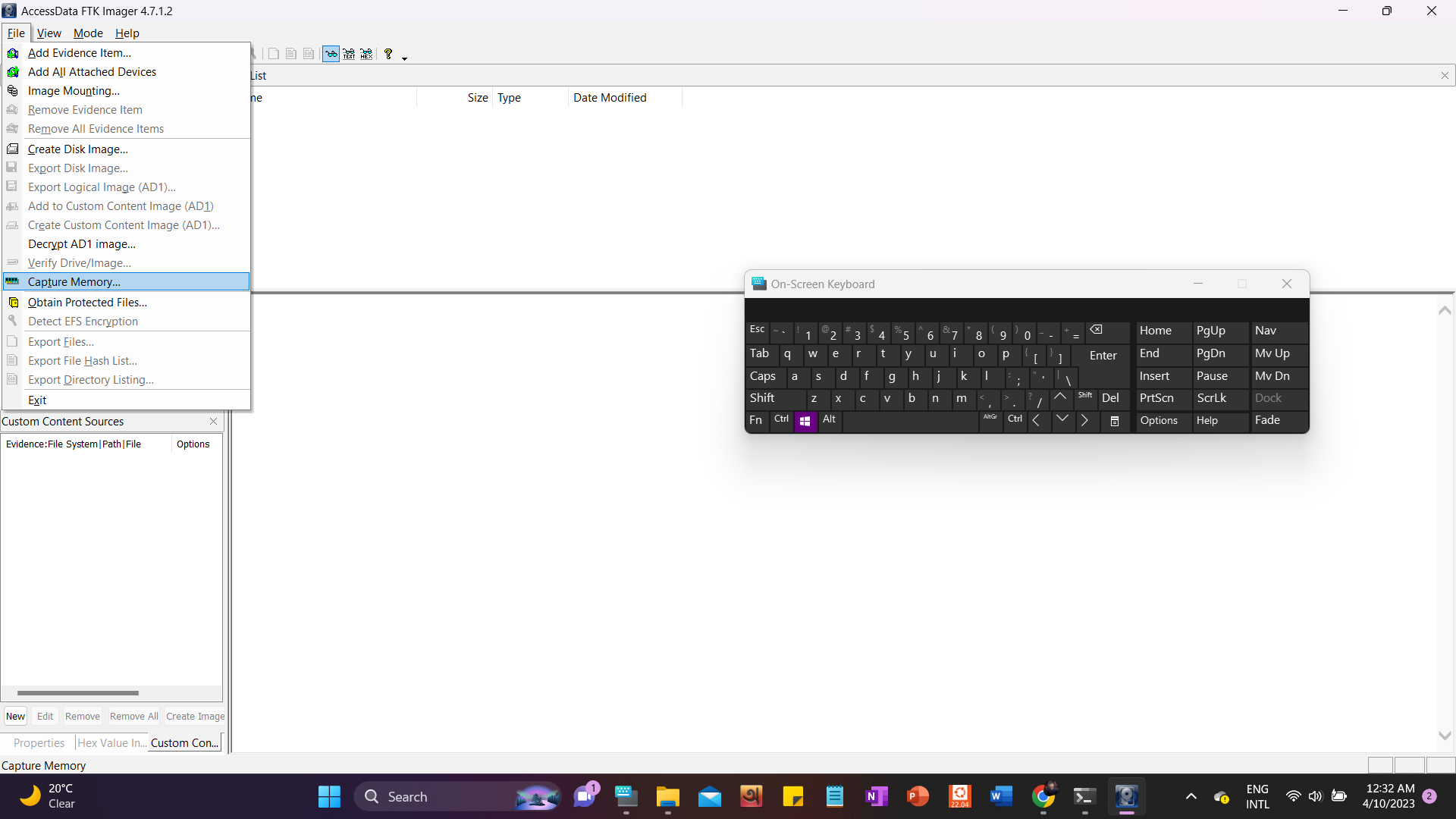
**Topic Name:** Use any open-source software to generate report to acquire and analyze the volatile data that is temporarily stored in random access memory of your machine.

