Beshir Said
WireShark HW

===== DAYTIME =====

1) TCP 3 way handshake Frame Summary

```
1   192.168.64.2   129.6.15.28   TCP   42296 → 13 [SYN]
2   129.6.15.28    192.168.64.2  TCP   13 → 42296 [SYN, ACK]
3   192.168.64.2   129.6.15.28   TCP   42296 → 13 [ACK]
```

2) The client uses port 42296

3) The client needs a port to store its unique connection info so that that system knows which program to send incoming packets to.

4) Frame summary

```
      4   129.6.15.28   192.168.64.2   DAYTIME   Response
```

5) [SYN] means synchronize and this is the start of the TCP handshake sent by the client. [ACK] means acknowledge and this is a confirmation that the message has been received by either the client or server.

6) The client initiated the closing of the TCP connection. You can tell because the first [FIN] [ACK] was sent from the client to the server; frame 5; 192.168.64.2   129.6.15.28   TCP   42296 13 [FIN, ACK]

===== HTTP =====

1) Frame Summary

```
      1   192.168.64.2   172.233.221.124   TCP   44258 → 80 [SYN]
      2   192.168.64.2   172.233.221.124   TCP   44264 → 80 [SYN]
      3   172.233.221.124 192.168.64.2    TCP   80 → 44258 [SYN, ACK]
```

-Two TCP connections were opened and you can tell from the two separate client ports

2) Frame Summary

```
5   192.168.64.2   172.233.221.124   HTTP   GET /index.html HTTP/1.1
```

-Yes, Frame 5 tells you where index.html was requested

3) Frame Summary

```
11   192.168.64.2   172.233.221.124   HTTP   GET /jeff-square-colorado.jpg HTTP/1.1
```

- Yes, Frame 11 tells you the jpg request