logo

NAME : FELIX TUNTERE SOROGHAYE

COURSE: CYBERSECURITY

SQUAD 1

**FINAL PROJECT PROPOSAL**

Title: Building a Virtual Cybersecurity Laboratory and Conducting Android Forensics

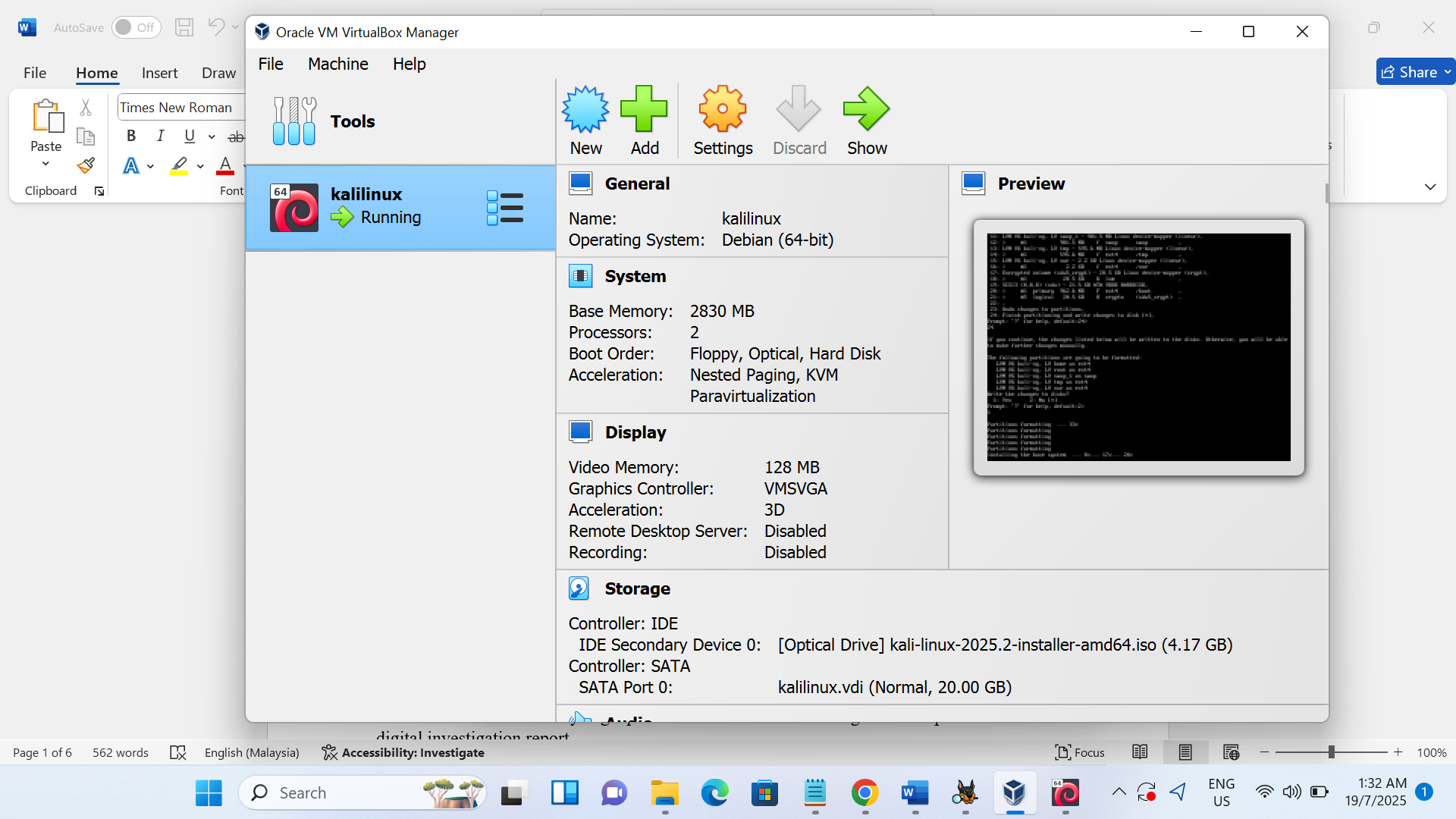
Investigations

Task 1 Objective

The task 1 objective is to create a virtual machine that will be able to communicate with each other, kali Linux and windows 10, also aimed at establishing internal virtual networking between the virtual machines. Also able to share directories, verify connectivity and service enumeration

Below is the virtual machine installed together with the extension and kali Linux. However, I have done everything withing me and check with some fellow students but the start appears in a command form as shown, I did follow the instruction provided but it still can’t work, as a result task 1 is not done, which is not a good one for me as a person. I will still keep trying to isolate the issue, although the due date for submission is today 18/7/2025

Figure 1 (Virtual Machine)



Also seek for further assistance during one of he mentorship class, I was asked to download via <https://www.kali.org/get-kali/#kali-virtual-machines> and choose the virtualbox. Sadly enough when get to select language the instruction will turn to command as shown in figure 3.

