**Pentest Report conducted on malware analysis on a network using wireshark.**

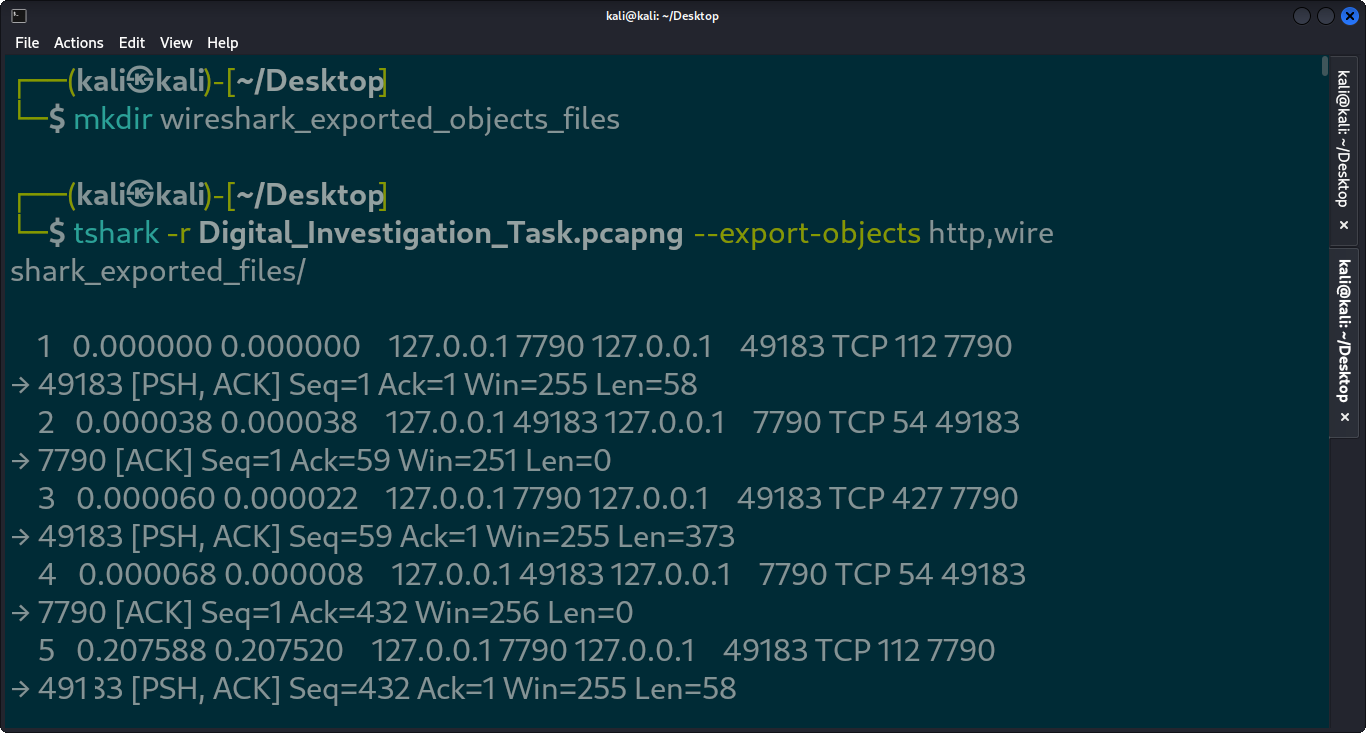
This report contains various malware analysis conducted on a network using the pcap file **“Digital\_Investigation\_Task”** that contained the malware.

The analysis was performed using the wireshark tool to identify and extract certain network packets that had been affected by the malware.

The following step by step procedures has been explained into details showing how each process was carried out using different tools specifically for extracting the images and the files that contained the malware. Tools like tshark and foremost was used to compare the results of how each of the extracted objects look like.

First, I used a command line tool that comes installed with wireshark called **tshark**. Tshark is a command line tool that functions just like that of wireshark and it’s intended purpose to capture and analyze network traffic in real-time or from saved capture files. The tool aided me to export objects using the http protocol and creating a directory to store them into.

The screenshot below shows how it was done.



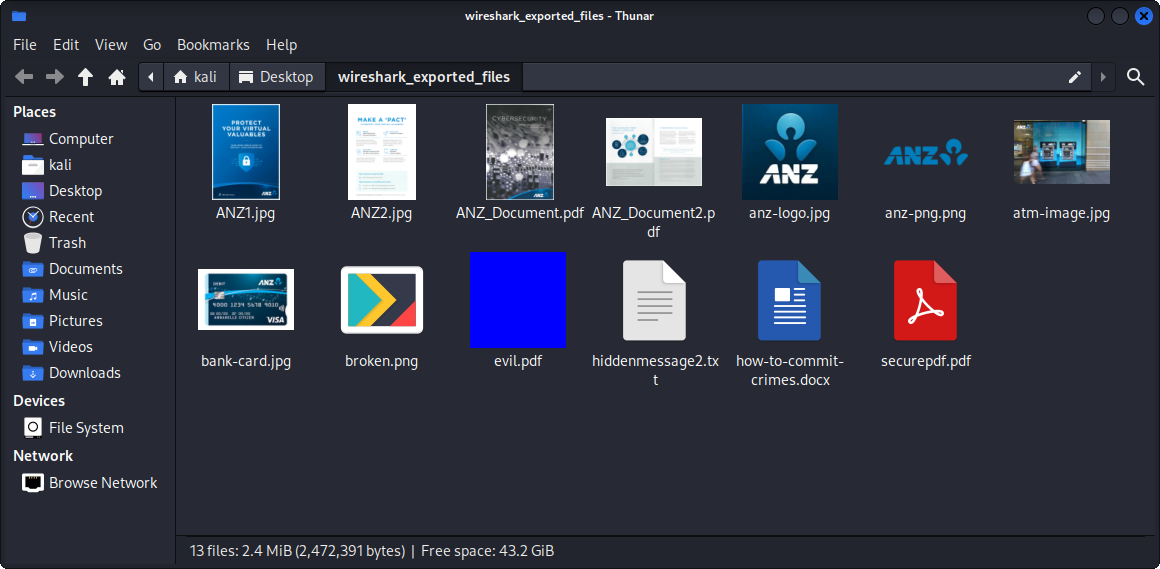
Image\_1.png

The screenshot below shows the directory created:



