Name: Ghulam Abbas
Roll No: Fa22-BSDFCS/030-A Sem3
Lahore Garrison University
Assignment Submitted to: -
Miss Fatima

Question#1: Explain Volatile Data and provide order of volatility from most to least volatile.

Volatile data in the context of digital forensics refers to information stored in a computer's memory (RAM) that is temporary and can be quickly lost or altered when the system is powered down or restarted. Digital forensic investigators often prioritize the collection and preservation of volatile data because it can provide valuable insights into the current state of a system, ongoing processes, and user activities at the time of an incident.

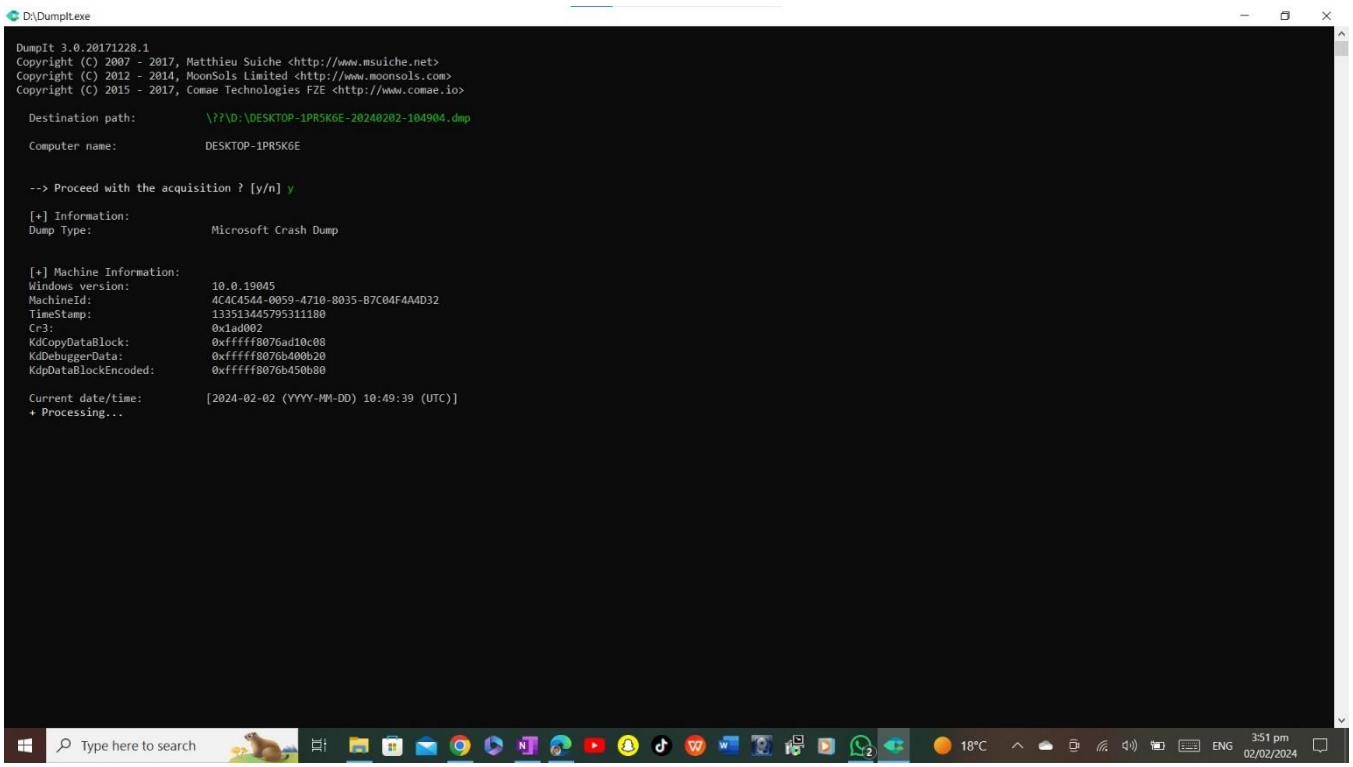
Here is a general order of volatility from most volatile to least volatile:

