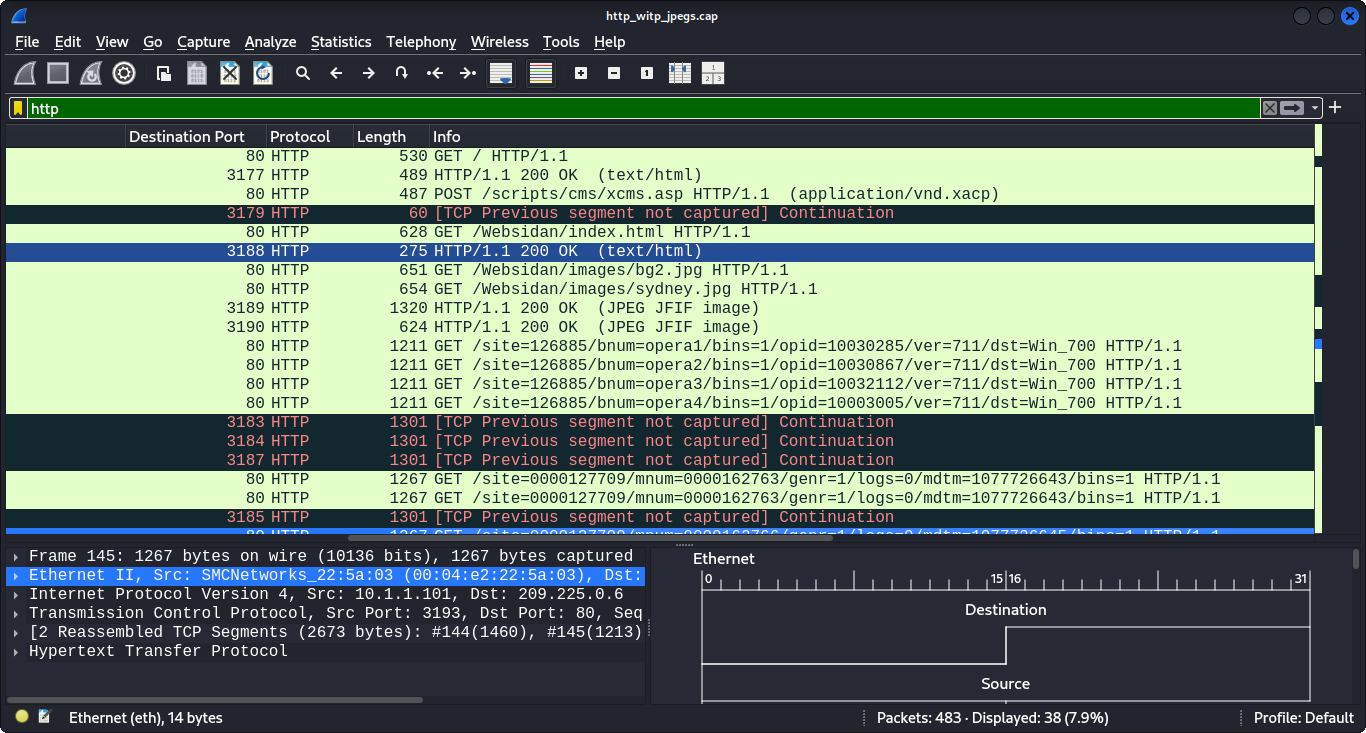
**Pentest Report on Network Analysis using wireshark**

Report on a pen testing activity conducted to extract files accessed through unsecured protocol on http

The activity was performed using tools such as wireshark and tshark which both of them are used to analyze and capture network traffic in real-time and offline too.

A pcap file which contained a list of networks captured packets was analyzed to retrieve information that a user had accessed through unsecured protocol.

The image below show’s wireshark tool in action being used to filter out the http connections that the user had made and what it had accessed through this protocol.



