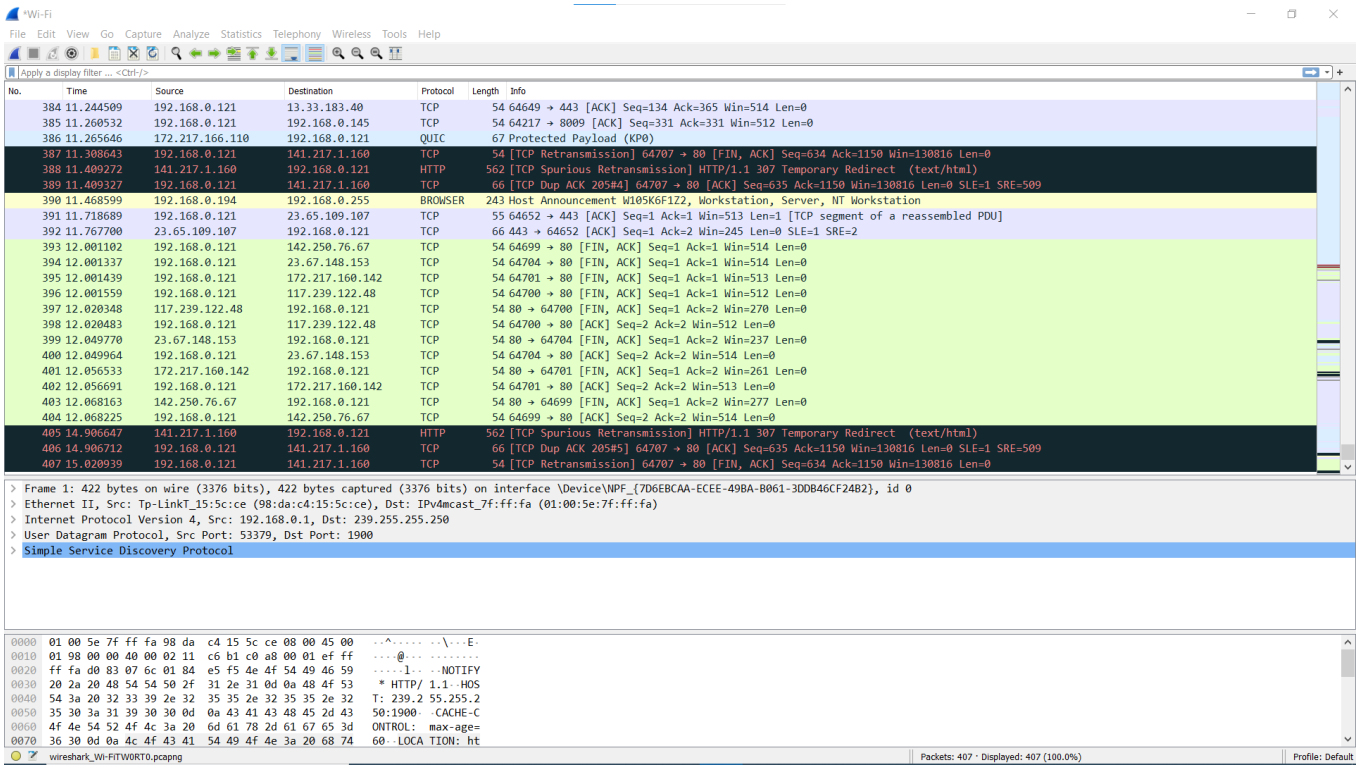
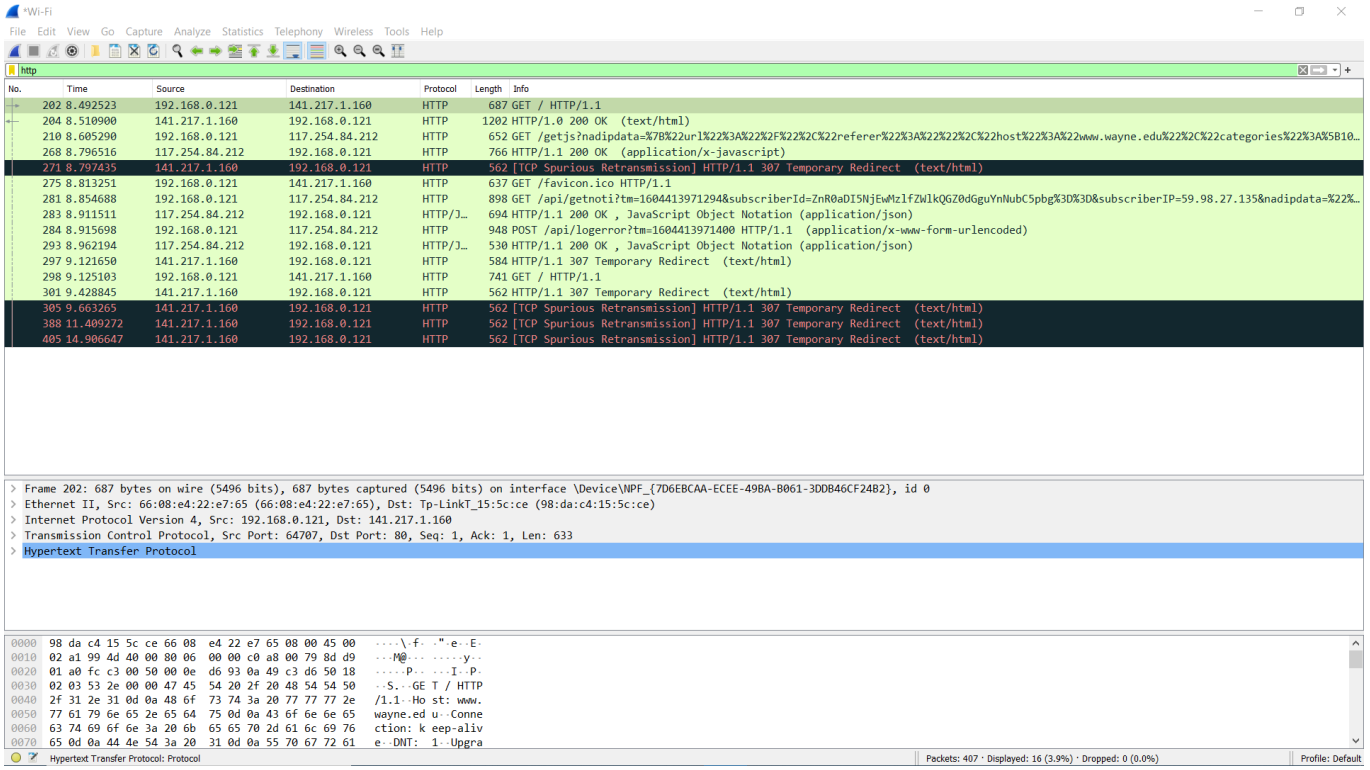
Cyber Security – Assignment 1

