

CA – 3 (Project)

Name: Prakhar Srivastava

Registration no.: 11904878

Roll no.: 55

Section: KE010

Submitted to: Mandeep Singh

School of Computer Science

1. Introduction

Digital forensics investigations are becoming increasingly important in today's world as more criminal activities are being carried out online. One crucial aspect of digital forensics investigations is the extraction of website artifacts. Web browsers such as Firefox, Edge, and Chrome are widely used by people for browsing the internet, and they store a significant amount of data, including browsing history, downloads, cookies, and cache files,subdomain which can provide valuable evidence in a digital investigation. By analysing these artifacts, digital forensic investigators can track the suspect's online activities, identify any criminal behaviour, and build a solid case against them.

Autopsy forensic tool is an open-source digital forensic tool that can be used to extract or restore images from disk, phone or any other flash drive. It provides various modules and tools that can help investigators search for specific keywords, analyse file metadata, and extract various types of files from disk images. In this task, we will focus on using Autopsy forensic tool to extract website artifacts from various web browsers and search for specific search terms.

By leveraging Autopsy's powerful keyword search capabilities, digital forensic investigators can search for specific search terms such as illegal activities, pornography, child exploitation, hacking, and terrorism, among others. By analysing the search results, investigators can identify potentially incriminating evidence and use it to build a solid case against the suspect.

Top of Form

* 1. Objective of the project

Extract the website artifacts from various providers such as Firefox, edge and chrome.

Find out the specific search terms on disk and phone using Autopsy forensic tool.

* 1. Description of the project

The above task project involves using forensic tool to extract website artifacts from various web browsers such as Firefox, Edge, and Chrome, and searching for specific search terms on disk images or phone images. The project is intended to provide an introduction to digital forensics investigations and demonstrate how digital forensic investigators can use Autopsy forensic tool to extract website artifacts and analyse them for incriminating evidence.

The project involves several steps, including creating a new case in Autopsy, adding disk images or phone images as evidence, creating a keyword list containing specific search terms, configuring the keyword search parameters to include web browser artifacts, running the keyword search job, reviewing the search results, and extracting any relevant website artifacts.

The specific search terms used in the project may vary depending on the investigation, but generally, they include keywords related to illegal activities, pornography, child exploitation, hacking, and terrorism. The project also emphasizes the importance of conducting digital forensics investigations within legal boundaries and with caution when interpreting search results.

Overall, the task project provides a practical demonstration of how Autopsy forensic tool can be used to extract website artifacts and search for specific search terms, and how digital forensic investigators can leverage this information to identify and prosecute criminals involved in online criminal activities.

* 1. Scope of the project

The scope of the project is to demonstrate the process of extracting website artifacts from various web browsers such as Firefox, Edge, and Chrome using forensic tool. The project also includes searching for specific search terms on disk images or phone images using Autopsy forensic tool.

The project focuses on using Autopsy forensic tool as the primary digital forensic tool for extracting website artifacts and searching for specific search terms. It does not cover other digital forensic tools or techniques that can be used for similar purposes.

The specific search terms used in the project are intended to provide general examples of potentially incriminating evidence that can be found in website artifacts. The project does not cover the investigation of specific criminal cases or provide legal advice.

The project assumes that the disk images or phone images used as evidence are legally obtained and within the boundaries of applicable laws and regulations. It also assumes that the investigation is conducted by trained and authorized digital forensic investigators.

Overall, the scope of the project is to provide an introduction to digital forensics investigations and demonstrate how Autopsy forensic tool can be used to extract deleted images from flash disk and how we can extract important information from website.

1. System Description

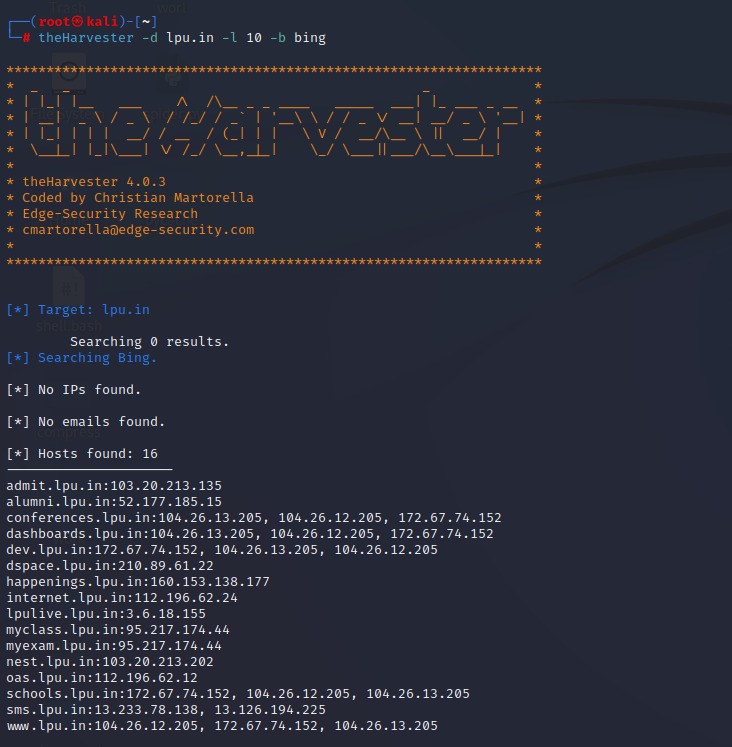
* The following is a system description for using Autopsy:
  + Operating System: Windows, macOS, or Linux
  + Autopsy Tool: Download the latest version of Autopsy from the official website and install it on your system.
* The following is a system description for using the Harvester:
  + Operating System: macOS or Linux
  + The Harvester tool: updated with API

