

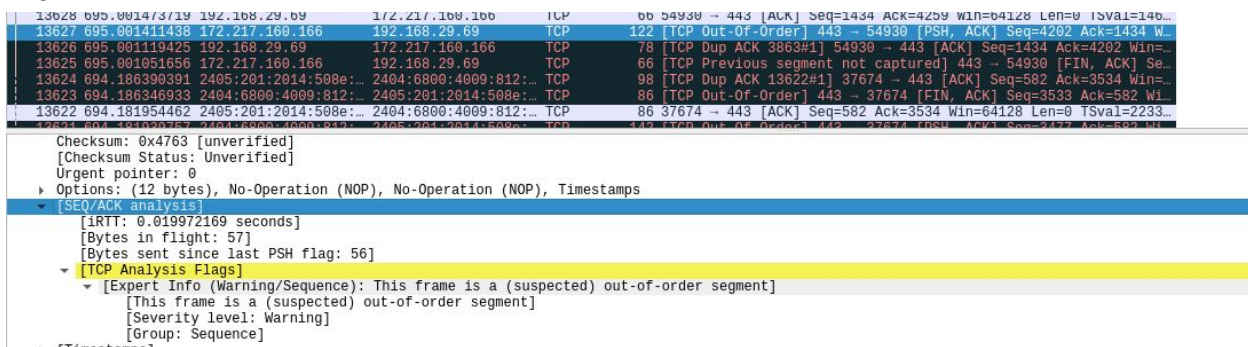
# Computer Networks

## 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:

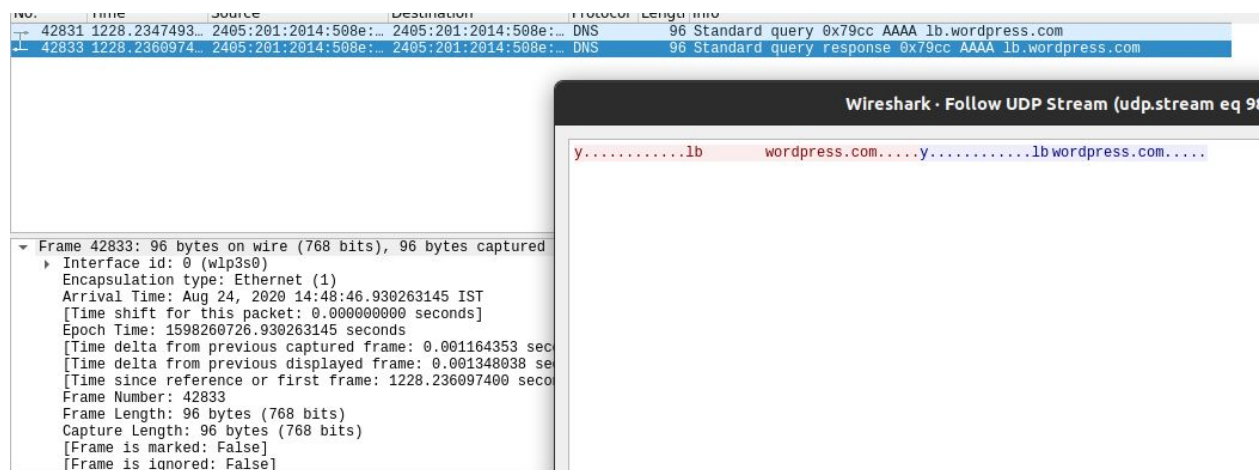
http

No.	Time	Source	Destination	Protocol	Length	Info
26882	903.07792727	35.224.99.156	192.168.29.69	HTTP	214	HTTP/1.1 204 No Content
26877	902.770950259	192.168.29.69	35.224.99.156	HTTP	153	GET / HTTP/1.1
13685	703.159312288	49.44.112.197	192.168.29.69	HTTP	3743	HTTP/1.1 200 OK (application/gzip)
13682	703.158409473	49.44.112.197	192.168.29.69	HTTP	1965	HTTP/1.1 200 OK (application/gzip)
13679	703.156894021	49.44.112.197	192.168.29.69	HTTP	3743	HTTP/1.1 200 OK (application/gzip)
13677	703.147813948	192.168.29.69	49.44.112.197	HTTP	343	GET /appinfo/294420/sha/647363dae0b13683737ae6b38e2931deb5a16...
13676	703.147788446	192.168.29.69	49.44.112.197	HTTP	343	GET /appinfo/251570/sha/17dcd328ae8ff1809e9dd4c9221bc64d6cd2e...
13675	703.147722529	192.168.29.69	49.44.112.197	HTTP	343	GET /appinfo/233780/sha/275e439f671e52acd37db2b453bf03bf9ebf0...
10945	603.046943817	35.224.99.156	192.168.29.69	HTTP	214	HTTP/1.1 204 No Content
10943	602.740270844	192.168.29.69	35.224.99.156	HTTP	153	GET / HTTP/1.1
435	302.809037277	192.168.29.69	35.222.85.5	HTTP	153	GET / HTTP/1.1
15	4.202375658	35.222.85.5	192.168.29.69	HTTP	214	HTTP/1.1 204 No Content

### 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.

Wireshark - Follow TCP Stream (tcp.stream eq 14) · wlp3s0

GET /appinfo/294420/sha/647363dae0b13683737ae6b38e2931deb5a16cb9.txt.gz HTTP/1.1  
 Host: clientconfig.akamai.steamstatic.com  
 Accept: text/html,\*/\*;q=0.9  
 accept-encoding: gzip,identity,\*;q=0  
 accept-charset: ISO-8859-1,utf-8,\*;q=0.7  
 user-agent: Valve/Steam HTTP Client 1.0

HTTP/1.1 200 OK  
 Content-Type: application/gzip  
 Content-Length: 1687  
 Last-Modified: Sat, 20 Jan 2018 01:00:00 GMT  
 Cache-Control: max-age=1209420  
 Date: Mon, 24 Aug 2020 09:10:01 GMT  
 Connection: keep-alive

#### 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:

```
krhero@hellblazer:~$ ftp ftp.cesca.es
Connected to verdaguer-ftp.cesca.cat.
220 Welcome to Anella Cientifica FTP service.
Name (ftp.cesca.es:krhero): krhero
530 This FTP server is anonymous only.
Login failed.
```

No.	Time	Source	Destination	Protocol	Length	Info
1093	2618.2257323	2495:201:2014:508e::	2a00:1800:1010::1	FTP	92	Request: QUIT
1180	2939.3356117	192.168.29.69	84.88.0.29	FTP	72	Request: QUIT
82724	2173.6805886	192.168.29.69	84.88.0.29	FTP	72	Request: SYST
82719	2173.4166437	192.168.29.69	84.88.0.29	FTP	79	Request: USER krhero
82671	2166.7173722	84.88.0.29	192.168.29.69	FTP	113	Response: 220 Welcome to Anella Cientifica FTP service.
99259	2473.9239103	84.88.0.29	192.168.29.69	FTP	80	Response: 421 Timeout.
82727	2173.8847762	84.88.0.29	192.168.29.69	FTP	104	Response: 530 Please login with USER and PASS.
82722	2173.6893388	84.88.0.29	192.168.29.69	FTP	106	Response: 530 This FTP server is anonymous only.