1. Lab Manual Steps followed with Screenshots.

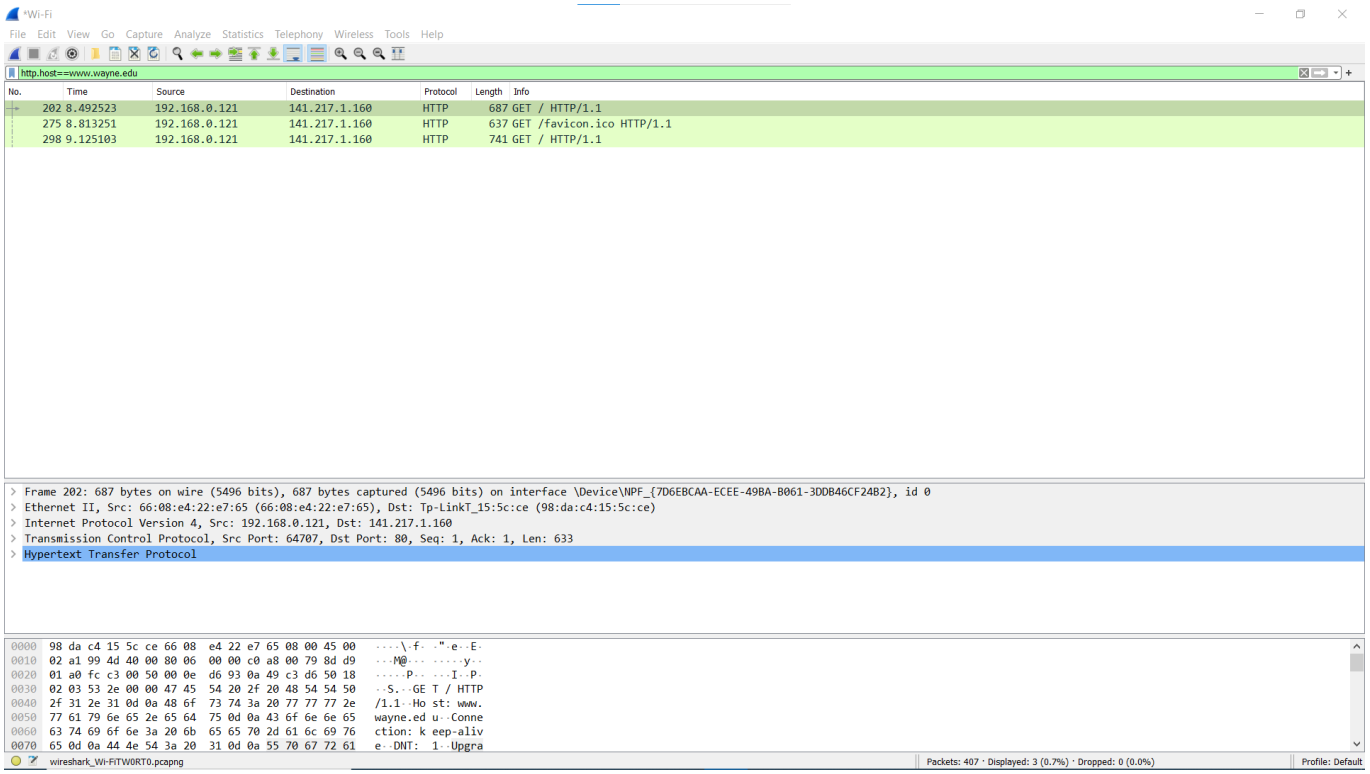
- **Wireshark screen after the traffic capture of www.wayne.edu**



