

Pulakesh Bag

Roll No: 120CS0131

Computer Science & Engineering
(2020-24)

Data Communications & Computer
Network Laboratory-3

Q1: Answer the following questions for captured file dns1.pcap (DNS Protocol)

Ans:

1.1. Locate the DNS query and response messages. Are they sent over UDP or TCP?

->

8 03:27:43.58...	128.238.38.160	128.238.29.23	DNS	72 Standard query 0x006e A www.ietf.org
9 03:27:43.58...	128.238.29.23	128.238.38.160	DNS	104 Standard query response 0x006e A www.ietf.org

They are sent over **UDP**

```
8 03:27:43... 128.238.38.160      128.238.29.23  DNS  72 Standard query 0x006e A www.ietf.org

> Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
< Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0x229e (8862)
    > 000. .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xd281 [validation disabled]
      [Header checksum status: Unverified]
    Source Address: 128.238.38.160
    Destination Address: 128.238.29.23
    > User Datagram Protocol, Src Port: 3163, Dst Port: 53
```

1.2. What is the destination port for the DNS query message? What is the source port of DNS response message?

->

Destination port for the DNS query message is **53**

```
8 03:27:43... 128.238.38.160      128.238.29.23  DNS  72 Standard query 0x006e A www.ietf.org

> Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
< Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0x229e (8862)
    > 000. .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xd281 [validation disabled]
      [Header checksum status: Unverified]
    Source Address: 128.238.38.160
    Destination Address: 128.238.29.23
    > User Datagram Protocol, Src Port: 3163, Dst Port: 53
    > Domain Name System (query)
```

source port of DNS response message is **53**

```
9 03:27:43... 128.238.29.23      128.238.38.160  DNS  104 Standard query response 0x006e A www.ietf.org A 132.1
> Frame 9: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
< Internet Protocol Version 4, Src: 128.238.29.23, Dst: 128.238.38.160
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 90
    Identification: 0xd595 (54677)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 126
  Protocol: UDP (17)
  Header Checksum: 0x216a [validation disabled]
    [Header checksum status: Unverified]
  Source Address: 128.238.29.23
  Destination Address: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3163
> Domain Name System (response)
```

1.3. To what IP address is the DNS query message sent? Use nm-tool command to determine the IP address of your local DNS server. Are these two IP addresses the same?

->

DNS query message sent is sent out to IP address **128.238.29.23**

```
8 03:27:43... 128.238.38.160      128.238.29.23  DNS  72 Standard query 0x006e A www.ietf.org
> Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
< Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0x229e (8862)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0xd281 [validation disabled]
    [Header checksum status: Unverified]
  Source Address: 128.238.38.160
  Destination Address: 128.238.29.23
> User Datagram Protocol, Src Port: 3163, Dst Port: 53
> Domain Name System (query)
```

1.4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

->

The DNS query is of type **Standard query(0x0100)**

```
8 03:27:43... 128.238.38.160      128.238.29.23  DNS  72 Standard query 0x006e A www.ietf.org
[Checksum Status: Unverified]
[Stream index: 1]
> [Timestamps]
  UDP payload (30 bytes)
< Domain Name System (query)
  Transaction ID: 0x006e
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    > Queries
      > www.ietf.org: type A, class IN
      [Response In: 9]
```

The query message contains ***no answers*** because Answer RRs: 0.

1.5. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

->

2 answers are provided in the response message.

9 03:27:4... 128.238.29.23 128.238.38... DNS 1... Standard query response 0x006e A www.ietf.org
 UDP payload (62 bytes)
 Domain Name System (response)
 Transaction ID: 0x006e
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 2
 Authority RRs: 0
 Additional RRs: 0
 Queries
 www.ietf.org: type A, class IN
 Answers
 www.ietf.org: type A, class IN, addr 132.151.6.75
 www.ietf.org: type A, class IN, addr 65.246.255.51
[Request In: 8]
[Time: 0.000811000 seconds]

The answers contain data regarding local DNS servers.

▼ Answers

- › www.ietf.org: type A, class IN, addr 132.151.6.75
- › www.ietf.org: type A, class IN, addr 65.246.255.51

1.6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

->

Destination IP address of the TCP SYN packet correspond to the IP address **132.151.6.75** which is also provided in the DNS response message.

10 03:27:43... 128.238.38.160 132.151.6.75 TCP 62 3369 → 80 [SYN] Seq=0 Win=64240 Len=0
 Frame 10: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
 Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
 Internet Protocol Version 4, Src: 128.238.38.160, Dst: 132.151.6.75
 Transmission Control Protocol, Src Port: 3369, Dst Port: 80, Seq: 0, Len: 0

1.7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

->

No, DNS location is retrieved once and then used in future until it expires, so we don't see

1.8. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

->

DNS query message is sent to the IP address **128.238.29.22**

No.	Time	Source	Destination	Protocol	Length	Info
488	02:50:35.848640	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.23
489	02:50:35.849007	128.238.29.22	128.238.38.160	DNS	1...	Standard query response 0x0001 PTR
490	02:50:35.849848	128.238.38.160	128.238.29.22	DNS	76	Standard query 0x0002 NS mit.edu.
491	02:50:35.850192	128.238.29.22	128.238.38.160	DNS	1...	Standard query response 0x0002 No
492	02:50:35.850423	128.238.38.160	128.238.29.22	DNS	67	Standard query 0x0003 NS mit.edu
493	02:50:35.850784	128.238.29.22	128.238.38.160	DNS	1...	Standard query response 0x0003 NS

No, this is not the IP address of my default local DNS server(192.168.1.250).

1.9. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

->

The three DNS query is of type **PTR**.

Query messages of the three queries contains **0** answer.

488 02:50:35.848640 128.238.38.160 128.238.29.22 DNS 86 Standard query 0x0001
Domain Name System (query) Transaction ID: 0x0001 Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries 22.29.238.128.in-addr.arpa: type PTR, class IN
490 02:50:35.849848 128.238.38.160 128.238.29.22 DNS 76 Standard query 0x0002
Domain Name System (query) Transaction ID: 0x0002 Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries
492 02:50:35.850423 128.238.38.160 128.238.29.22 DNS 67 Standard query 0x0003 NS mit.edu
Domain Name System (query) Transaction ID: 0x0003 Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries mit.edu: type NS, class IN

1.10. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

->

This message provide IP addresses of the MIT nameservers

bitsy.mit.edu(18.72.0.3), strawb.mit.edu(18.71.0.151), w20ns.mit.edu(18.70.0.160)

```
+-- 493 02:50:35.850784 128.238.29.22      128.238.38.160  DNS      176 Standard query response 0x0003
    |
    |   ✓ Answers
    |   > mit.edu: type NS, class IN, ns bitsy.mit.edu
    |   > mit.edu: type NS, class IN, ns strawb.mit.edu
    |   > mit.edu: type NS, class IN, ns w20ns.mit.edu
    |   ✓ Additional records
    |   > bitsy.mit.edu: type A, class IN, addr 18.72.0.3
    |   > strawb.mit.edu: type A, class IN, addr 18.71.0.151
    |   > w20ns.mit.edu: type A, class IN, addr 18.70.0.160
    |   [Request In: 492]
```

Q2. Answer the following questions for captured file tcp.pcap (TCP Protocol)

2.1. What is the IP address and TCP port number used by the client computer (source) that is transferring the 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" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows.

->

IP address is 192.168.1.102 and port number is 1161, that is used by the client computer (source) that is transferring the file to gaia.cs.umass.edu.

Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 50
[122 Reassembled TCP Segments (164090 bytes): #4(565), #5(1460), #7(1460), #8(1460), #10(1460), #11(1460), #13(114)
Hypertext Transfer Protocol
POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nUser-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20030208 Netscape/7.02\r\nAccept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpg,*/*;q=0.5\r\nAccept-Language: en-us, en;q=0.50\r\nAccept-Encoding: gzip, deflate, compress;q=0.9\r\n

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

->

IP address of gaia.cs.umass.edu is **128.119.245.12**.

Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 50
[122 Reassembled TCP Segments (164090 bytes): #4(565), #5(1460), #7(1460), #8(1460), #10(1460), #11(1460), #13(114)
Hypertext Transfer Protocol
POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nUser-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20030208 Netscape/7.02\r\nAccept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpg,*/*;q=0.5\r\nAccept-Language: en-us, en;q=0.50\r\nAccept-Encoding: gzip, deflate, compress;q=0.9\r\n

It is sending and receiving TCP segments for this connection on port number **80**.

2.3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

->

IP address and TCP port number used by my client computer (source) to transfer the file to gaia.cs.umass.edu is **192.168.1.102** and **1161** respectively.

2.4. 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? What is it in the segment that identifies the segment as a SYN segment?

->

Sequence number of the TCP SYN segment is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu. The value is 0 in this trace. The SYN flag is set to 1 and it indicates that this segment is a SYN segment.

The SYN flag is set to 1 and it indicates that this segment is a SYN segment.

A screenshot of the Wireshark network traffic analyzer. The interface shows a list of captured packets. The first two packets are highlighted in green. The first packet is a SYN from 192.168.1.102 to 128.119.245.12. The second packet is a SYNACK from 128.119.245.12 to 192.168.1.102. Below the packet list, the TCP flags for the first packet are expanded. The SYN flag is highlighted in blue, indicating it is set. Other flags like ACK, FIN, PSH, RST, and URG are shown as not set.

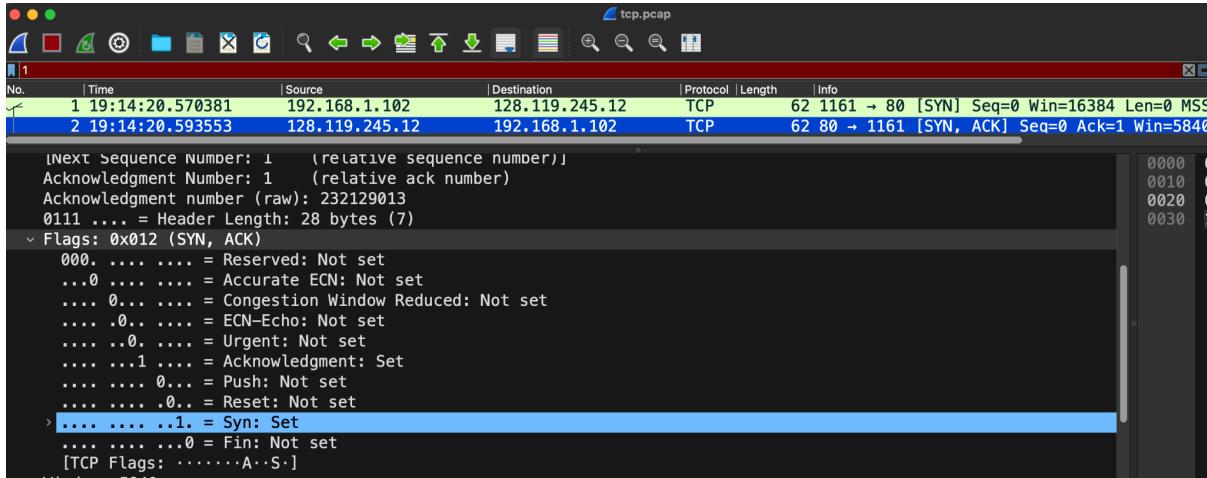
2.5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a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

->

Sequence number of the SYNACK segment from gaia.cs.umass.edu to the client computer in reply to the SYN has the value of 0 in this trace.

The value of the Acknowledgement field in the SYNACK segment is 1. The value of the Acknowledgement field in the SYNACK segment is determined by gaia.cs.umass.edu by adding 1 to the initial sequence number of SYN segment from the client computer (i.e. the sequence number of the SYN segment initiated by the client computer is 0.).

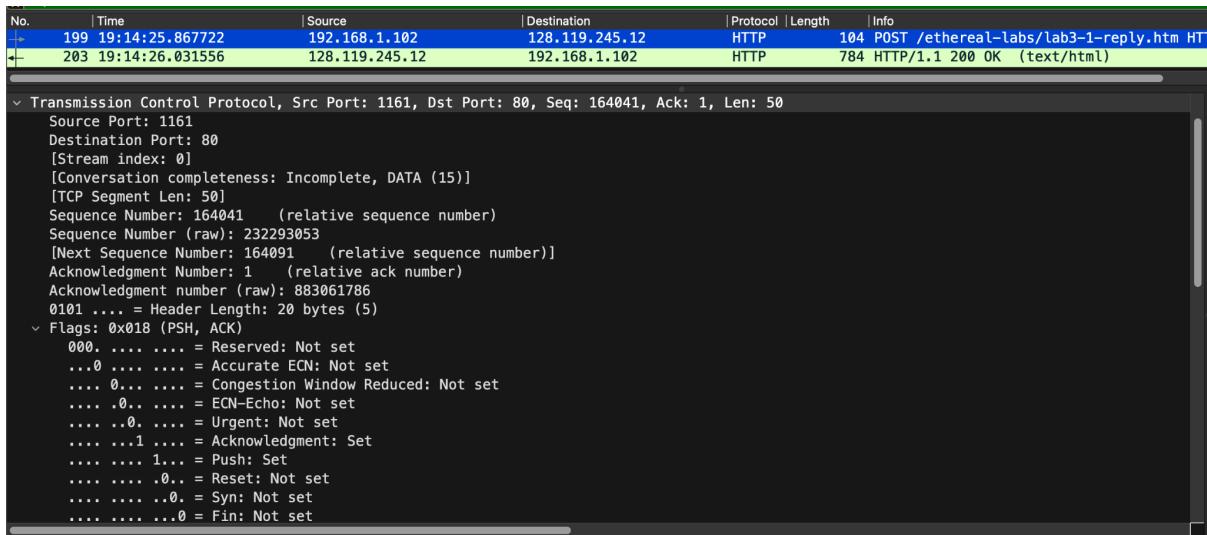
The SYN flag and Acknowledgement flag in the segment are set to 1 and they indicate that this segment is a SYNACK segment.



2.6. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command; you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

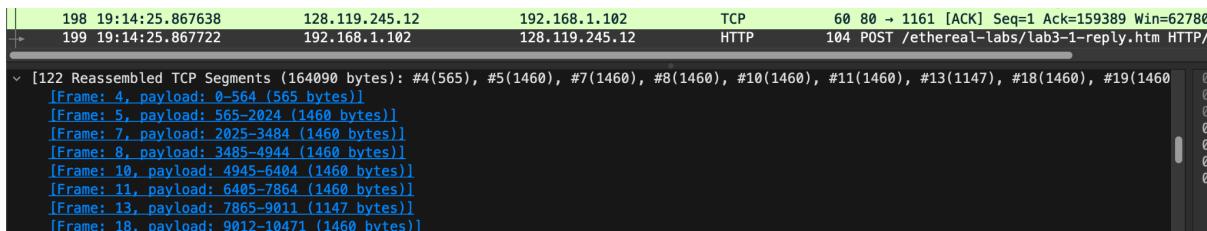
->

No. 199 segment is the TCP segment containing the HTTP POST command. The sequence number of this segment has the value of **164041**.



2.7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What is the length of each of the first six TCP segments?

->Length of the first segment is 565 Bytes and the next 5 packet contains 1460 Bytes each.



2.8. What is the EstimatedRTT value (see Section 3.5.3, page 239 in text from Kurose Book) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment. [Hint: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the “listing of captured packets” window that is being sent from the client to the gaia.cs.umass.edu server. Select as Statistics->TCP Stream Graph->Round Trip Time Graph.]

->

The HTTP POST segment is considered as the first segment. Segments 1 – 6 are No. 4, 5, 7, 8, 10, and 11 in this trace respectively. The ACKs of segments 1 – 6 are No. 6, 9, 12, 14, 15, and 16 in this trace.

	Sent time	ACK Received time	RTT (seconds)
Segment 1	0.026477	0.053937	0.02746
Segment 2	0.041737	0.077294	0.035557
Segment 3	0.054026	0.124085	0.070059
Segment 4	0.054690	0.169118	0.11443
Segment 5	0.077405	0.217299	0.13989
Segment 6	0.078157	0.267802	0.18964

$$\text{EstimatedRTT} = 0.875 * \text{EstimatedRTT} + 0.125 * \text{SampleRTT}$$

EstimatedRTT after the receipt of the ACK of segment 1:

$$\text{EstimatedRTT} = \text{RTT for Segment 1} = 0.02746 \text{ second}$$

EstimatedRTT after the receipt of the ACK of segment 2:

$$\text{EstimatedRTT} = 0.875 * 0.02746 + 0.125 * 0.035557 = 0.0285$$

EstimatedRTT after the receipt of the ACK of segment 3:

$$\text{EstimatedRTT} = 0.875 * 0.0285 + 0.125 * 0.070059 = 0.0337$$

EstimatedRTT after the receipt of the ACK of segment 4:

$$\text{EstimatedRTT} = 0.875 * 0.0337 + 0.125 * 0.11443 = 0.0438$$

EstimatedRTT after the receipt of the ACK of segment 5:

$$\text{EstimatedRTT} = 0.875 * 0.0438 + 0.125 * 0.13989 = 0.0558$$

EstimatedRTT after the receipt of the ACK of segment 6:

$$\text{EstimatedRTT} = 0.875 * 0.0558 + 0.125 * 0.18964 = 0.0725 \text{ second}$$

tcp.pcap

Apply a display filter ... <None>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
8	0.054698	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1147]
14	0.169118	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17	0.304887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]

Segments 1-6

tcp.pcap

Apply a display filter ... <None>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
8	0.054698	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1147]
14	0.169118	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17	0.304887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460 [TCP segment of ACK 1 ACK 1 Win=17520 Len=1460]

ACK of Segments 1-6