

COMPUTER NETWORKS LAB

Understanding Transport and Network Layer using Wireshark WEEK 6

NAME: VISHWA MEHUL MEHTA

SRN: PES2UG20CS389

SECTION: F

DATE: 09/04/2022

I. UDP and DNS:

1.

```
vishwa@vishwa-VirtualBox:~/Documents$ dig www.pluralsight.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.pluralsight.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58981
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.pluralsight.com.                IN      A

;; ANSWER SECTION:
www.pluralsight.com.        60      IN      CNAME   www.pluralsight.com.cdn.cloudflare.net.
www.pluralsight.com.cdn.cloudflare.net. 299 IN A 104.19.162.127
www.pluralsight.com.cdn.cloudflare.net. 299 IN A 104.19.161.127

;; Query time: 43 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Apr 03 16:12:14 IST 2022
;; MSG SIZE rcvd: 132
```

2.

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The second pane shows the details of the selected packet (Frame 1: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface enp0s3, id 0). The third pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.149398431	192.168.145.51	10.0.2.15	DNS	163	Standard query response 0x2cc9 A www.pluralsight.com CNAME ww...
8	1.212940425	192.168.145.51	10.0.2.15	DNS	201	Standard query response 0x19ce A connectivity-check.ubuntu.co...
1	0.000000000	10.0.2.15	192.168.145.51	DNS	79	Standard query 0x2cc9 A www.pluralsight.com
7	1.035850293	10.0.2.15	192.168.145.51	DNS	89	Standard query 0x19ce A connectivity-check.ubuntu.com

Frame 1: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface enp0s3, id 0

- Interface id: 0 (enp0s3)
- Encapsulation type: Ethernet (1)
- Arrival Time: Mar 31, 2022 14:35:41.353566755 IST
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1648717541.353566755 seconds
- [Time delta from previous captured frame: 0.000000000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 0.000000000 seconds]
- Frame Number: 1
- Frame Length: 79 bytes (632 bits)
- Capture Length: 79 bytes (632 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:udp:dns]
- [Coloring Rule Name: UDP]
- [Coloring Rule String: udp]
- Ethernet II, Src: PcsCompu_83:72:38 (08:00:27:83:72:38), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.145.51
- User Datagram Protocol, Src Port: 37351, Dst Port: 53
- Source Port: 37351
- Destination Port: 53

Raw packet data (hex and ASCII):

```
0000 52 54 00 12 35 00 08 00 27 83 72 38 08 00 45 00  RT..5...r8..E.
0010 00 41 d5 16 40 00 40 11 07 ab 0a 00 02 0f c0 a8  .A..@..
0020 91 33 31 e7 00 35 00 2d 5b 29 2c c9 01 00 00 01  .3...5...[.)...
0030 00 00 00 00 00 00 03 77 77 77 0b 70 6c 75 72 61  ....WWW...plura
0040 6c 73 69 67 68 74 03 63 6f 6d 00 00 01 00 01  .l...ght c om....
```

3.

The UDP segment headers expected are:

Source Port Number – 2 bytes, Destination Port Number – 2 bytes, Length – 2 bytes, Checksum – 2 bytes and rest are payload.

4.

As per the above mentioned predictions the headers in the UDP segment are as shown:

The screenshot shows a Wireshark packet capture on interface enp0s3. The filter is 'dns && ip.addr==10.0.2.15'. The packet list shows four packets: a DNS query response (163 bytes), a DNS query response (201 bytes), a DNS query (79 bytes), and a DNS query (89 bytes). The selected packet is the third one, a DNS query from 10.0.2.15 to 192.168.145.51. The packet details pane shows the User Datagram Protocol (UDP) header with Source Port: 37351, Destination Port: 53, Length: 45, and Checksum: 0x5e29 [unverified]. Below the UDP header is the Domain Name System (query) section, showing Transaction ID: 0x2cc9, Flags: 0x0100 Standard query, Questions: 1, Answer RRs: 0, Authority RRs: 0, and Additional RRs: 0. The packet bytes pane shows the raw data of the packet, with the first 12 bytes highlighted in blue, corresponding to the UDP header.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.149398431	192.168.145.51	10.0.2.15	DNS	163	Standard query response 0x2cc9 A www.pluralsight.com CNAME ww...
8	1.212940425	192.168.145.51	10.0.2.15	DNS	201	Standard query response 0x19ce A connectivity-check.ubuntu.co...
1	0.000000000	10.0.2.15	192.168.145.51	DNS	79	Standard query 0x2cc9 A www.pluralsight.com
7	1.035850293	10.0.2.15	192.168.145.51	DNS	89	Standard query 0x19ce A connectivity-check.ubuntu.com

Frame 1: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_83:72:38 (08:00:27:83:72:38), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.145.51
User Datagram Protocol, Src Port: 37351, Dst Port: 53

Source Port: 37351
Destination Port: 53
Length: 45
Checksum: 0x5e29 [unverified]
[Checksum Status: Unverified]
[Stream Index: 0]
[Timestamps]

Domain Name System (query)
Transaction ID: 0x2cc9
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 2]

0000 52 54 00 12 35 00 08 00 27 83 72 38 08 00 45 00 RT 5...r8..E.
0010 00 41 d5 16 40 00 40 11 07 ab 0a 00 02 0f c0 a8 A..@..@.....
0020 91 33 91 e7 00 35 00 2d 5e 29 2c c9 01 00 00 01 3...5...A),.....
0030 00 00 00 00 00 00 03 77 77 77 0b 70 6c 75 72 61www.plura
0040 6c 73 69 67 68 74 03 63 6f 6d 00 00 01 00 01 l...sight.c om.....

User Datagram Protocol (udp), 8 bytes

Packets: 19 · Displayed: 4 (21.1%) · Dropped: 0 (0.0%) · Profile: Default

5.

The UDP checksum covers UDP header and the UDP data.

The screenshot shows a Wireshark packet capture on interface enp0s3. The filter is 'dns && ip.addr==10.0.2.15'. The packet list shows four packets: a DNS query response (163 bytes), a DNS query response (201 bytes), a DNS query (79 bytes), and a DNS query (89 bytes). The selected packet is the third one, a DNS query from 10.0.2.15 to 192.168.145.51. The packet details pane shows the User Datagram Protocol (UDP) header with Source Port: 37351, Destination Port: 53, Length: 45, and Checksum: 0x5e29 [unverified]. Below the UDP header is the Domain Name System (query) section, showing Transaction ID: 0x2cc9, Flags: 0x0100 Standard query, Questions: 1, Answer RRs: 0, Authority RRs: 0, and Additional RRs: 0. The packet bytes pane shows the raw data of the packet, with the first 12 bytes highlighted in blue, corresponding to the UDP header.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.149398431	192.168.145.51	10.0.2.15	DNS	163	Standard query response 0x2cc9 A w
8	1.212940425	192.168.145.51	10.0.2.15	DNS	201	Standard query response 0x19ce A c
1	0.000000000	10.0.2.15	192.168.145.51	DNS	79	Standard query 0x2cc9 A www.plura
7	1.035850293	10.0.2.15	192.168.145.51	DNS	89	Standard query 0x19ce A connectivi

Frame 1: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_83:72:38 (08:00:27:83:72:38), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.145.51
User Datagram Protocol, Src Port: 37351, Dst Port: 53

Source Port: 37351
Destination Port: 53
Length: 45
Checksum: 0x5e29 [unverified]
[Checksum Status: Unverified]
[Stream Index: 0]
[Timestamps]

Domain Name System (query)
Transaction ID: 0x2cc9
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 2]

0000 52 54 00 12 35 00 08 00 27 83 72 38 08 00 45 00 RT 5...r8..E.
0010 00 41 d5 16 40 00 40 11 07 ab 0a 00 02 0f c0 a8 A..@..@.....
0020 91 33 91 e7 00 35 00 2d 5e 29 2c c9 01 00 00 01 3...5...A),.....
0030 00 00 00 00 00 00 03 77 77 77 0b 70 6c 75 72 61www.plura
0040 6c 73 69 67 68 74 03 63 6f 6d 00 00 01 00 01 l...sight.c om.....

II. TCP:

9.

14-740 Lab 2: File Upload — Mozilla Firefox

14-740 Lab 2: File Upload x +

www.ini740.com/Lab2/lab2a.html

If you are following the lab handout properly, you should have already downloaded a copy of *Canterbury Tales* and have Wireshark running.

Click on the following button and select the file where you stored *Canterbury Tales*:

Browse... pg2383.txt

Now that you have selected the file, click on the following button to start the upload. This will cause your browser to send the file over HTTP (using TCP, of course) to the web server.

Upload File

WS XHTML 1.0

11.