**Submitted To:** Navjot Kaur

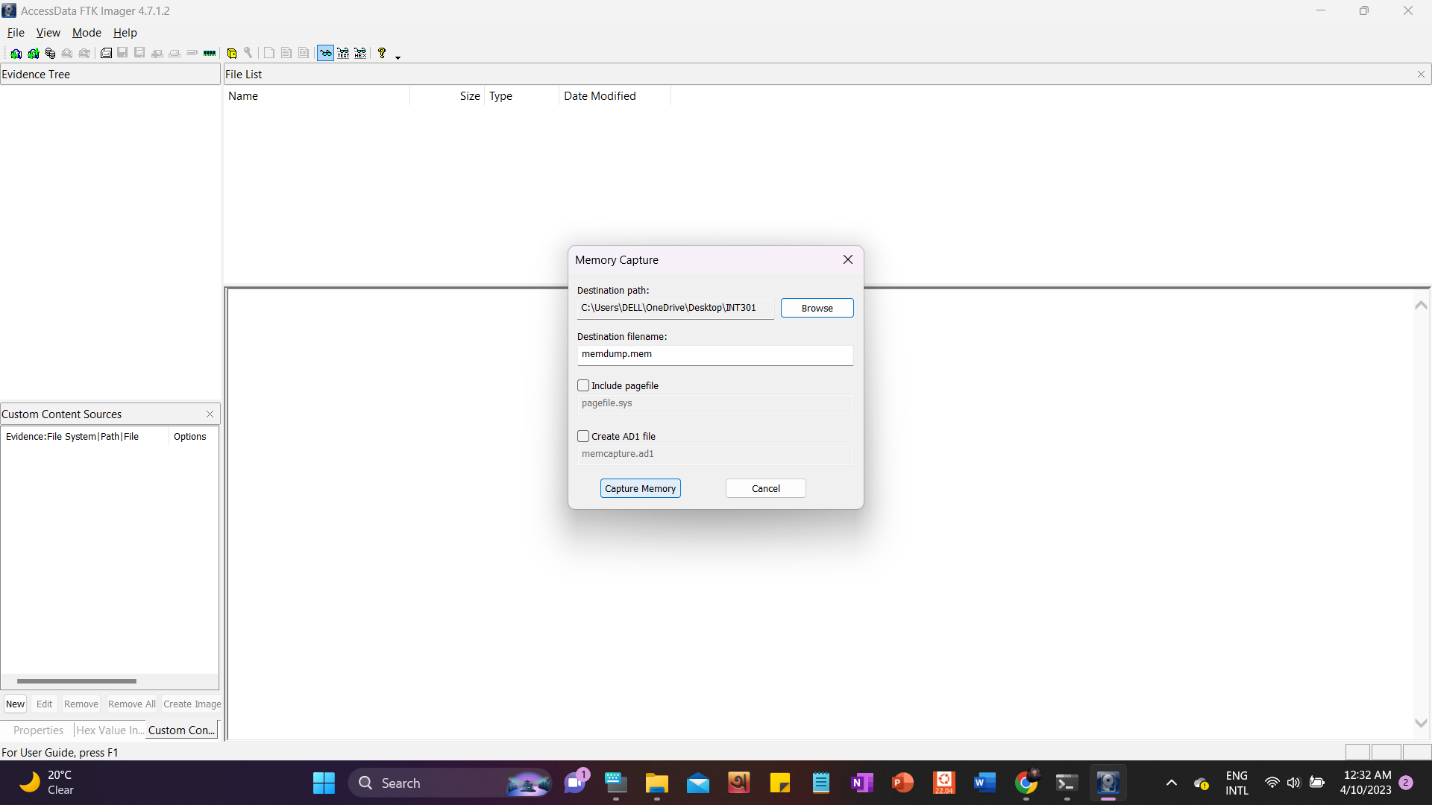
I used **FTK Imager** to acquire and **Volatility** for analyze the data which is temporarily stored in random access memory of my machine.

**Steps for acquiring the data by using FTK Imager are given below:**

**Step:1**



File🡺Capture Memory



**Step:2**

Browse:

Chose any destination folder to store the RAM data

Capture Memory:  
This button will start capturing the data to our destination folder. After getting the data we will analyze the data using volatile.