1. **Registers and Cache:** These are small, fast storage locations within the CPU. They contain data that is actively being processed and can change rapidly.
2. **RAM (Random Access Memory):** This is the main system memory where the operating system, applications, and data currently in use are stored. RAM is highly volatile and loses its content when the power is cut off.
3. **Network Connections and Open Ports:** Information about network connections, open ports, and active network sessions. This data can be crucial for understanding network-based attacks or unauthorized access.
4. **Running Processes:** Details about the currently running processes, including their memory space and execution status. This information helps in understanding the activities happening on the system.
5. **Temporary File Systems (TempFS):** Areas in memory used for temporary storage. Some operating systems use memory-based file systems for temporary data, and this information is volatile.
6. **System and Process Information:** Non-volatile data about the system configuration, user accounts, and active processes. While this information is less volatile than data stored in memory, it can still change between system reboots.
7. **System Logs:** Records of system events and activities. While logs are typically stored on disk, certain logs may be kept in memory temporarily before being written to storage.

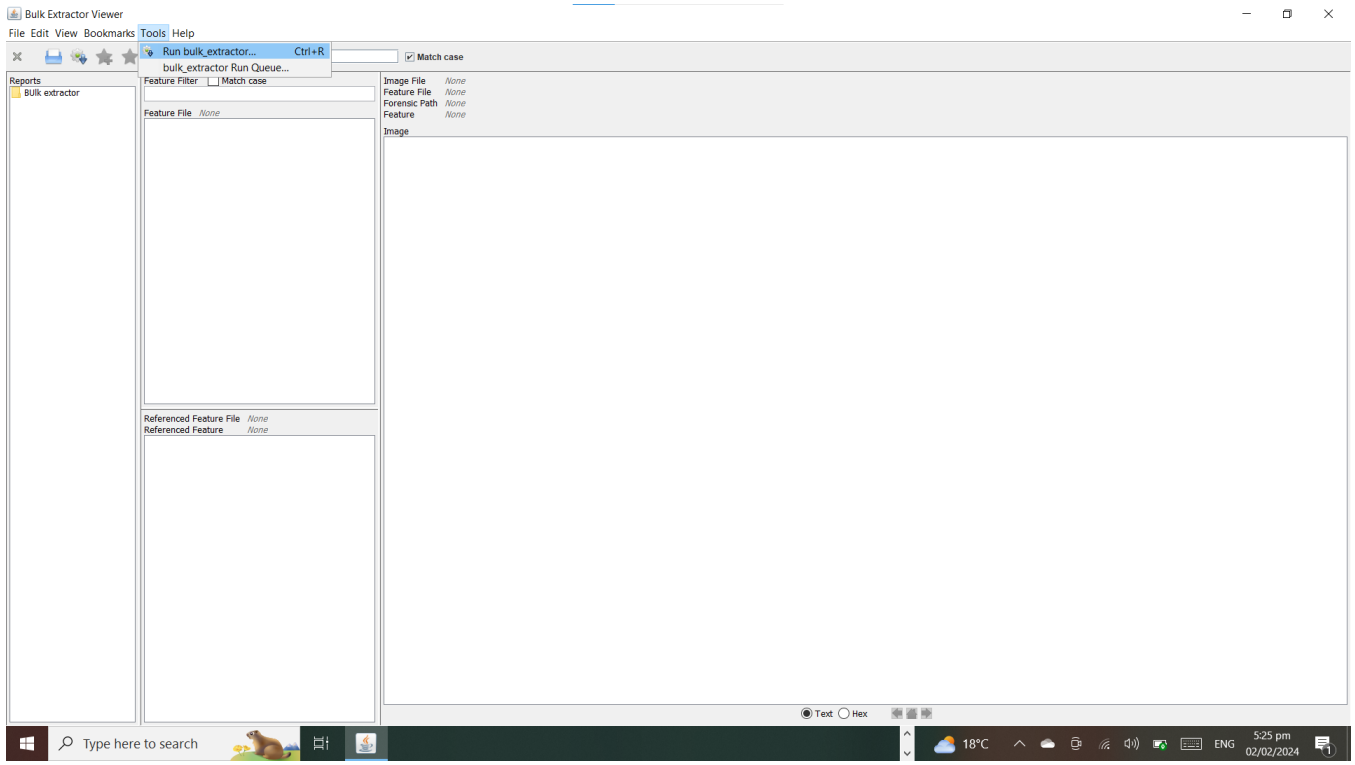
Question#2: Capture the RAM of your own Live Running System using any available forensic tool preferably command line.

Here we are capturing the RAM

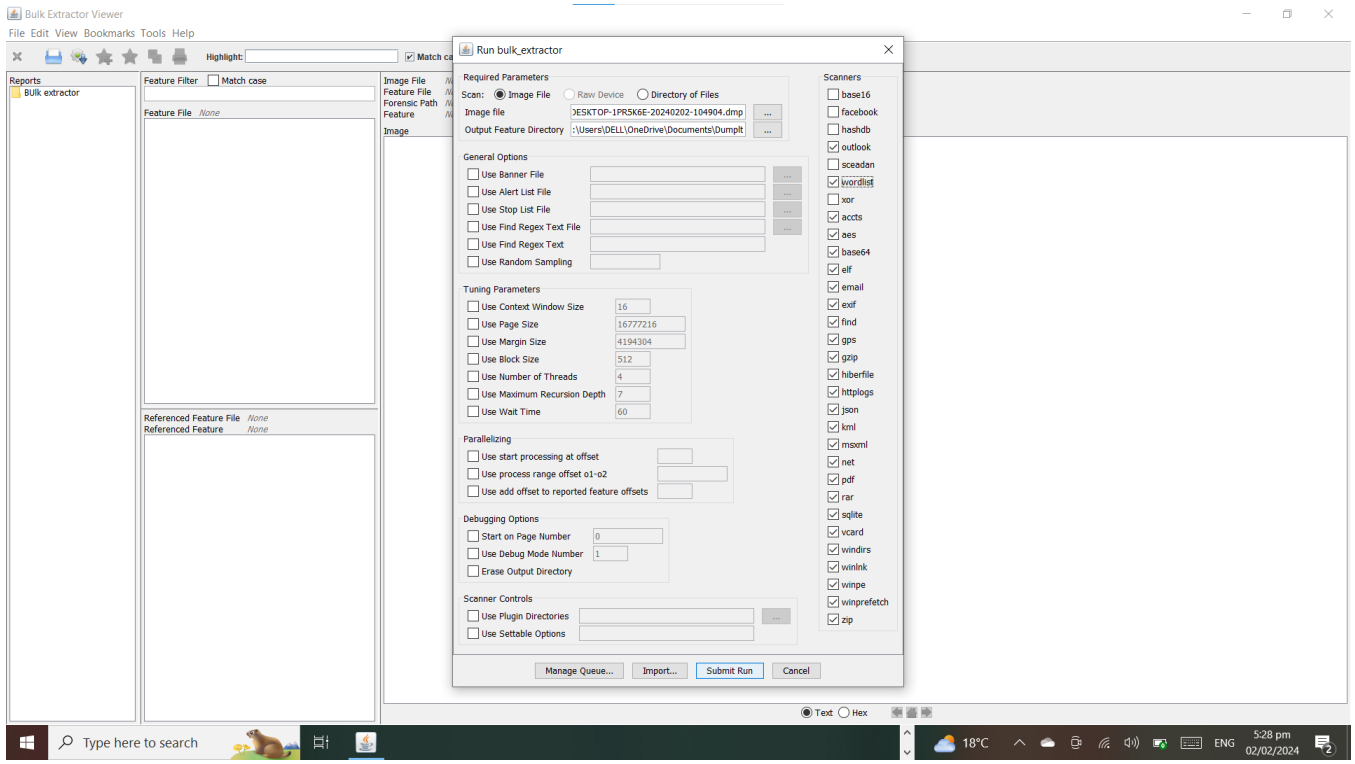
Here, I have network connection and open browser to use google classroom, YouTube, ChatGPT and google.



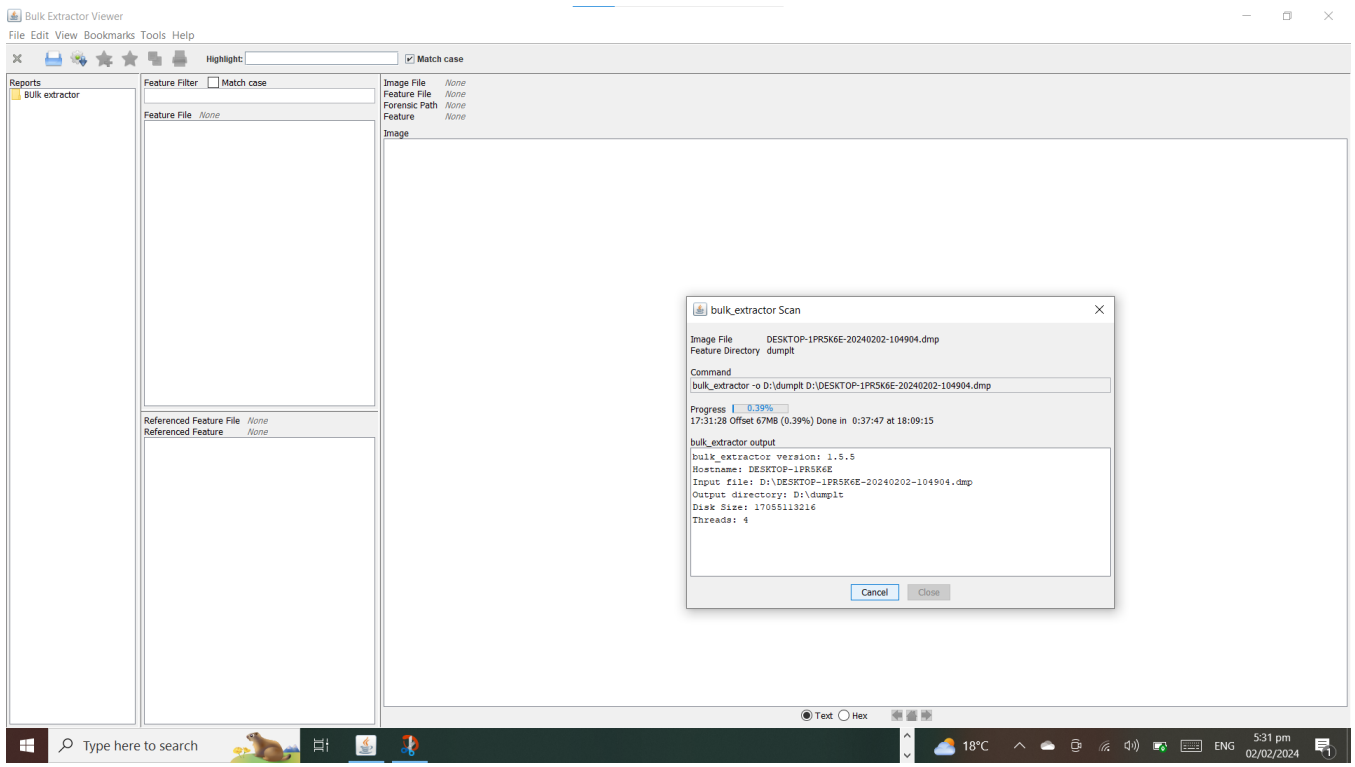
Here we open the bulk extractor and analyze the DMP file.



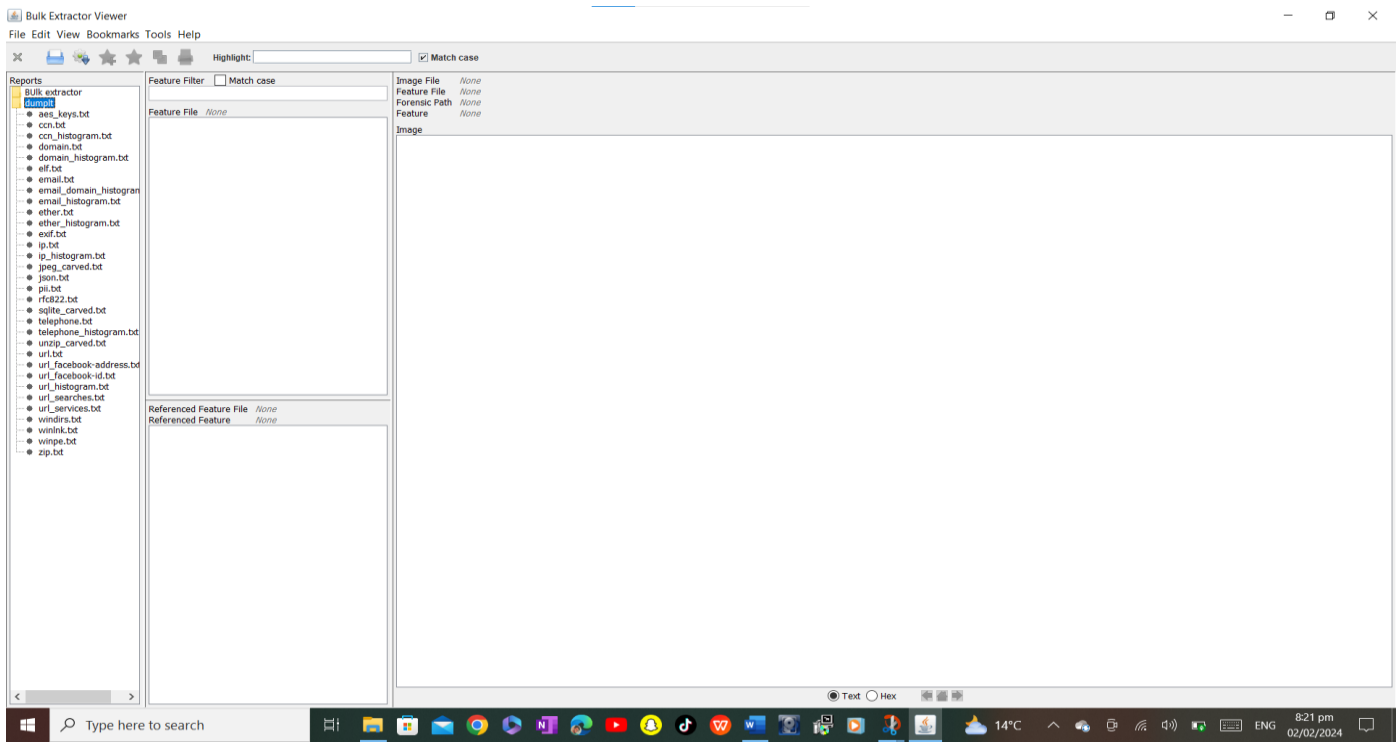
Here we select the image file that we have capture from dumplt and select the folder where we store the analyzes file