3-Way Handshake:

*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp && ip.addr==10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
5	0.338870752	10.0.2.15	128.2.131.88	TCP	74	47008 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
6	0.346050130	10.0.2.15	128.2.131.88	TCP	74	47010 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
7	0.617871873	10.0.2.15	128.2.131.88	TCP	74	47012 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
8	0.793472237	128.2.131.88	10.0.2.15	TCP	60	80 → 47010 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
9	0.793472491	128.2.131.88	10.0.2.15	TCP	60	80 → 47008 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
10	0.793501921	10.0.2.15	128.2.131.88	TCP	54	47010 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
11	0.793574524	10.0.2.15	128.2.131.88	TCP	54	47008 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
12	0.794594225	10.0.2.15	128.2.131.88	HTTP	405	GET /Lab2/lab2a.html HTTP/1.1
13	0.918162876	128.2.131.88	10.0.2.15	TCP	60	80 → 47008 [ACK] Seq=1 Ack=352 Win=32417 Len=0
14	1.153704113	128.2.131.88	10.0.2.15	TCP	60	80 → 47012 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
15	1.153704495	128.2.131.88	10.0.2.15	TCP	1354	80 → 47008 [PSH, ACK] Seq=1 Ack=352 Win=32417 Len=1300 [TCP s...
16	1.153762038	10.0.2.15	128.2.131.88	TCP	54	47012 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
17	1.153867636	10.0.2.15	128.2.131.88	TCP	54	47008 → 80 [ACK] Seq=352 Ack=1301 Win=63700 Len=0
18	1.154488721	128.2.131.88	10.0.2.15	HTTP	198	HTTP/1.1 200 OK (text/html)
19	1.154497689	10.0.2.15	128.2.131.88	TCP	54	47008 → 80 [ACK] Seq=352 Ack=1445 Win=63700 Len=0

Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0

Interface id: 0 (enp0s3)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 31, 2022 15:03:36.155107037 IST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1648719216.155107037 seconds

[Time delta from previous captured frame: 0.079092040 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.338870752 seconds]

Frame Number: 5

Frame Length: 74 bytes (592 bits)

Capture Length: 74 bytes (592 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp]

[Coloring Rule Name: HTTP]

Protocol Rule: ...

Time delta from previous displayed frame (frame.time_delta_displayed)

Packets: 1358 · Displayed: 1327 (97.7%) · Marked: 1 (0.1%) · Dropped: 0 (0.0%) Profile: Default

HTTP POST:

1336	24.005572280	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1667157 Win=32768 Len=0
1337	24.005572299	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1669265 Win=32768 Len=0
1338	24.005572318	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1672185 Win=32768 Len=0
1339	24.005572336	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1675105 Win=32768 Len=0
1340	24.005572355	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1678025 Win=32768 Len=0
1341	24.005579306	10.0.2.15	128.2.131.88	TCP	11734	47020 → 80 [PSH, ACK] Seq=1683865 Ack=1 Win=64240 Len=11680 [...]
1342	24.005618622	10.0.2.15	128.2.131.88	TCP	866	47020 → 80 [ACK] Seq=1695545 Ack=1 Win=64240 Len=812 [TCP seq...]
1343	24.005784431	10.0.2.15	128.2.131.88	HTTP	6460	POST /Lab2/lab2b.html HTTP/1.1 (text/plain)
1344	24.005902632	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1680133 Win=32768 Len=0
1345	24.005902677	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1681757 Win=32768 Len=0
1346	24.005902699	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1683865 Win=32768 Len=0
1347	24.005902725	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1686785 Win=32768 Len=0
1348	24.005902749	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1689705 Win=32768 Len=0
1349	24.005902773	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1692625 Win=32768 Len=0
1350	24.005902799	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1695545 Win=32768 Len=0
1351	24.005902827	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1697817 Win=32768 Len=0
1352	24.005906067	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1700737 Win=32768 Len=0
1353	24.005906099	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1702763 Win=32768 Len=0
1354	24.888724139	128.2.131.88	10.0.2.15	HTTP	929	HTTP/1.1 200 OK (text/html)
1355	24.888747250	10.0.2.15	128.2.131.88	TCP	54	47020 → 80 [ACK] Seq=1702763 Ack=876 Win=63875 Len=0
1356	29.842406571	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [FIN, ACK] Seq=876 Ack=1702763 Win=32768 Len=0
1357	29.842744021	10.0.2.15	128.2.131.88	TCP	54	47020 → 80 [FIN, ACK] Seq=1702763 Ack=877 Win=63875 Len=0

12.

Client:-

IP Address: 10.0.2.15

Port: 47008

Server IP Address: 128.2.131.88

Server Port number: 80

13.

tcp && ip.addr==10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
50	0.338870752	10.0.2.15	128.2.131.88	TCP	74	47008 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
60	0.346050130	10.0.2.15	128.2.131.88	TCP	74	47010 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
70	0.617871873	10.0.2.15	128.2.131.88	TCP	74	47012 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
80	0.793472237	128.2.131.88	10.0.2.15	TCP	60	80 → 47010 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
90	0.793472491	128.2.131.88	10.0.2.15	TCP	60	80 → 47008 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
100	0.793501921	10.0.2.15	128.2.131.88	TCP	54	47010 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
110	0.793574524	10.0.2.15	128.2.131.88	TCP	54	47008 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
120	0.794594225	10.0.2.15	128.2.131.88	TCP	405	47008 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=351
130	0.918162876	128.2.131.88	10.0.2.15	TCP	60	80 → 47008 [ACK] Seq=1 Ack=352 Win=32417 Len=0
141	1.153704113	128.2.131.88	10.0.2.15	TCP	60	80 → 47012 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
151	1.153704495	128.2.131.88	10.0.2.15	TCP	1354	80 → 47008 [PSH, ACK] Seq=1 Ack=352 Win=32417 Len=1300
161	1.153762038	10.0.2.15	128.2.131.88	TCP	54	47012 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
171	1.153867636	10.0.2.15	128.2.131.88	TCP	54	47008 → 80 [ACK] Seq=352 Ack=1301 Win=63700 Len=0

[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Sequence number (raw): 215365
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 972146686
0110 = Header Length: 24 bytes (6)
Flags: 0x012 (SYN, ACK)
0000 = Reserved: Not set
...0 = None: Not set
....0... = Congestion Window Reduced (CWR): Not set
....0... = ECN-Echo: Not set
....0... = Urgent: Not set
....1... = Acknowledgment: Set
....0... = Push: Not set
....0... = Reset: Not set
....1... = SYN: Set
....0... = FIN: Not set
[TCP Flags:A..S]
Window size value: 32768
[Calculated window size: 32768]
Checksum: 0x0582 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

0020 02 0f 00 50 07 a2 00 03 49 45 39 f1 c7 fe 60 12 ...P... IE9...
Destination Port (tcp.dstport), 2 bytes

Packets: 1358 · Displayed: 1327 (97.7%) · Marked: 1 (0.1%) · Dropped: 0 (0.0%) Profile: Default

A. TCP Basics:

14.

Sequence Number of TCP SYN:

Relative: 0

Raw: 2410673663

The absolute sequence number is the raw sequence number given in the packet info.

tcp && ip.addr==10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
1342	24.005618622	10.0.2.15	128.2.131.88	TCP	866	47020 → 80 [ACK] Seq=1696357 Ack=1 Win=64240 Len=812 [TCP seq...
1343	24.005618622	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1696357 Win=32768 Len=0
1344	24.005618622	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1696357 Win=32768 Len=0
1345	24.005618622	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1696357 Win=32768 Len=0
1346	24.005618622	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1696357 Win=32768 Len=0
1347	24.005618622	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1696357 Win=32768 Len=0
1348	24.005618622	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1696357 Win=32768 Len=0
1349	24.005618622	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1696357 Win=32768 Len=0
1350	24.005618622	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1696357 Win=32768 Len=0
1351	24.005618622	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1696357 Win=32768 Len=0
1352	24.005618622	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1696357 Win=32768 Len=0
1353	24.005618622	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=1696357 Win=32768 Len=0
1354	24.005618622	128.2.131.88	10.0.2.15	HTTP	929	HTTP/1.1 200 OK (text/html)

Frame 1343: 6460 bytes on wire (51680 bits), 6460 bytes captured (51680 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu, 83:72:38 (08:00:27:83:72:38), Dst: RealtekU, 12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.2.131.88
Transmission Control Protocol, Src Port: 47020, Dst Port: 80, Seq: 1696357, Ack: 1, Len: 6406
Source Port: 47020
Destination Port: 80
[Stream index: 8]
[TCP Segment Len: 6406]
Sequence number: 1696357 (relative sequence number)
Sequence number (raw): 294495804
[Next sequence number: 1702763 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 224749
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x208a [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (6406 bytes)

Frame 1343 (6460 bytes) · Reassemble TCP (12/02/02 bytes)
Time delta from previous displayed frame (frame.time_delta_displayed)

Packets: 1358 · Displayed: 1327 (97.7%) · Marked: 1 (0.1%) · Dropped: 0 (0.0%) Profile: Default

15.

The image shows a Wireshark packet capture window titled '*enp0s3'. The display filter is 'tcp && ip.addr==10.0.2.15'. The packet list shows several TCP segments. The selected packet is a SYNACK segment (No. 17, Time 0.000000000, Source 10.0.2.15, Destination 128.2.131.88, Protocol TCP, Length 60). The packet details pane shows the following information:

- [Stream index: 1]
- [TCP Segment Len: 0]
- Sequence number: 0 (relative sequence number)
- Sequence number (raw): 215365
- [Next sequence number: 1 (relative sequence number)]
- Acknowledgment number: 1 (relative ack number)
- Acknowledgment number (raw): 972146686
- 0110 = Header Length: 24 bytes (6)
- Flags: 0x012 (SYN, ACK)
- 0000 = Reserved: Not set
- ...0 = Nonce: Not set
-0... = Congestion Window Reduced (CWR): Not set
-0... = ECN-Echo: Not set
-0... = Urgent: Not set
-1... = Acknowledgment: Set
-0... = Push: Not set
-0... = Reset: Not set
-1... = Syn: Set
-0... = Fin: Not set
- [TCP Flags:A..S.]
- Window size value: 32768
- [Calculated window size: 32768]
- Checksum: 0x6582 [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0

The packet bytes pane shows the raw data: 0020 02 0f 00 50 07 12 00 03 49 45 39 f1 c7 fe 60 12 ...P... IE9... .

Packets: 1358 · Displayed: 1327 (97.7%) · Marked: 1 (0.1%) · Dropped: 0 (0.0%) · Profile: Default

Sequence Number of the SYNACK segment: 0

Acknowledgement field in SYNACK: 1

The server determines the acknowledgement using the sequence number of the next expected packet.

The acknowledgement and the syn bits are set to 1 which determines that it is a SYNACK segment.

16.

The image shows a Wireshark packet capture window titled 'TCP_1.pcapng'. The display filter is 'Apply a display filter ... <Ctrl-/>'. The packet list shows several TCP segments. The selected packet is an HTTP POST segment (No. 1343, Time 24.005784431, Source 10.0.2.15, Destination 128.2.131.88, Protocol HTTP, Length 6460). The packet details pane shows the following information:

- Source Port: 47020
- Destination Port: 80
- [Stream index: 8]
- [TCP Segment Len: 6406]
- Sequence number: 1696357 (relative sequence number)
- Sequence number (raw): 294495904
- [Next sequence number: 1702763 (relative sequence number)]
- Acknowledgment number: 1 (relative ack number)
- Acknowledgment number (raw): 224749
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window size value: 64240
- [Calculated window size: 64240]
- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0x288a [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- [SEQ/ACK analysis]
- [Timestamps]
- TCP payload (6406 bytes)
- TCP segment data (6406 bytes)
- [540 Reassembled TCP Segments (1702762 bytes): #118(2920), #119(2920), #122(2920), #123(2920), #126(2920), #128(2920), #130(2920), #131(2920), #134(2920), #135(2920), #138(2920), #139(2920), #140(2920), #141(2920), #142(2920), #143(2920), #144(2920), #145(2920), #146(2920), #147(2920), #148(2920), #149(2920), #150(2920), #151(2920), #152(2920), #153(2920), #154(2920), #155(2920), #156(2920), #157(2920), #158(2920), #159(2920), #160(2920), #161(2920), #162(2920), #163(2920), #164(2920), #165(2920), #166(2920), #167(2920), #168(2920), #169(2920), #170(2920), #171(2920), #172(2920), #173(2920), #174(2920), #175(2920), #176(2920), #177(2920), #178(2920), #179(2920), #180(2920), #181(2920), #182(2920), #183(2920), #184(2920), #185(2920), #186(2920), #187(2920), #188(2920), #189(2920), #190(2920), #191(2920), #192(2920), #193(2920), #194(2920), #195(2920), #196(2920), #197(2920), #198(2920), #199(2920), #200(2920), #201(2920), #202(2920), #203(2920), #204(2920), #205(2920), #206(2920), #207(2920), #208(2920), #209(2920), #210(2920), #211(2920), #212(2920), #213(2920), #214(2920), #215(2920), #216(2920), #217(2920), #218(2920), #219(2920), #220(2920), #221(2920), #222(2920), #223(2920), #224(2920), #225(2920), #226(2920), #227(2920), #228(2920), #229(2920), #230(2920), #231(2920), #232(2920), #233(2920), #234(2920), #235(2920), #236(2920), #237(2920), #238(2920), #239(2920), #240(2920), #241(2920), #242(2920), #243(2920), #244(2920), #245(2920), #246(2920), #247(2920), #248(2920), #249(2920), #250(2920), #251(2920), #252(2920), #253(2920), #254(2920), #255(2920), #256(2920), #257(2920), #258(2920), #259(2920), #260(2920), #261(2920), #262(2920), #263(2920), #264(2920), #265(2920), #266(2920), #267(2920), #268(2920), #269(2920), #270(2920), #271(2920), #272(2920), #273(2920), #274(2920), #275(2920), #276(2920), #277(2920), #278(2920), #279(2920), #280(2920), #281(2920), #282(2920), #283(2920), #284(2920), #285(2920), #286(2920), #287(2920), #288(2920), #289(2920), #290(2920), #291(2920), #292(2920), #293(2920), #294(2920), #295(2920), #296(2920), #297(2920), #298(2920), #299(2920), #300(2920), #301(2920), #302(2920), #303(2920), #304(2920), #305(2920), #306(2920), #307(2920), #308(2920), #309(2920), #310(2920), #311(2920), #312(2920), #313(2920), #314(2920), #315(2920), #316(2920), #317(2920), #318(2920), #319(2920), #320(2920), #321(2920), #322(2920), #323(2920), #324(2920), #325(2920), #326(2920), #327(2920), #328(2920), #329(2920), #330(2920), #331(2920), #332(2920), #333(2920), #334(2920), #335(2920), #336(2920), #337(2920), #338(2920), #339(2920), #340(2920), #341(2920), #342(2920), #343(2920), #344(2920), #345(2920), #346(2920), #347(2920), #348(2920), #349(2920), #350(2920), #351(2920), #352(2920), #353(2920), #354(2920), #355(2920), #356(2920), #357(2920), #358(2920), #359(2920), #360(2920), #361(2920), #362(2920), #363(2920), #364(2920), #365(2920), #366(2920), #367(2920), #368(2920), #369(2920), #370(2920), #371(2920), #372(2920), #373(2920), #374(2920), #375(2920), #376(2920), #377(2920), #378(2920), #379(2920), #380(2920), #381(2920), #382(2920), #383(2920), #384(2920), #385(2920), #386(2920), #387(2920), #388(2920), #389(2920), #390(2920), #391(2920), #392(2920), #393(2920), #394(2920), #395(2920), #396(2920), #397(2920), #398(2920), #399(2920), #400(2920), #401(2920), #402(2920), #403(2920), #404(2920), #405(2920), #406(2920), #407(2920), #408(2920), #409(2920), #410(2920), #411(2920), #412(2920), #413(2920), #414(2920), #415(2920), #416(2920), #417(2920), #418(2920), #419(2920), #420(2920), #421(2920), #422(2920), #423(2920), #424(2920), #425(2920), #426(2920), #427(2920), #428(2920), #429(2920), #430(2920), #431(2920), #432(2920), #433(2920), #434(2920), #435(2920), #436(2920), #437(2920), #438(2920), #439(2920), #440(2920), #441(2920), #442(2920), #443(2920), #444(2920), #445(2920), #446(2920), #447(2920), #448(2920), #449(2920), #450(2920), #451(2920), #452(2920), #453(2920), #454(2920), #455(2920), #456(2920), #457(2920), #458(2920), #459(2920), #460(2920), #461(2920), #462(2920), #463(2920), #464(2920), #465(2920), #466(2920), #467(2920), #468(2920), #469(2920), #470(2920), #471(2920), #472(2920), #473(2920), #474(2920), #475(2920), #476(2920), #477(2920), #478(2920), #479(2920), #480(2920), #481(2920), #482(2920), #483(2920), #484(2920), #485(2920), #486(2920), #487(2920), #488(2920), #489(2920), #490(2920), #491(2920), #492(2920), #493(2920), #494(2920), #495(2920), #496(2920), #497(2920), #498(2920), #499(2920), #500(2920), #501(2920), #502(2920), #503(2920), #504(2920), #505(2920), #506(2920), #507(2920), #508(2920), #509(2920), #510(2920), #511(2920), #512(2920), #513(2920), #514(2920), #515(2920), #516(2920), #517(2920), #518(2920), #519(2920), #520(2920), #521(2920), #522(2920), #523(2920), #524(2920), #525(2920), #526(2920), #527(2920), #528(2920), #529(2920), #530(2920), #531(2920), #532(2920), #533(2920), #534(2920), #535(2920), #536(2920), #537(2920), #538(2920), #539(2920), #540(2920), #541(2920), #542(2920), #543(2920), #544(2920), #545(2920), #546(2920), #547(2920), #548(2920), #549(2920), #550(2920), #551(2920), #552(2920), #553(2920), #554(2920), #555(2920), #556(2920), #557(2920), #558(2920), #559(2920), #560(2920), #561(2920), #562(2920), #563(2920), #564(2920), #565(2920), #566(2920), #567(2920), #568(2920), #569(2920), #570(2920), #571(2920), #572(2920), #573(2920), #574(2920), #575(2920), #576(2920), #577(2920), #578(2920), #579(2920), #580(2920), #581(2920), #582(2920), #583(2920), #584(2920), #585(2920), #586(2920), #587(2920), #588(2920), #589(2920), #590(2920), #591(2920), #592(2920), #593(2920), #594(2920), #595(2920), #596(2920), #597(2920), #598(2920), #599(2920), #600(2920), #601(2920), #602(2920), #603(2920), #604(2920), #605(2920), #606(2920), #607(2920), #608(2920), #609(2920), #610(2920), #611(2920), #612(2920), #613(2920), #614(2920), #615(2920), #616(2920), #617(2920), #618(2920), #619(2920), #620(2920), #621(2920), #622(2920), #623(2920), #624(2920), #625(2920), #626(2920), #627(2920), #628(2920), #629(2920), #630(2920), #631(2920), #632(2920), #633(2920), #634(2920), #635(2920), #636(2920), #637(2920), #638(2920), #639(2920), #640(2920), #641(2920), #642(2920), #643(2920), #644(2920), #645(2920), #646(2920), #647(2920), #648(2920), #649(2920), #650(2920), #651(2920), #652(2920), #653(2920), #654(2920), #655(2920), #656(2920), #657(2920), #658(2920), #659(2920), #660(2920), #661(2920), #662(2920), #663(2920), #664(2920), #665(2920), #666(2920), #667(2920), #668(2920), #669(2920), #670(2920), #671(2920), #672(2920), #673(2920), #674(2920), #675(2920), #676(2920), #677(2920), #678(2920), #679(2920), #680(2920), #681(2920), #682(2920), #683(2920), #684(2920), #685(2920), #686(2920), #687(2920), #688(2920), #689(2920), #690(2920), #691(2920), #692(2920), #693(2920), #694(2920), #695(2920), #696(2920), #697(2920), #698(2920), #699(2920), #700(2920), #701(2920), #702(2920), #703(2920), #704(2920), #705(2920), #706(2920), #707(2920), #708(2920), #709(2920), #710(2920), #711(2920), #712(2920), #713(2920), #714(2920), #715(2920), #716(2920), #717(2920), #718(2920), #719(2920), #720(2920), #721(2920), #722(2920), #723(2920), #724(2920), #725(2920), #726(2920), #727(2920), #728(2920), #729(2920), #730(2920), #731(2920), #732(2920), #733(2920), #734(2920), #735(2920), #736(2920), #737(2920), #738(2920), #739(2920), #740(2920), #741(2920), #742(2920), #743(2920), #744(2920), #745(2920), #746(2920), #747(2920), #748(2920), #749(2920), #750(2920), #751(2920), #752(2920), #753(2920), #754(2920), #755(2920), #756(2920), #757(2920), #758(2920), #759(2920), #760(2920), #761(2920), #762(2920), #763(2920), #764(2920), #765(2920), #766(2920), #767(2920), #768(2920), #769(2920), #770(2920), #771(2920), #772(2920), #773(2920), #774(2920), #775(2920), #776(2920), #777(2920), #778(2920), #779(2920), #780(2920), #781(2920), #782(2920), #783(2920), #784(2920), #785(2920), #786(2920), #787(2920), #788(2920), #789(2920), #790(2920), #791(2920), #792(2920), #793(2920), #794(2920), #795(2920), #796(2920), #797(2920), #798(2920), #799(2920), #800(2920), #801(2920), #802(2920), #803(2920), #804(2920), #805(2920), #806(2920), #807(2920), #808(2920), #809(2920), #810(2920), #811(2920), #812(2920), #813(2920), #814(2920), #815(2920), #816(2920), #817(2920), #818(2920), #819(2920), #820(2920), #821(2920), #822(2920), #823(2920), #824(2920), #825(2920), #826(2920), #827(2920), #828(2920), #829(2920), #830(2920), #831(2920), #832(2920), #833(2920), #834(2920), #835(2920), #836(2920), #837(2920), #838(2920), #839(2920), #840(2920), #841(2920), #842(2920), #843(2920), #844(2920), #845(2920), #846(2920), #847(2920), #848(2920), #849(2920), #850(2920), #851(2920), #852(2920), #853(2920), #854(2920), #855(2920), #856(2920), #857(2920), #858(2920), #859(2920), #860(2920), #861(2920), #862(2920), #863(2920), #864(2920), #865(2920), #866(2920), #867(2920), #868(2920), #869(2920), #870(2920), #871(2920), #872(2920), #873(2920), #874(2920), #875(2920), #876(2920), #877(2920), #878(2920), #879(2920), #880(2920), #881(2920), #882(2920), #883(2920), #884(2920), #885(2920), #886(2920), #887(2920), #888(2920), #889(2920), #890(2920), #891(2920), #892(2920), #893(2920), #894(2920), #895(2920), #896(2920), #897(2920), #898(2920), #899(2920), #900(2920), #901(2920), #902(2920), #903(2920), #904(2920), #905(2920), #906(2920), #907(2920), #908(2920), #909(2920), #910(2920), #911(2920), #912(2920), #913(2920), #914(2920), #915(2920), #916(2920), #917(2920), #918(2920), #919(2920), #920(2920), #921(2920), #922(2920), #923(2920), #924(2920), #925(2920), #926(2920), #927(2920), #928(2920), #929(2920), #930(2920), #931(2920), #932(2920), #933(2920), #934(2920), #935(2920), #936(2920), #937(2920), #938(2920), #939(2920), #940(2920), #941(2920), #942(2920), #943(2920), #944(2920), #945(2920), #946(2920), #947(2920), #948(2920), #949(2920), #950(2920), #951(2920), #952(2920), #953(2920), #954(2920), #955(2920), #956(2920), #957(2920), #958(2920), #959(2920), #960(2920), #961(2920), #962(2920), #963(2920), #964(2920), #965(2920), #966(2920), #967(2920), #968(2920), #969(2920), #970(2920), #971(2920), #972(2920), #973(2920), #974(2920), #975(2920), #976(2920), #977(2920), #978(2920), #979(2920), #980(2920), #981(2920), #982(2920), #983(2920), #984(2920), #985(2920), #986(2920), #987(2920), #988(2920), #989(2920), #990(2920), #991(2920), #992(2920), #993(2920), #994(2920), #995(2920), #996(2920), #997(2920), #998(2920), #999(2920), #1000(2920), #1001(2920), #1002(2920), #1003(2920), #1004(2920), #1005(2920), #1006(2920), #1007(2920), #1008(2920), #1009(2920), #1010(2920), #1011(2920), #1012(2920), #1013(2920), #1014(2920), #1015(2920), #1016(2920), #1017(2920), #1018(2920), #1019(2920), #1020(2920), #1021(2920), #1022(2920), #1023(2920), #1024(2920), #1025(2920), #1026(2920), #1027(2920), #1028(2920), #1029(2920), #1030(2920), #1031(2920), #1032(2920), #1033(2920), #1034(2920), #1035(2920), #1036(2920), #1037(2920), #1038(2920), #1039(2920), #1040(2920), #1041(2920), #1042(2920), #1043(2920), #1044(2920), #1045(2920), #1046(2920), #1047(2920), #1048(2920), #1049(2920), #1050(2920), #1051(2920), #1052(2920), #1053(2920), #1054(2920), #1055(2920), #1056(2920), #1057(2920), #1058(2920), #1059(2920), #1060(2920), #1061(2920), #1062(2920), #1063(2920), #1064(2920), #1065(2920), #1066(2920), #1067(2920), #1068(2920), #1069(2920), #1070(2920), #1071(2920), #1072(2920), #1073(2920), #1074(2920), #1075(2920), #1076(2920), #1077(2920), #1078(2920), #1079(2920), #1080(2920), #1081(2920), #1082(2920), #1083(2920), #1084(2920), #1085(2920), #1086(2920), #1087(2920), #1088(2920), #1089(2920), #1090(2920), #1091(2920), #1092(2920), #1093(2920), #1094(2920), #1095(2920), #1096(2920), #1097(2920), #1098(2920), #1099(2920), #1100(2920), #1101(2920), #1102(2920), #1103(2920), #1104(2920), #1105(2920), #1106(2920), #1107(2920), #1108(2920), #1109(2920), #1110(2920), #1111(2920), #1112(2920), #1113(2920), #1114(2920), #1115(2920), #1116(2920), #1117(2920), #1118(2920), #1119(2920), #1120(2920), #1121(2920), #1122(2920), #1123(2920), #1124(2920), #1125(2920), #1126(2920), #1127(2920), #1128(2920), #1129(2920), #1130(2920), #1131(2920), #1132(2920), #1133(2920), #1134(2920), #1135(2920), #1136(2920), #1137(2920), #1138(2920), #1139(2920), #1140(2920), #1141(2920), #1142(2920), #1143(2920), #1144(2920), #1145(2920), #1146(2920), #1147(2920), #1148(2920), #1149(2920), #1150(2920), #1151(2920), #1152(2920), #1153(2920), #1154(2920), #1155(2920), #1156(2920), #1157(2920), #1158(2920), #1159(2920), #1160(2920), #1161(2920), #1162(2920), #1163(2920), #1164(2920), #1165(2920), #1166(2920), #1167(2920), #1168(2920), #1169(2920), #1170(2920), #1171(2920), #1172(2920), #1173(2920), #1174(2920), #1175(2920), #1176(2920), #1177(2920), #1178(2920), #1179(2920), #1180(2920), #1181(2920), #1182(2920), #1183(2920), #1184(2920), #1185(2920), #1186(2920), #1187(2920), #1188(2920), #1189(2920), #1190(2920), #1191(2920), #1192(2920), #1193(2920), #1194(2920), #1195(2920), #1196(2920), #1197(2920), #1198(2920), #1199(2920), #1200(2920), #1201(2920), #1202(2920), #1

TCP_1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
118	11.899663631	10.0.2.15	128.2.131.88	TCP	2974	47020 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2920 [TCP seq...
119	11.899942265	10.0.2.15	128.2.131.88	TCP	2974	47020 → 80 [PSH, ACK] Seq=2921 Ack=1 Win=64240 Len=2920 [TCP ...
120	11.900133975	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=2921 Win=32768 Len=0
121	11.900134063	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=5841 Win=32768 Len=0
122	11.900420206	10.0.2.15	128.2.131.88	TCP	2974	47020 → 80 [PSH, ACK] Seq=5841 Ack=1 Win=64240 Len=2920 [TCP ...
123	11.900645718	10.0.2.15	128.2.131.88	TCP	2974	47020 → 80 [PSH, ACK] Seq=8761 Ack=1 Win=64240 Len=2920 [TCP ...
124	11.900830590	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=8761 Win=32768 Len=0
125	11.900830672	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=11681 Win=32768 Len=0
126	11.901172328	10.0.2.15	128.2.131.88	TCP	2974	47020 → 80 [PSH, ACK] Seq=11681 Ack=1 Win=64240 Len=2920 [TCP...
127	11.901342844	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=14601 Win=32768 Len=0
128	11.901590736	10.0.2.15	128.2.131.88	TCP	2974	47020 → 80 [PSH, ACK] Seq=14601 Ack=1 Win=64240 Len=2920 [TCP...
129	11.901757075	128.2.131.88	10.0.2.15	TCP	60	80 → 47020 [ACK] Seq=1 Ack=17521 Win=32768 Len=0
130	11.901998938	10.0.2.15	128.2.131.88	TCP	2974	47020 → 80 [PSH, ACK] Seq=17521 Ack=1 Win=64240 Len=2920 [TCP...
131	11.902036668	10.0.2.15	128.2.131.88	TCP	2974	47020 → 80 [PSH, ACK] Seq=20441 Ack=1 Win=64240 Len=2920 [TCP...