Image\_1.png

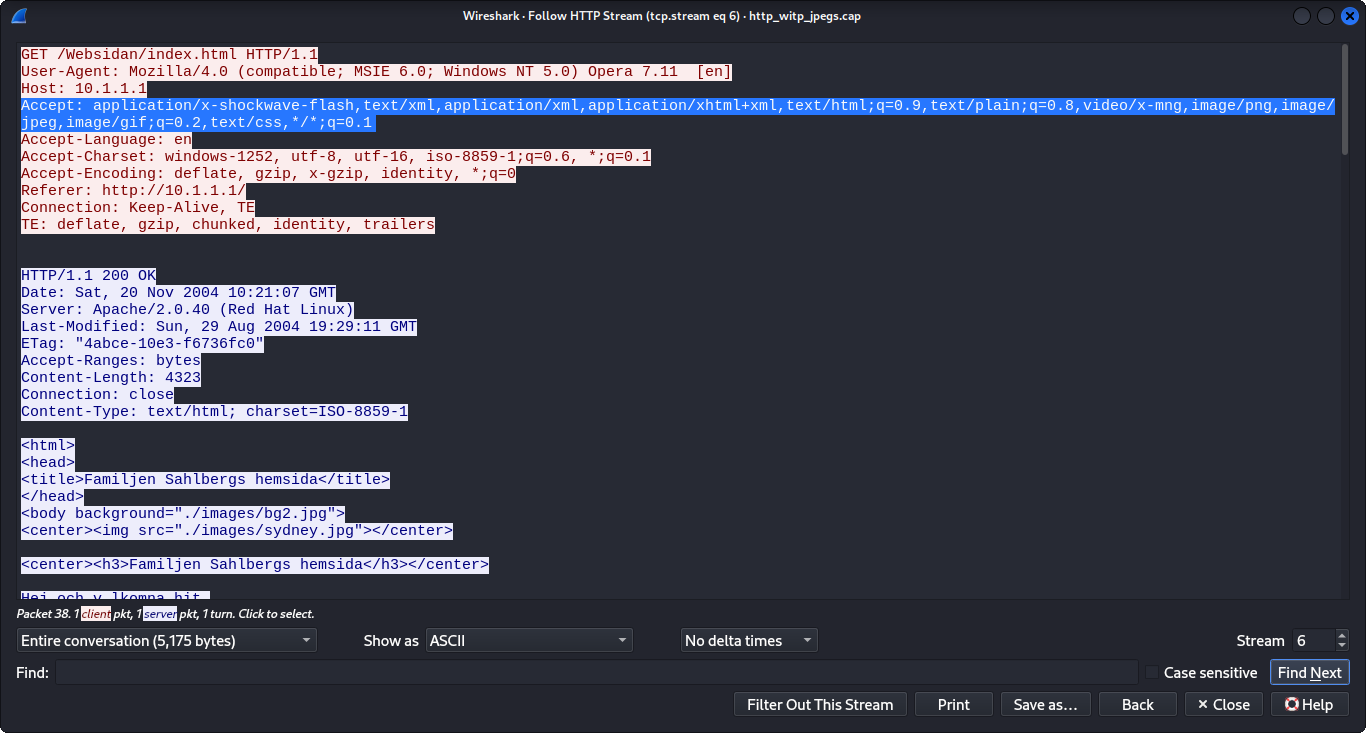
The image above signifies that the user had connected to an http server to access an html file.

Following further investigation, I analyzed the html file to see if indeed it was a legit one that used a well known IP address.

After careful investigation, I realized that the IP address was one that was used for server testing basis. The IP address started with **“10.1.1.1”** which contained image files on it for access by the user.

It is very common to see such IP address as most often it’s used within a company server to host several or some important user files or data.