Figure 2 (kali.org)

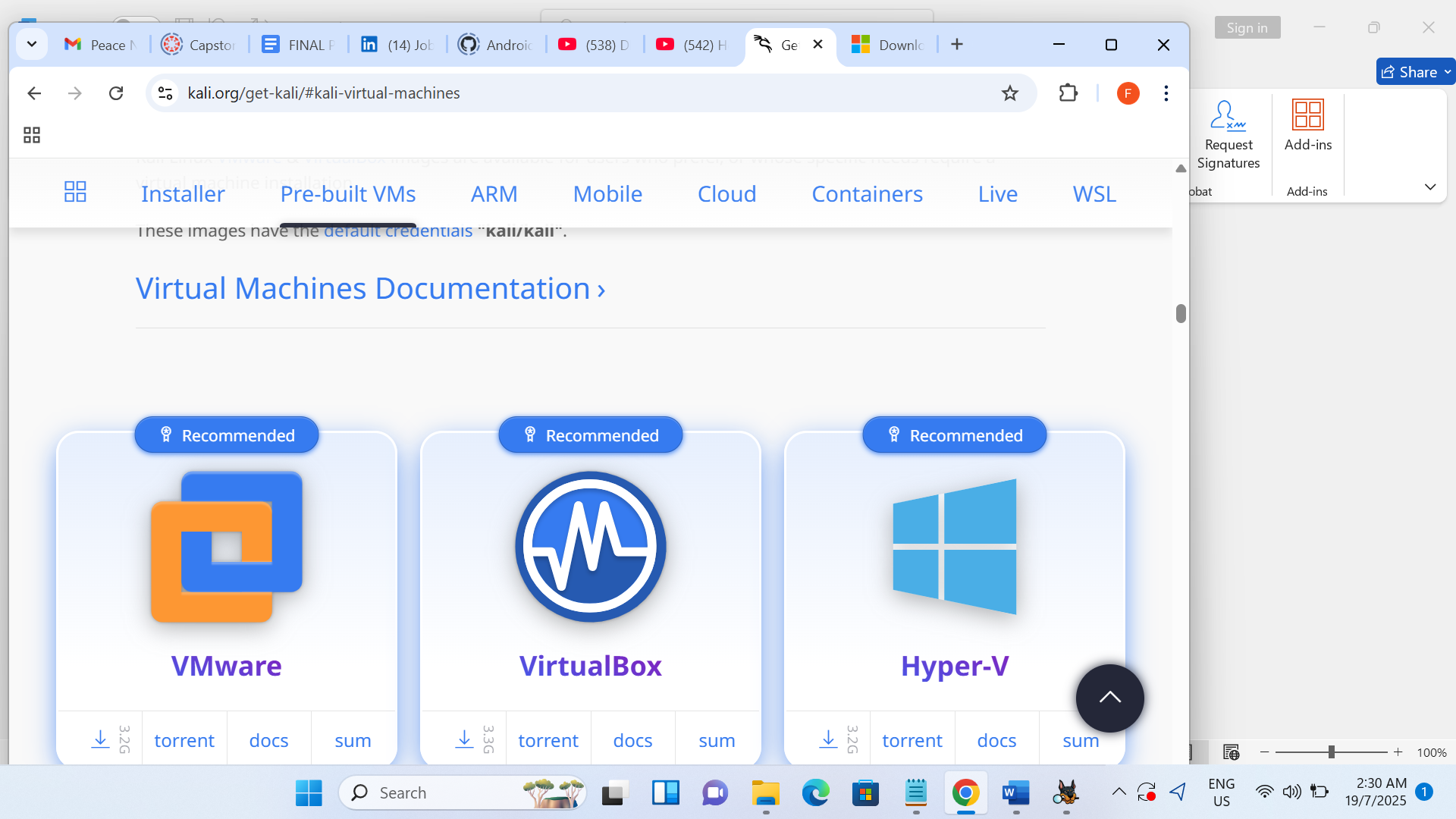
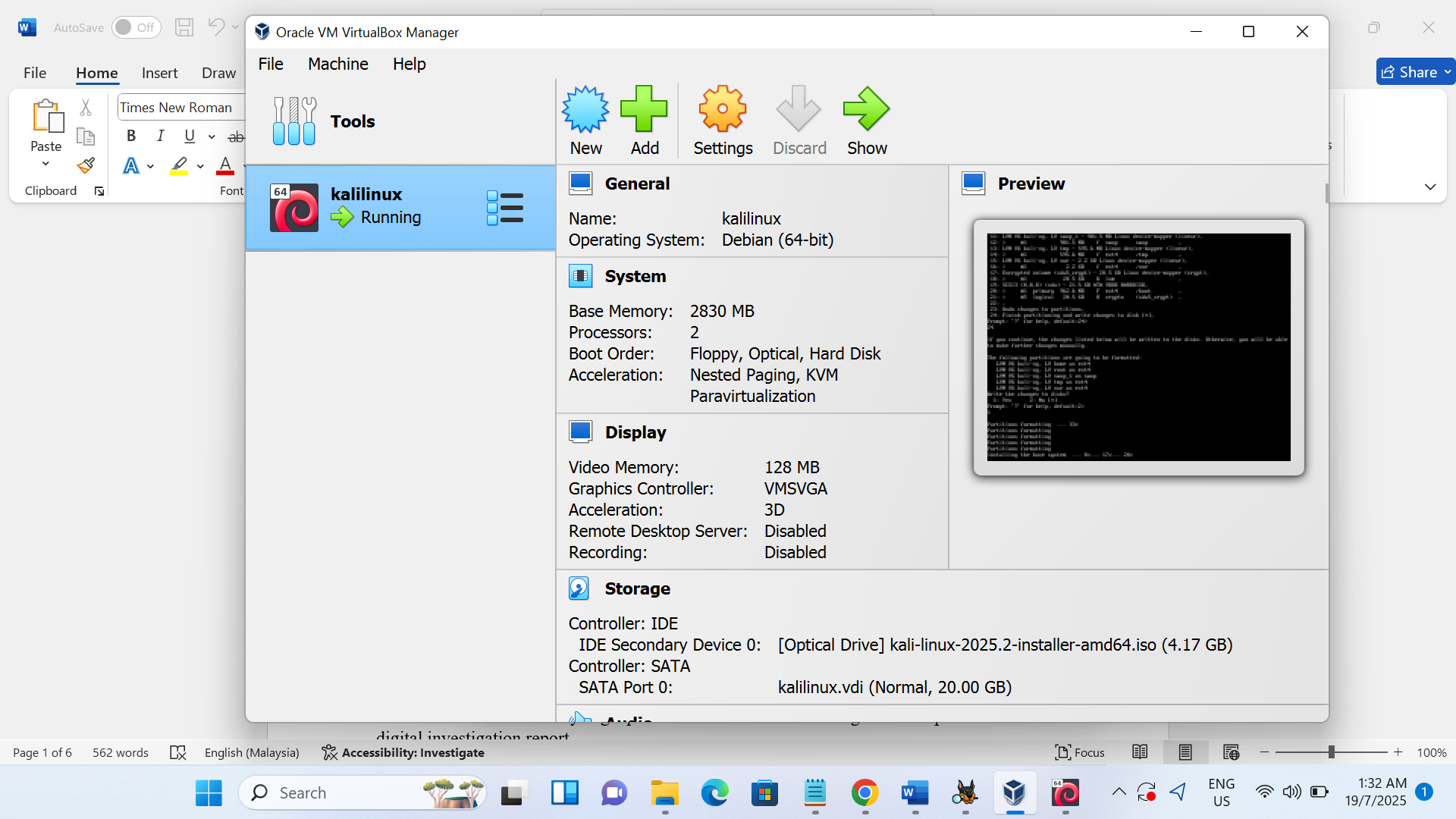