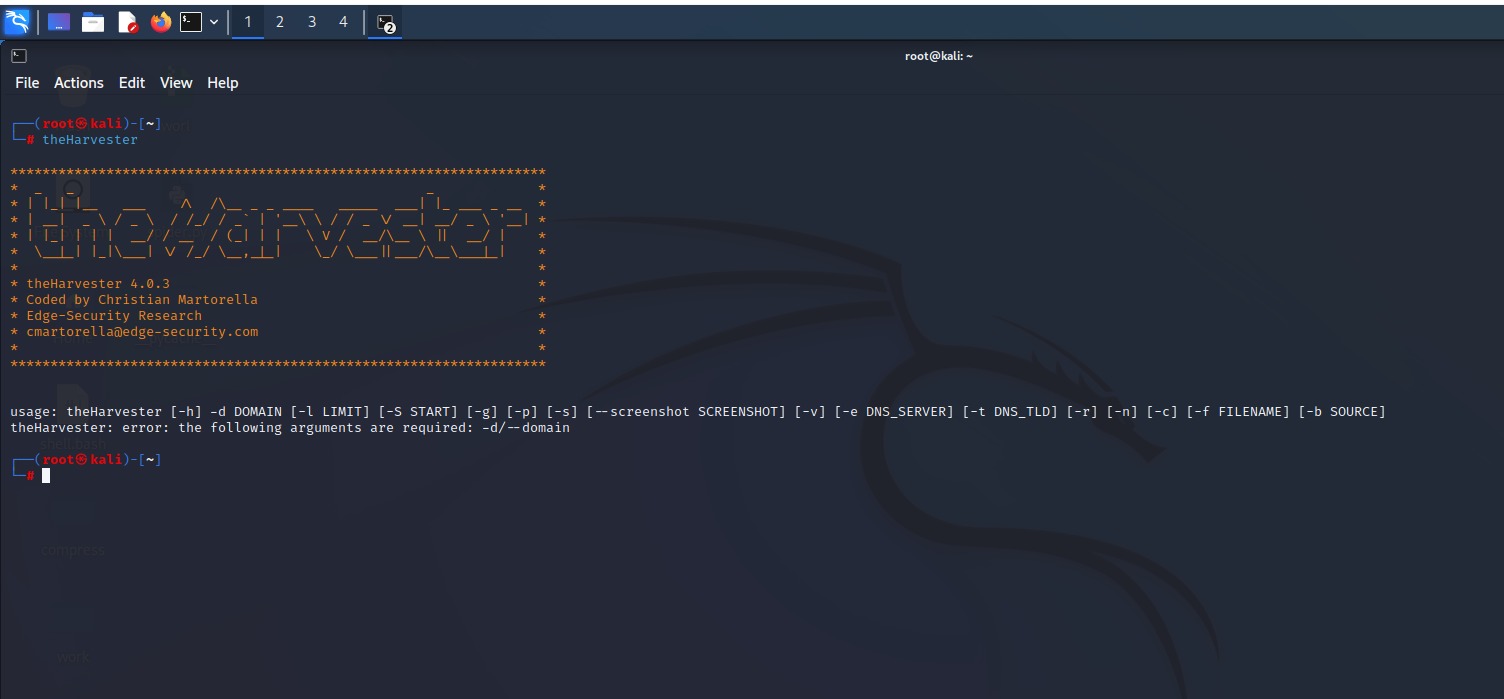
* 1. Target system description
* For website I am using lpu.in domain.
* For Autopsy, I am using a flash drive or pen drive which contains 8GB of storage.

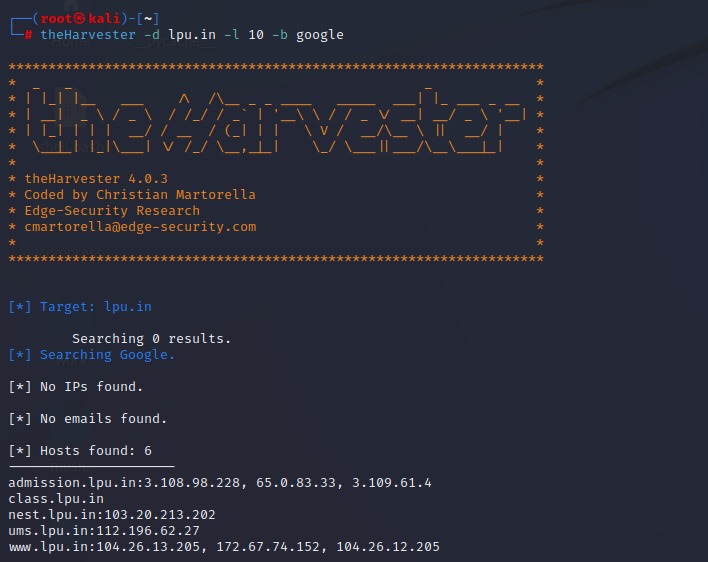
3. Analysis Report

3.1 System snapshots and full analysis report

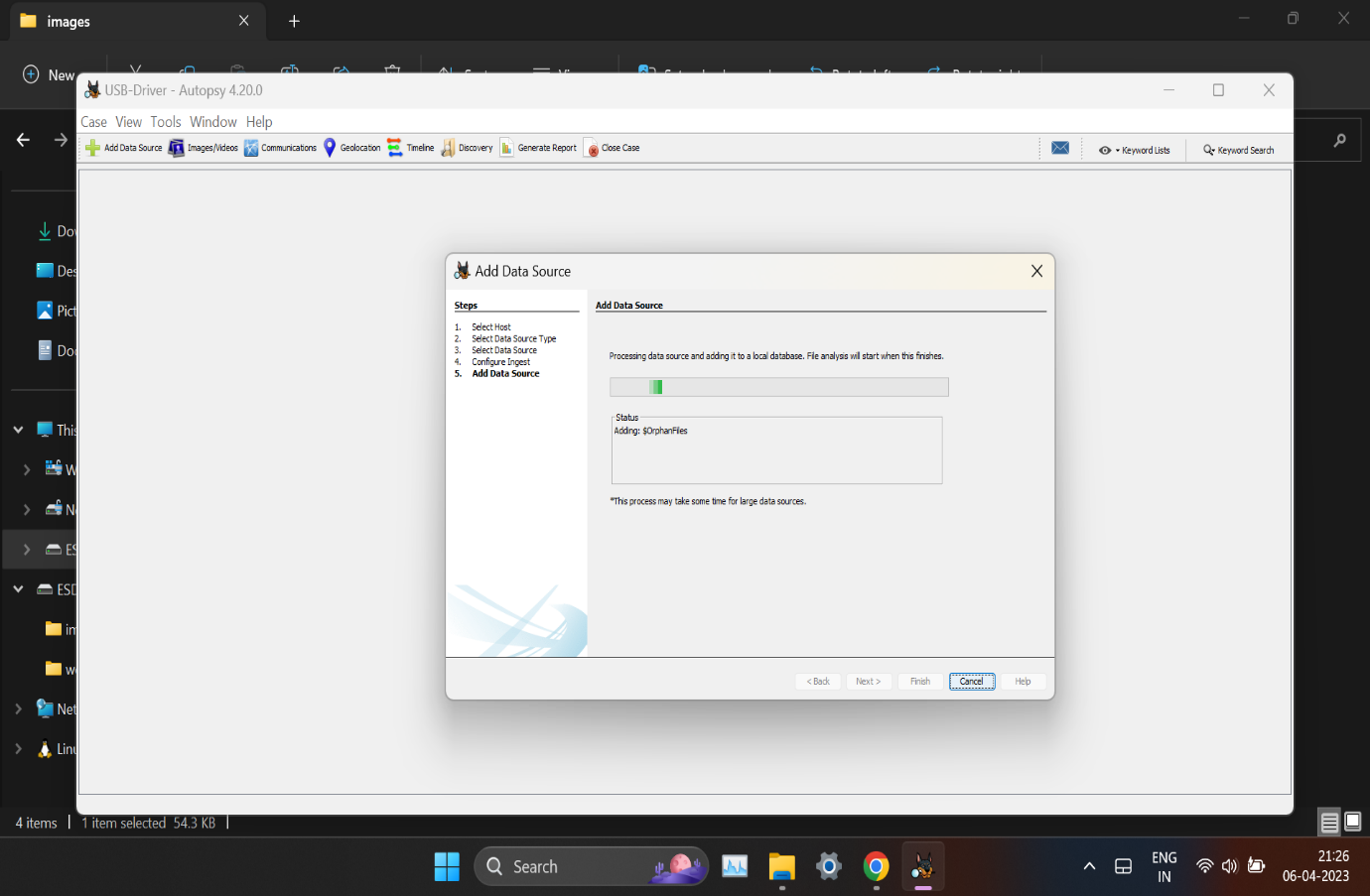
* Extract the website artifacts from various providers such as Firefox, edge and chrome.