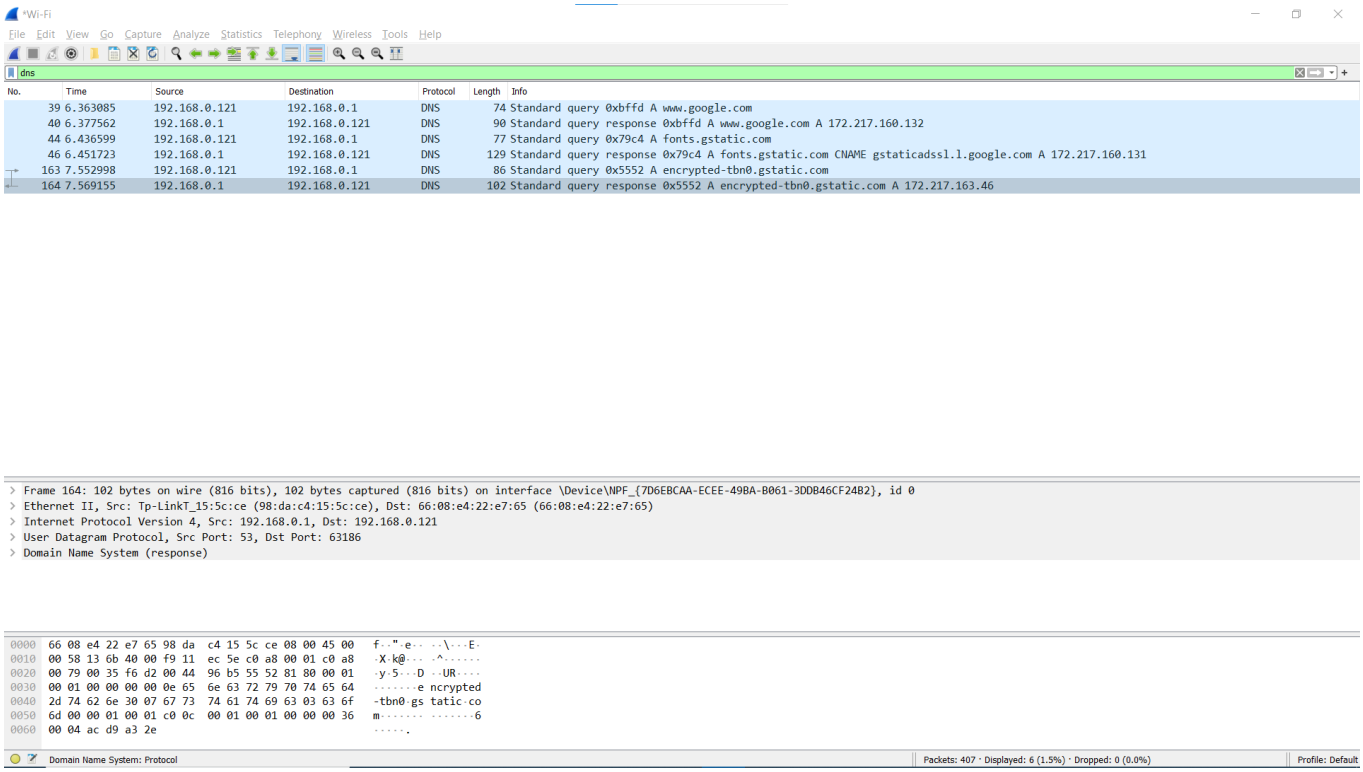
- **Wireshark screen after applying http filter.**



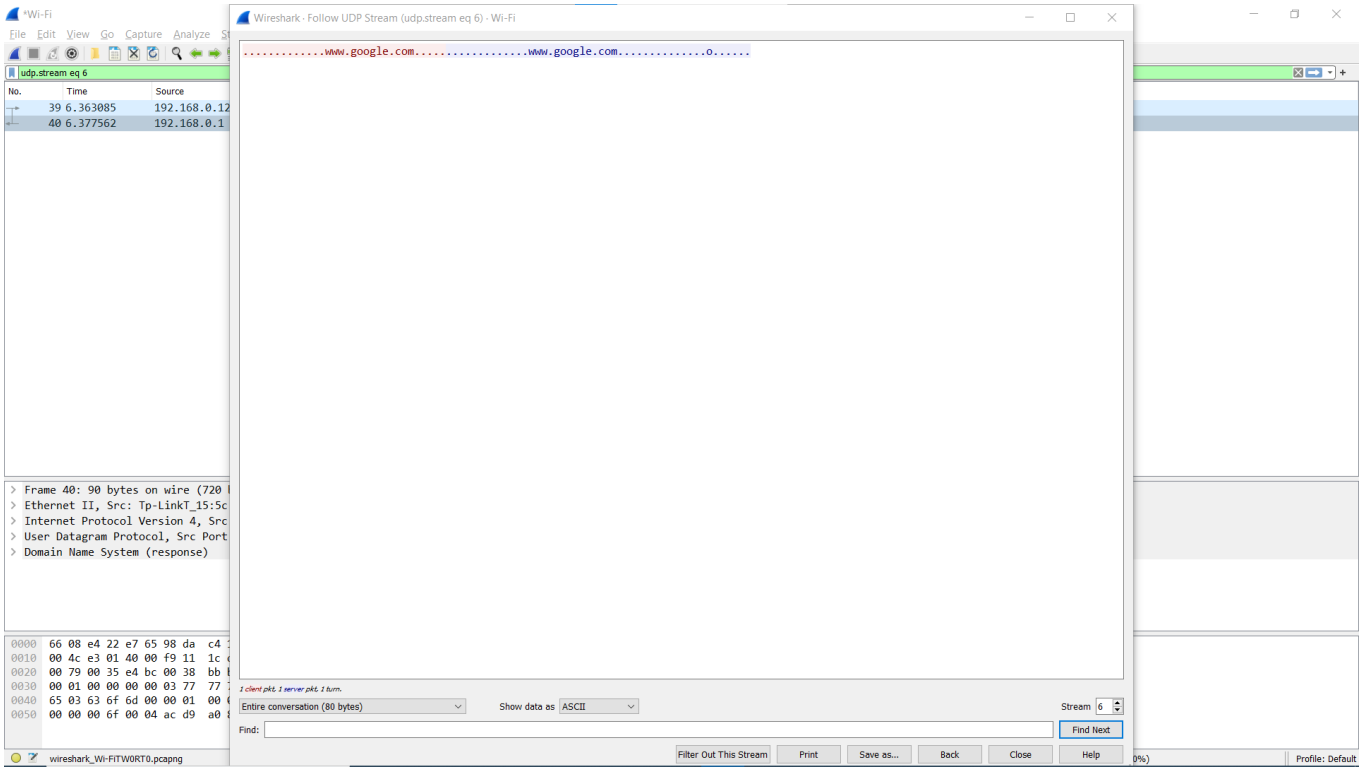
- **Wireshark screen after applying filter http.host=www.wayne.edu**