Figure 3 (command prompt)



**Recommendation and Request if possible**

I would like to request or ask the if anyone can assist with this issue during the mentorship class, as really would like to have the solution as a learning cove if possible.

**Task 2 Objective:**

The task 2 is aimed at analysing a provided Android forensic image and compile a formal digital investigation report.

Specific Tools used for the Android forensic investigation

* 1 Autopsy
* 2 7Zip
* 3 https://github.com/Akobe-Ajibolu/Android\_Image

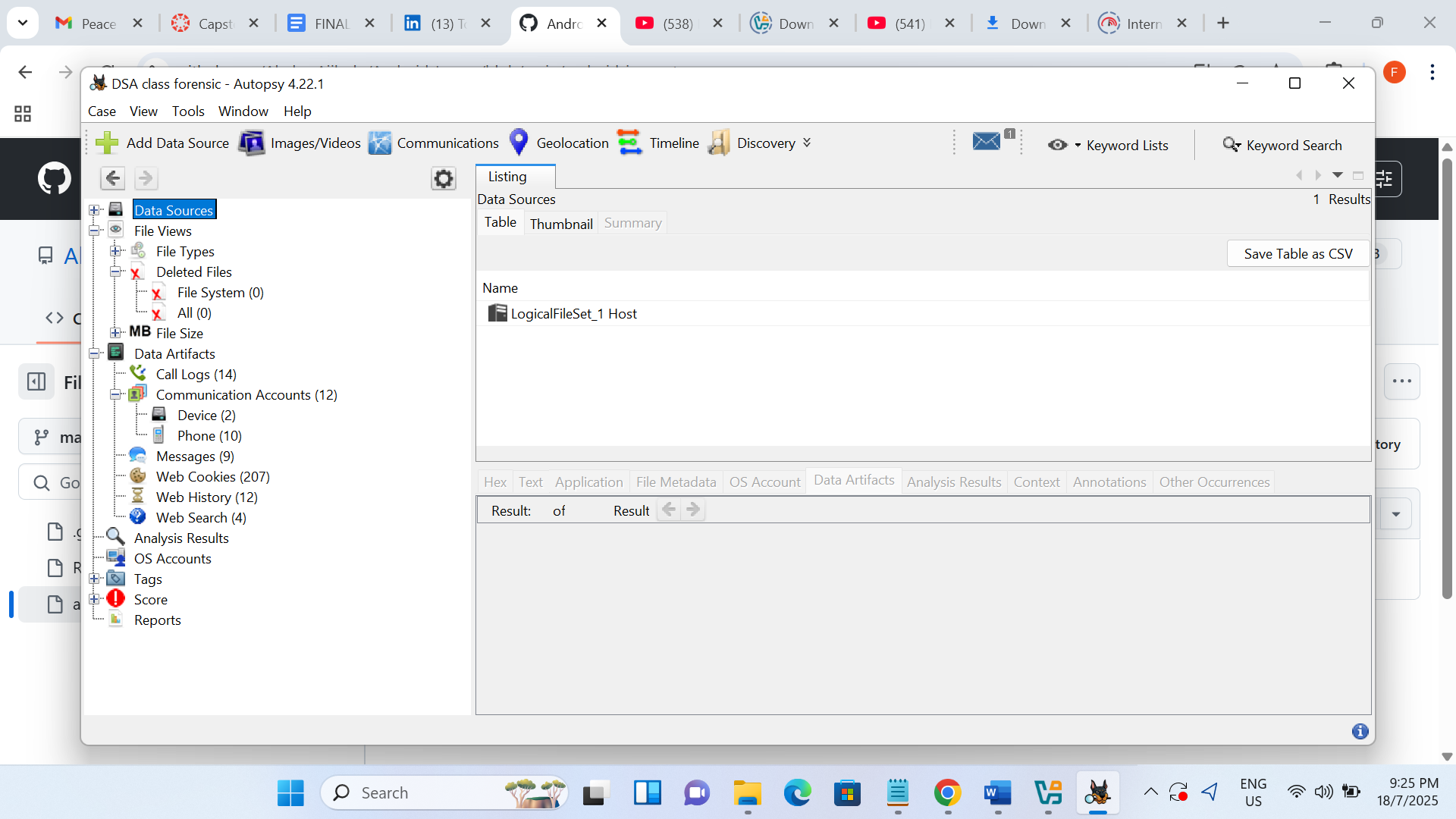
**Autopsy** is an end-end open-source digital forensic platform. It is used in different field like the police force, law, for commercial investigation etc. it can be beneficial for personal use with respect to investigation reports.

**7Zip** is a tool that is used to compress and decompress files. It is a tool that enables users to create compress files into smaller archives which are extracted from existing archive or folders.