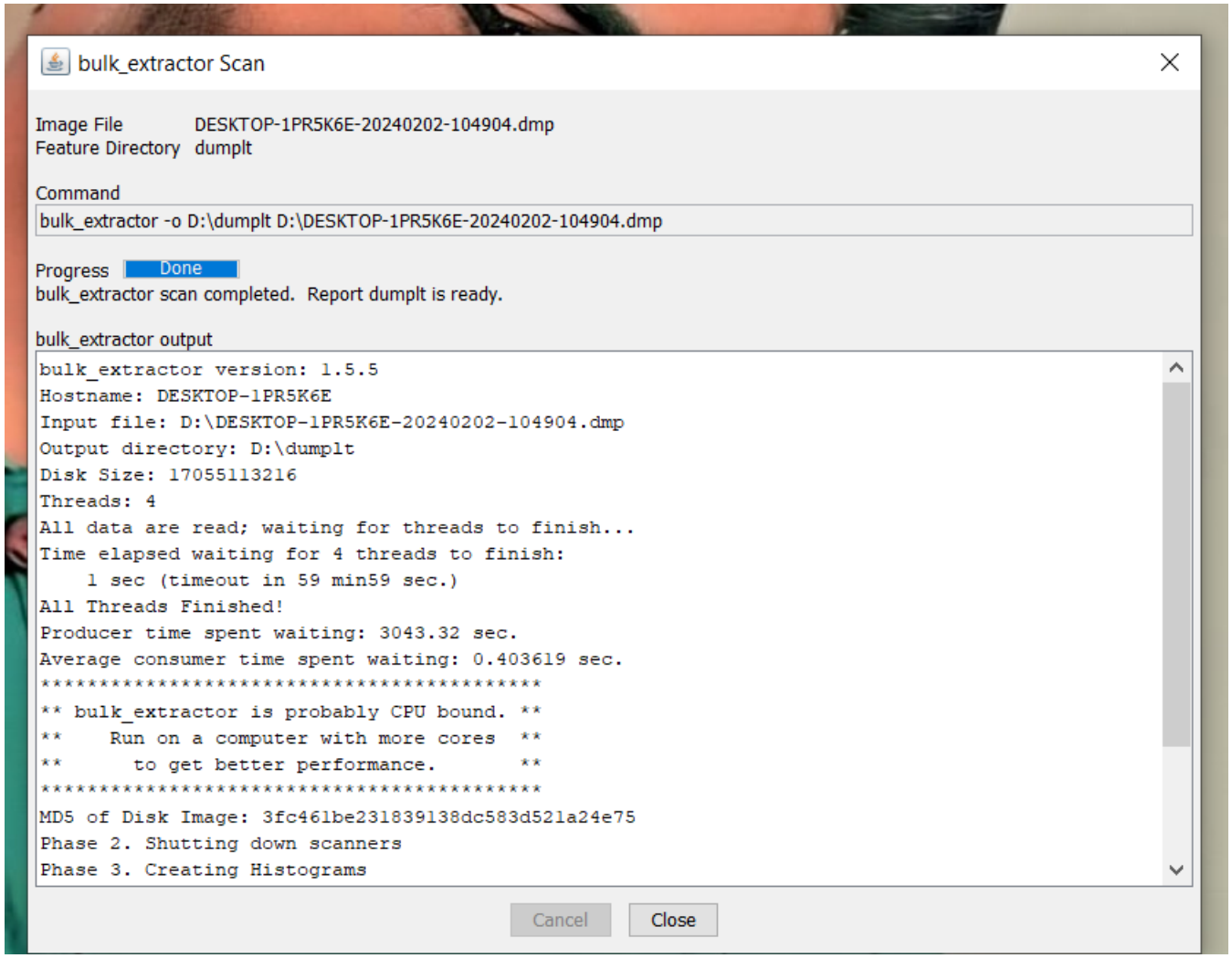
The DMP file is extracting



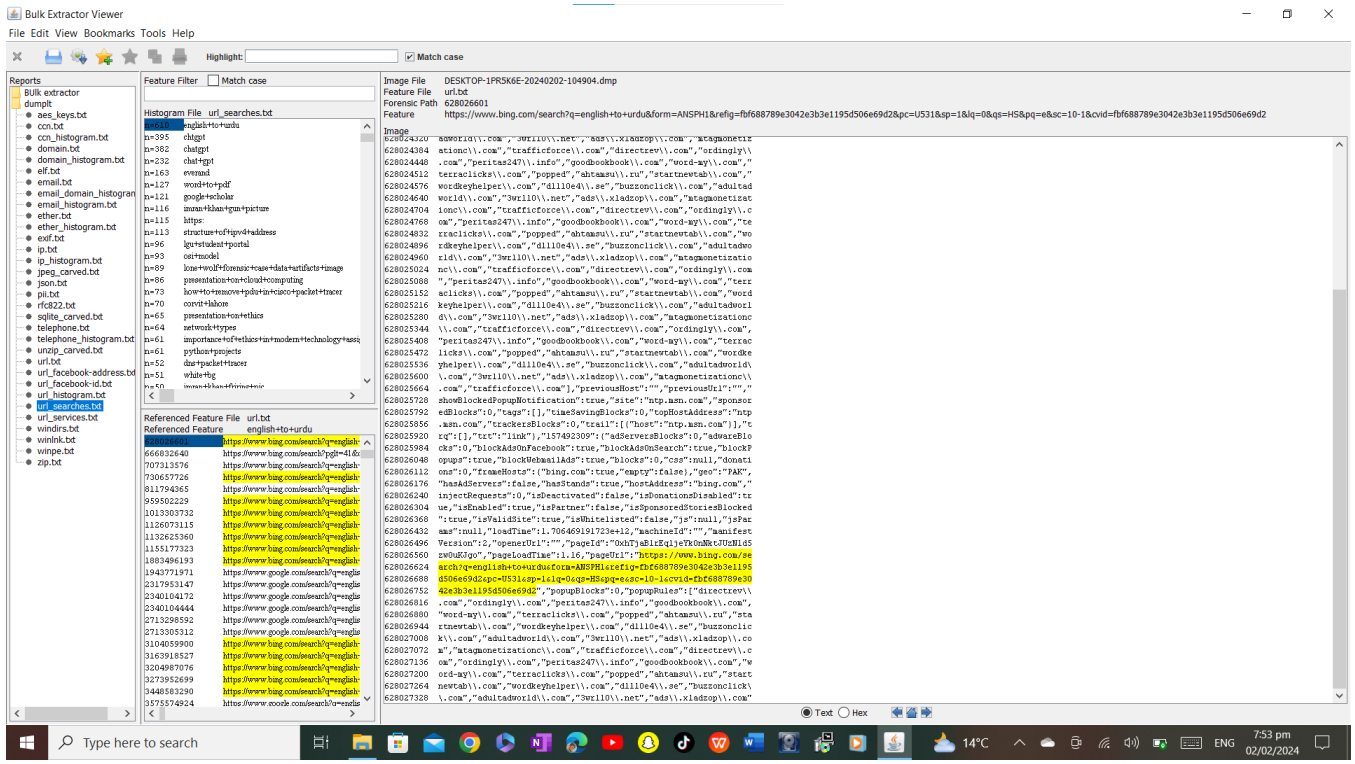
Here we open the extract file



