**Analyzing the Packet Capture File: p3.pcap**

Examine the wireshark window and find answers to the following questions:

1. This packet capture file contains two TCP handshakes. Find the first handshake and write down the packet numbers of those packets (the column labeled "No.").

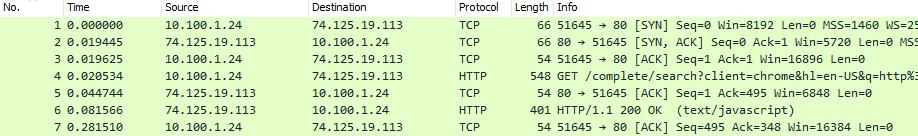
To establish a connection, the three-way (or 3-step) handshake occurs:

**SYN:** The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A.

**SYN-ACK:** In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B.

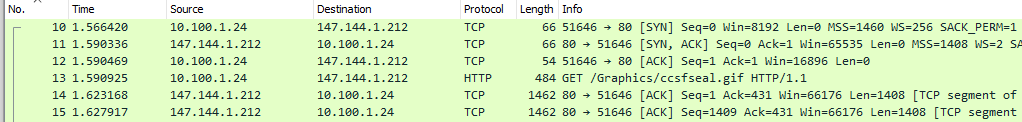
**ACK:** Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1.

**1st Handshake:**



Packet No: 1,2 and 3

**2nd Handshake:**



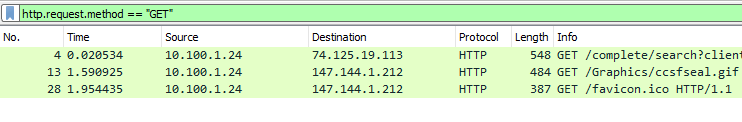
Packet No: 10, 11 and 12

1. In this session, a client machine initiated a connection to a server and then downloaded a file. What is the client's IP address?

**Client’s IP Address:** 10.100.1.24

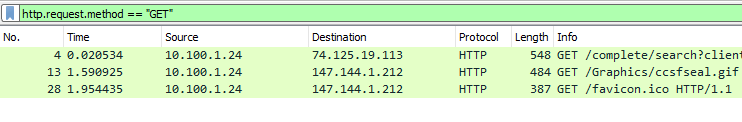
Since client sends the TCP SYN request to the server for connection we can get the client IP address by looking at that request

1. How many HTTP GET request packets are there?



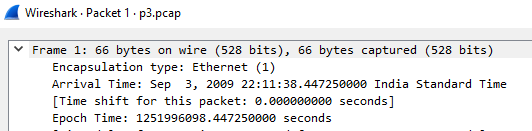
There are 3 HTTP get requests packets

1. Find the first HTTP GET request packet. What was the server's IP address? (The server is the Destination).



For first HTTP get request packet server IP (Destination IP) is 74.125.19.113

1. Examine the first packet. Look at the center pane in Wireshark. How many bytes were sent on the wire to form this packet?



For the first packet 66 bytes were sent on the wire to form this packet