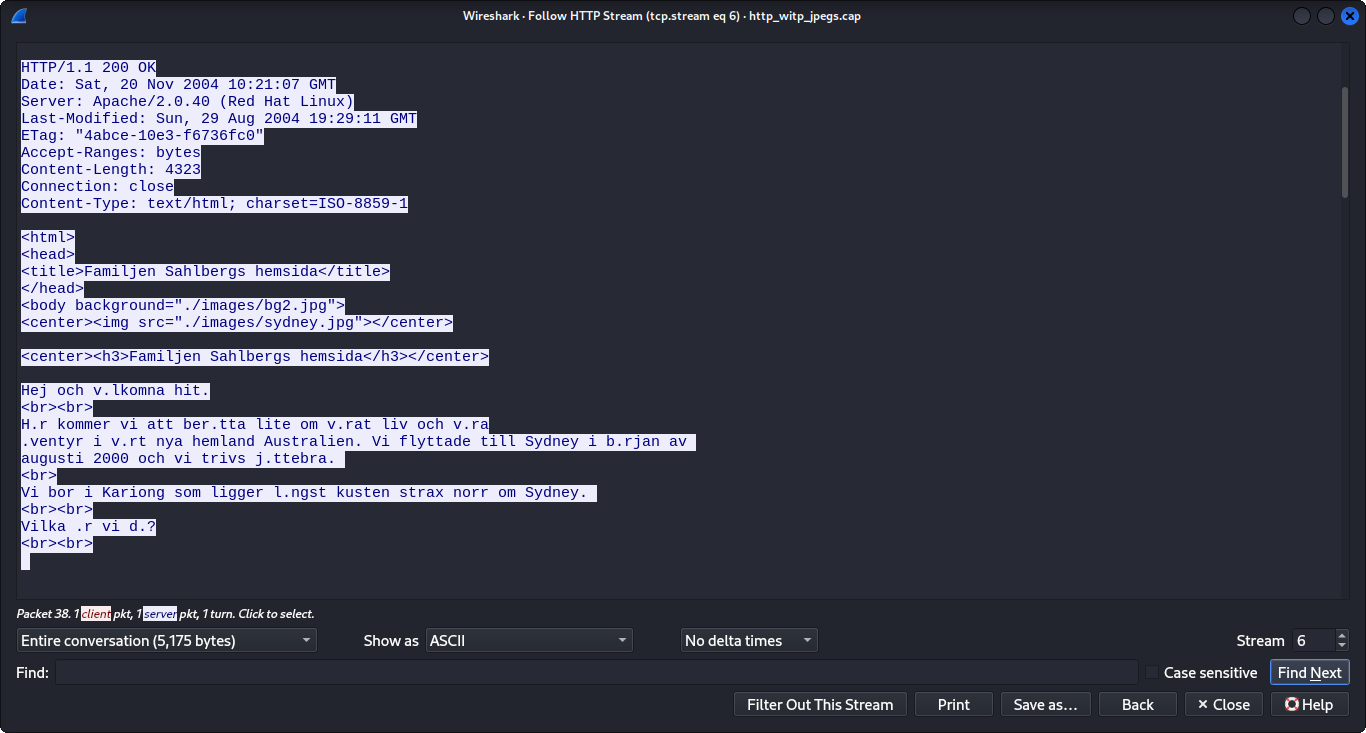
The image below shows what image was contained or found on the server:



Image\_2.png

The highlighted text shows what images was hosted on the server with the ip address as “10.1.1.1”.

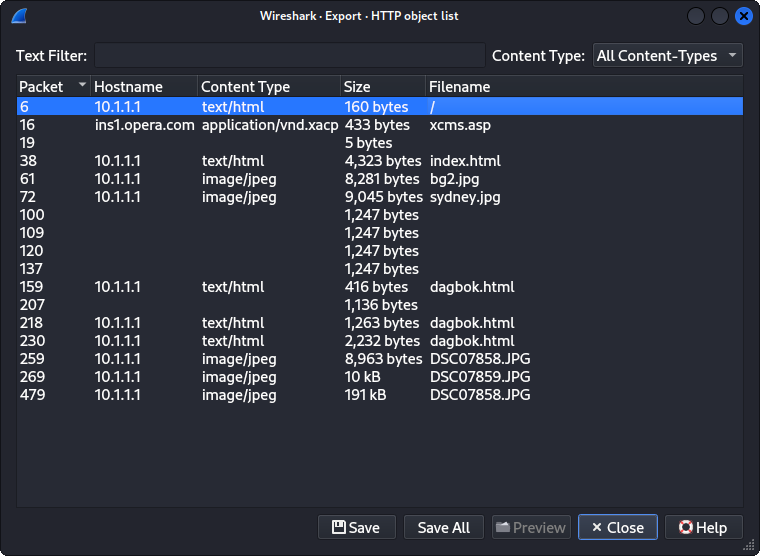
The second image of the second section of the http conversation is shown below:



Image\_3.png

Image three shows the conversation between the user and the server along with the html code that was contained on the server.

After carefully analyzing the html file I then exported it to a folder that was created using tshark on the command line. An image and explanation of how I used the tshark to export the objects to will be shown soon:



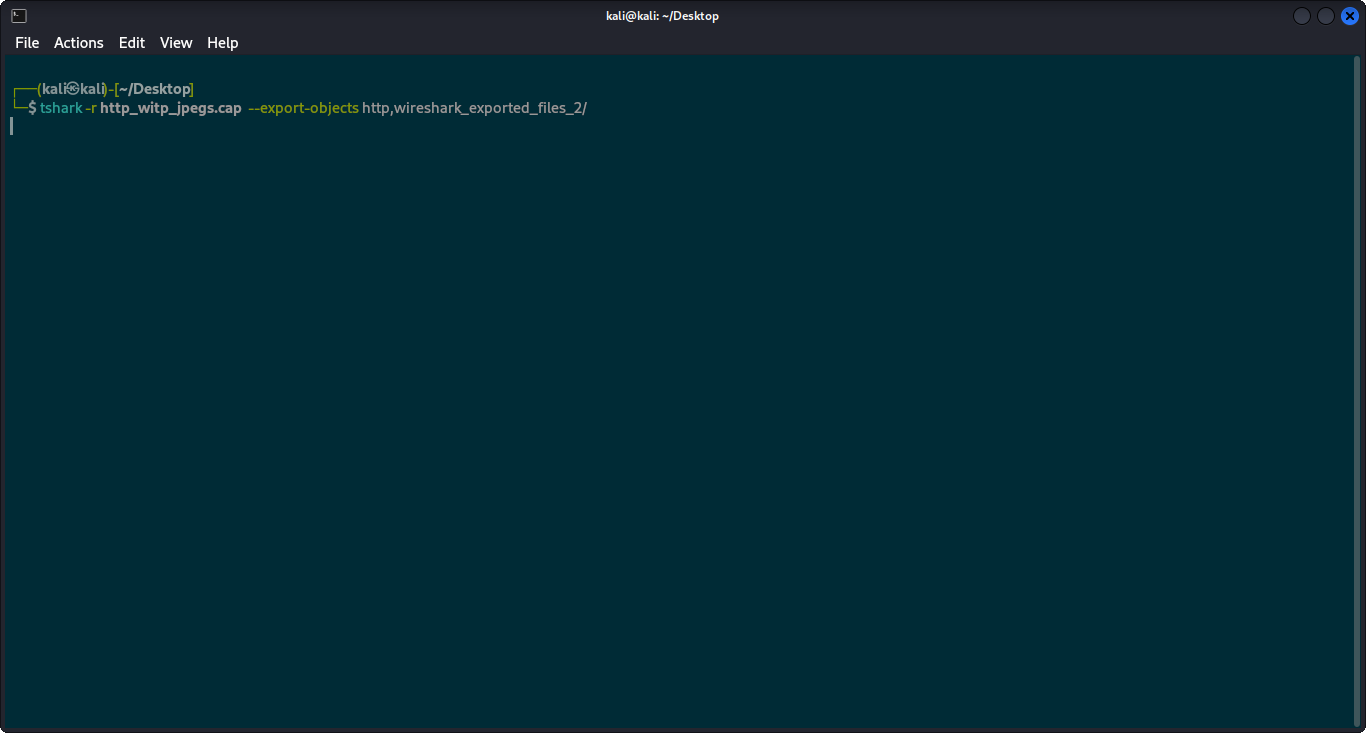
Image\_4.png

The image above shows the list of object files that the user had accessed and downloaded to the users machine.

