

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.

No.	Time	Source	Destination	Protocol	Length	Info
0	0.000000	145.254.160.237	65.208.228.223	TCP	42	3323 → 80 [RST] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1
1	0.911310	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
2	0.911310	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
3	0.911310	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1
5	1.472116	65.208.228.223	145.254.160.237	TCP	54	80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
6	1.682419	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
7	1.812696	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0
8	1.812696	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
9	2.012894	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0
10	2.443513	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
11	2.553672	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
12	2.553672	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
13	2.553672	145.254.160.237	145.253.2.203	DNS	89	Standard query 0x0023 A pagead2.googleadsyndication.com
14	2.633787	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
15	2.814046	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0
16	2.894161	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
17	2.914198	145.253.2.203	145.254.160.237	DNS	188	Standard query response 0x0023 A pagead2.googleadsyndication.com CNAME pagead2.google.com CNAME pagead.google.akadns.net A 216.239.59.184 A ...
18	2.904291	145.254.160.237	216.239.59.99	HTTP	775	GET /pagead/adsclient=ca-pub-2309191946873629&ad=1084443430285&int=1082467020&format=468x60&js_output=html&url=http%3A%2F%2Fwww.ether...
19	3.014334	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=8281 Win=9660 Len=0
20	3.374852	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
21	3.495025	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
22	3.495025	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=1041 Win=9660 Len=0
23	3.635227	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
24	3.645241	216.239.59.99	145.254.160.237	TCP	54	80 → 3371 [ACK] Seq=1 Ack=722 Win=31460 Len=0
25	3.815486	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=12421 Win=9660 Len=0
26	3.915630	216.239.59.99	145.254.160.237	TCP	1484	[TCP segment of a reassembled PDU]
27	3.955688	216.239.59.99	145.254.160.237	HTTP	214	HTTP/1.1 200 OK (text/html)
28	3.955688	145.254.160.237	216.239.59.99	TCP	54	3371 → 80 [ACK] Seq=722 Ack=1591 Win=8760 Len=0
29	4.105904	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
30	4.216062	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=13801 Win=9660 Len=0
31	4.226076	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
32	4.356264	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
33	4.356264	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=10561 Win=9660 Len=0
34	4.496465	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
35	4.496465	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=17941 Win=9660 Len=0
36	4.776868	216.239.59.99	145.254.160.237	TCP	1484	[TCP Spurious Retransmission] 80 → 3371 [PSH, ACK] Seq=1 Ack=722 Win=31460 Len=1438
37	4.776868	145.254.160.237	216.239.59.99	TCP	54	[TCP Dup ACK 28#1] 3371 → 80 [ACK] Seq=722 Ack=1591 Win=8760 Len=0
38	4.846969	65.208.228.223	145.254.160.237	HTTP/XML	478	HTTP/1.1 200 OK
39	5.017214	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=18365 Win=9236 Len=0
40	17.985747	65.208.228.223	145.254.160.237	TCP	54	80 → 3372 [FIN, ACK] Seq=18365 Ack=480 Win=6432 Len=0
41	17.985747	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=18366 Win=9236 Len=0
42	30.063228	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [FIN, ACK] Seq=480 Ack=18366 Win=9236 Len=0

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.