Frame 118: 2974 bytes on wire (23792 bits), 2974 bytes captured (23792 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu.83:72:38 (08:00:27:83:72:38), Dst: RealtekU.12:35:00 (52:54:00:12:35:00)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.2.131.88
 Transmission Control Protocol, Src Port: 47020, Dst Port: 80, Seq: 1, Ack: 1, Len: 2920

```

0000 52 54 00 12 35 00 08 00 27 83 72 38 08 00 45 00 RT...5...r8...E:
0010 0b 90 b9 94 40 00 40 06 66 6a 0a 00 02 0f 80 02 ...@. fj.....
0020 83 58 b7 ac 00 50 af 6f 2f 78 00 03 6d ed 50 18 -X...P.o /x...m.P-
0030 fa f0 1a ec 00 00 50 4f 53 54 20 2f 4c 61 62 32 .....P0 ST /Lab2
0040 2f 6c 61 62 32 62 2e 68 74 6d 6c 20 48 54 54 50 /lab2b.h tml HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www.
0060 69 6e 69 37 34 30 2e 63 6f 6d 0d 0a 55 73 65 72 ini740.c om..User
0070 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
0080 35 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 5.0 (X11 ; Linux
0090 78 38 36 5f 36 34 3b 20 72 76 3a 39 38 2e 30 29 x86_64; rv:98.0)
00a0 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 Gecko/2.0100101
00b0 46 69 72 65 66 6f 78 2f 39 38 2e 30 0d 0a 41 63 Firefox/98.0..Ac
00c0 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: te xt/html,
00d0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d applicat ion/xhtm
00e0 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f l+xml,ap plicatio
00f0 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 n/xml;q= 0.9,imag
0100 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 e/avif,i mage/web
0110 70 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 p,*/*;q= 0.8..Acc
0120 65 70 74 2d 4c 61 66 67 75 61 67 65 3a 20 65 6e ept-Lang uage: en
  
```

TCP_1.pcapng Packets: 1358 · Displayed: 1358 (100.0%)

Segments: 118, 119, 122, 123, 126, 128

Segment sequence numbers: 1, 2921, 5841, 8761, 11681, 14601

Segment Acknowledgements: 120, 121, 124, 125, 127, 129

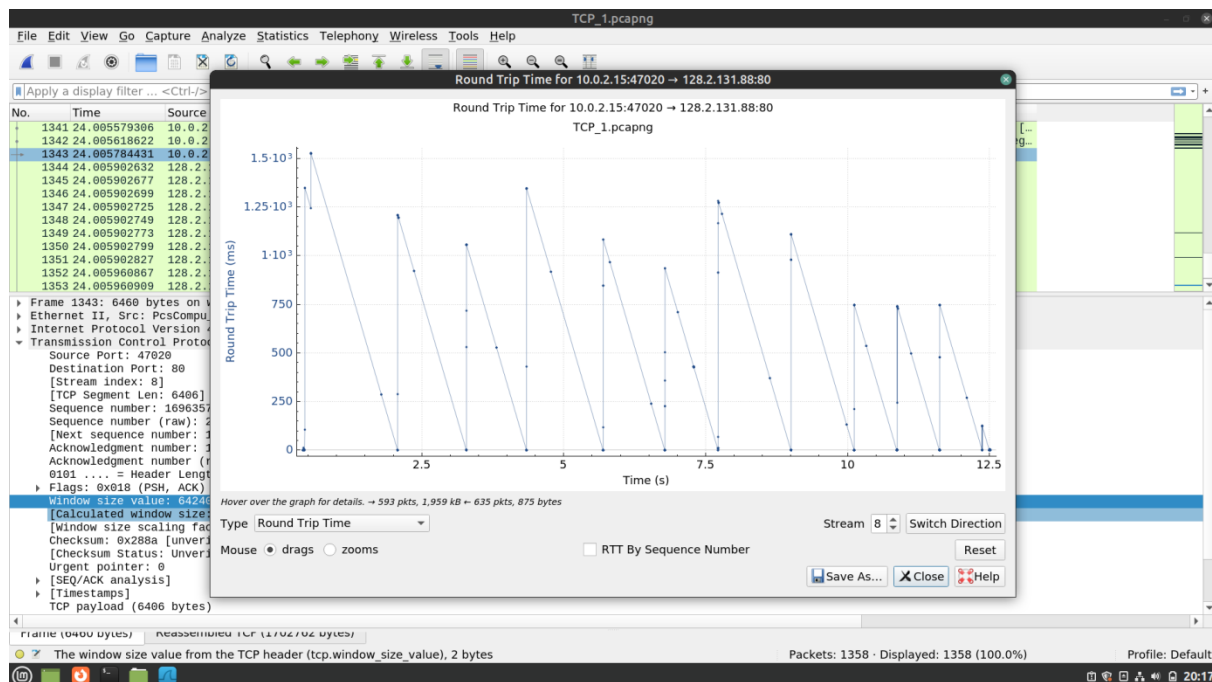
Round Trip Time (RTT) is the measure of how long it takes for a very small packet to travel across the network and for an acknowledgement of that packet to be returned.

Using the formula,

$$\text{EstimatedRTT} = (1 - \alpha) \cdot \text{EstimatedRTT} + \alpha \cdot \text{SampleRTT}$$

Where, $\alpha = 0.125$

Segment Number	Sample RTT	Estimated RTT
118	0.00047034	0.00047034
119	0.00019179	0.00043552
122	0.00041038	0.00043237
123	0.00018495	0.00040144
126	0.00017051	0.00037257
128	0.00016633	0.00034679

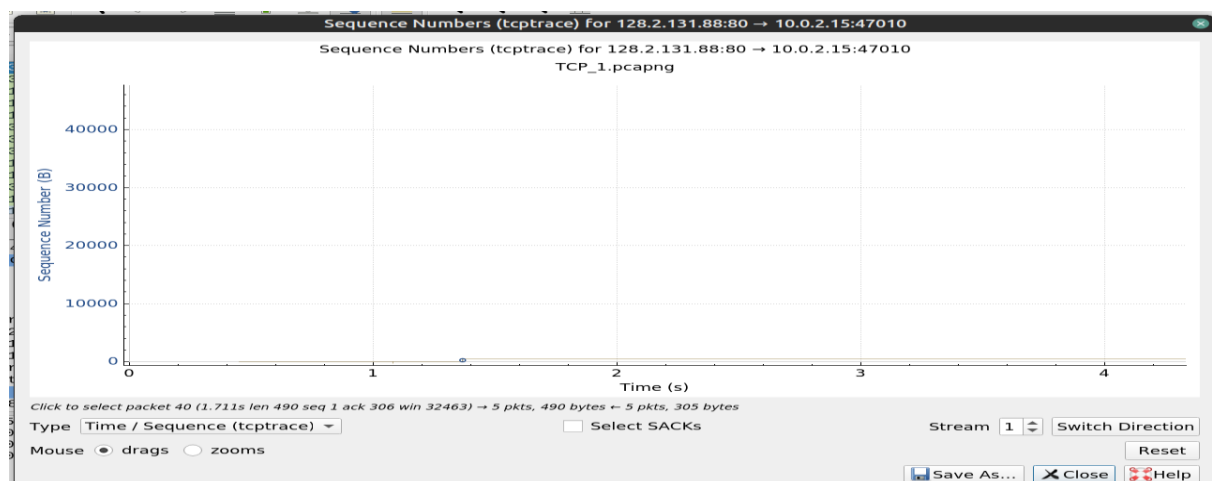


18.

- Acknowledgment number (raw): 372140000
- 0110 = Header Length: 24 bytes (6)
- **Flags: 0x012 (SYN, ACK)**
- Window size value: 32768
- [Calculated window size: 32768]
- Checksum: 0x0582 [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- Options: (4 bytes), Maximum segment size
- [SEQ/ACK analysis]
- [Timestamps]

Minimum buffer space available is 32768. The lack of buffer does not throttle the sender due to effective congestion avoidance.

19.



No segments have been retransmitted.

20.

The receiver acknowledges about 2920 packets after every 2 segments sent. There were no delayed ACKs found as there was no congestion in the network.

21.