**Steps for analyze the acquired data command are given below:**

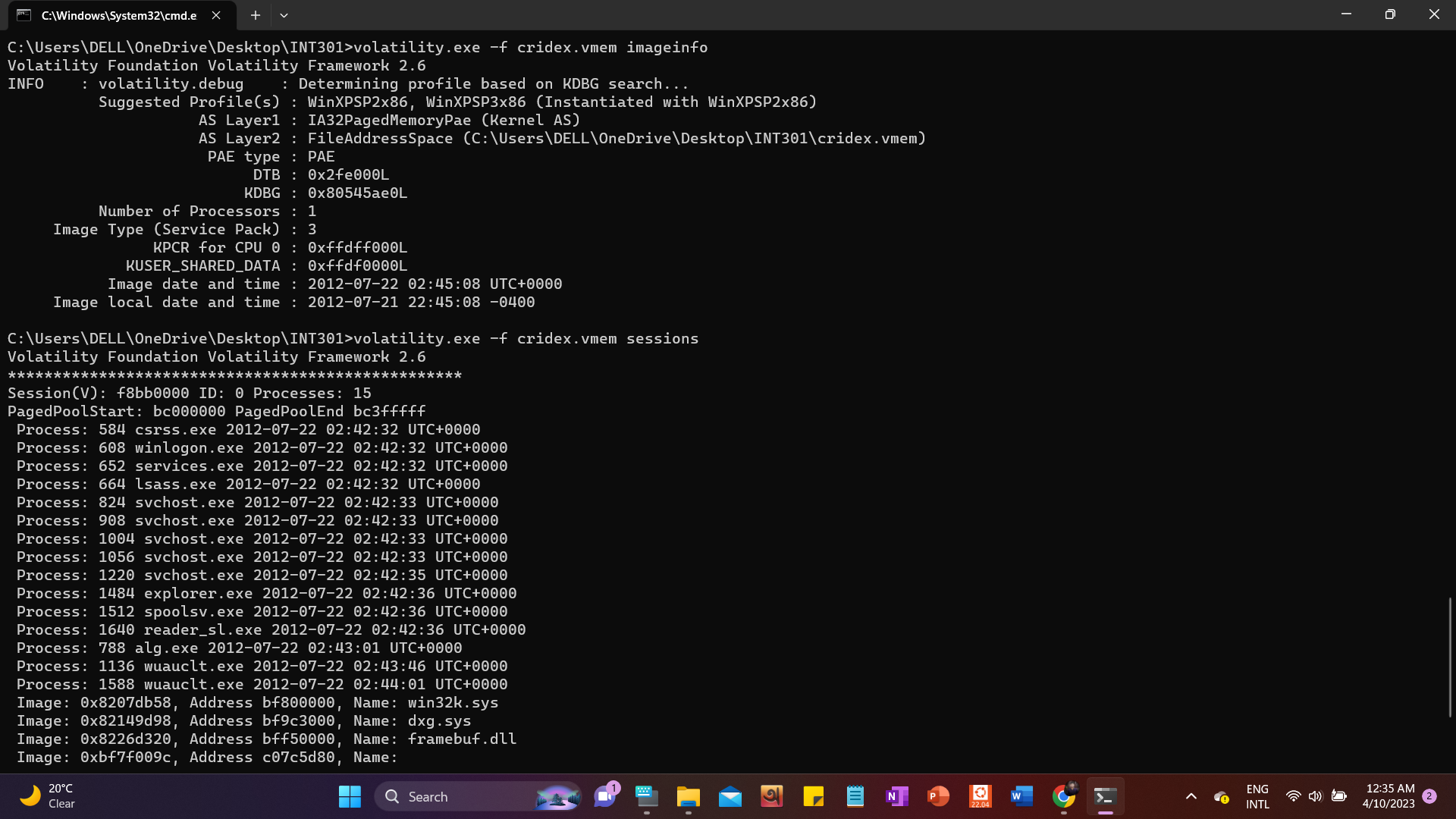
I used **Volatility** as a open source software to analyze the acquired data.