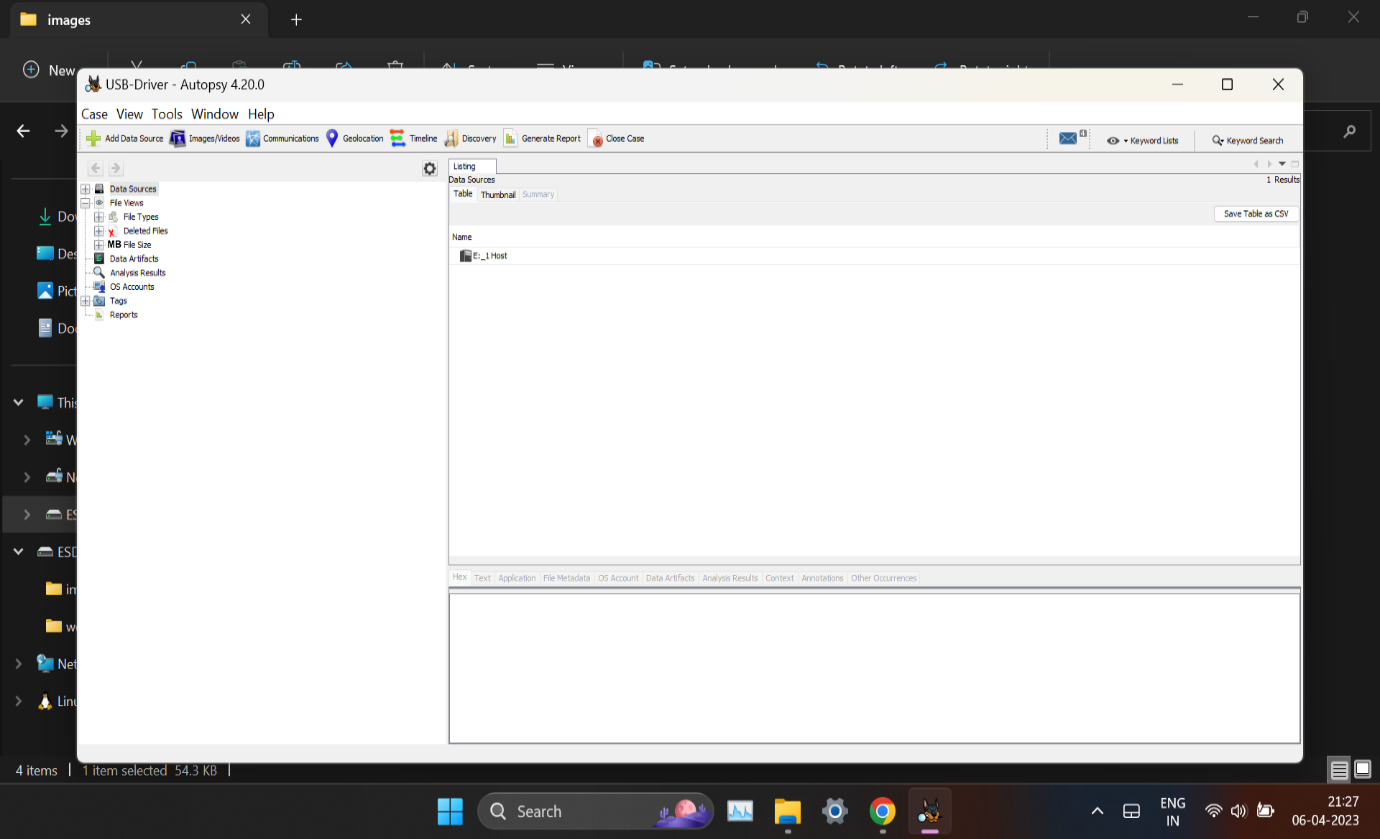


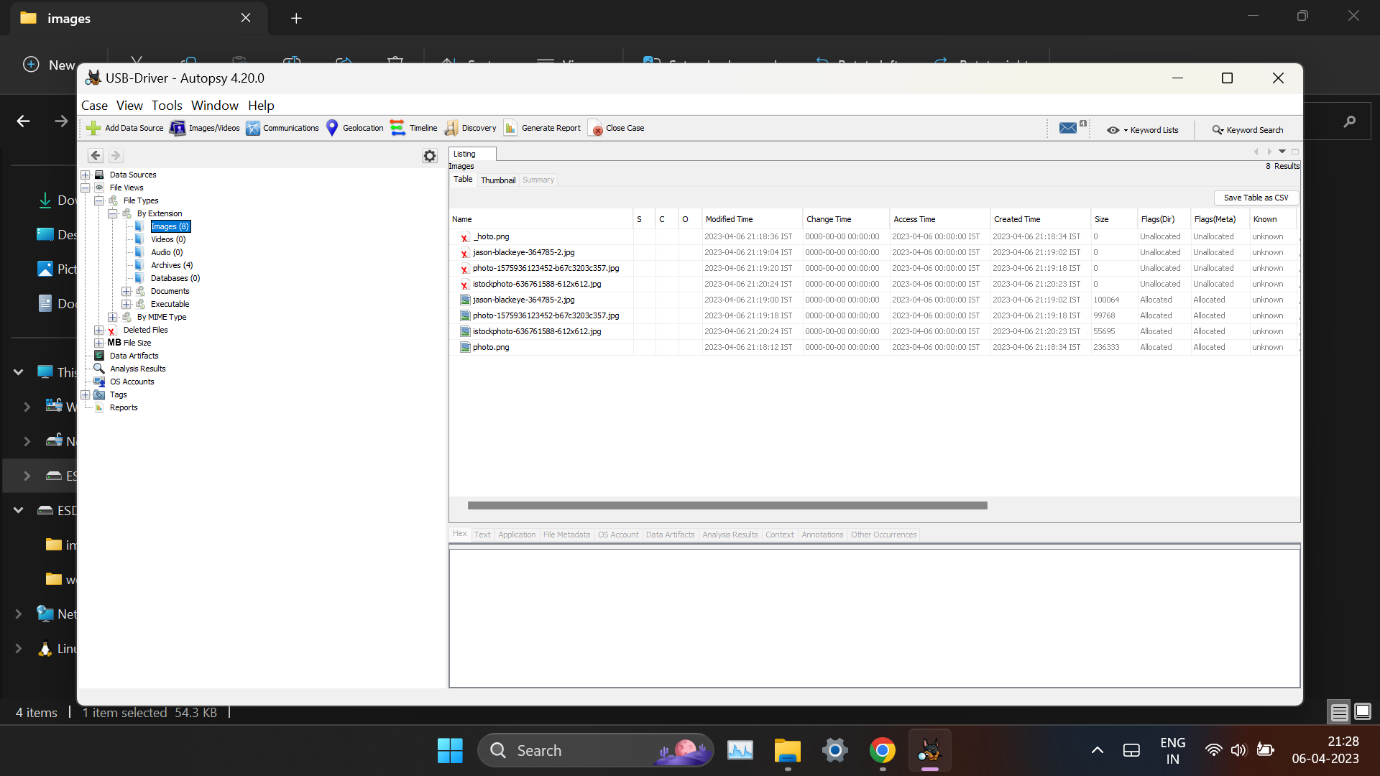
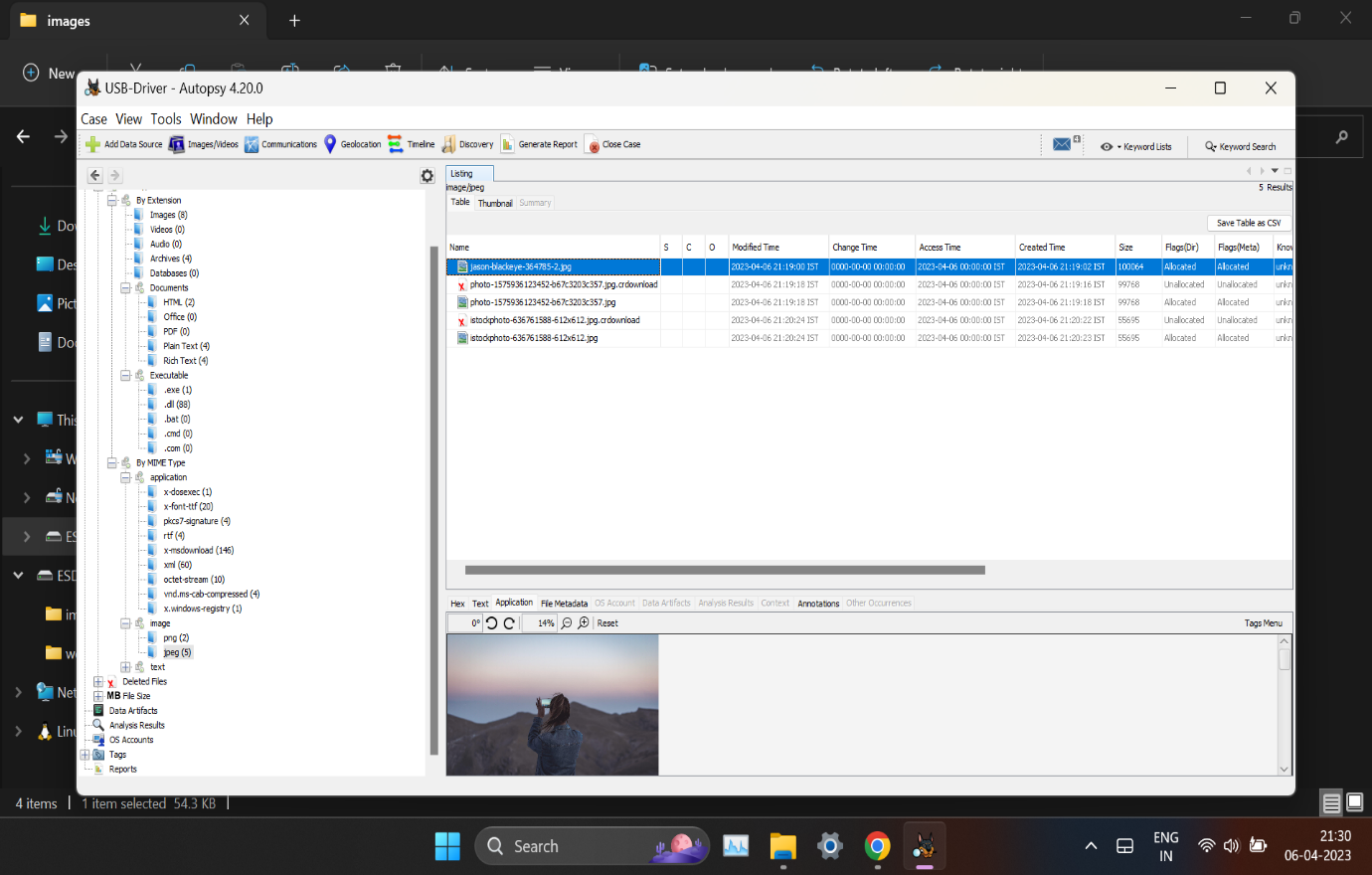