A much simpler and easy way of extracting this object files was performed using the command line with a tool called tshark.

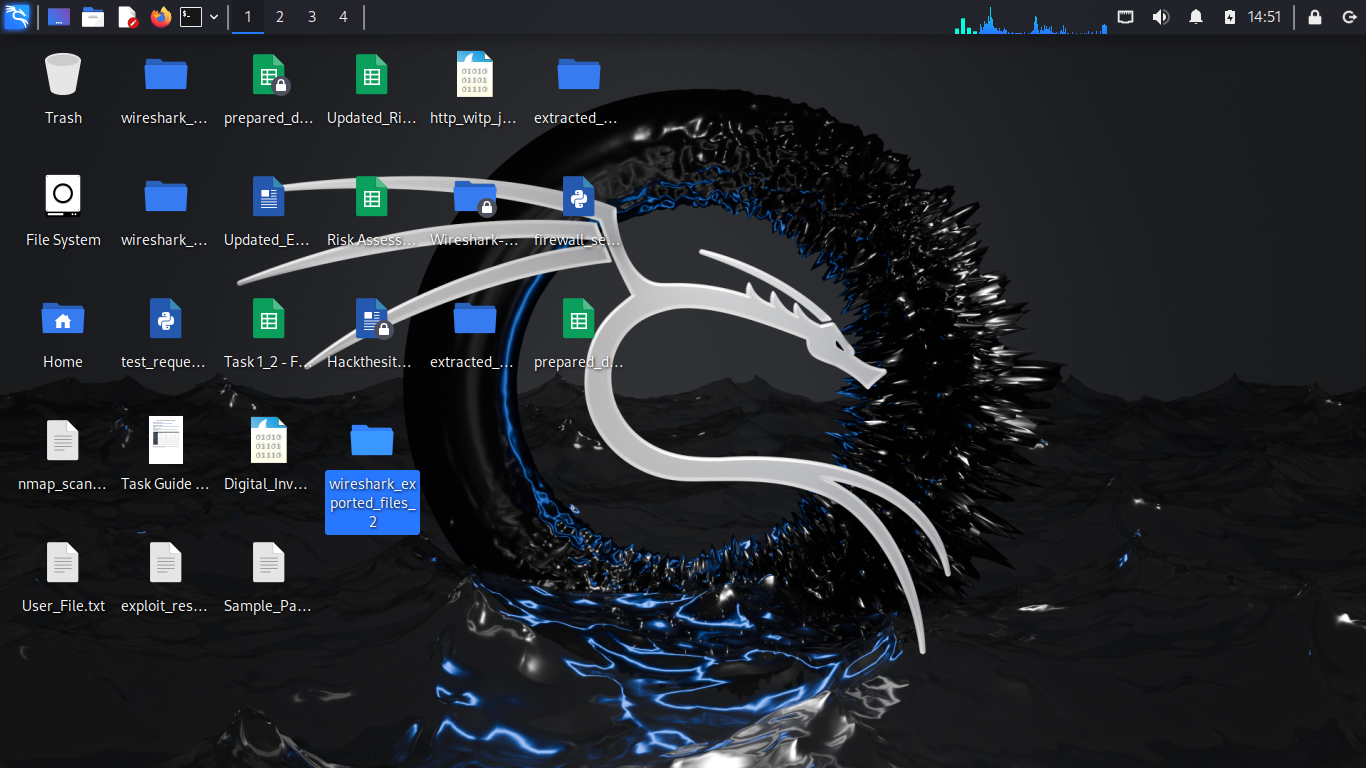
Although I could have extracted these files to a specified folder by clicking “Save All” but as a cybersecurity analyst you should be dynamic as to how you want to attain your results.

The image below shows how tshark was used to create a folder and export the objects in the pcap file called **“http\_wtp\_jpegs.cap”** .