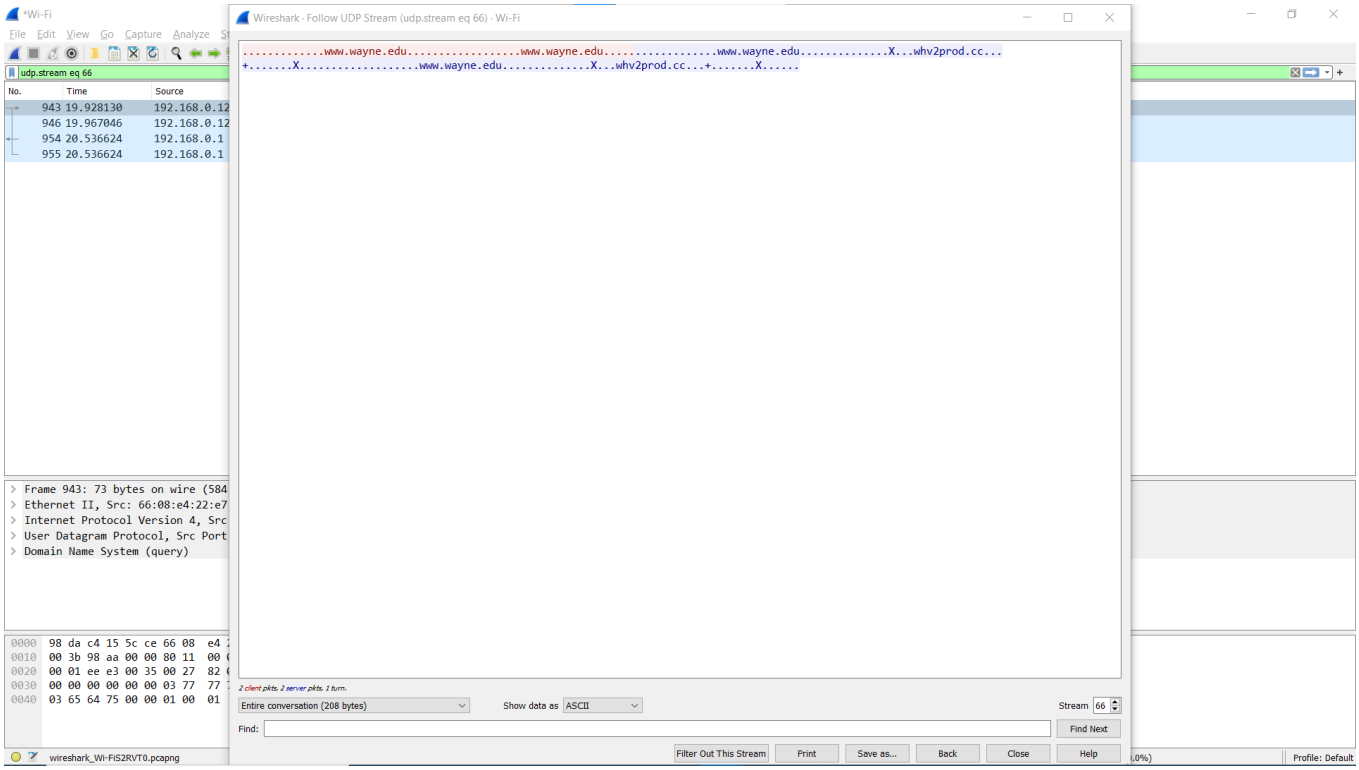
- **Wireshark screen with dns filter**



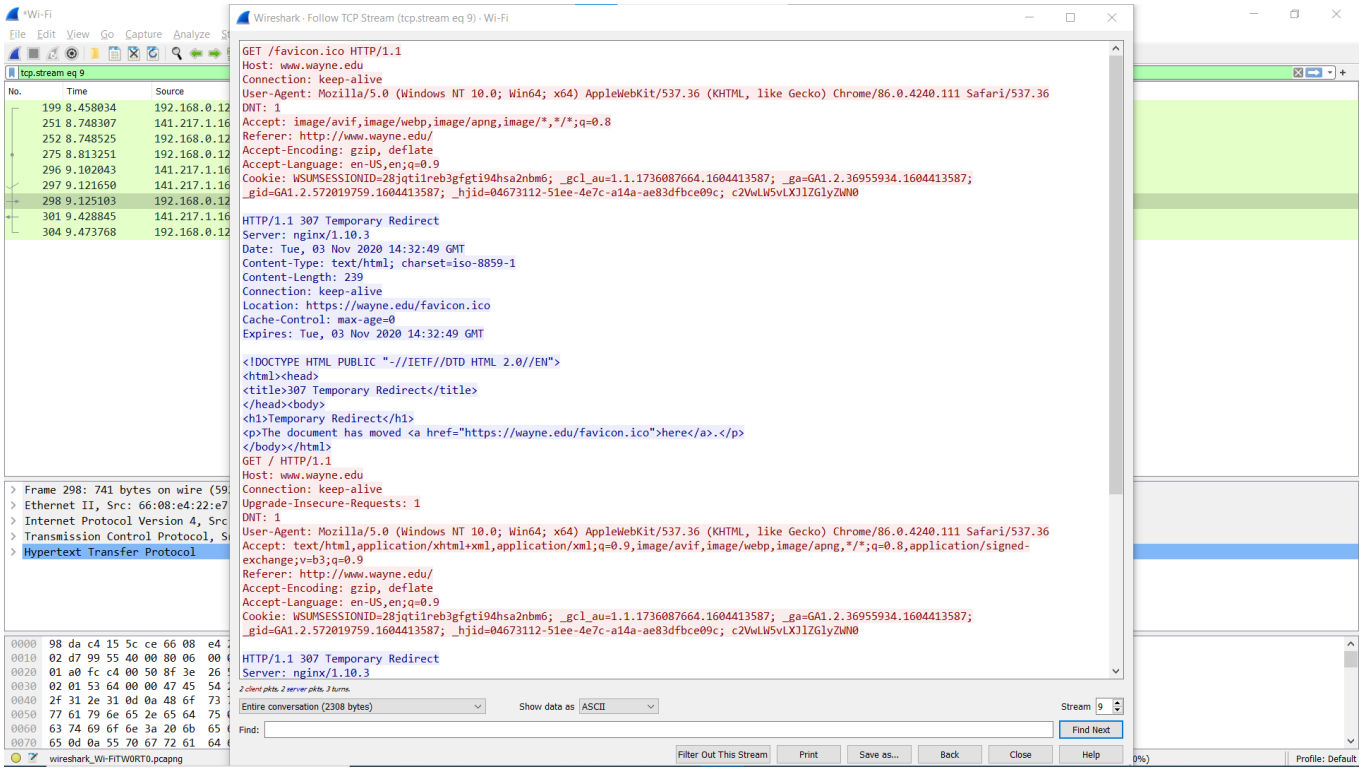
- **Wireshark screen after UDP follow option**



Another example



- # Wireshark screen after TCP stream follow



Questions from the Assignment and Answers

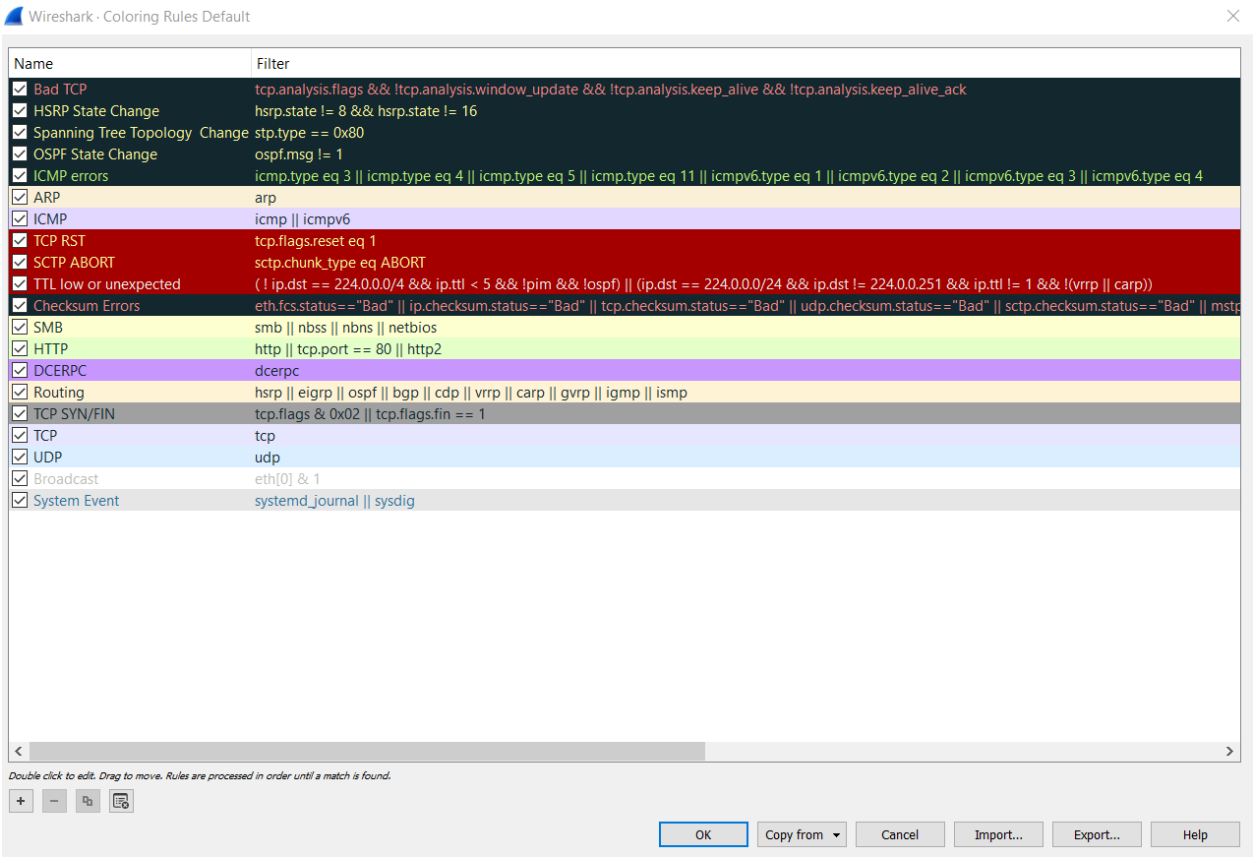
1. If a packet is highlighted by black, what does it mean for the packet?