The Android Image is was provided as the case study for the project, made available via github.com/Akobe-Ajibolu/.

The below screen shot shows the dashboard after installation and configuration of Autopsy.

Figure 1 (Autopsy page)

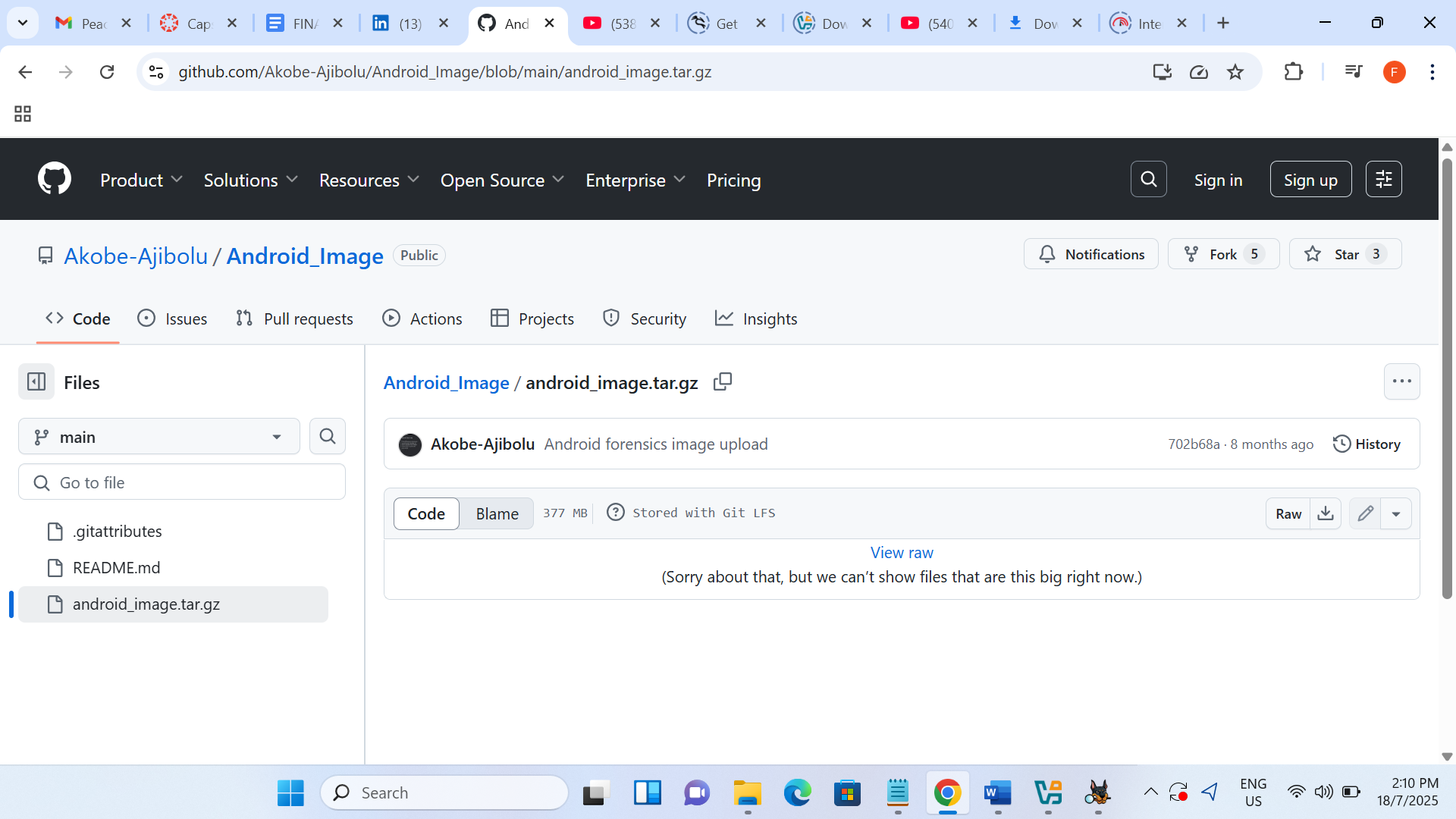


Conduct forensic analysis of the Android image:

**Extract and document:**

The files were downloaded from the Android image provided by lecture Akobe-Ajibolu github.com account as displayed in the below screen shot. After the download 7zip tool was used to Extract the files from the Android image folder.

Figure 2 (github.com(Akobe)



**SMS messages, call logs, contact lists**

The SMS messages with the screen shot below shows a sms message that is not ethical as their intentions looks suspicious, which can be further investigated. For example, (he/she was making it know that he have a new Scam idea that is he want to share or discuss,

figure 3 SMS Messages (Request to Discuss about it)

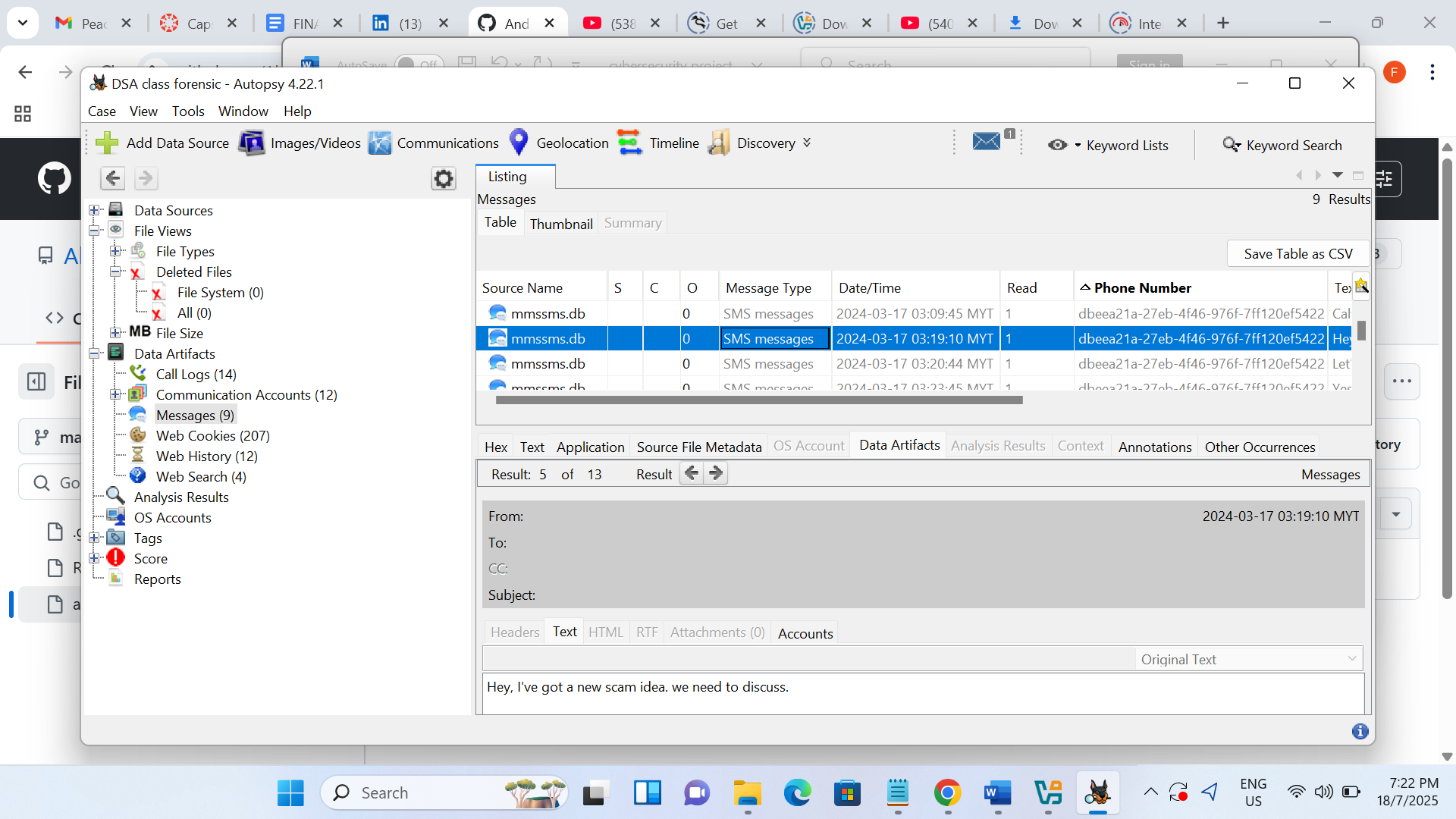


figure 4 SMS (Create a fake investment website to lure people)