**Command 1:** volatility -h

This command will provide all the options available to analyze any our obtained file that we generate in our previous step. Examples are given below

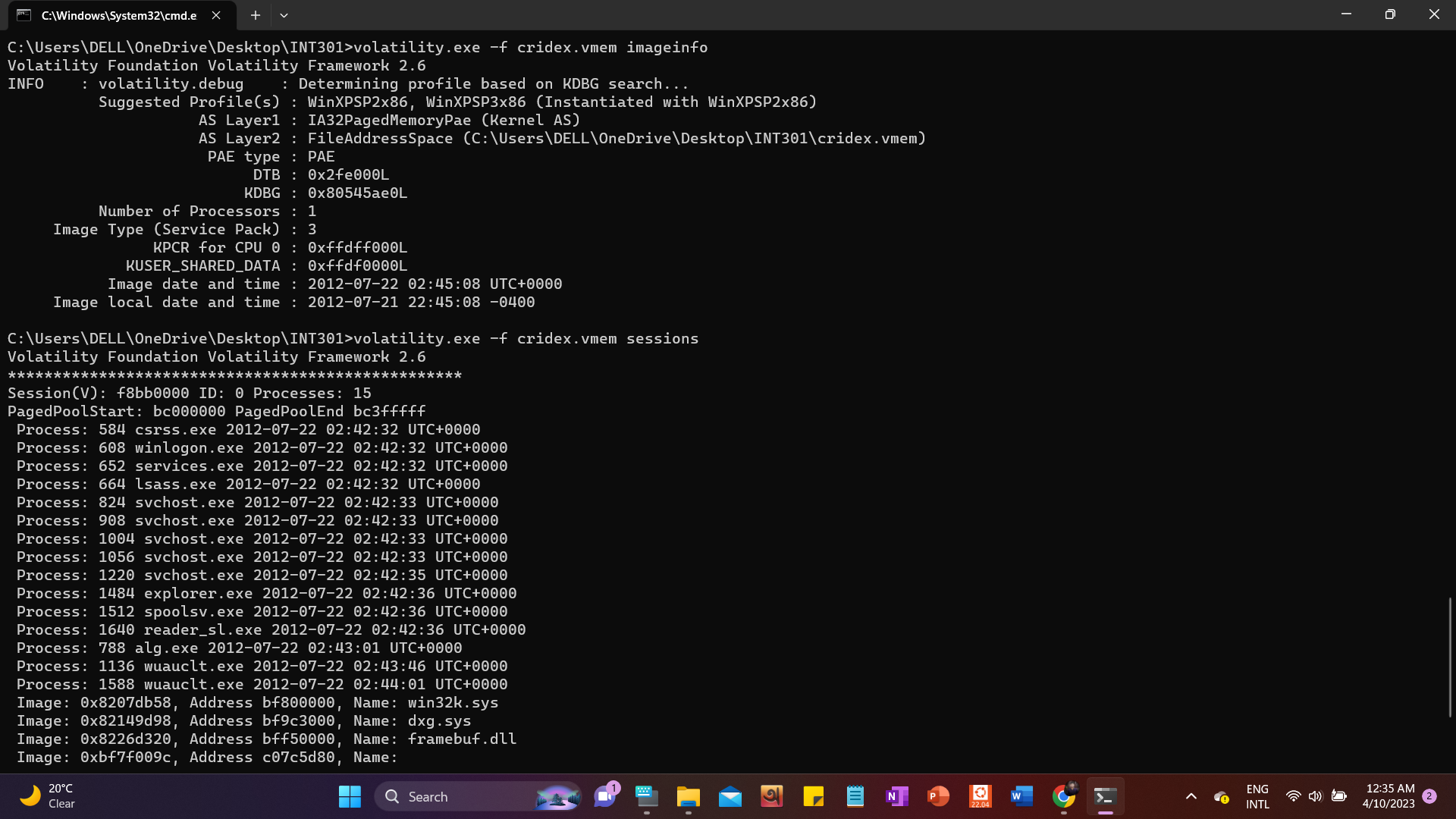
**Command 2:** volatility -f cridex.vmem imageinfo

This command will display the information about our acquired volatile data.

****

**Command 3:** volatility -f cridex.vmem sessions

This is an example where it will show all the active sessions when we capture our RAM data



GitHub repository link: <https://github.com/Maasuuum/INT301>