

CSE 3501

INFORMATION SECURITY ANALYSIS & AUDIT



Lab FAT Exam

L9+L10 | PLBG04
Dr. Vimala Devi K

FALL SEMESTER 2021-22

by

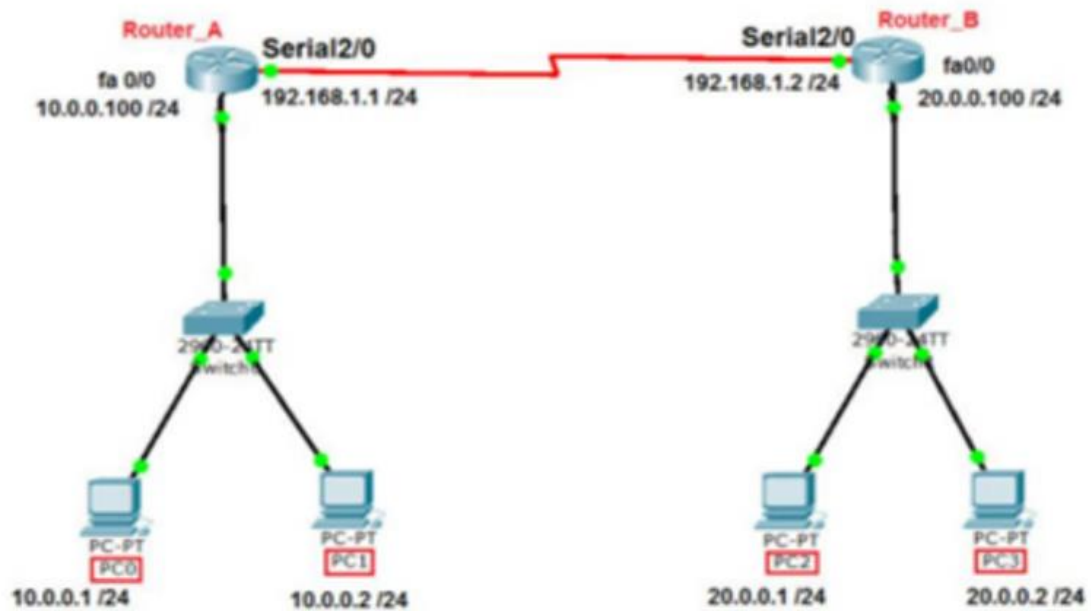
SHARADINDU ADHIKARI

19BCE2105

SET B Group 2

Question 1

1. Create a network infrastructure given below and implement the static routing for the routers present in the network. Do all IP address assignment and show ping messages from one network to another. (35 marks)



Q1.