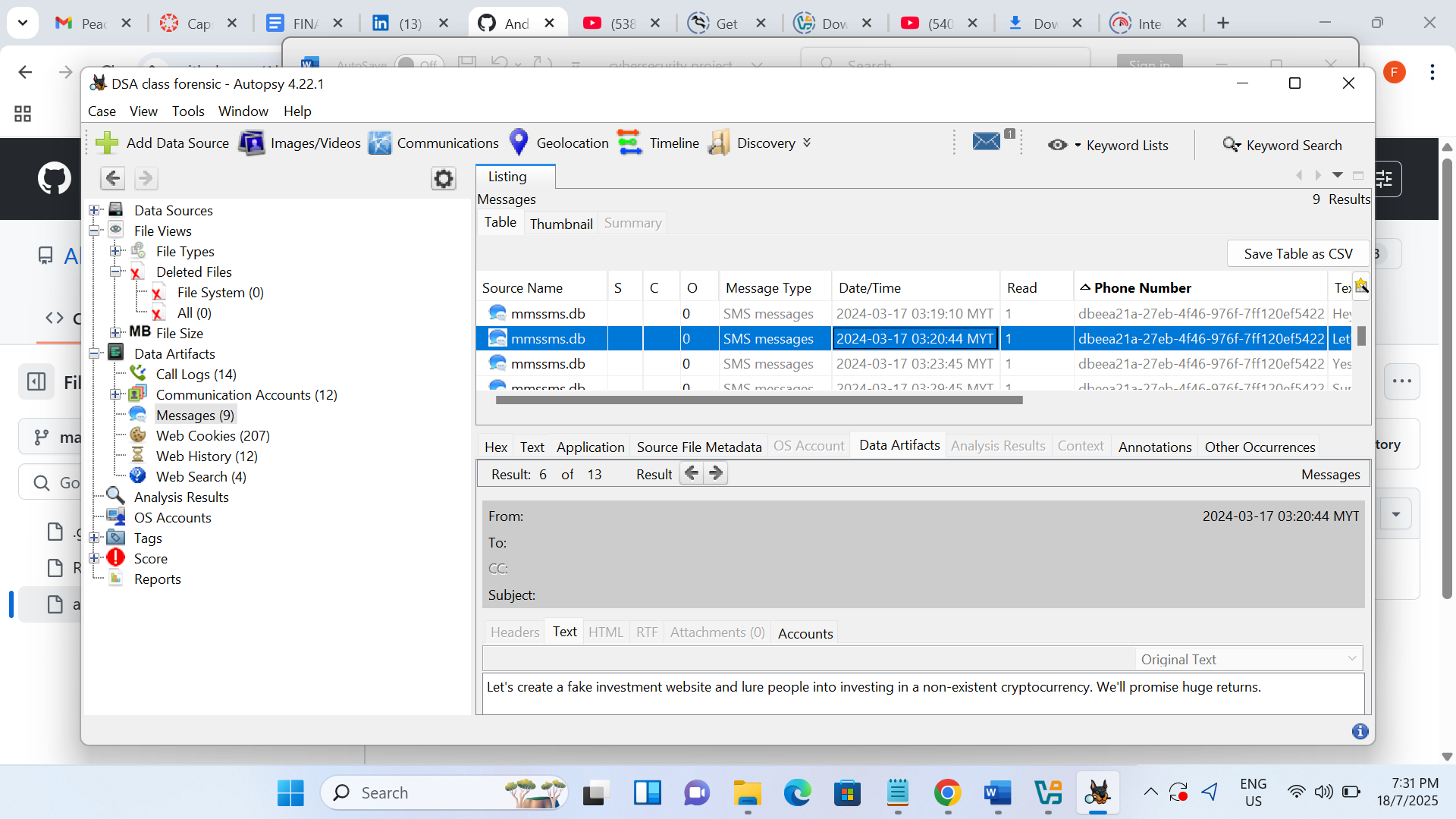
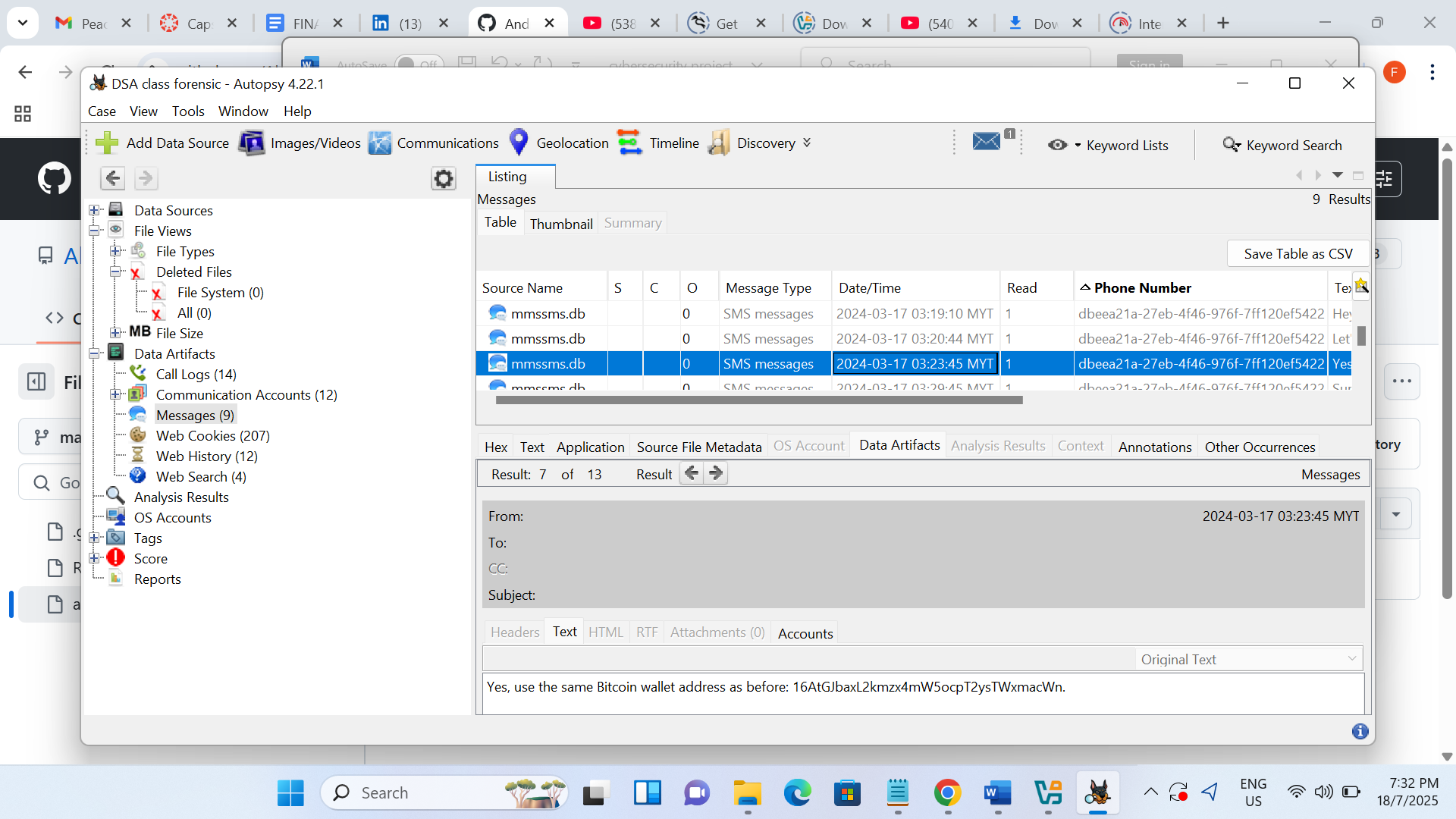


Figure 5 SMS (Using the same Bitcoin)



Call Log 14

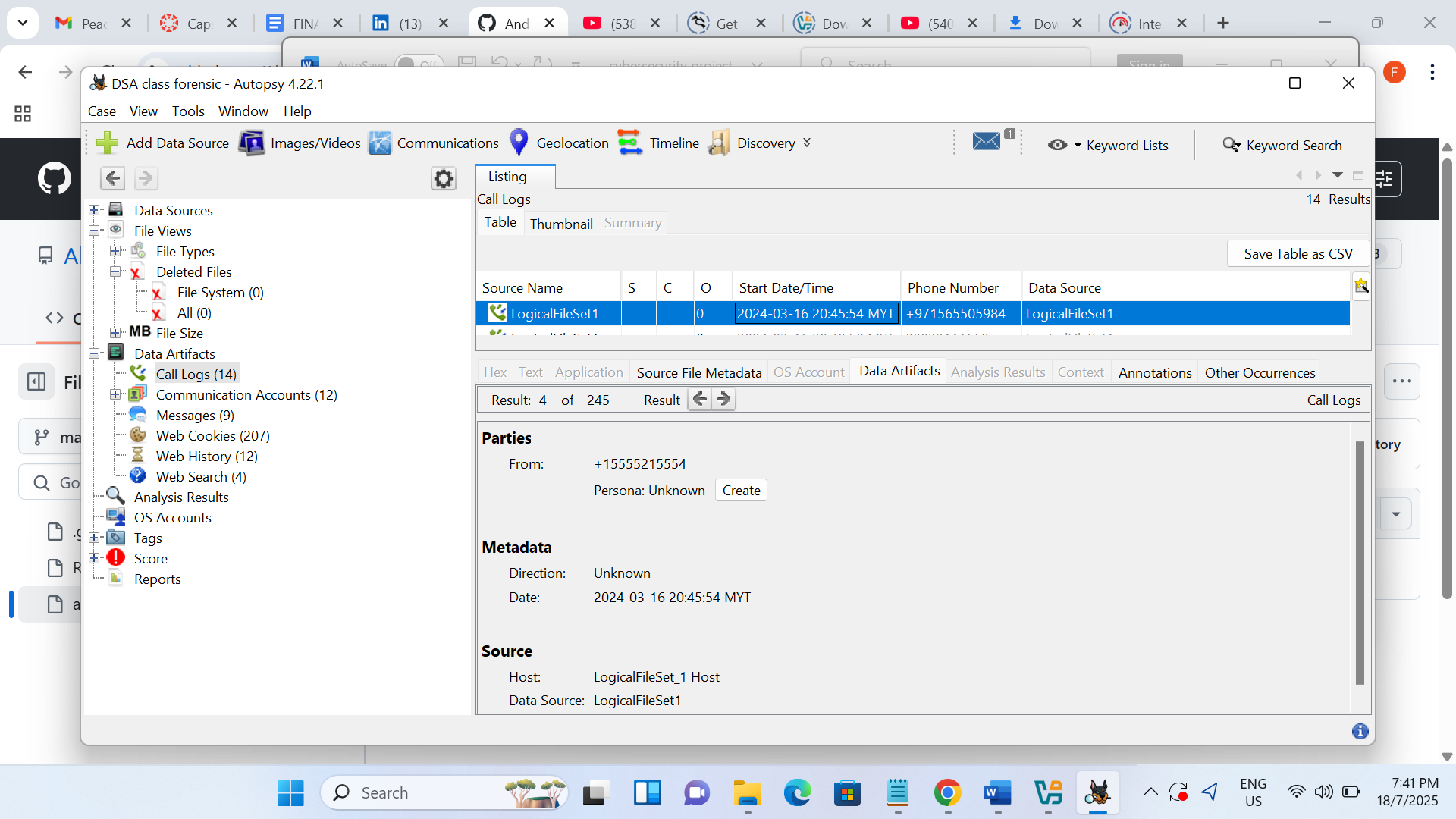
The call log is 14, however, the focus will be on the screen shot below with the information provided. As shown the start

Date and time (2024-03=16 20:45:54 MYT,)

Phone (+971565505985)

Data Source (Logicalfileset)

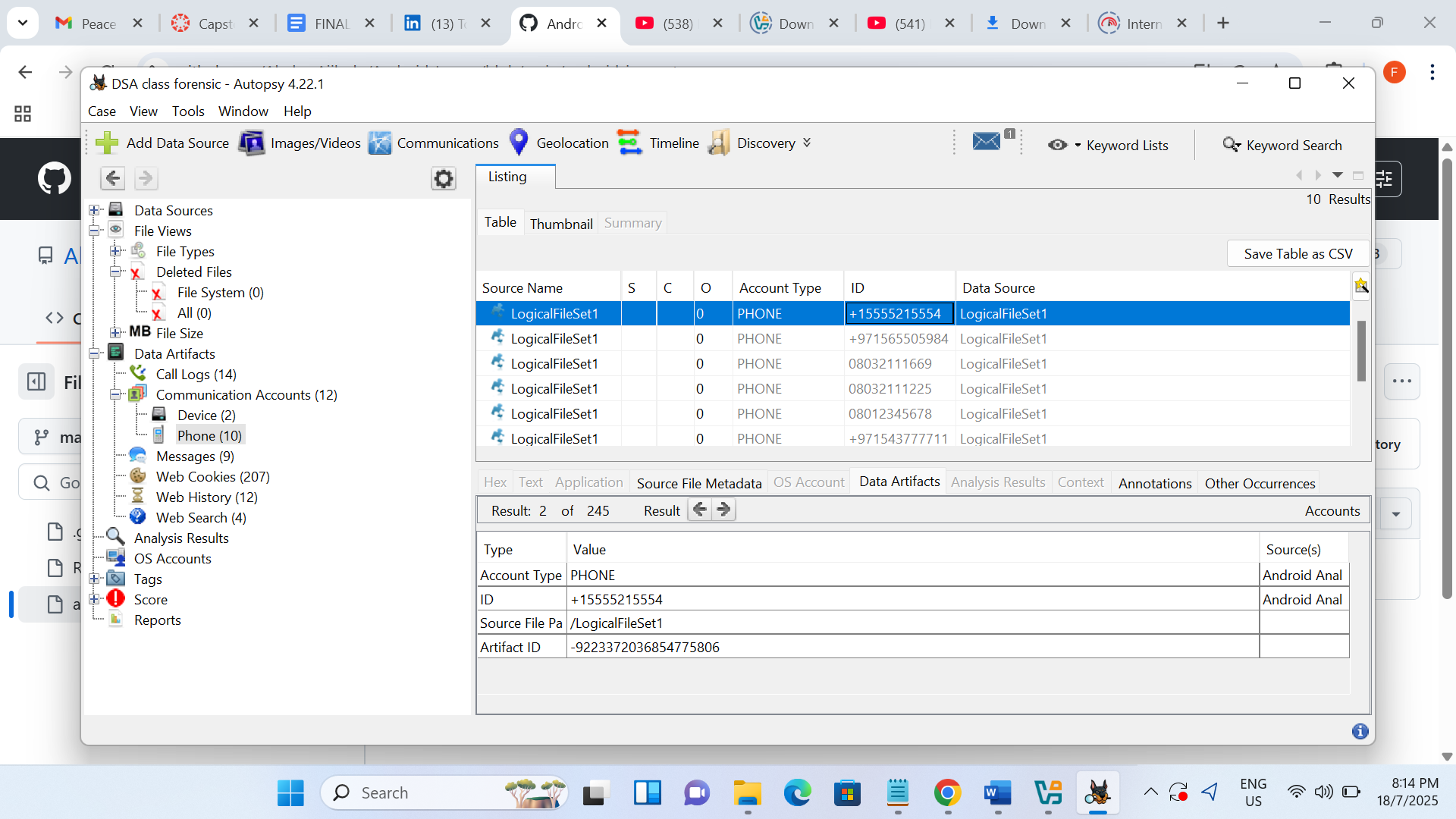
Figure 6 (Call log )