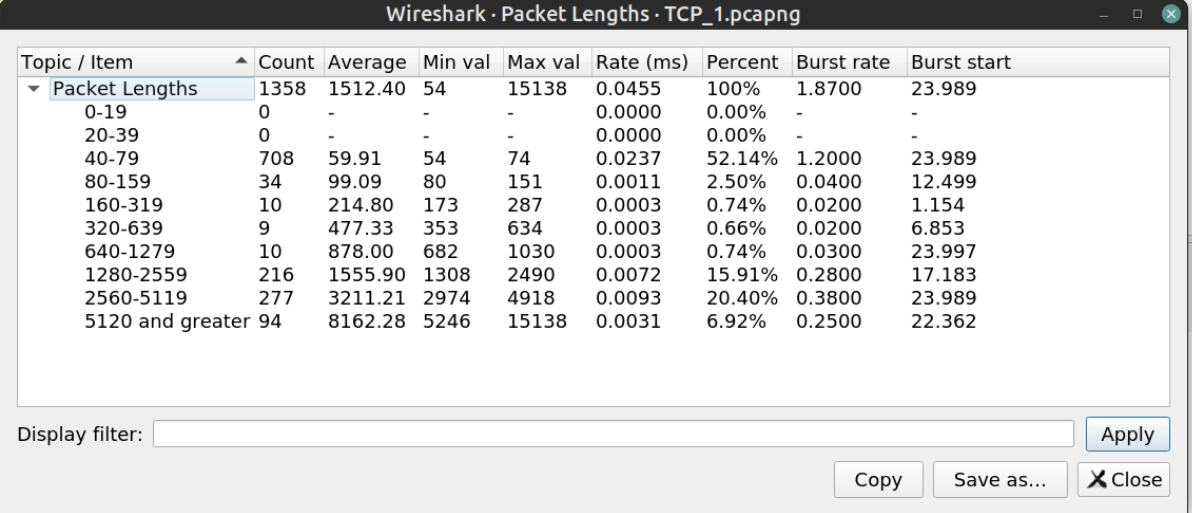
Total file size = 17,82,579.2 bytes

Total download time = (29.842 - 24.888)s = 4.954s

Throughput = 17,82,579.2 / 4.954 = 3,59,826.24 bytes/s
= 351.39 KBps

B. TCP Statistics:

22.



The image shows the 'Wireshark · Packet Lengths · TCP_1.pcapng' window. It displays a table of packet length statistics. The table has columns for Topic / Item, Count, Average, Min val, Max val, Rate (ms), Percent, Burst rate, and Burst start. The 'Packet Lengths' section is expanded, showing various ranges from 0-19 to 5120 and greater. The 40-79 range has the highest count (708) and percentage (52.14%).

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ Packet Lengths	1358	1512.40	54	15138	0.0455	100%	1.8700	23.989
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	708	59.91	54	74	0.0237	52.14%	1.2000	23.989
80-159	34	99.09	80	151	0.0011	2.50%	0.0400	12.499
160-319	10	214.80	173	287	0.0003	0.74%	0.0200	1.154
320-639	9	477.33	353	634	0.0003	0.66%	0.0200	6.853
640-1279	10	878.00	682	1030	0.0003	0.74%	0.0300	23.997
1280-2559	216	1555.90	1308	2490	0.0072	15.91%	0.2800	17.183
2560-5119	277	3211.21	2974	4918	0.0093	20.40%	0.3800	23.989
5120 and greater	94	8162.28	5246	15138	0.0031	6.92%	0.2500	22.362

Display filter: Apply Copy Save as... Close

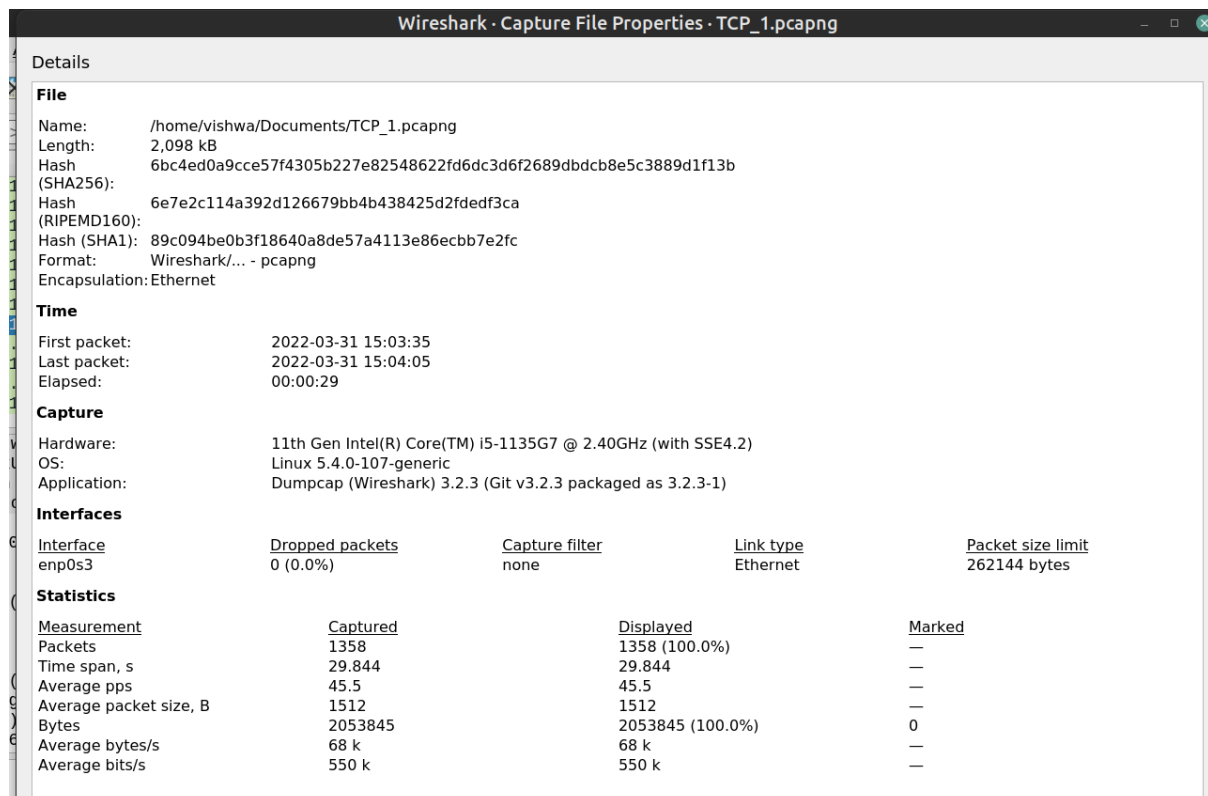
The most common packet length is in the range of 40-79 bytes.

The second-most common packet length range is 2560-5119 bytes.

The length of packets <40 bytes is 0 as the minimum header length is 40 bytes and any packet with <40 bytes contains no data.

Navigate to "Statistics -> Packet Lengths" to get the information.

23.



Average Throughput = $2053845 / 29.844 = 68819.36$ bytes/s = 0.065 MBps

Packets captured in the session = 1358

Total bytes = 2053845

Go to “Statistics -> Capture File Properties” to find the above observations.

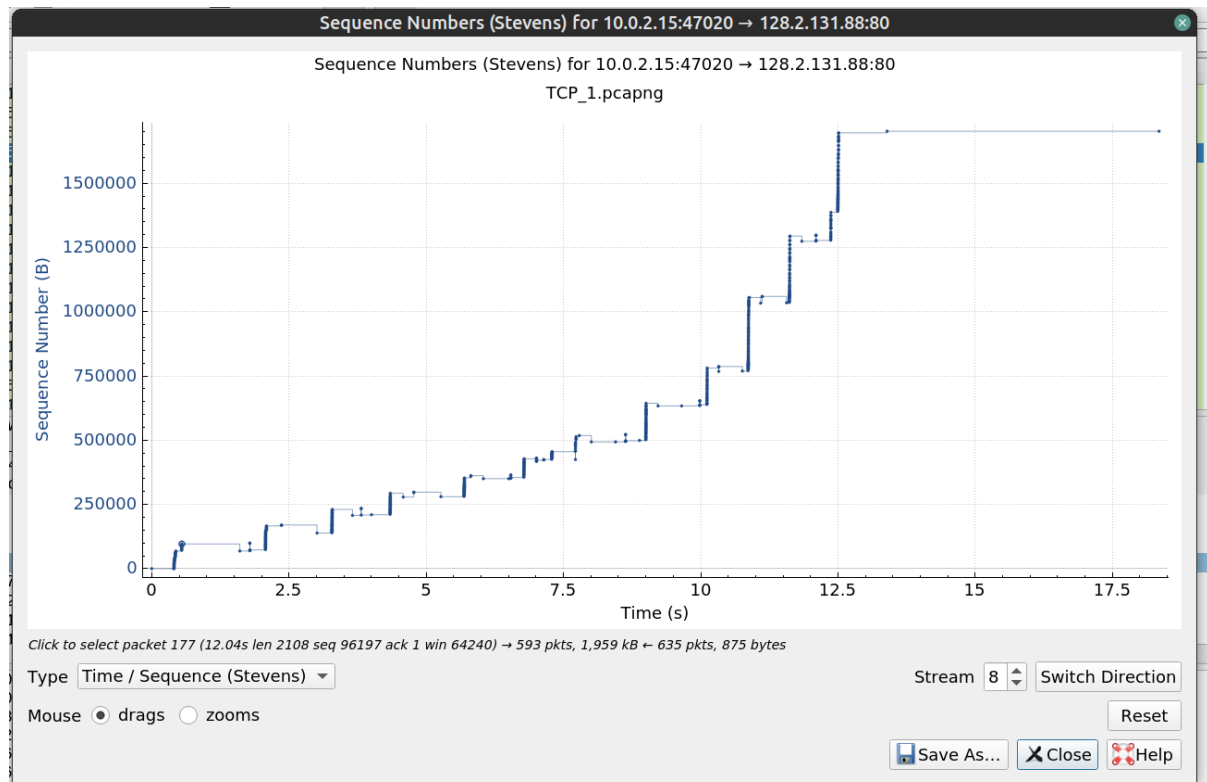
24.