Ans: By default the black colour code is given to packets which have some sort of problem or state change when they were received.

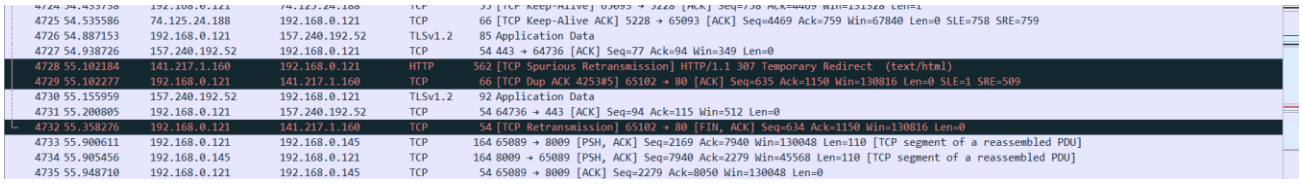
By default, following are the conditions for black coloured packets.

1. Bad TCP like Spurious transmission or Duplicate or out of order packet.
2. HSRP State change
3. Spanning Tree Topology change
4. OSPF State Change
5. ICMP errors

However, this colour coding can be customised by the user.



Examples are below:



2. **What is the filter command for listing all outgoing http traffic?**

Ans: To filter all outgoing http traffic, use this

ip.src == <host or local ip address> && http

or in ipv6

ipv6.src == <host or local ipv6 address> && http

3. **Why does DNS use Follow UDP Stream while HTTP use Follow TCP Stream?**

Ans: DNS uses UDP protocol on the transport layer by default. Although it can fallback to TCP protocol when packet size is large. UDP is preferred in DNS because it is fast and has low overhead. A DNS query is a single UDP request from the DNS client followed by a single UDP reply from the server.

So, to trace the Stream of UDP we use Follow UDP Stream.

HTTP uses TCP protocol on the Transport layer by default. So to trace stream we use Follow TCP Stream.

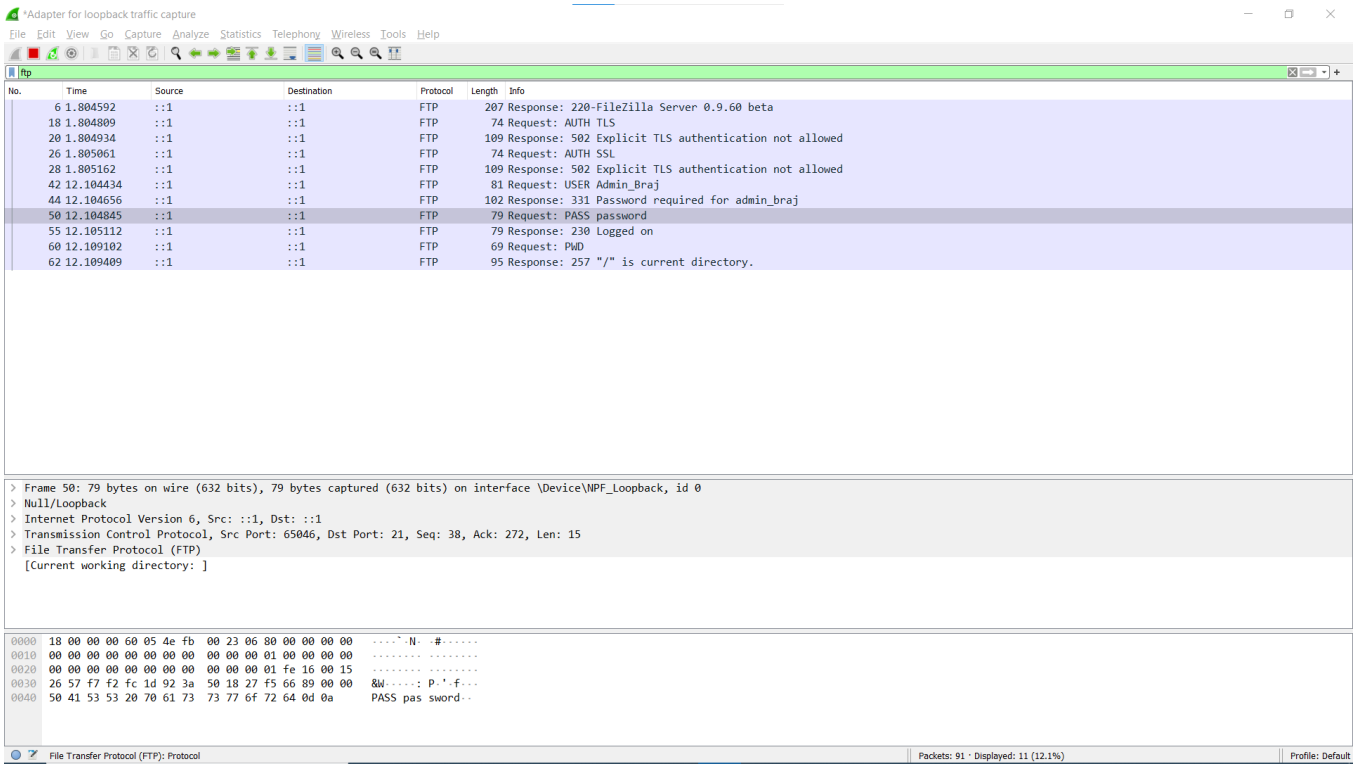
4. **Using Wireshark to capture the FTP password.**