Contact List

The Contact list as shown below, contains the phone ID (numbers) and data source, it also shows the Actifact ID (-9223372036854775806)

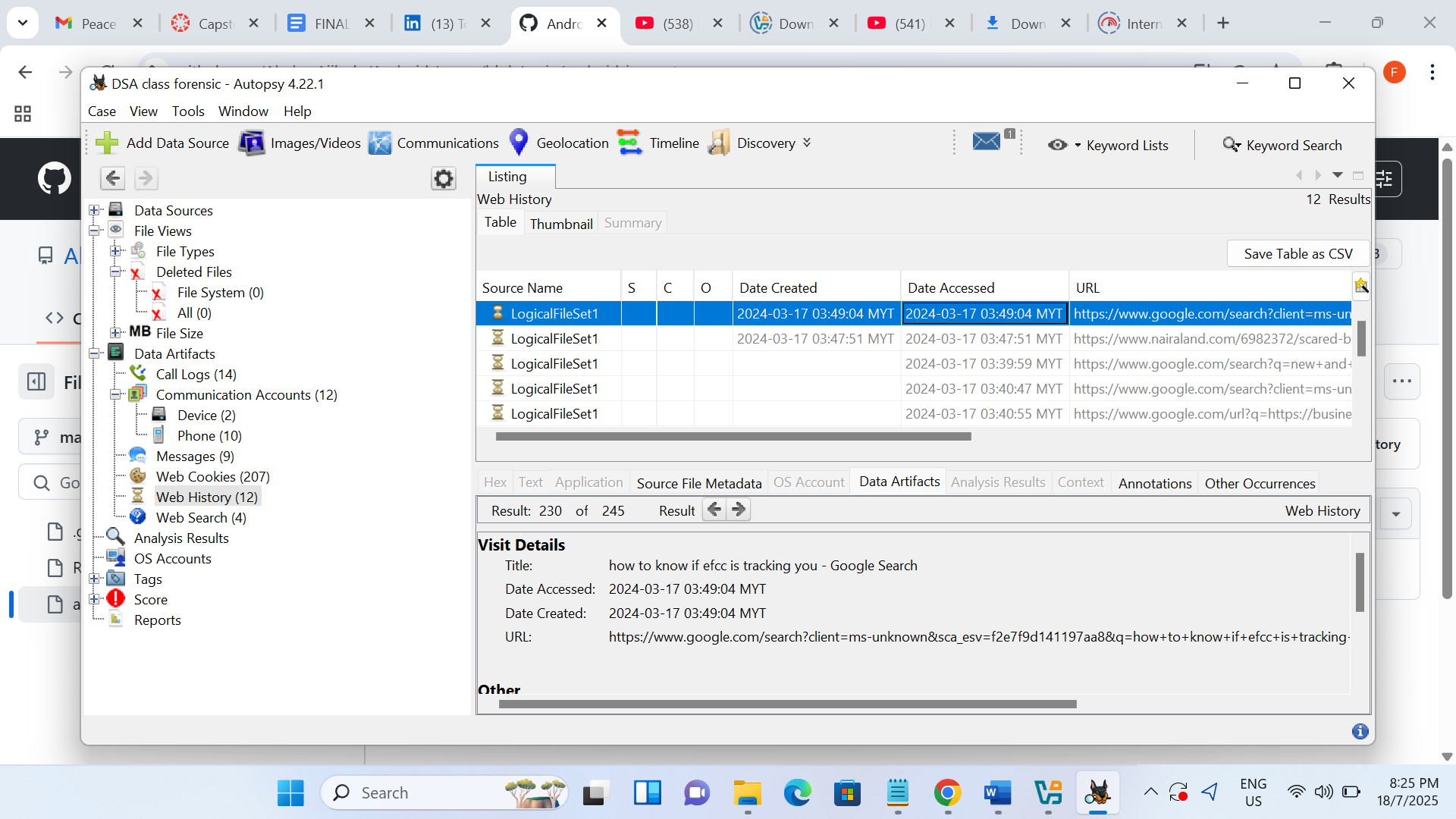
Figure 7 (Contact list)



Application usage history

the screen shot below shows the visit detail, that includes title, for example (how to know if EFCC is tracking you – Google Search), date Accessed, date created and the URL. It also contains the source, like the host, data source and file

figure 6 (history)



**Methodology and tools used**

The forensic analysis was carried out with the information provided from the Android Image as the case study for the analysis. One of the methods used was the extraction of the file from the folder using 7zip as the tool used and Autopsy as the main tool for the analysis.

**Conclusion**

In conclusion, the primary aim of this project is understood and know how the various tools can be used for forensic investigation that will lead to expectation. However, it should be known that some information which maybe vital to the investigation main be missing or not able to access due to human and machine factors.