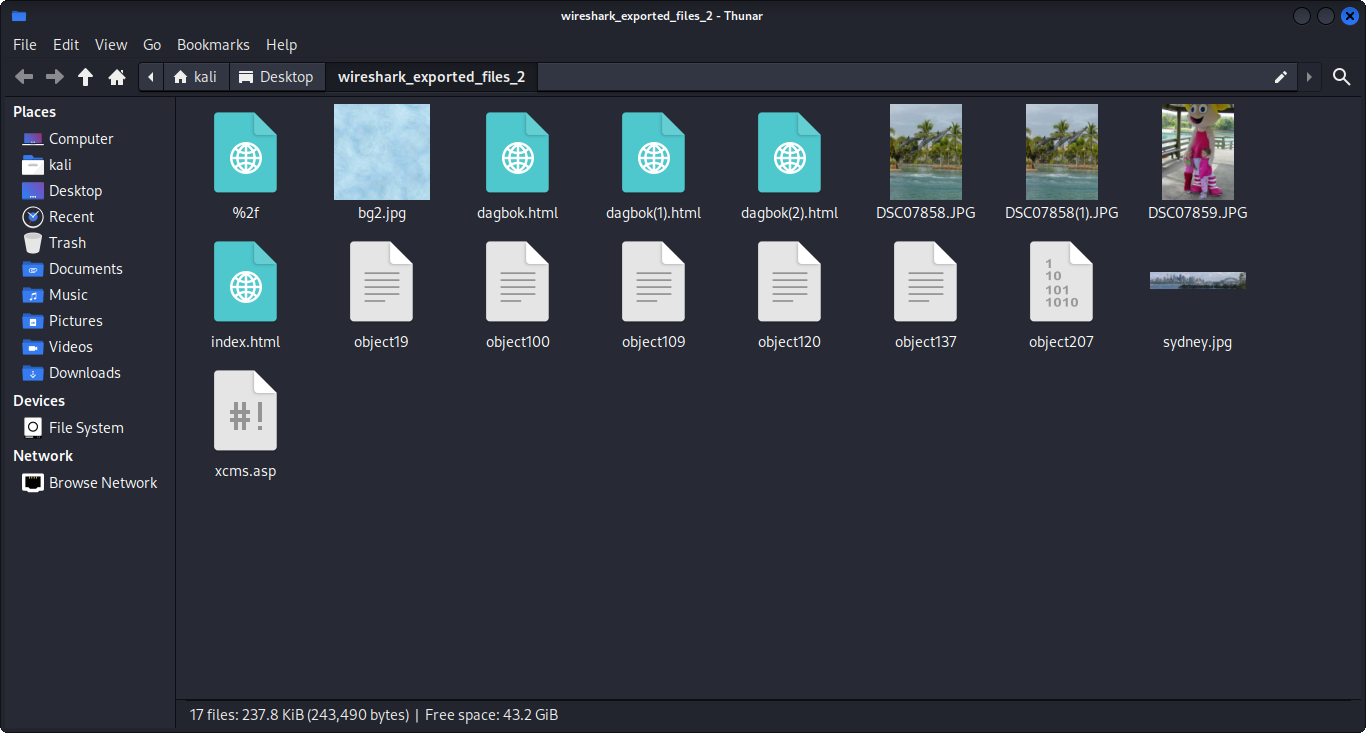
Image\_5.png

The below image shows the successful creation of the folder that was created using this command line tool.



Image\_6.png

The image below entails what files and images that are included after extracting the objects.



Image\_7.png

Successfully, I was able to export all the files and images that the user had accessed through the http protocol. A further analysis can be conducted to view the html views if you choose to.

Remediations:

1. Ensure to always connect to secure network protocols such as https
2. Use secure passwords to protect vital information on individual machine and servers like these included.
3. Always verify to check if you’ve made secure connections over a network when sending vital information. Such secure network protocols include SSL/TLS to help mitigate the dangers of man-in-the-middle attack where an attacker can view your message unknowingly.