Image\_2.png

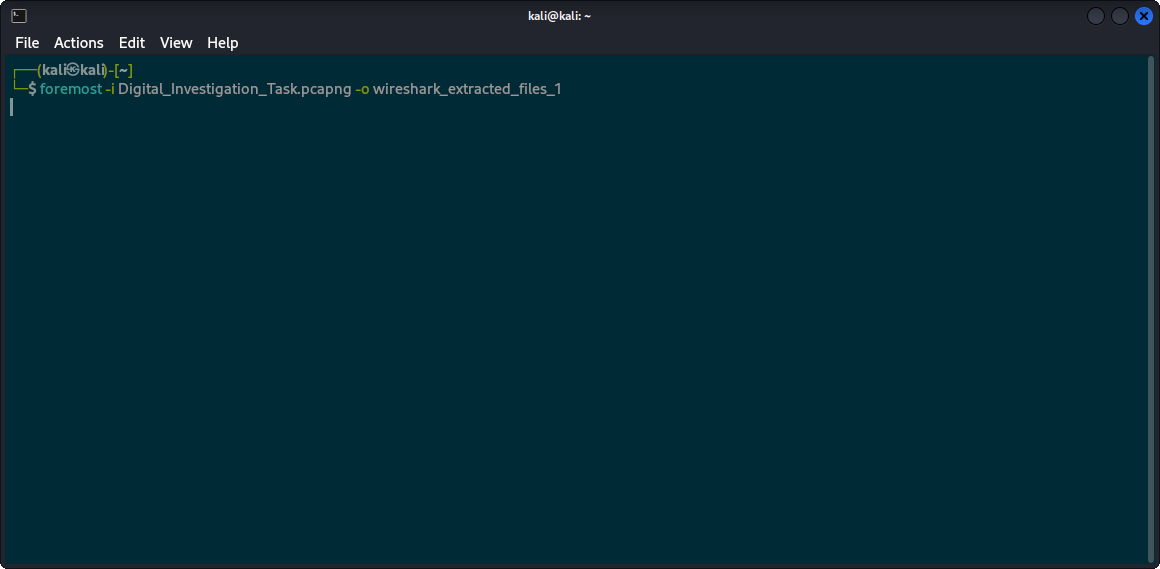
When you open the directory you should see the exported images in them just like the image shown below:



Image\_3.png

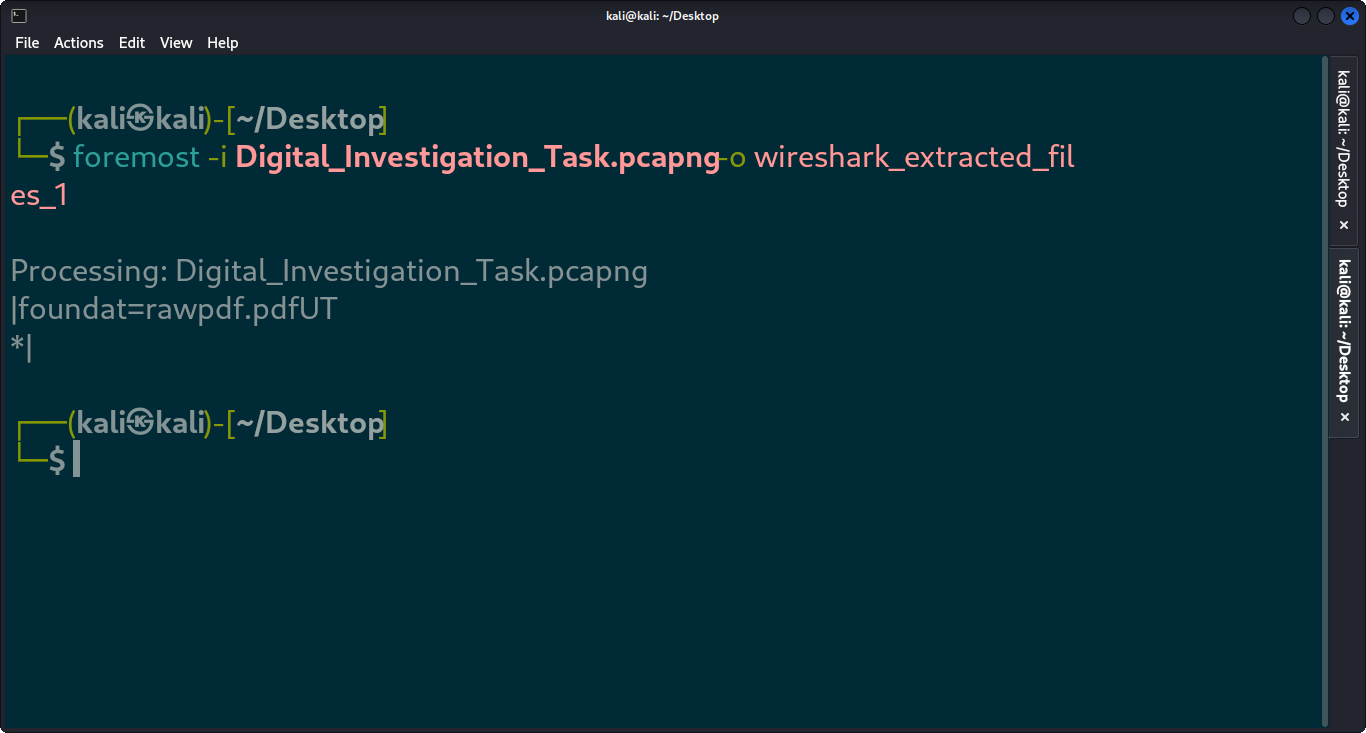
Moreover, to further analyze the pcap file to see if I had indeed extracted all the objects that contained the malware, I then used the tool called **foremost.** This tool is one that is use to extract files of any extension along with images of any kind. To use this tool, you must first install it on your terminal using **“sudo apt install foremost”** to get it installed. Hint: Before you do install it endeavor to update and upgrade your kali system before you go ahead with the installation.

