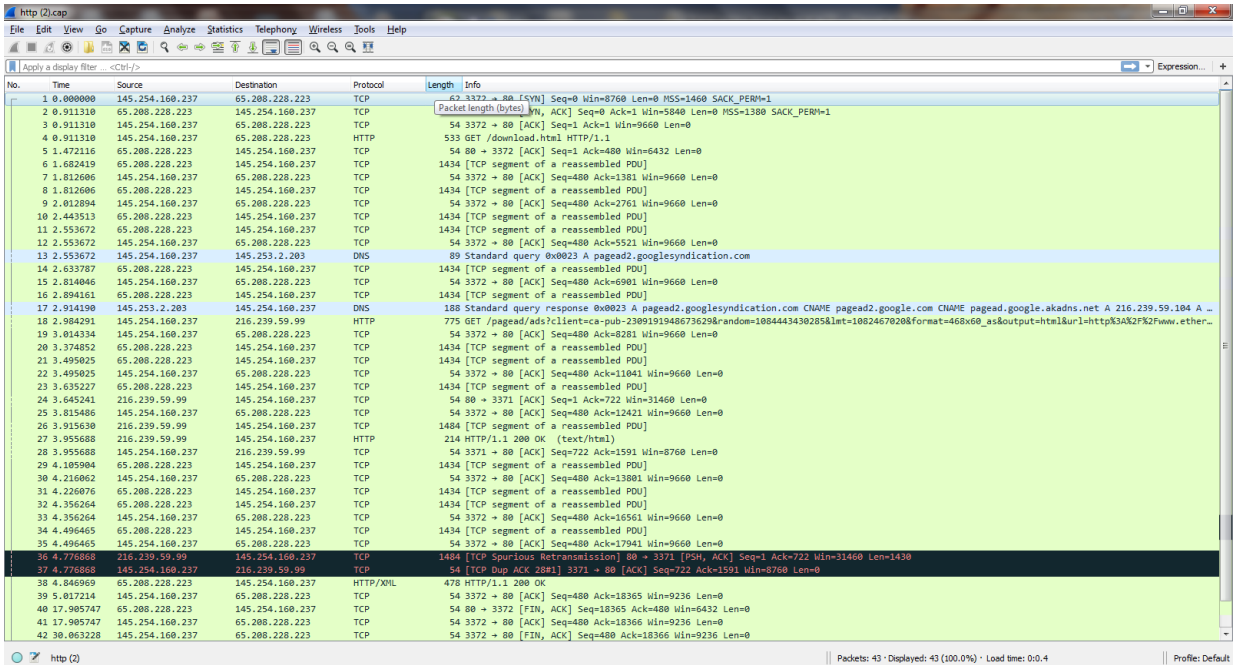
Wireshark Packet Analysis

Scenario:

I used Wireshark to capture packets exchanged between the two systems. I then analyzed the traffic to understand what was occurring.



Packet Analysis:

The packet capture presented largely illustrates communications between two machines the host identified by its Internet Protocol (IP) address 145.254.160.237 and the server identified by its IP address 65.208.228.223. Furthermore, the machines are communicating via the Transmission Control Protocol (TCP) exemplified using the three-way handshake i.e., 1. SYN 2. SYN, ACK 3. ACK taking place in packets 1 through 3. Additionally, the use of port 80 signifies HTTP (which is an unsecured internet protocol) is being used to access the website. Another IP address 216.239.59.99 is present in this packet capture that is also connected/communicating with the server IP address 65.208.228.223. This IP could either signify a separate host that has already connected via a 3-way handshake before the packet capture began, or it could signify the original host machine (IP address 145.254.160.237) has another IP address assigned to it. There is one last IP address (145.253.2.203) resulting from Google ads being transmitted. Lastly, the length of the numbers and the lack of letters used in the IP addresses indicate that IPv4 is being used.

Packets #5 through #12, #14 through #16, #19 through #26, #28 through #35, and #39 through #42 represent normal traffic activity relative to the requests for data made by the host machine and the server machine transferring the data requested using the TCP. Some details of note for these segments of packets are there is minor network congestion occurring throughout packets #5 through #12, #14 through #16, #19 through #35 and there is extreme network

congestion occurring between the transfer of packets #39 through #42 which is when the connection is being terminated (FIN, ACK) by both machines. Moreover, the phrase ‘TCP segment of a reassembled PDU’ appears nearly every time the host requests data from the server. This phrase appears for packets when they include a payload that forms part of a larger application message or document, which is completed in a subsequent packet.
Packet #4 shows that a file was downloaded by the host from the server. Packets #13 and #17 have ‘pagead2.googlesyndication.com’ in their info section indicating they are advertisements from Google. Packets #27 and #38 indicate that a previous HTTP request was successful as shown by ‘HTTP 200 OK’. Packets #36 and #37 show that a packet was lost during transmission and was then retransmitted because the TCP rules state that lost/unrecognized packets be retransmitted to guarantee message reliability.