Wireshark - Conversations - TCP_1.pcapng										
Ethernet · 1		IPv4 · 6		IPv6		TCP · 10		UDP · 15		
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
10.0.2.15	192.168.145.51	31	3,328	16	1,393	15	1,935	0.000000	15.5912	714
10.0.2.15	128.2.131.88	1,264	2,032,440	612	1,293,144	652	4,112	0.2338321	29.83240	540 k
10.0.2.15	34.120.208.123	11	2,110	5	1,580	6	530	1.213968	0.7930	15 k
10.0.2.15	128.30.52.100	21	4,276	11	933	10	3,343	1.576460	6.7222	1,110
10.0.2.15	34.117.237.239	27	8,576	16	1,938	11	6,638	6.597846	0.8345	18 k
10.0.2.15	35.82.103.10	4	288	2	143	2	145	9.963252	0.2426	4,716

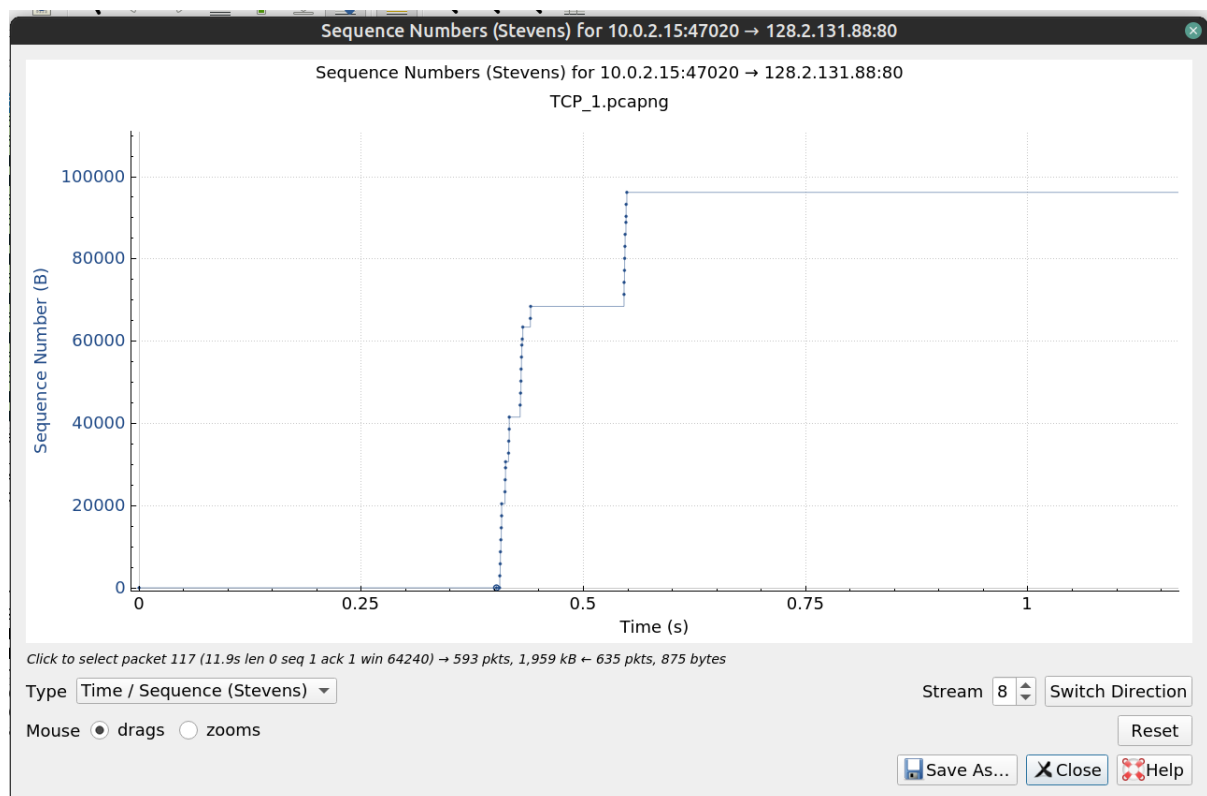
The local host conversed with the remote host with IP address 128.2.131.88 the most. 612 packets were sent to the remote host and 652 packets were sent from the remote host.

III. Congestion Control:

25.



26.



Slow start phase begins: 0.402s

Slow start phase ends: 0.440s

IV. The Network Layer:

27.

The image shows a Wireshark packet capture of a DNS query and response. The filter is 'dns && ip.addr==10.0.2.15'. The packet list shows four packets: a DNS query from 10.0.2.15 to 192.168.145.51 (packet 1), and three DNS responses from 192.168.145.51 to 10.0.2.15 (packets 2, 7, and 8). The packet details pane for packet 1 shows the User Datagram Protocol (Source Port: 37351, Destination Port: 53) and the Domain Name System (query) section. The query is for 'www.pluralsight.com' with transaction ID 0x2cc9. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.168.145.51	DNS	79	Standard query 0x2cc9 A www.pluralsight.com
2	0.149398431	192.168.145.51	10.0.2.15	DNS	163	Standard query response 0x2cc9 A www.pluralsight.com CNAME ww...
7	0.886451862	10.0.2.15	192.168.145.51	DNS	89	Standard query 0x19ce A connectivity-check.ubuntu.com
8	0.177090132	192.168.145.51	10.0.2.15	DNS	201	Standard query response 0x19ce A connectivity-check.ubuntu.co...

Frame 1: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_83:72:38 (08:00:27:83:72:38), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.145.51
User Datagram Protocol, Src Port: 37351, Dst Port: 53
Source Port: 37351
Destination Port: 53
Length: 45
Checksum: 0x5e29 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
Domain Name System (query)
Transaction ID: 0x2cc9
Flags: 0x0100 Standard query
0... .. = Response: Message is a query
0000... .. = Opcode: Standard query (0)
...0... .. = Truncated: Message is not truncated
...1... .. = Recursion desired: Do query recursively
...0... .. = Z: reserved (0)
...0... .. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0

0000 52 54 00 12 35 00 08 00 27 83 72 38 08 00 45 00 RT..5...'.r8..E.
0010 00 41 d5 16 40 00 40 11 07 ab 0a 00 02 0f c0 a8 .A..@... ..
0020 91 33 91 e7 00 35 00 2d 5e 29 2c c9 01 00 00 01 .3...5...^),....
0030 00 00 00 00 00 00 03 77 77 77 0b 70 6c 75 72 61w ww.plura
0040 6c 73 69 67 68 74 03 63 6f 6d 00 00 01 00 01 lsight.c om.....

29.

Datagram Length: 45 bytes

Upper Layer Protocol: IPv4

IP Address Fields:-

Src: 10.0.2.15

Dest: 192.168.145.51

31.

The image shows a Wireshark packet capture of an IP packet. The packet list shows four packets: a DNS query from 10.0.2.15 to 192.168.145.51 (packet 1), and three DNS responses from 192.168.145.51 to 10.0.2.15 (packets 2, 7, and 8). The packet details pane for packet 1 shows the Internet Protocol Version 4 section. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Leng
1	0.000000000	10.0.2.15	192.168.145.51	DNS	
2	0.149398431	192.168.145.51	10.0.2.15	DNS	
7	0.886451862	10.0.2.15	192.168.145.51	DNS	
8	0.177090132	192.168.145.51	10.0.2.15	DNS	

Frame 7: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on in
Ethernet II, Src: PcsCompu_83:72:38 (08:00:27:83:72:38), Dst: RealtekU_1
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.145.51
0100 = Version: 4
...0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 75
Identification: 0xd5fe (54782)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0x06b9 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.15
Destination: 192.168.145.51

