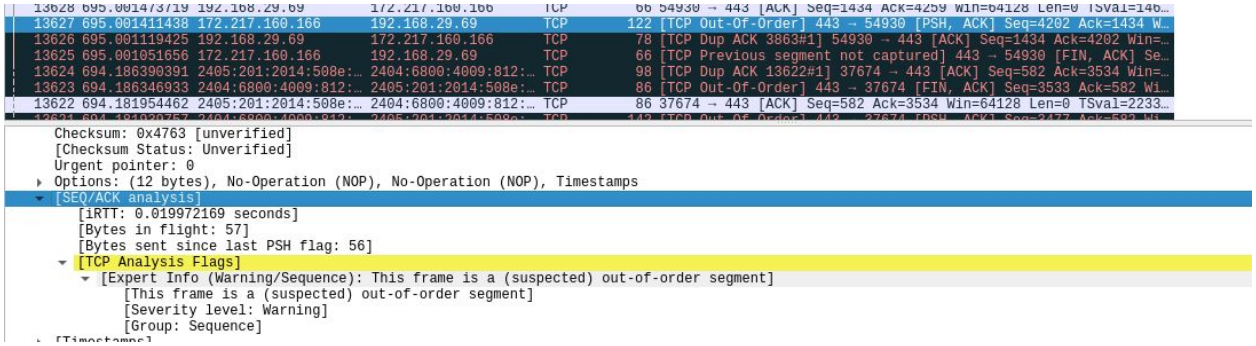
Computer Networks
Practical 1

Name: **Krunal Rank**
Roll No: **U18CO081**

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

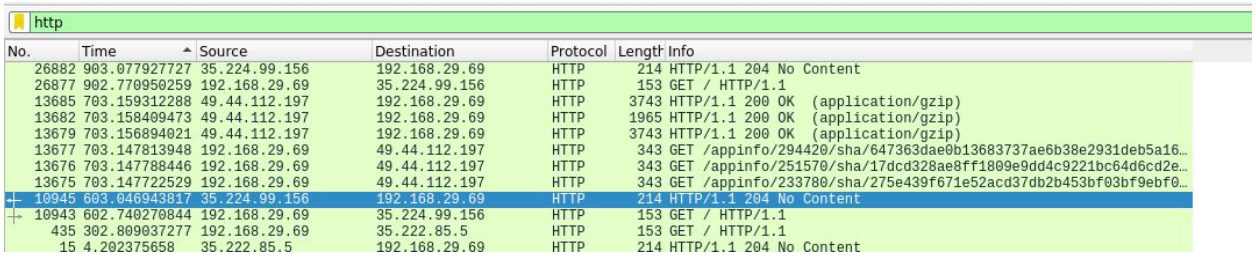
If a packet is highlighted by Black background, it conveys that the packet has some potential problems as detected by Wireshark. For example, in the below screenshot as clicked by me, you can see the TCP protocol has some flags set suggesting out of segment order.



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

The filter command for listing all outgoing http traffic is as follows:

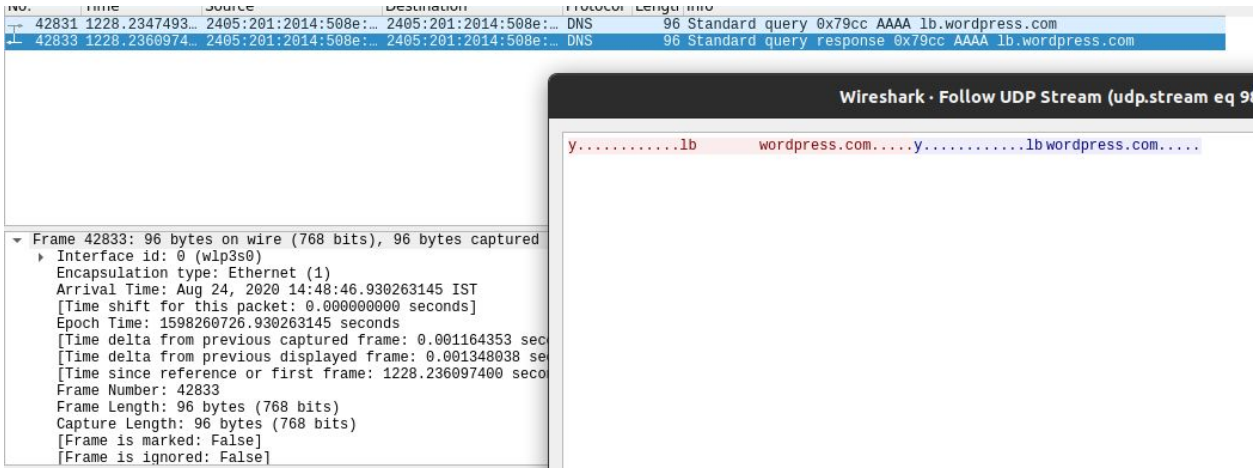
```
http
```



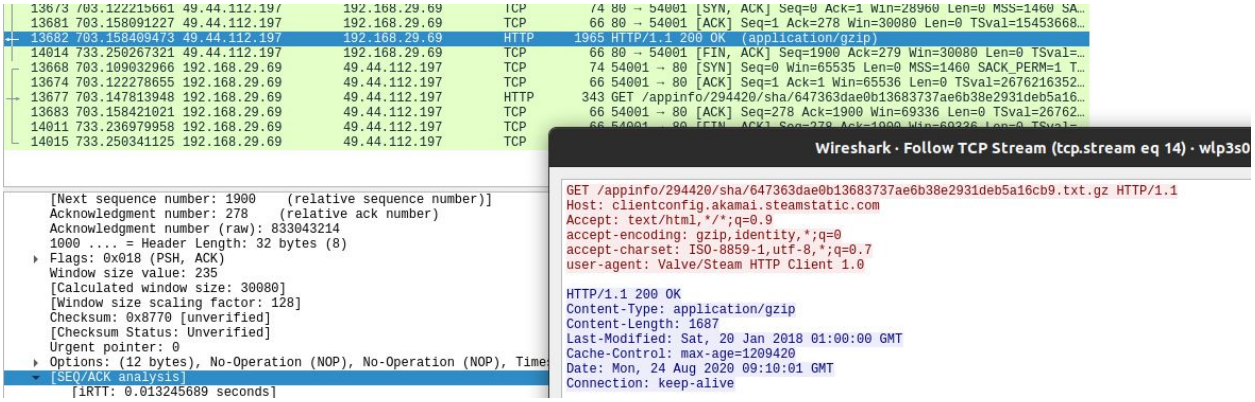
3. Why does DNS use “Follow UDP Stream” while HTTP uses “Follow TCP Stream”?

DNS uses the User Datagram Protocol (UDP) on port 53 to serve DNS queries. UDP is preferred 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.

If a DNS response is larger than 512 bytes, or if a DNS server is managing tasks like zone transfers (transferring DNS records from primary to secondary DNS server), the Transmission Control Protocol (TCP) is used instead of UDP, to enable data integrity checks.



The layer underneath HTTP is a transport layer protocol.
Most HTTP traffic travels over TCP (short for Transmission Control Protocol) in this layer, although TCP isn't required by HTTP.
When a user types a URL into the browser, the browser opens a TCP socket by specifying the server address and port, then starts writing data into the socket.
All the browser needs to worry about is writing the proper HTTP message into the socket.
The TCP layer accepts the data and ensures the data gets delivered to the server without getting lost or duplicated.
TCP will automatically resend any information that might get lost in transit.
The application doesn't have to worry about lost data, and this is why TCP is known as a reliable protocol. In addition to error detection, TCP also provides flow control.
Flow control ensures the sender does not send data too fast for the receiver or the network to process the data.
In short, TCP provides many vital services for the successful delivery of HTTP messages, but it does so in a transparent way. Most applications don't need to worry about TCP.
And, TCP is just the first layer beneath HTTP. After TCP at the transport layer comes IP as a network layer protocol.



4. Use wireshark to capture FTP password.

I tried connecting to the FTP server of cesca.es However I was not able to connect to the server due to no login credentials. However, below are the screenshots for the same process: