

Name : Ramzy Izza Wardhana
NIM : 21/472698/PA/20322
Class : IUP CS B

Activity 6.1 – Computer Networking Lab 6

Answer the following questions

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the alice.txt file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the “details of the selected packet header window.”

> Internet Protocol Version 4, Src: 10.6.173.105, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 53240, Dst Port: 80, Seq: 149931, Ack: 1, Len: 3067
Source Port: 53240
Destination Port: 80
[Stream index: 46]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 3067]
Sequence Number: 149931 (relative sequence number)
Sequence Number (raw): 733188650
[Next Sequence Number: 152998 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1194840967
0101 = Header Length: 20 bytes (5)

Source	Destination
10.6.173.105	34.107.221.82
10.6.173.105	104.18.21.226
34.107.221.82	10.6.173.105
10.6.173.105	34.104.35.123
34.104.35.123	10.6.173.105
10.6.173.105	34.104.35.123
34.104.35.123	10.6.173.105
10.6.173.105	128.119.245.12
128.119.245.12	10.6.173.105
104.18.20.226	10.6.173.105

53240

Answer:

Source IP Address: 10.6.173.105, TCP port Number: 53250 (Source), 80 (Destination)

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

Source	Destination
10.6.173.105	34.107.221.82
10.6.173.105	104.18.21.226
34.107.221.82	10.6.173.105
10.6.173.105	34.104.35.123
34.104.35.123	10.6.173.105
10.6.173.105	34.104.35.123
34.104.35.123	10.6.173.105
10.6.173.105	128.119.245.12
128.119.245.12	10.6.173.105
104.18.20.226	10.6.173.105

> Internet Protocol Version 4, Src: 10.6.173.105, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 53240, Dst Port: 80, Seq: 149931, Ack: 1, Len: 3067
Source Port: 53240
Destination Port: 80
[Stream index: 46]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 3067]
Sequence Number: 149931 (relative sequence number)
Sequence Number (raw): 733188650
[Next Sequence Number: 152998 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1194840967
0101 = Header Length: 20 bytes (5)

53240

Answer:

IP Address Destination: 128.119.245.12, Port Destination: 80

3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? (Note: this is the “raw” sequence number carried in the TCP segment itself; it is NOT the packet # in the “No.” column in the Wireshark window. Remember there is no such thing as a “packet number” in TCP or UDP; as you know, there are sequence numbers in TCP and that’s what we’re after here. Also note that this is not the relative sequence number with respect to the starting sequence number of this TCP session.). What is it in this TCP segment that identifies the segment as a SYN segment?

```

1064 3.468428 10.6.173.105 34.104.35.123 TCP 54 53241 → 80 [ACK] Seq=663 Ack=2305 Win=132096 Len=0
1065 3.479512 10.6.173.105 128.119.245.12 TCP 66 53245 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1066 3.498638 10.6.173.105 31.13.68.61 TCP 315 [TCP Retransmission] 53213 → 5222 [PSH, ACK] Seq=1 Ack=1 Win=516 Len=261
1067 3.517075 128.119.245.12 10.6.173.105 TCP 66 80 → 53240 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1363 SACK_PERM=1 WS=128
1068 3.517212 10.6.173.105 128.119.245.12 TCP 54 53240 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
1069 3.518041 10.6.173.105 128.119.245.12 TCP 13684 53240 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=13630 [TCP segment of a reassembled
1101 3.783033 10.6.173.105 34.107.221.82 TCP 66 [TCP Retransmission] [TCP Port numbers reused] 53238 → 80 [SYN] Seq=0 Win=64240
1102 3.792608 128.119.245.12 10.6.173.105 TCP 66 80 → 53245 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1363 SACK_PERM=1 WS=128
1103 3.792708 10.6.173.105 128.119.245.12 TCP 54 53245 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0

Source Port: 53245
Destination Port: 80
[Stream index: 49]
[Conversation completeness: Incomplete, ESTABLISHED (7)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2956721891
[Next Sequence Number: 1 (relative sequence number)]

Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... ....0.. = Push: Not set
.... .....0.. = Reset: Not set
> .... ....1. = Syn: Set
.... .......0 = Fin: Not set
[TCP Flags: .....S.]

```

Answer:

TCP Sequence Number (raw) : 2956721891, to identify that it is a SYN TCP segment is to observe the [SYN] Flag which denoted as 1 (set)

4. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is it in the segment that identifies the segment as a SYNACK segment? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value?

```

1066 3.498638 10.6.173.105 31.13.68.61 TCP 315 [TCP Retransmission] 53213 → 5222 [PSH, ACK] Seq=1 Ack=1 Win=516 Len=261
1067 3.517075 128.119.245.12 10.6.173.105 TCP 66 80 → 53240 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1363 SACK_PERM=1 WS=128
1068 3.517212 10.6.173.105 128.119.245.12 TCP 54 53240 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
1069 3.518041 10.6.173.105 128.119.245.12 TCP 13684 53240 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=13630 [TCP segment of a reassembled PDU]
1101 3.783033 10.6.173.105 34.107.221.82 TCP 66 [TCP Retransmission] [TCP Port numbers reused] 53238 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS
1102 3.792608 128.119.245.12 10.6.173.105 TCP 66 80 → 53245 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1363 SACK_PERM=1 WS=128
1103 3.792708 10.6.173.105 128.119.245.12 TCP 54 53245 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0

Source Port: 80
Destination Port: 53240
[Stream index: 46]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1194840966
[Next Sequence Number: 1 (relative sequence number)]

Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Set
.... ....0.. = Push: Not set
.... .....0.. = Reset: Not set
> .... ....1. = Syn: Set
.... .......0 = Fin: Not set
[TCP Flags: .....A..S.]
Sequence Number (raw): 1194840966
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 733038720

```

Answer:

TCP Sequence Number (raw) : 1194840866, Segment that identifies it as SYN, ACK is located in flags which denote ACK and SYN as 1 (set). The value of ACK field is

1 (relative) and 733038720 (raw). The way that the gaia.cs.umass.edu determine that value is to increment it by 1 to its initial sequence of SYN segment received by the client computer.

5. What is the sequence number of the TCP segment containing the header of the HTTP POST command? Note that in order to find the POST message header, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with the ASCII text "POST" within its DATA field^{1,2}. How many bytes of data are contained in the payload (data) field of this TCP segment? Did all of the data in the transferred file alice.txt fit into this single segment?

Stream index: 46
 [Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 13630]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 733038720
 [Next Sequence Number: 13631 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)

> [SEQ/ACK analysis]
 TCP payload (13630 bytes)
 [Reassembled PDU in frame: 1269]
 TCP segment data (13630 bytes)

Answer:

Sequence Number (raw): 733038720 | Bytes of data contained in TCP payload: 13630 bytes | Observe that the text content illustrated above only represents parts of the whole text. As a consequence, all the data contained in alice.txt does not fit into a single segment of this TCP

6. What is the length (header plus payload) of the segment that contains POST?

Acknowledgment Number: 1 (relative ack nu
 Acknowledgment number (raw): 1194840967
 0101 = Header Length: 20 bytes (5)
 > Flags: 0x0101 (ACK)
 Window: 516

Answer:

Header length of the segment that contains POST is : 20 bytes

7. How many retransmitted segments are there? What did you check in order to answer this question?

No.	Time	Source	Destination	Protocol	Length	Info
11003	1.792780	10.6.173.105	128.119.245.12	TCP	54	53245 → 80 [ACK] Seq=1 Ack=1 Min=12096 Len=0
10603	1.479512	10.6.173.105	128.119.245.12	TCP	66	53245 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13344	1.709123	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=103589 Win=182528 Len=0
13354	1.717996	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=106315 Win=182528 Len=0
11113	1.847446	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=10995 Win=15456 Len=0
13364	1.723085	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=111767 Win=183296 Len=0
13374	1.735365	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=115856 Win=183296 Len=0
13384	1.735734	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=118882 Win=183296 Len=0
13394	1.742256	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=122671 Win=183296 Len=0
11243	1.892399	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=122680 Win=54480 Len=0
13404	1.752921	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=125297 Win=183296 Len=0
13414	1.763996	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=128123 Win=183296 Len=0
13424	1.772019	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=130849 Win=183296 Len=0
13614	1.814891	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=133575 Win=183296 Len=0
11103	1.900669	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=13611 Win=17344 Len=0
11043	1.807630	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=1364 Win=32128 Len=0
13624	1.816563	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=137664 Win=183296 Len=0
13634	1.820640	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=141753 Win=182528 Len=0
13644	1.845406	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=147205 Win=183296 Len=0
11644	1.091148	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=14994 Win=60160 Len=0
13654	1.858072	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=152998 Win=183296 Len=0
11664	1.100908	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=16357 Win=63104 Len=0
11684	1.116540	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=17720 Win=60840 Len=0
11704	1.126400	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=20046 Win=17352 Len=0
11724	1.135891	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=21809 Win=74368 Len=0
11744	1.149757	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=27261 Win=85376 Len=0
11864	1.185647	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=29987 Win=108976 Len=0
11884	1.195550	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=32773 Win=106256 Len=0
11904	1.205240	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=35439 Win=106132 Len=0
11924	1.212184	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=38165 Win=107136 Len=0
11944	1.221445	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=40891 Win=112640 Len=0
11063	1.808072	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=4090 Win=37632 Len=0
12164	1.389762	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=43617 Win=118016 Len=0
12184	1.398124	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=46343 Win=123520 Len=0
12204	1.406781	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=49069 Win=122896 Len=0
12224	1.418090	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=52158 Win=137088 Len=0
11924	1.494433	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=54543 Win=140832 Len=0
11904	1.205240	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=57439 Win=106132 Len=0
11924	1.212184	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=58165 Win=107136 Len=0
11944	1.221445	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=60891 Win=112640 Len=0
11063	1.808072	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=6090 Win=37632 Len=0
12164	1.389762	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=63617 Win=118016 Len=0
12184	1.398124	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=66343 Win=123520 Len=0
12204	1.406781	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=69069 Win=122896 Len=0
12224	1.418090	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=71795 Win=137088 Len=0
12244	1.428421	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=74521 Win=146144 Len=0
12264	1.440085	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=77247 Win=145536 Len=0
12284	1.452015	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=79973 Win=150912 Len=0
12304	1.464213	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=82699 Win=156416 Len=0
12064	1.409760	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=84862 Win=159360 Len=0
12624	1.501533	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=85425 Win=162304 Len=0
12644	1.501906	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=86788 Win=165120 Len=0
12664	1.510381	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=88151 Win=168064 Len=0
11083	1.822020	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=8816 Win=43136 Len=0
12684	1.510513	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=89877 Win=173568 Len=0
12704	1.520706	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=92240 Win=178512 Len=0
12714	1.520819	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=93603 Win=179328 Len=0
12724	1.533790	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=96329 Win=182528 Len=0
12744	1.533790	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=97592 Win=181632 Len=0
12764	1.544062	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=99055 Win=186048 Len=0
12754	1.547351	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=81781 Win=182528 Len=0
11093	1.822020	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=8179 Win=45952 Len=0
12784	1.554004	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=83144 Win=191616 Len=0
12774	1.555877	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=84507 Win=183296 Len=0
13094	1.611963	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=85870 Win=183296 Len=0
13104	1.611963	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=87233 Win=183296 Len=0
13114	1.621078	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=88596 Win=183296 Len=0
13124	1.631012	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=89959 Win=183296 Len=0
13134	1.647156	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=95411 Win=180800 Len=0
13164	1.640861	128.119.245.12	10.6.173.105	TCP	56	80 → 53240 [ACK] Seq=1 Ack=95900 Win=185152 Len=0
10673	1.517075	128.119.245.12	10.6.173.105	TCP	66	80 → 53240 [SYN, ACK] Seq=0 Ack=1 Win=20200 Len=0 MSS=1363 SACK_PERM=1 WS=128
11023	1.792608	128.119.245.12	10.6.173.105	TCP	66	80 → 53245 [SYN, ACK] Seq=0 Ack=1 Win=20200 Len=0 MSS=1363 SACK_PERM=1 WS=128
13624	1.921980	128.119.245.12	10.6.173.105	HTTP	8121	HTTP/1.1 200 OK (text/plain)
12694	1.516530	10.6.173.105	128.119.245.12	HTTP	3121	POST /ultrashark-labs/Lab3-1-reply.htm HTTP/1.1 (text/plain)
10603	1.518041	10.6.173.105	128.119.245.12	TCP	13684	53240 → 80 [ACK] Seq=1 Ack=1 Min=12096 Len=13630 [TCP segment of a reassembled PDU]
12194	1.398364	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [ACK] Seq=100863 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
12214	1.408021	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [ACK] Seq=106315 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
12234	1.418127	10.6.173.105	128.119.245.12	TCP	8212	53240 → 80 [ACK] Seq=111767 Ack=1 Min=12096 Len=8178 [TCP segment of a reassembled PDU]
12254	1.428467	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=115945 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
12274	1.440123	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [ACK] Seq=122671 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
12314	1.464254	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [ACK] Seq=133575 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
11053	1.807698	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=13631 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
12614	1.490614	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=139827 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
12634	1.501596	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=141753 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
12654	1.501935	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=144479 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
12674	1.516436	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=147205 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
12814	1.563638	10.6.173.105	128.119.245.12	TCP	54	53240 → 80 [ACK] Seq=152998 Ack=778 Win=131328 Len=0
11073	1.808182	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [ACK] Seq=16357 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
11103	1.822071	10.6.173.105	128.119.245.12	TCP	8232	53240 → 80 [ACK] Seq=21809 Ack=1 Min=12096 Len=8178 [TCP segment of a reassembled PDU]
11253	1.892453	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=35439 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
11273	1.902707	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=38165 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
11654	1.009209	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=40891 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
11674	1.100153	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=43617 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
11694	1.116597	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=46343 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
11714	1.126449	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [ACK] Seq=49069 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
11734	1.135931	10.6.173.105	128.119.245.12	TCP	2780	53240 → 80 [ACK] Seq=54521 Ack=1 Min=12096 Len=2726 [TCP segment of a reassembled PDU]
11874	1.185795	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [ACK] Seq=60151 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
11894	1.195610	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [ACK] Seq=73603 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
11914	1.205281	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [ACK] Seq=79055 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
11934	1.212253	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [ACK] Seq=84507 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
11954	1.221489	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [ACK] Seq=89959 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
12294	1.452071	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [PSH, ACK] Seq=128123 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
11123	1.847488	10.6.173.105	128.119.245.12	TCP	5506	53240 → 80 [PSH, ACK] Seq=29987 Ack=1 Min=12096 Len=5452 [TCP segment of a reassembled PDU]
11754	1.140796	10.6.173.105	128.119.245.12	TCP	10958	53240 → 80 [PSH, ACK] Seq=57247 Ack