Below is how you can use the tool to extract the objects to a folder:



Image\_4.png

This image tells us that the objects has been successfully been extracted to the specified folder:



Image\_5.png

The image below shows the folder or directory was successfully created:



Image\_6.png

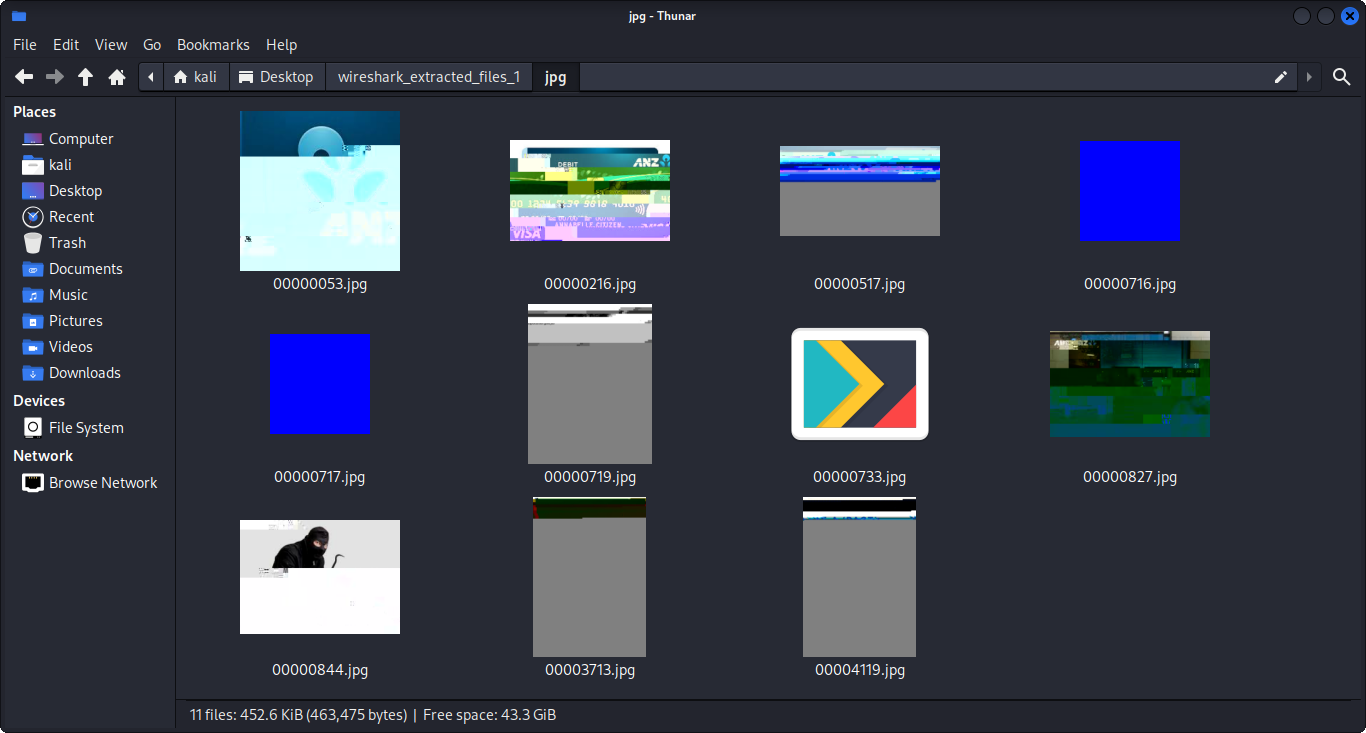
When you open the folder, you should see three sub folders or directories created in the created folder. The three directories include **jpg, pdf, zip** and a separate text file named **“audit.txt”.**  The image below should give you a better view of the explanation above:



Image\_7.png

After successfully creating the folder using the tool, I then went through each of the folders thoroughly to see if I had missed any of the objects ie: files that contained the malware. I first started by opening the **jpg** directory to check if there had been addition files added to it.

The image below shows what images had been added to the **jpg** folder:



Image\_8.png

The image above shows that additional images has been added though look blurred or fabricated and this could mean some reasons:

First, it may certainly be that the packets that contained the image had been fabricated or not well composed before sending it as a payload to the user to access.

Second, the tool used to extract the objects is one that does not clearly extract the image to look good but rather make it look blurred when extracted. Hint: Although, the foremost tool is one you can use to extract all types of object files it does sometimes make these objects appear fabricated or look blurred when extracted.

The above reasons can be taking into consideration when performing such pen testing activities involving networks that has been hit by malware.

After carefully checking the jpg directory and verifying my investigation, I then went ahead to investigate the second folder which is pdf.

The image below shows the pdf contained in the pdf directory:

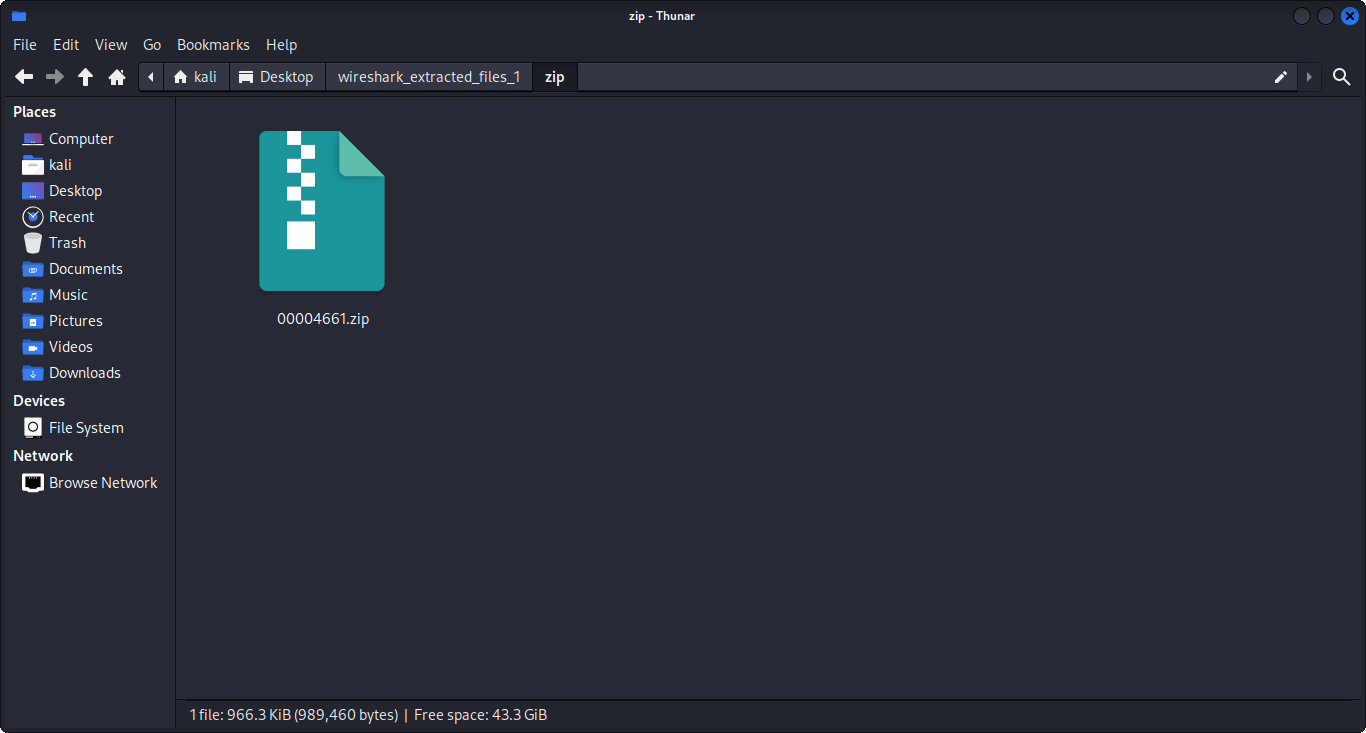


Image\_9.png

When I opened the folder, I only saw one pdf document instead of two as seen when we previously used the **tshark** tool which came with other pdf’s and along with various text files.

After confirming my investigation, I then proceeded to opening the last directory which is the zip directory to check if there was a zip file that also had a malware included in it.

The image below shows what is inside the zip directory:



Image\_10.png

After a successful investigation, I then proceeded to further investigate to check if genuinely I have extracted the object files.

By doing this, I then used the **wireshark** tool to do a thorough investigation to check if I had missed out any objects that needed to be extracted and had contained or included a malware in it.

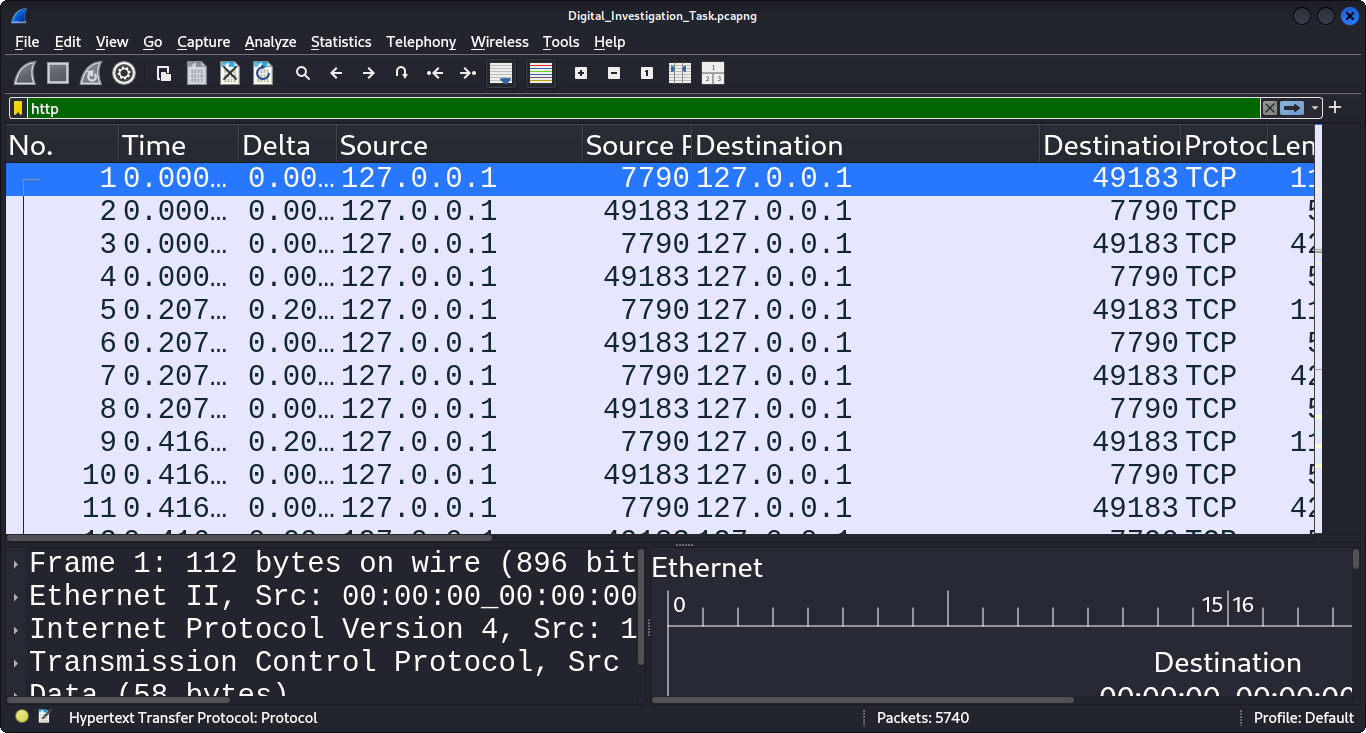
In addition, the investigation was to aid me to confirm if truly both tools used previously which are **tshark** and **foremost** gave me the exact information I needed.

To conduct this analysis using **wireshark,** I first entered the protocol that was used by the attacker to simulate the attack on the user network. The protocol used to filter out the various objects that needed to be exported by **wireshark** was “http” protocol.

The Hypertext protocol (http) is one that is used to host various web pages and other files and folders on the web for users to access. This protocol is one that is unsecured and as such it is advised that one should not intend to use it for any communication means.

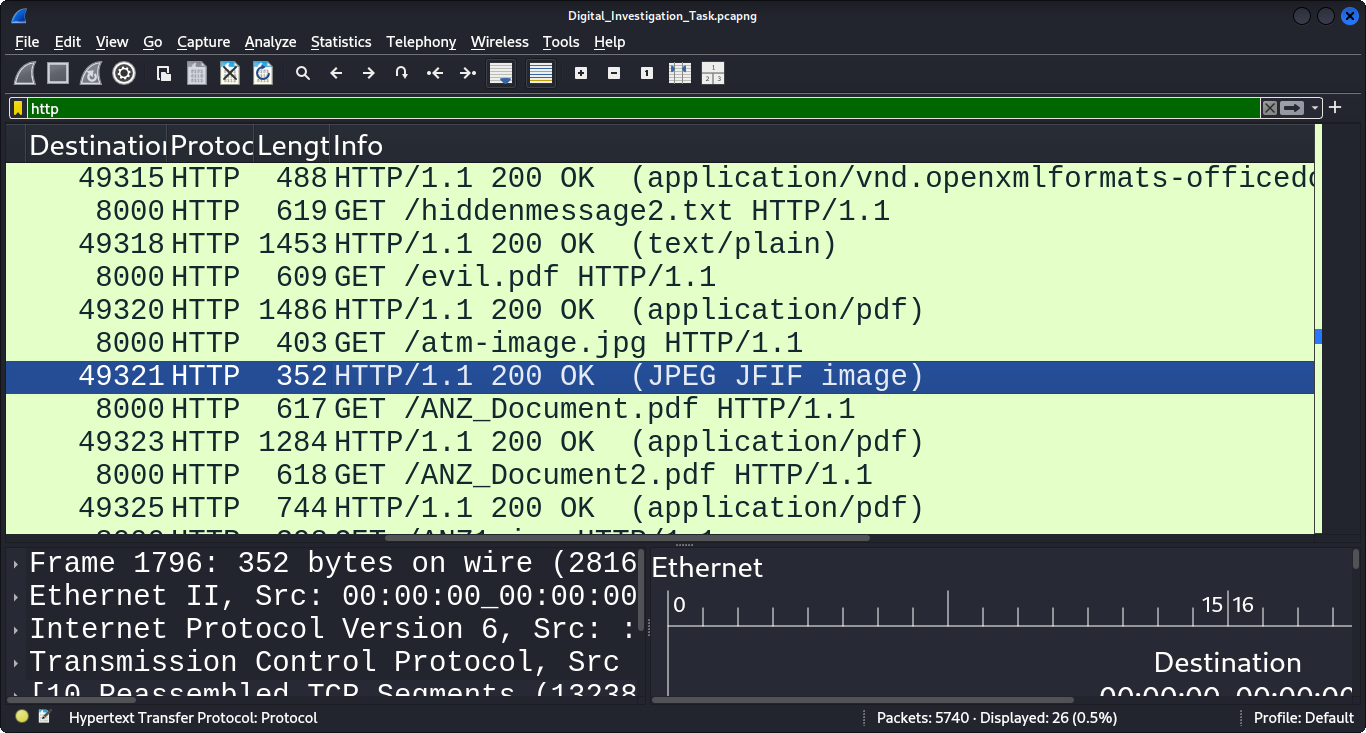
This protocol due to its nature of being unsecured, attackers usually prefer to use this protocol to simulate their attack on their target which is what the **pcap** file had included during the network capture.

The image below shows what the http protocol displays in the filter tab**:**



Image\_11.png

The second image below shows what was retrieved from user when it made its connection to the http protocol:

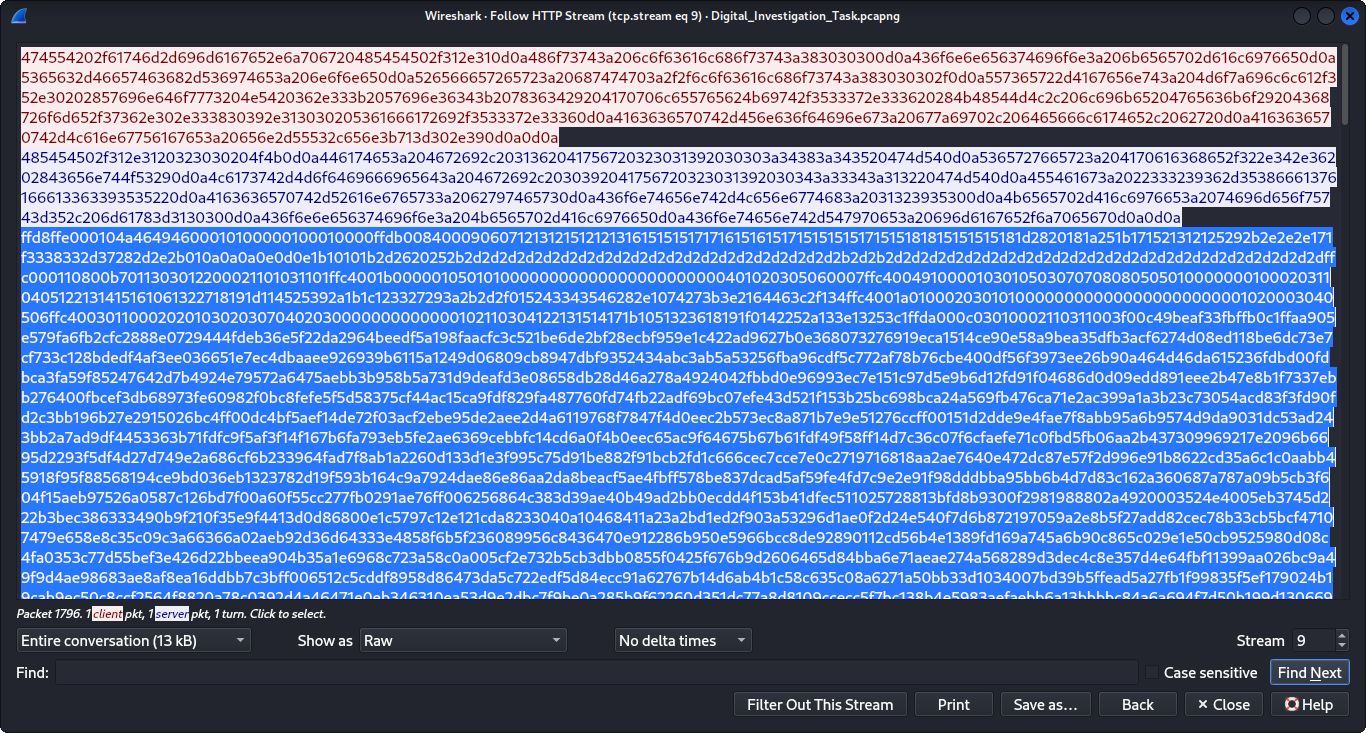


Image\_12.png

The results show that the user had accessed a jpeg file that was hosted on the http server.

In order to further perform the analysis, I clicked on the packet and clicked on an option called **follow** which gave me two sub options to choose from which are **“HTTP Stream and TCP Stream”.** Since I was dealing with http protocol I choose to follow the http stream.

The image below shows the raw format of the image file that the user had accessed that contained the malware:

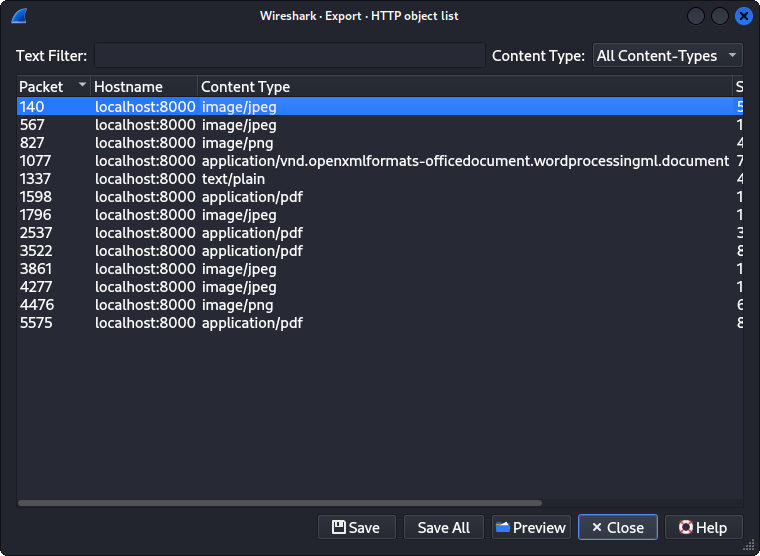


Image\_13.png

From the image shown above, the highlighted raw text shows the image that the user accessed. Usually, to an image has its raw value starting with **“ffd8”** as you can see from the highlighted text.

Successfully, after I had identified one file that the user had accessed, I then decided to export the object following this procedure: **File>Export Objects>HTTP** in **wireshark.**

The image below shows the output after clicking the HTTP option in the export objects option under the file option in **wireshark**.