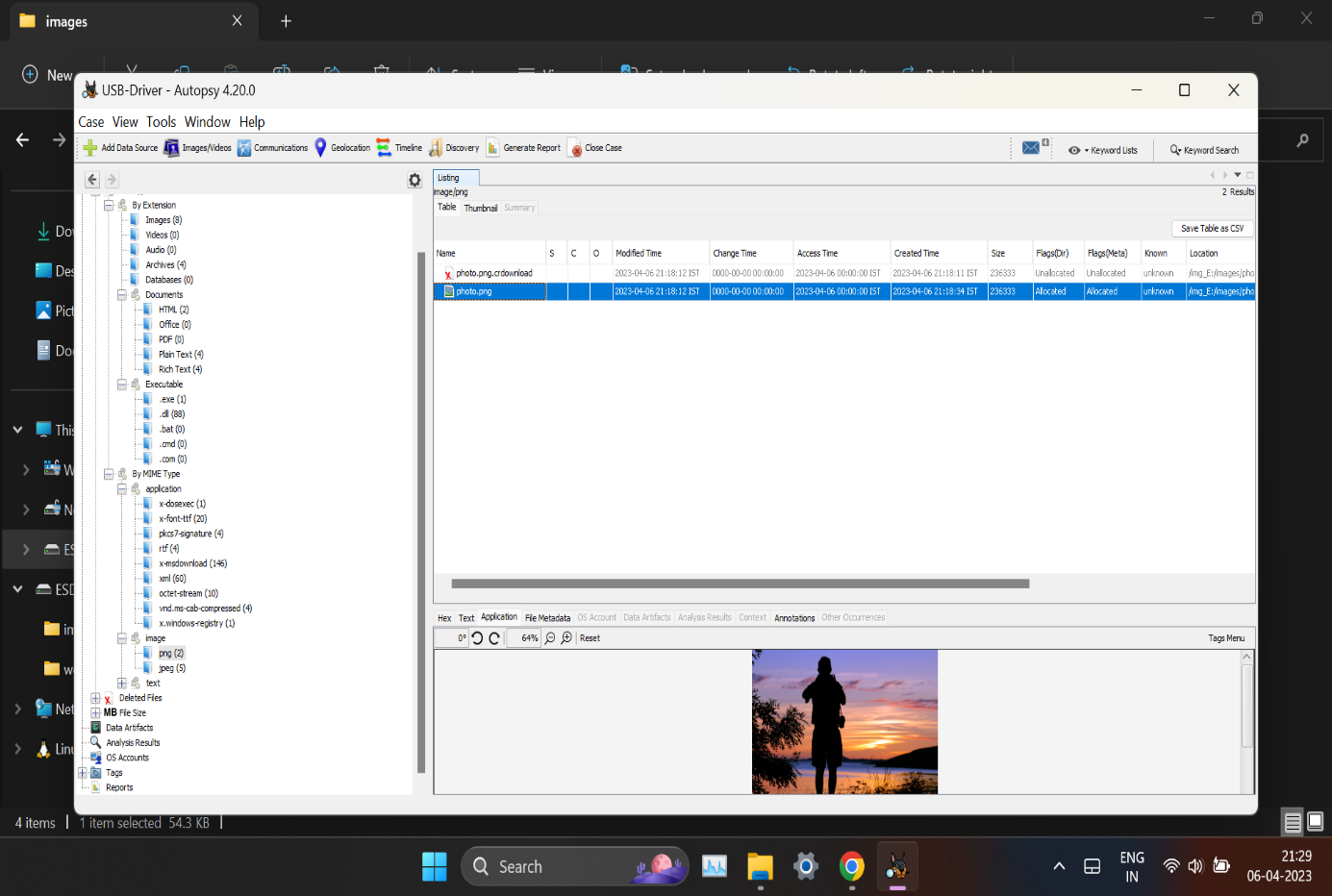
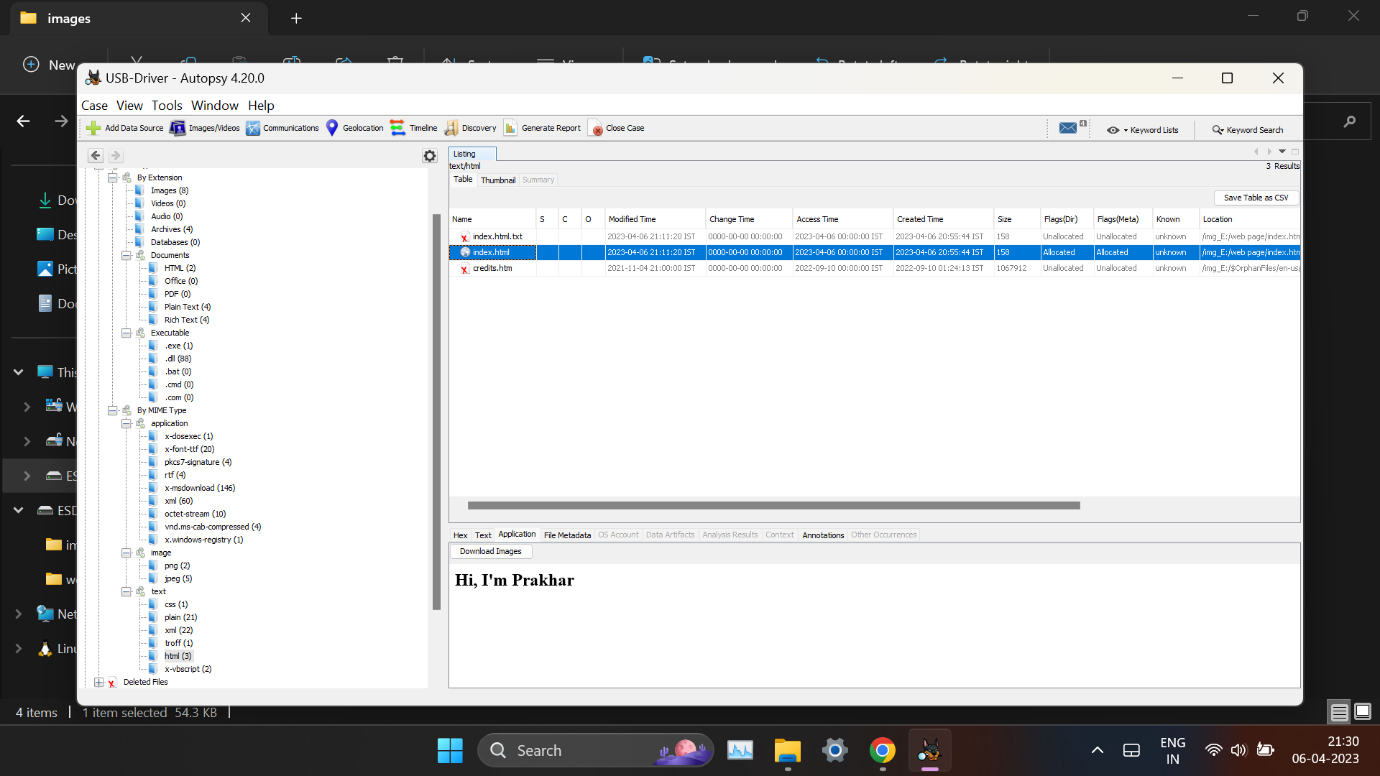