Ans: Here I have used a Filezilla local FTP server hosted on my local machine and Filezilla client to connect to the server.

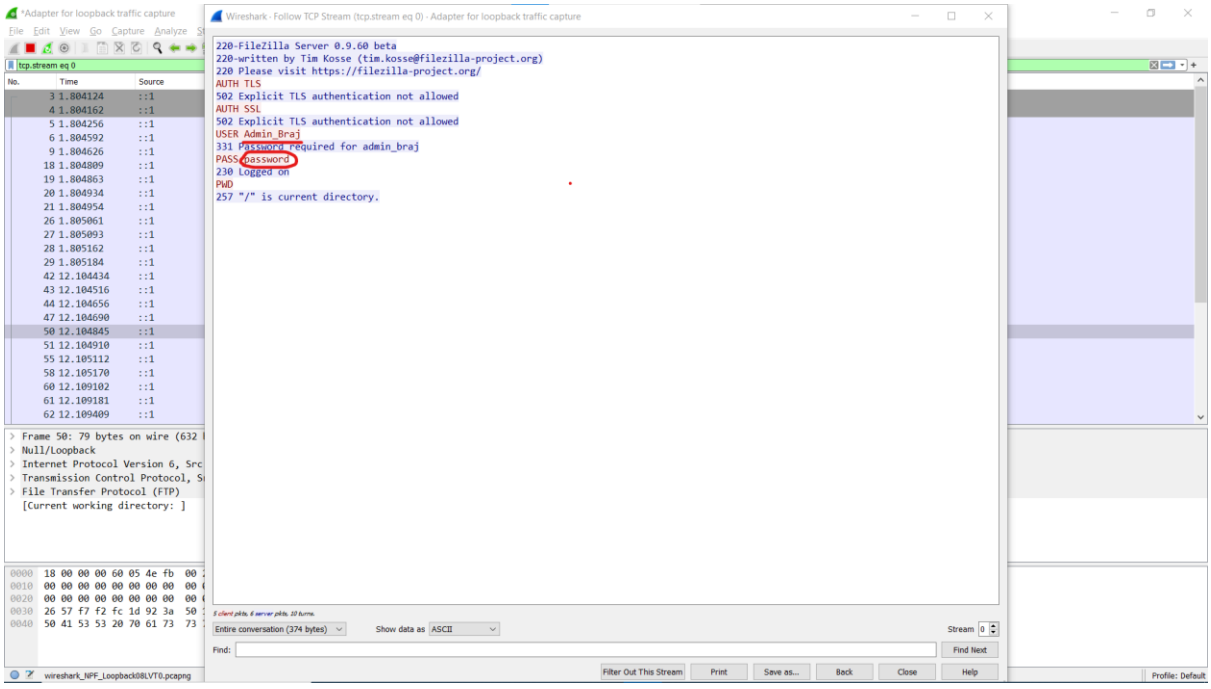
Step by step demo for capturing the FTP password and a possible fix to protect against password leak is shown below.