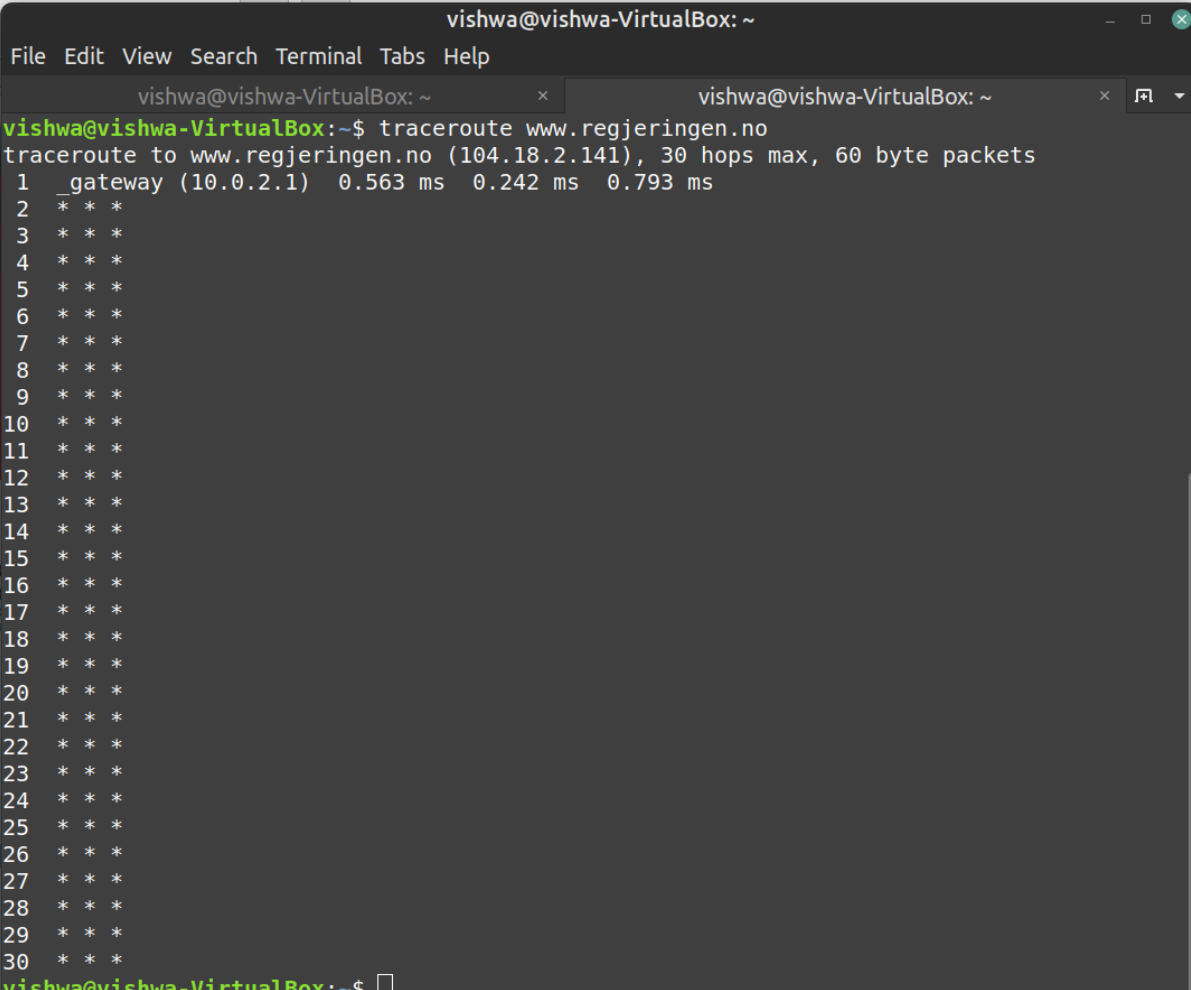
TTL: 64

OS: Linux Mint 20.3 Cinnamon

OS Version: 5.2.7

V. ICMP:

32.



```
vishwa@vishwa-VirtualBox: ~  
File Edit View Search Terminal Tabs Help  
vishwa@vishwa-VirtualBox: ~ x vishwa@vishwa-VirtualBox: ~ x  
vishwa@vishwa-VirtualBox:~$ traceroute www.regjeringen.no  
traceroute to www.regjeringen.no (104.18.2.141), 30 hops max, 60 byte packets  
1 _gateway (10.0.2.1) 0.563 ms 0.242 ms 0.793 ms  
2 * * *  
3 * * *  
4 * * *  
5 * * *  
6 * * *  
7 * * *  
8 * * *  
9 * * *  
10 * * *  
11 * * *  
12 * * *  
13 * * *  
14 * * *  
15 * * *  
16 * * *  
17 * * *  
18 * * *  
19 * * *  
20 * * *  
21 * * *  
22 * * *  
23 * * *  
24 * * *  
25 * * *  
26 * * *  
27 * * *  
28 * * *  
29 * * *  
30 * * *  
vishwa@vishwa-VirtualBox:~$
```

Traceroute.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.addr == 10.0.2.15						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	104.18.2.141	UDP	74	47750 → 33434 Len=32
2	0.000556921	10.0.2.1	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3	0.000998731	10.0.2.15	104.18.2.141	UDP	74	46271 → 33435 Len=32
4	0.000237551	10.0.2.1	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5	0.000342881	10.0.2.15	104.18.2.141	UDP	74	44897 → 33436 Len=32
6	0.000789109	10.0.2.1	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7	0.000645816	10.0.2.15	104.18.2.141	UDP	74	54913 → 33437 Len=32
8	0.000316272	10.0.2.15	104.18.2.141	UDP	74	57389 → 33438 Len=32
9	0.000326611	10.0.2.15	104.18.2.141	UDP	74	50635 → 33439 Len=32
10	0.000346958	10.0.2.15	104.18.2.141	UDP	74	34407 → 33440 Len=32
11	0.000343709	10.0.2.15	104.18.2.141	UDP	74	46621 → 33441 Len=32
12	0.000342998	10.0.2.15	104.18.2.141	UDP	74	33206 → 33442 Len=32
13	0.000355095	10.0.2.15	104.18.2.141	UDP	74	38778 → 33443 Len=32
14	0.000318372	10.0.2.15	104.18.2.141	UDP	74	43517 → 33444 Len=32
15	0.000344126	10.0.2.15	104.18.2.141	UDP	74	34348 → 33445 Len=32
16	0.014261356	10.0.2.15	104.18.2.141	UDP	74	56964 → 33446 Len=32
17	0.000237286	10.0.2.15	104.18.2.141	UDP	74	36952 → 33447 Len=32
▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0 ▶ Ethernet II, Src: PcsCompu_83:72:38 (08:00:27:83:72:38), Dst: RealtekU_12:35:00 (52:54:00:12:35:00) ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.18.2.141 ▶ User Datagram Protocol, Src Port: 47750, Dst Port: 33434 Source Port: 47750 Destination Port: 33434 Length: 40 Checksum: 0x76e7 [unverified] [Checksum Status: Unverified] [Stream index: 0] ▶ [Timestamps] ▶ Data (32 bytes)						
0000	52 54 00 12 35 00	08 00 27 83 72 38	08 00 45 00	RT=5	00 00 00 00	E
0010	00 3c f3 a0 00 00	01 11 4f 63 0a 00	02 0f 68 12	<<.....	0c	h
0020	02 8d ba 86 82 9a	00 28 76 e7 40 41	42 43 44 45(v @ABCDE	
0030	46 47 48 49 4a 4b	4c 4d 4e 4f 50 51	52 53 54 55	FGHIJKLM	NOPQRSTU	
0040	56 57 58 59 5a 5b	5c 5d 5e 5f		VWXYZ[\]	^_	

35.

When traceroute was used:-

First Destination Port: 33434

Second Destination Port: 33435

Third Destination Port: 33436

And so on...

Destination Port number increases by 1 every hop.

36.

To inspect the ICMP reply packet ping was used instead of traceroute as the traceroute was not showing any proper routes to be examined.

```
vishwa@vishwa-VirtualBox: ~
File Edit View Search Terminal Tabs Help

vishwa@vishwa-VirtualBox: ~ x vishwa@vishwa-VirtualBox: ~ x
vishwa@vishwa-VirtualBox:~$ ping www.regjeringen.no
PING www.regjeringen.no (104.18.3.141) 56(84) bytes of data.
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=1 ttl=59 time=6.22 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=2 ttl=59 time=7.59 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=3 ttl=59 time=9.46 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=4 ttl=59 time=7.87 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=5 ttl=59 time=6.36 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=6 ttl=59 time=7.21 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=7 ttl=59 time=4.89 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=8 ttl=59 time=3.31 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=9 ttl=59 time=5.74 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=10 ttl=59 time=7.32 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=11 ttl=59 time=9.60 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=12 ttl=59 time=7.23 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=13 ttl=59 time=6.03 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=14 ttl=59 time=7.64 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=15 ttl=59 time=9.21 ms
64 bytes from 104.18.3.141 (104.18.3.141): icmp_seq=16 ttl=59 time=6.74 ms
^C
--- www.regjeringen.no ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15039ms
rtt min/avg/max/mdev = 3.307/7.026/9.597/1.603 ms
```

Ping_1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.168.1.1	DNS	89	Standard query 0xc901 A www.regjeringen.no OPT
2	0.000395922	10.0.2.15	192.168.1.1	DNS	89	Standard query 0x11be AAAA www.regjeringen.no OPT
3	0.235189130	192.168.1.1	10.0.2.15	DNS	145	Standard query response 0x11be AAAA www.regjeringen.no AAAA 2...
4	4.766962597	10.0.2.15	192.168.1.1	DNS	89	Standard query 0xc901 A www.regjeringen.no OPT
5	0.014678604	192.168.1.1	10.0.2.15	DNS	121	Standard query response 0xc901 A www.regjeringen.no A 104.18...
6	0.000841944	10.0.2.15	104.18.3.141	ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 7)
7	0.006161892	104.18.3.141	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=59 (request in...
8	0.000392683	10.0.2.15	192.168.1.1	DNS	96	Standard query 0x1012 PTR 141.3.18.104.in-addr.arpa OPT
9	0.010151521	PcsCompu_83:72:38	RealtekU_12:35:00	ARP	42	Who has 10.0.2.1? Tell 10.0.2.15
10	0.000377041	RealtekU_12:35:00	PcsCompu_83:72:38	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
11	0.009869902	192.168.1.1	10.0.2.15	DNS	158	Standard query response 0x1012 No such name PTR 141.3.18.104...

Frame 7: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0

Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_83:72:38 (08:00:27:83:72:38)

Internet Protocol Version 4, Src: 104.18.3.141, Dst: 10.0.2.15

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0xc558 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256 (0x0100)

[Request frame: 6]

[Response time: 6.162 ms]

Timestamp from icmp data: Apr 9, 2022 20:10:01.000000000 IST

[Timestamp from icmp data (relative): 0.126390446 seconds]

Data (48 bytes)

```
0000 08 00 27 83 72 38 52 54 00 12 35 00 08 00 45 00  ..rRRT..5...E
0010 00 54 30 ec 00 00 3b 01 d7 0f 68 12 03 8d 0a 00  T0...;...h...
0020 02 0f 00 00 c5 58 00 01 00 01 c1 9a 51 62 00 00  ....X...Qb...
0030 00 00 67 d5 01 00 00 00 00 00 10 11 12 13 14 15  ..g.....!#$%
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..:.....!*+,-./012345
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060 36 37 67
```

ICMP Type: 0

ICMP Code: 0

Identifiers: 1(BE), 256(LE)

Sequence numbers: 1(BE), 256(LE)

37.

Timestamp from icmp data is mentioned to relate to the sent packets.

38.

Both ping and traceroute screenshots are pasted above for reference.

Ping does not show the port numbers for every hop unlike traceroute.