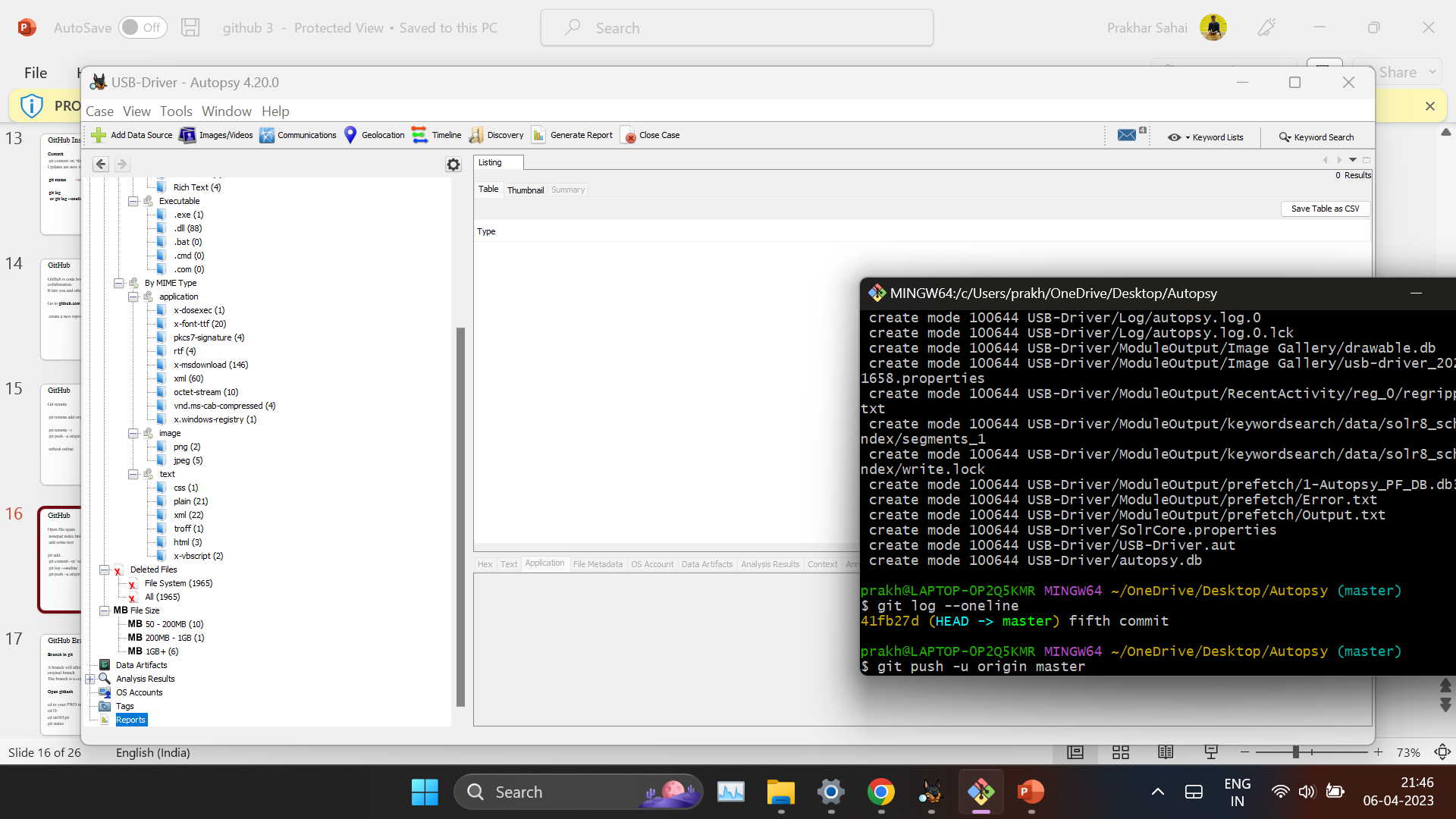


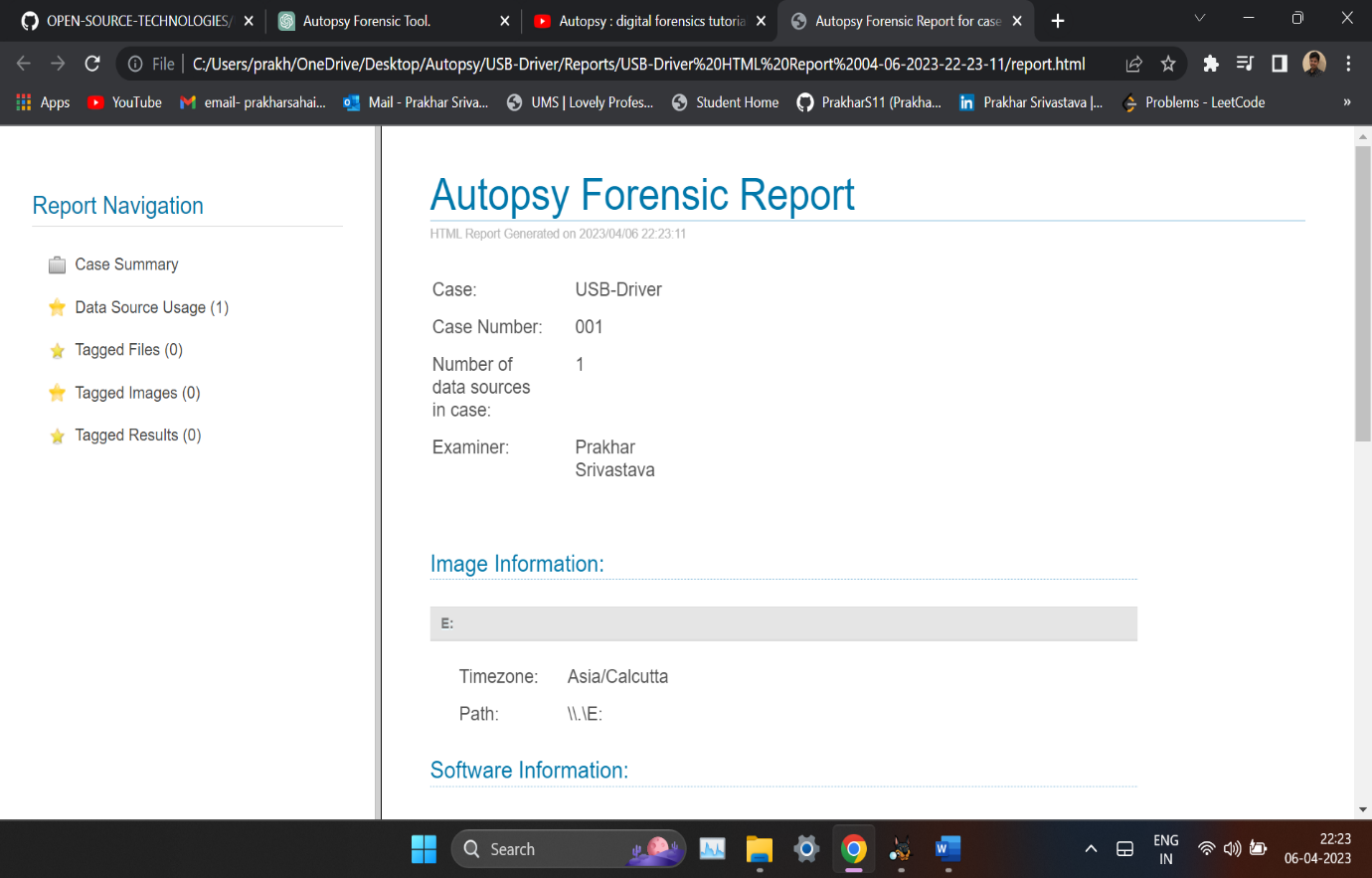
* Find out the specific search terms on disk and phone using Autopsy forensic tool.