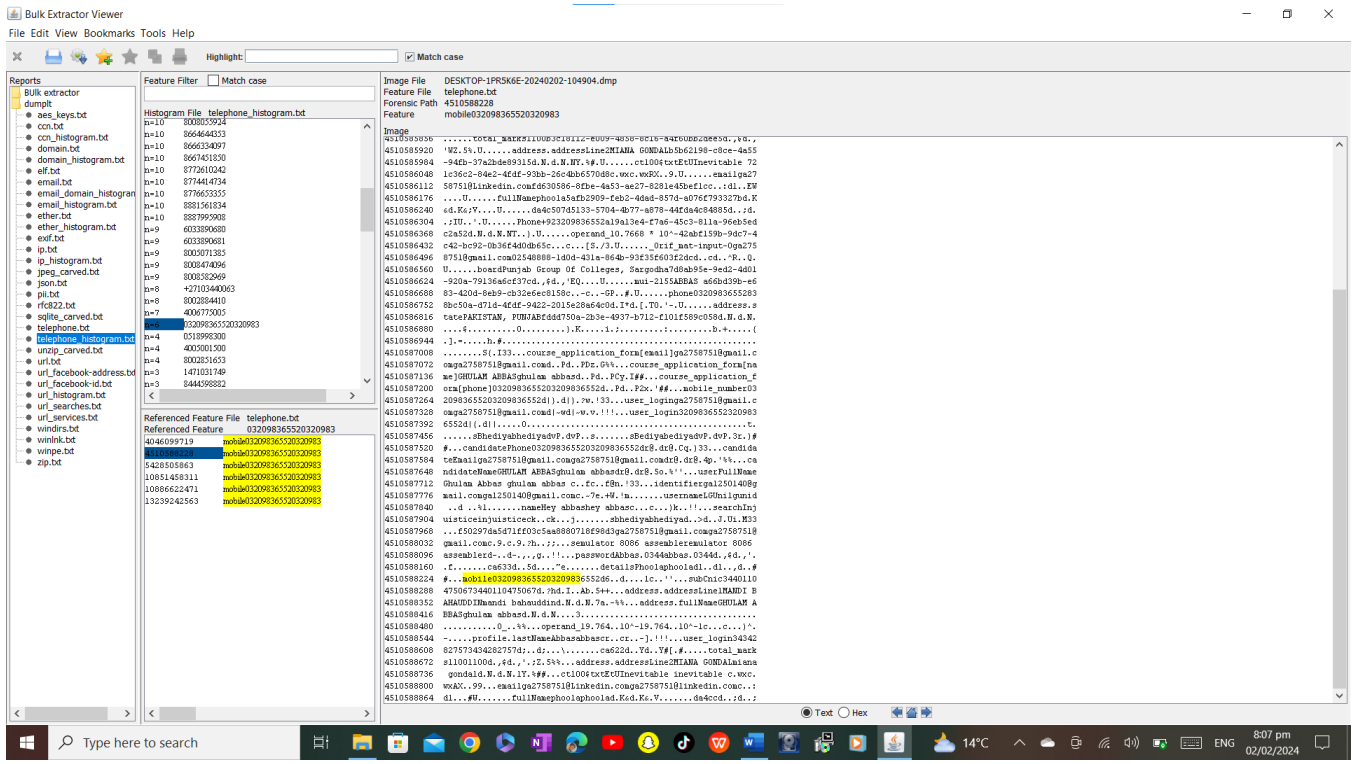
The processes is done



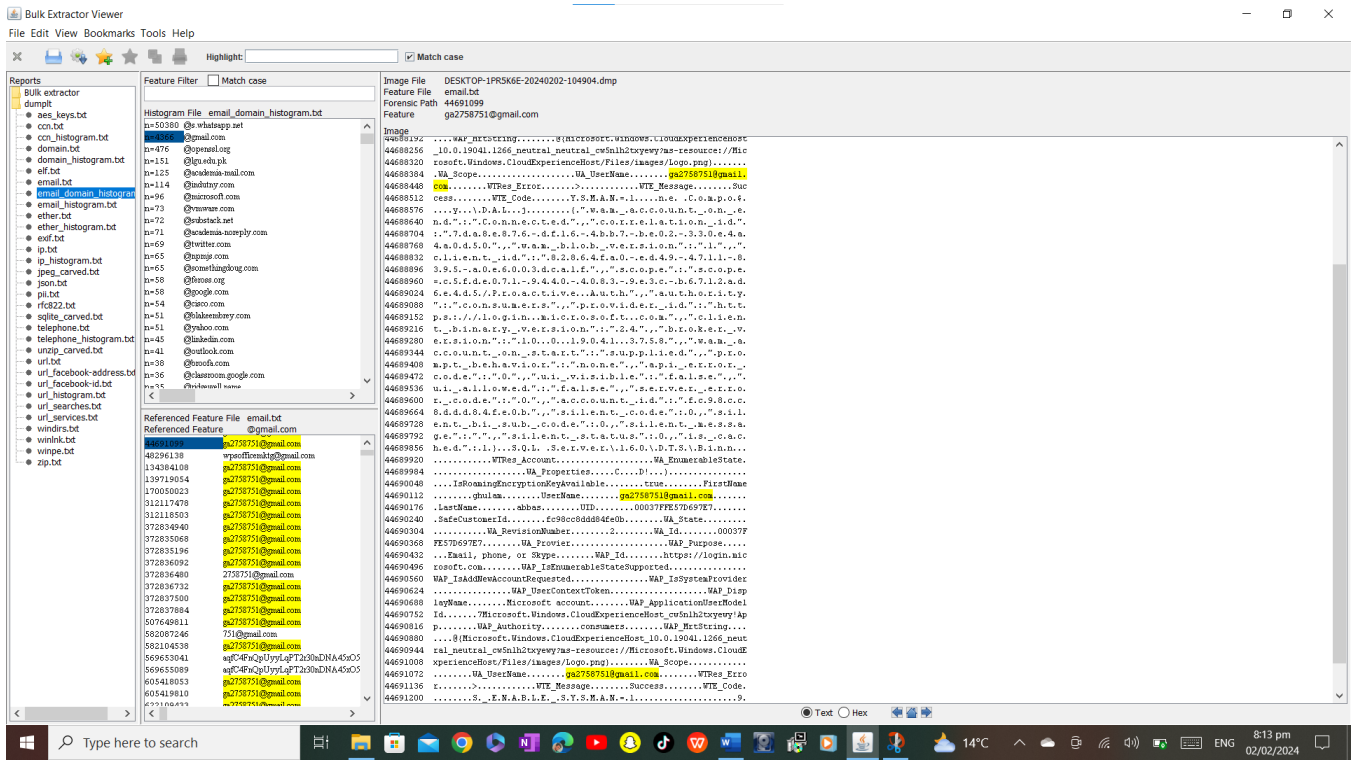
These are browsing history that are capture from my RAM



My phone number that are used in login information



Email account that are used for login into web and other email account that are in my Gmail software



WhatsApp chat history