Wireshark – Capturing password of the FTP communication

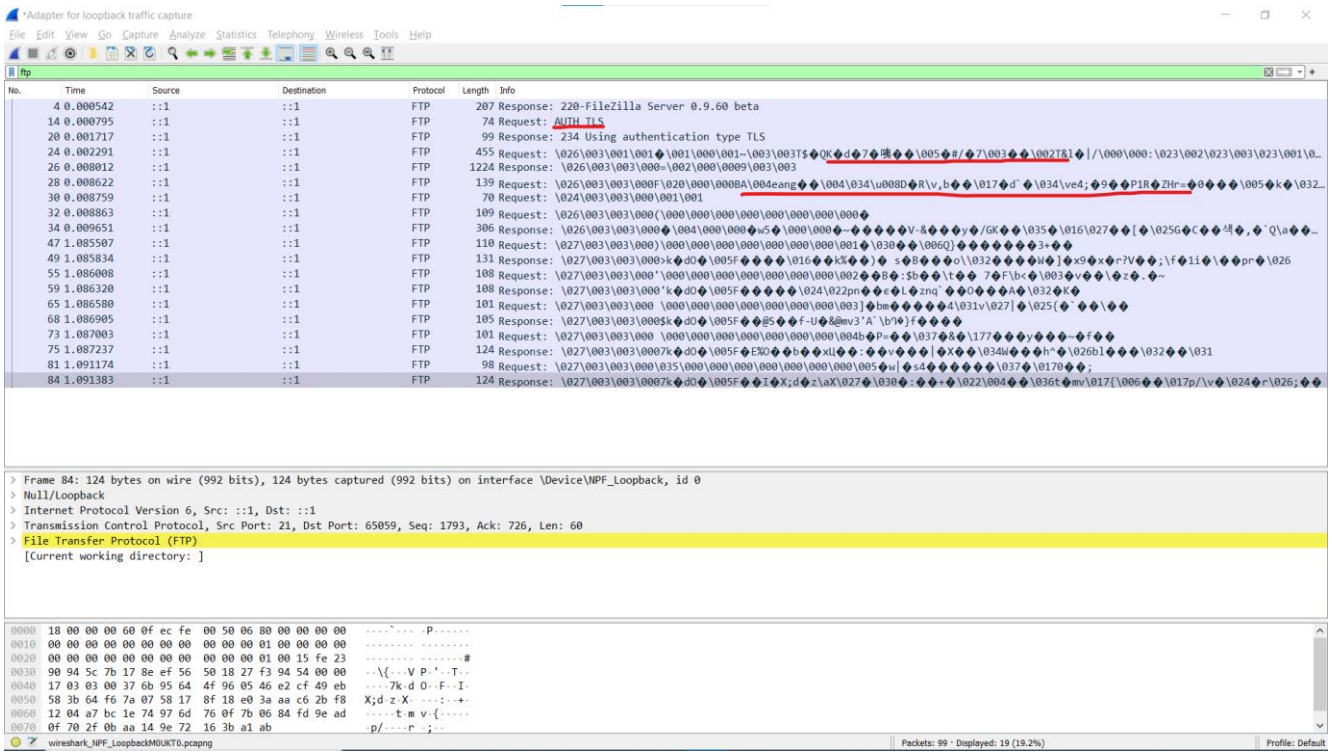
Username and Password can be seen here if we apply filter as ftp.

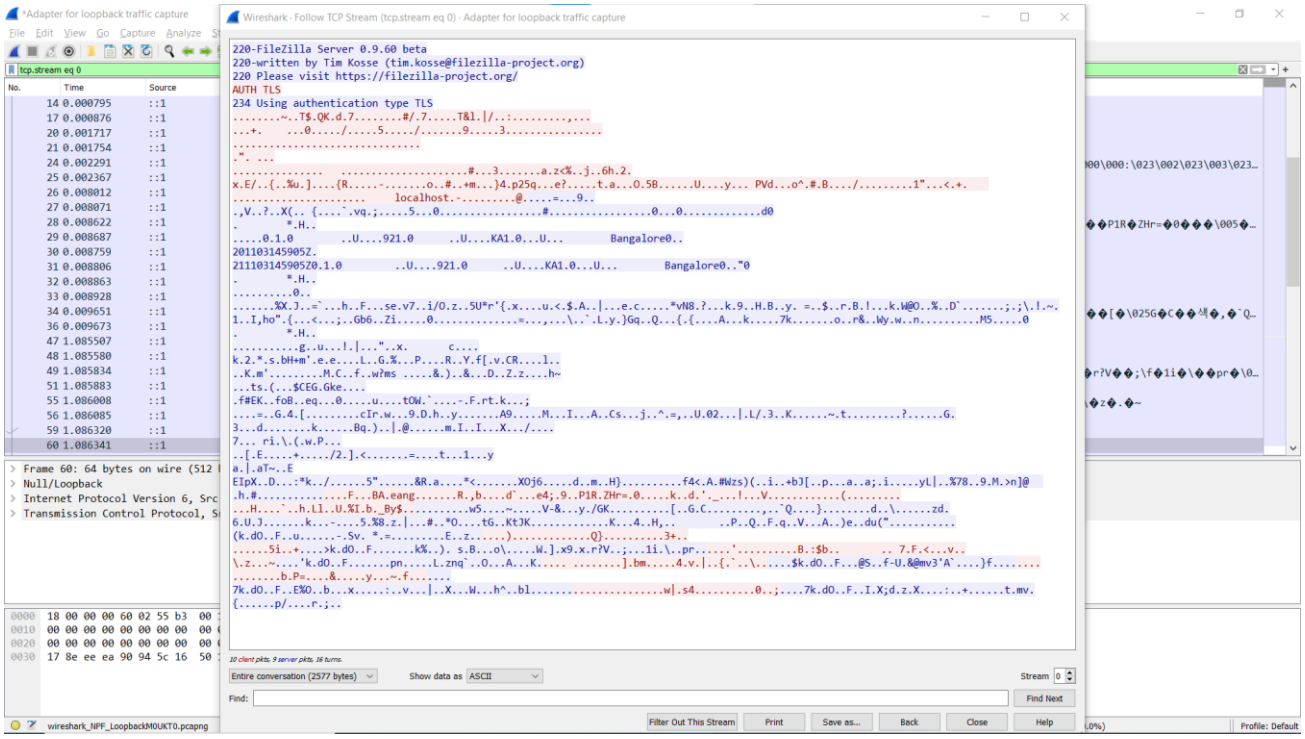


Password is clearly visible here if you merely follow the TCP Stream



To protect leaking password, we should always prefer SFTP or FTP over TLS instead of FTP. Using FTP shares the username and password as clear text whereas the SFTP or FTP over TLS will encrypt the username and password as seen below.





Using TLS over FTP caused the user credentials to be encrypted with the public key of the server and can be decrypted only by the private key of the server on the server's end.