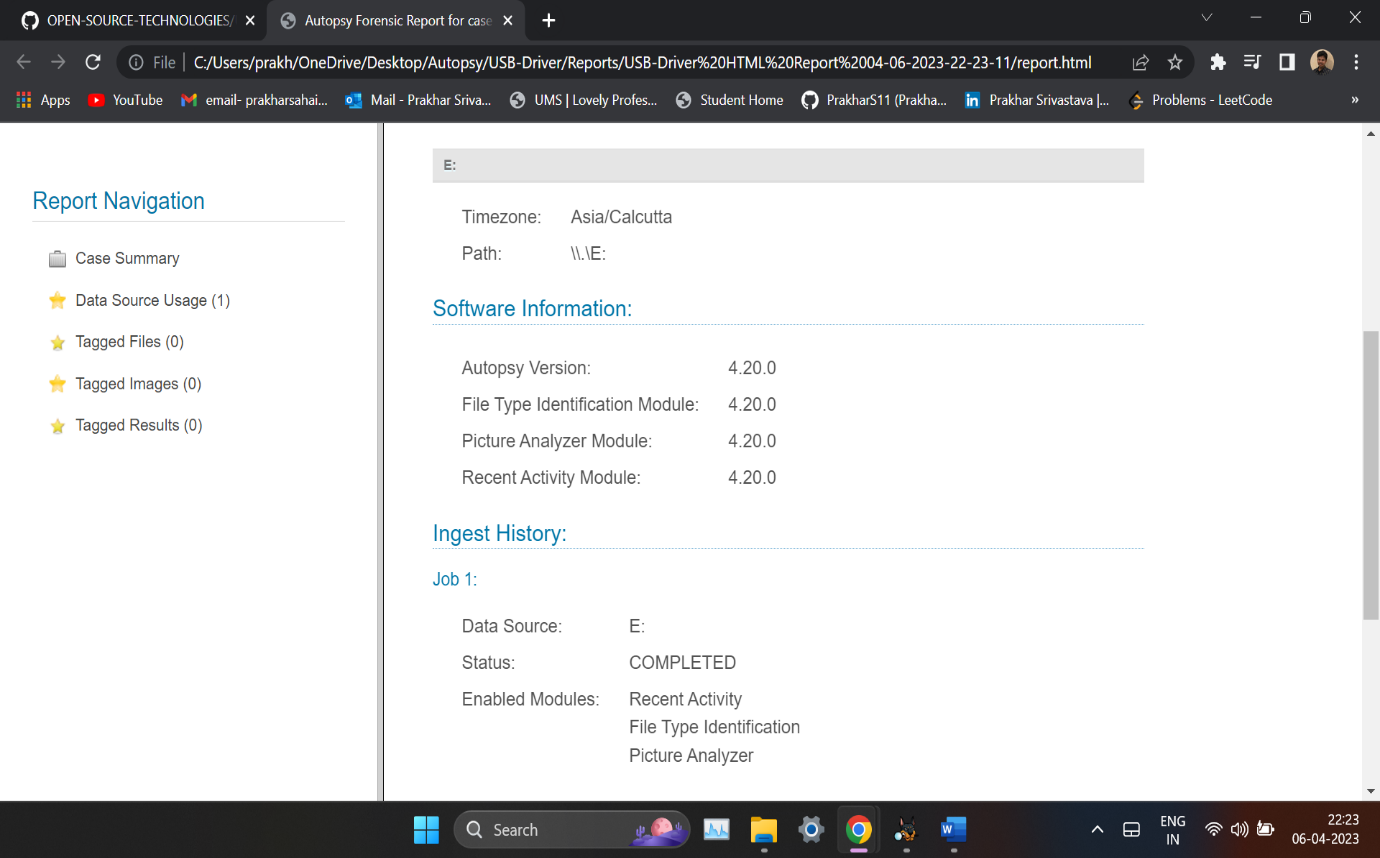


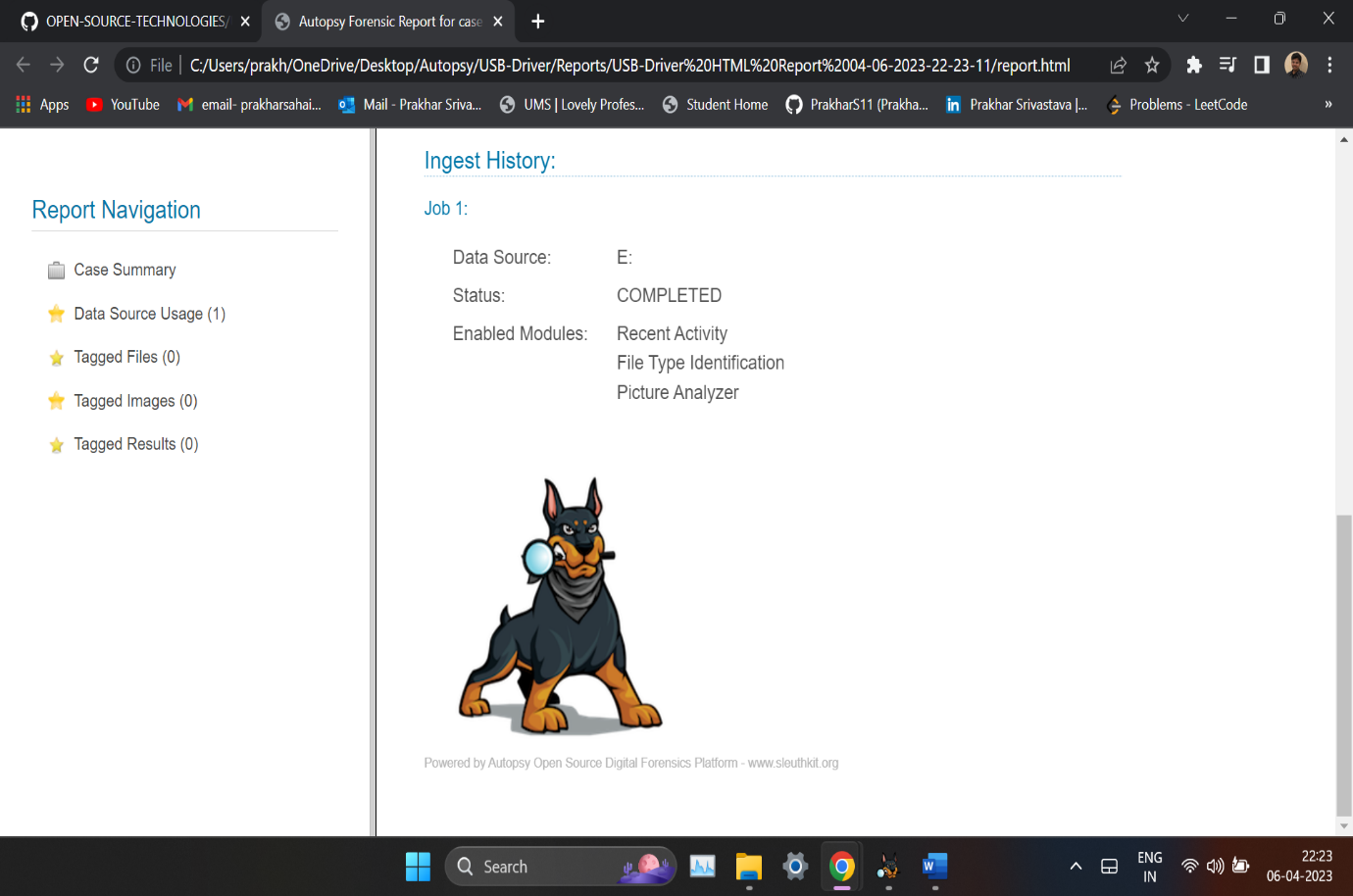










4. Reference/ Bibliography

* https://www.autopsy.com/
* https://www.kali.org/tools/theharvester/#:~:text=The%20package%20contains%20a%20tool,Installed%20size%3A%201.72%20MB
* https://www.youtube.com/watch?v=S6V66G2tVr8
* https://www.youtube.com/watch?v=cDryilcK39c
* https://en.wikipedia.org/wiki/Autopsy\_(software)
* https://www.kali.org/tools/theharvester/#:~:text=The%20package%20contains%20a%20tool,engines%2C%20pgp%20key%20servers).
* https://www.oreilly.com/library/view/web-penetration-testing/9781788623377/71203ba9-3894-4192-af66-1003405ab8ed.xhtml