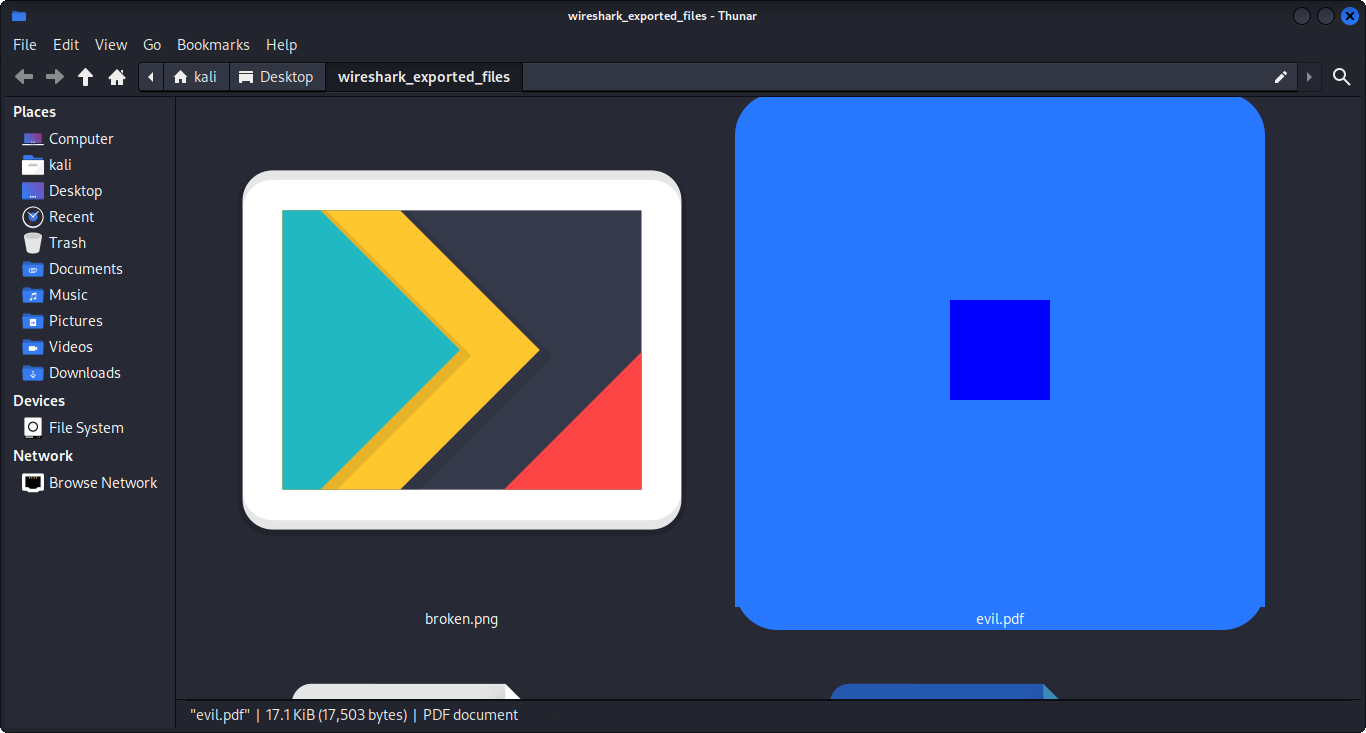


Image\_14.png

After exporting the objects, I am given various object files to export from my **wireshark** interface. After a successful investigation, the images appeared looked the same as compared to when we used the **tshark** tool to extract them on the command line.

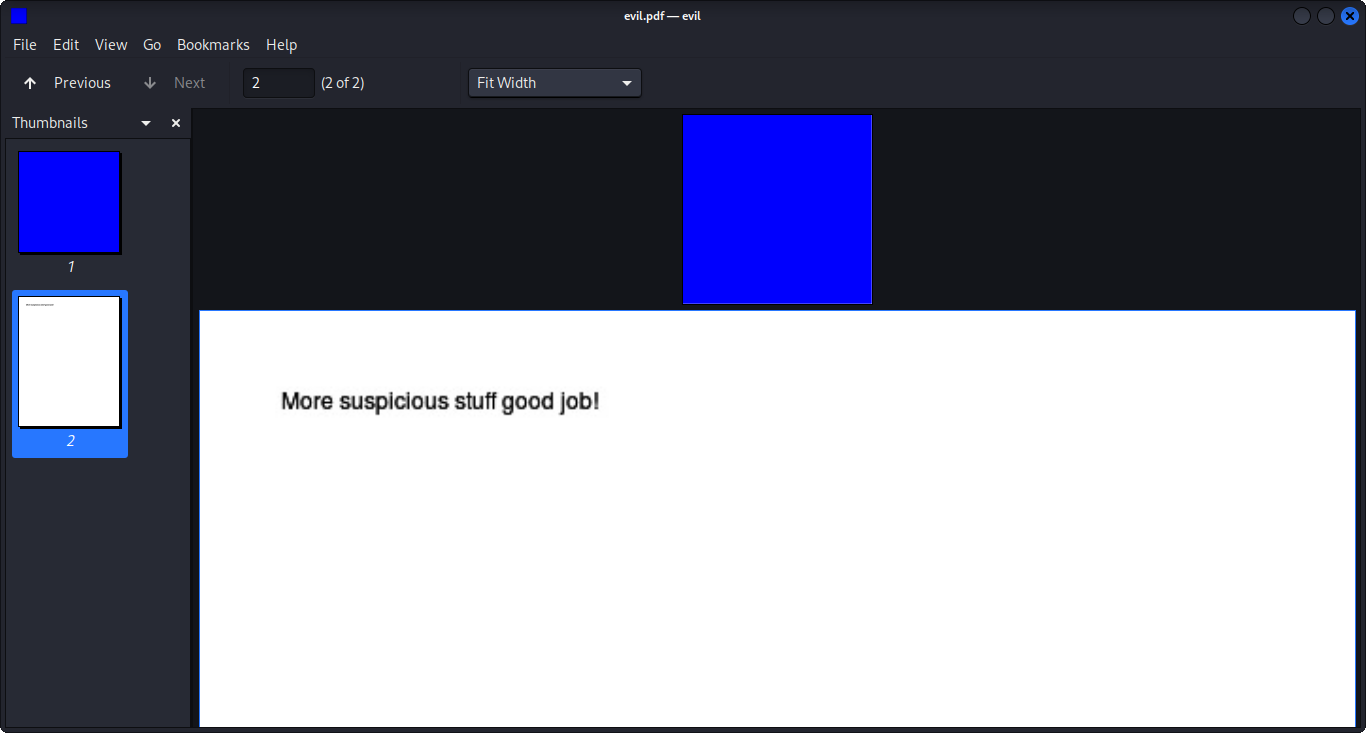
After successfully confirming my investigation, I then decided to view some of the text files and the pdfs that I had successfully exported to my folder.

The various images show the text files that I viewed to check what was contained in them:



Image\_15.png

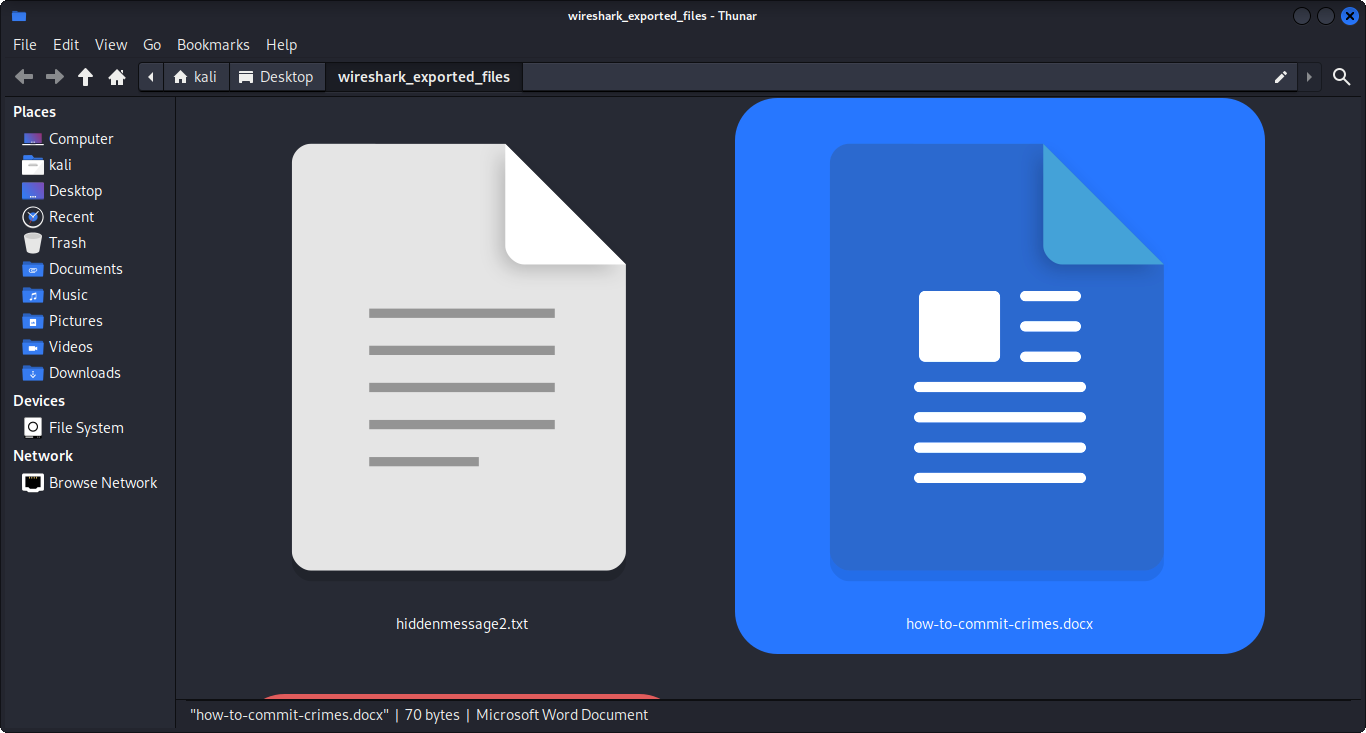
The image above shows one document I viewed.



Image\_16.png

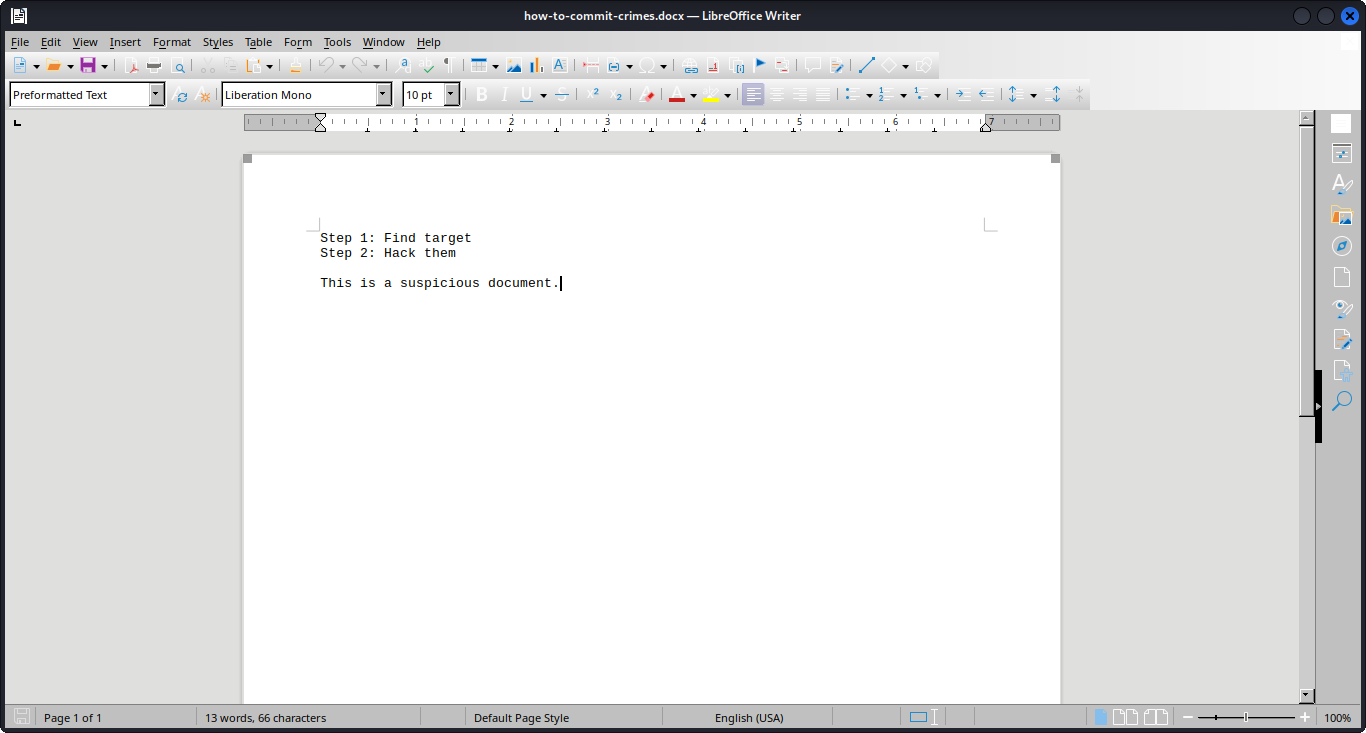
The above image shows what is contained in the pdf file.

The image below shows another file that I accessed to view what contained in it:



Image\_17.png

The image below shows what was contained in the text file when viewed:



Image\_18.png

Remediations to put in place when you encounter such attacks:

1. Always connect to web pages using secure protocols such as https instead of http.
2. Endeavour to take precaution when visiting sites that are not known or unknown.
3. Endeavour to use secure network protocols such SSL/TLS to ensure smooth delivery of messages.
4. Practice the habit of using secure passwords to help mitigate against such attacks.