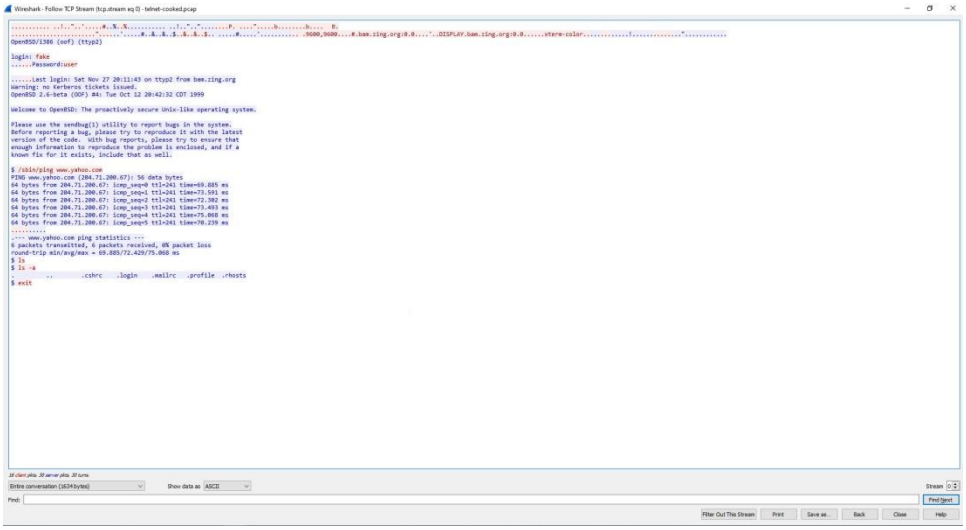
# OVERVIEW:

The purpose of this lab is to analyze capture files using network traffic analysis tools such as Wireshark and NetworkMiner. These tools provide insight into network activity by extracting valuable information, including logins, images, and other data. Through this process, we gain hands-on experience in utilizing these tools for effective packet analysis and data extraction.

# ANALYSIS:

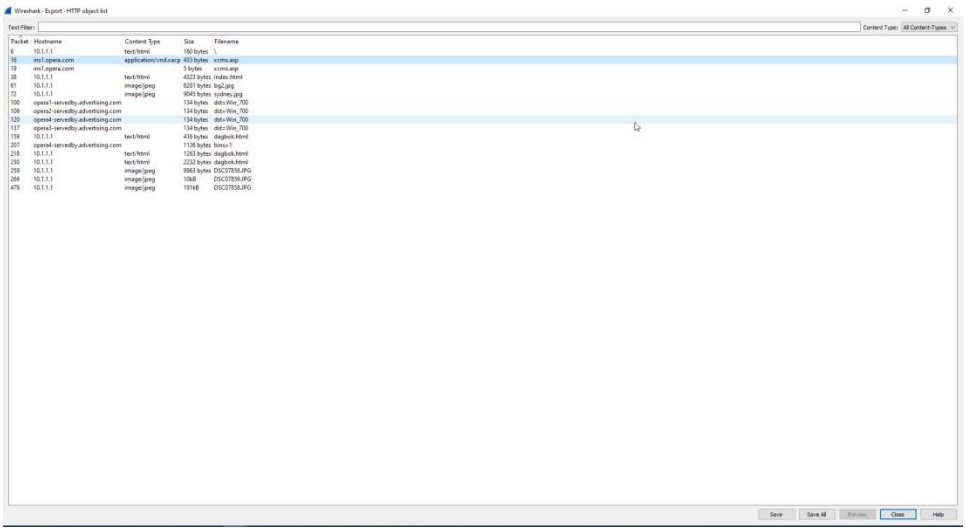
The first step TASK1 was to download the telnet-cooked.pcap file from Wiresharks' website. After downloading the file, it was opened in Wireshark. After following the TCP stream, the following information was presented.




You can clearly see that the user login and password are listed.

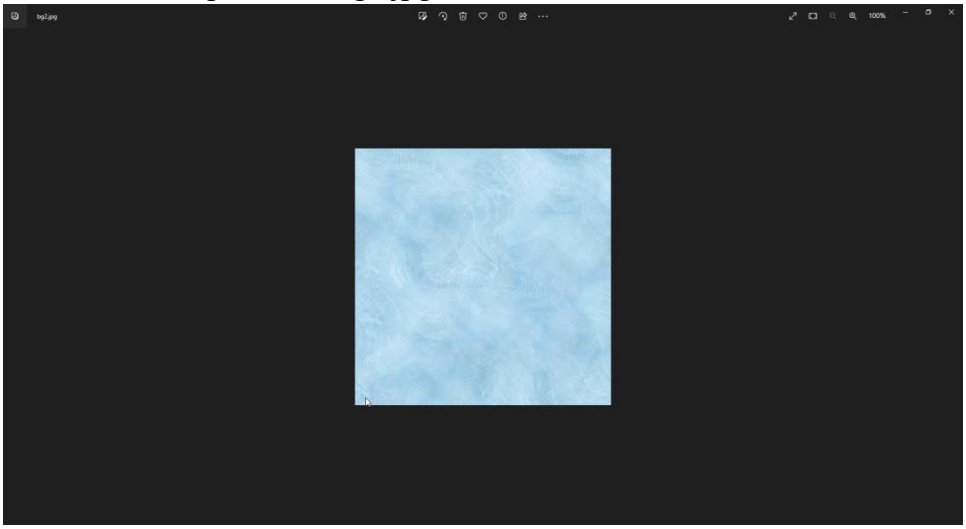
- Login: fake
- Password: user

Next for TASK2 the http_with_jpegs.cap file was downloaded and loaded into Wireshark. Going to files and extracting http we were presented with different http objects



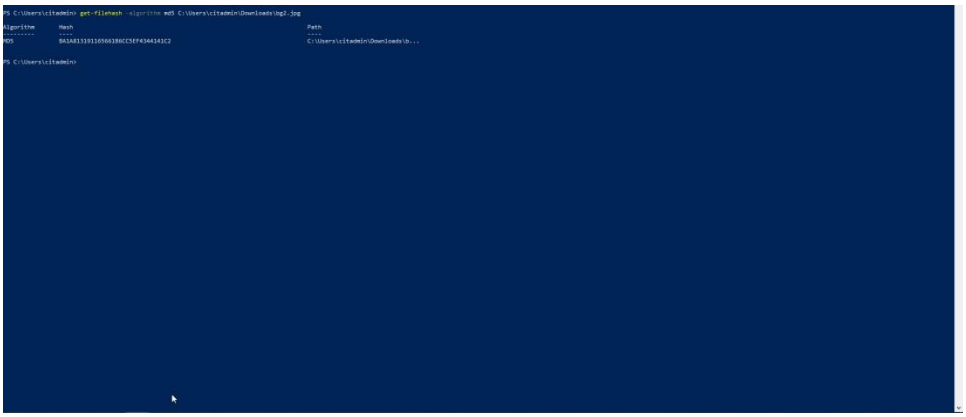
We can see that there are five Jpeg files. If you want to see them, you can click the preview button and view the images.

Here is an example of the bg2.jpg:



To find the md5 hash you can do so in windows PowerShell with the following command.

get-filehash -algorithm md5 C:\Users\citadmin\Downloads\bg2.jpg



The MD5 hash: BA1A813191165661B6CC5EF4344141C2

## What does it mean if a packet is highlighted black in Wireshark?

A black packet is a packet with errors.

## What filter in Wireshark would you use if you only want to see icmp communications?

You can simply type icmp is the display filter in Wireshark


## How can Network monitoring be useful when analyzing network traffic?

You can gain a lot of valuable information. Just in this lab we were able to obtain a user's login credentials that were in plain text. You also saw jpeg files through http traffic. If someone was using Wireshark oven an open network, they might be able to steal peoples information, especially if it is an unprotected network.