19BCE2105

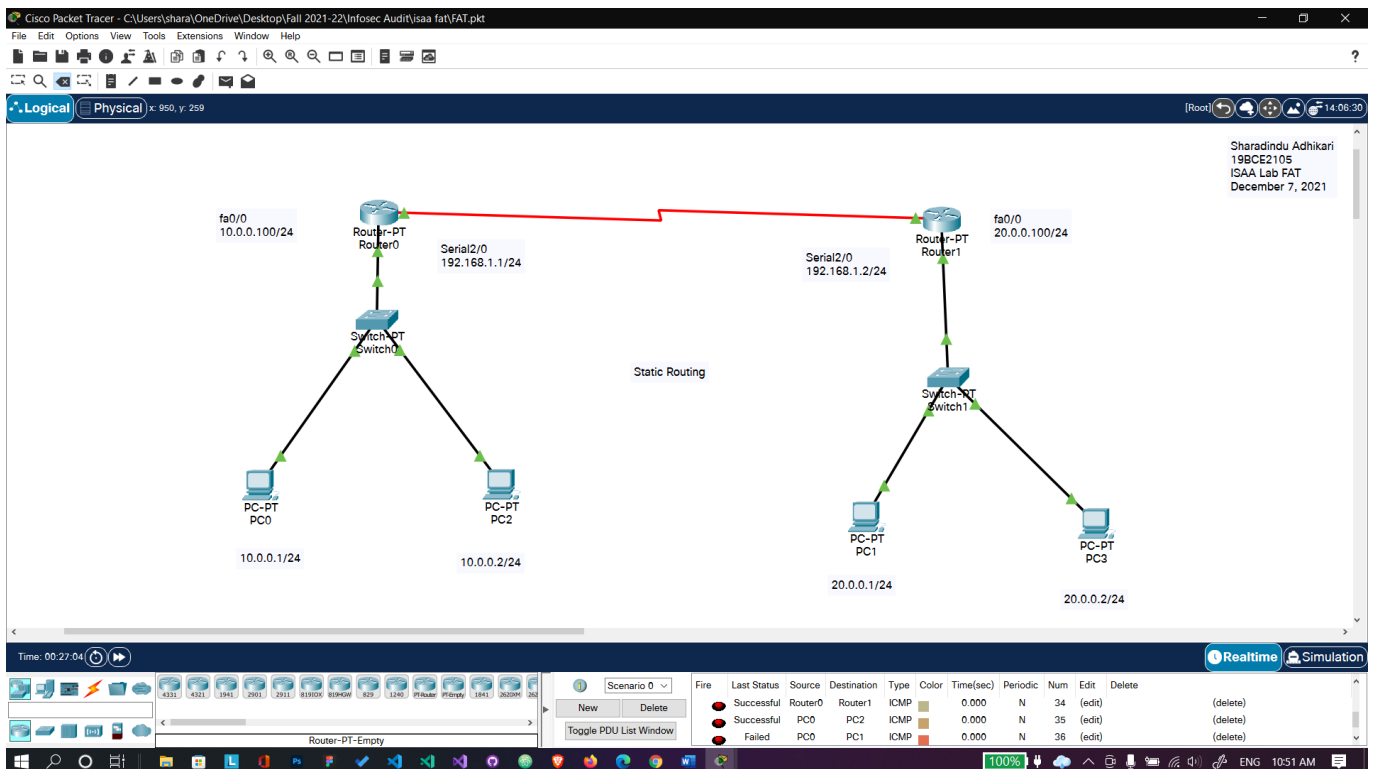
AIM: To create a network infrastructure given, and implement the static routing for the routers present in the network.

Given: IP addresses: PCs: 10.0.0.1/24
10.0.0.2/24
20.0.0.1/24
20.0.0.2/24

procedure:

- I've first configured all PCs according to the given IPs.
- Followed by configuring the fa and serial ports of Routers.
- ~~Initially~~, we then ~~we~~ I've sent PDU, from one network to another.
- Followed by marking all of them with comments.
- Finally I sent ping messages from CLI.
- Taken the screenshots.

Conclusion: I've thus implemented static routing for the routers.



PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	PC1	ICMP		0.000	N	24	(edit)	(delete)
●	Successful	PC0	PC2	ICMP		0.000	N	25	(edit)	(delete)
●	Successful	PC2	PC1	ICMP		0.000	N	26	(edit)	(delete)
●	Successful	PC3	PC1	ICMP		0.000	N	27	(edit)	(delete)
●	Successful	PC3	PC2	ICMP		0.000	N	28	(edit)	(delete)
●	Successful	PC0	PC3	ICMP		0.000	N	29	(edit)	(delete)
●	Successful	Router1	Router0	ICMP		0.000	N	30	(edit)	(delete)
●	Successful	PC1	PC2	ICMP		0.000	N	31	(edit)	(delete)

PC2

Physical Config Desktop Programming Attributes

Command Prompt

```

Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```

Packet Tracer PC Command Line 1.0
C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time<1ms TTL=128
Reply from 20.0.0.2: bytes=32 time<1ms TTL=128
Reply from 20.0.0.2: bytes=32 time<1ms TTL=128
Reply from 20.0.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

```
Router#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#
```

```
Router(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.1
```

```
Router(config)#
```

```
Router#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#
```

```
Router(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.1
```

```
Router(config)#
```

Question 2

Wireshark experiment (15 marks)

2. a) In Wireshark List 5 different protocols that appear in the protocol column in the unfiltered packet-listing window.
- b) In Wire shark If a packet is highlighted by black, what does it mean for the packet?
- c) In Wire shark What is the filter command for listing all outgoing http traffic?

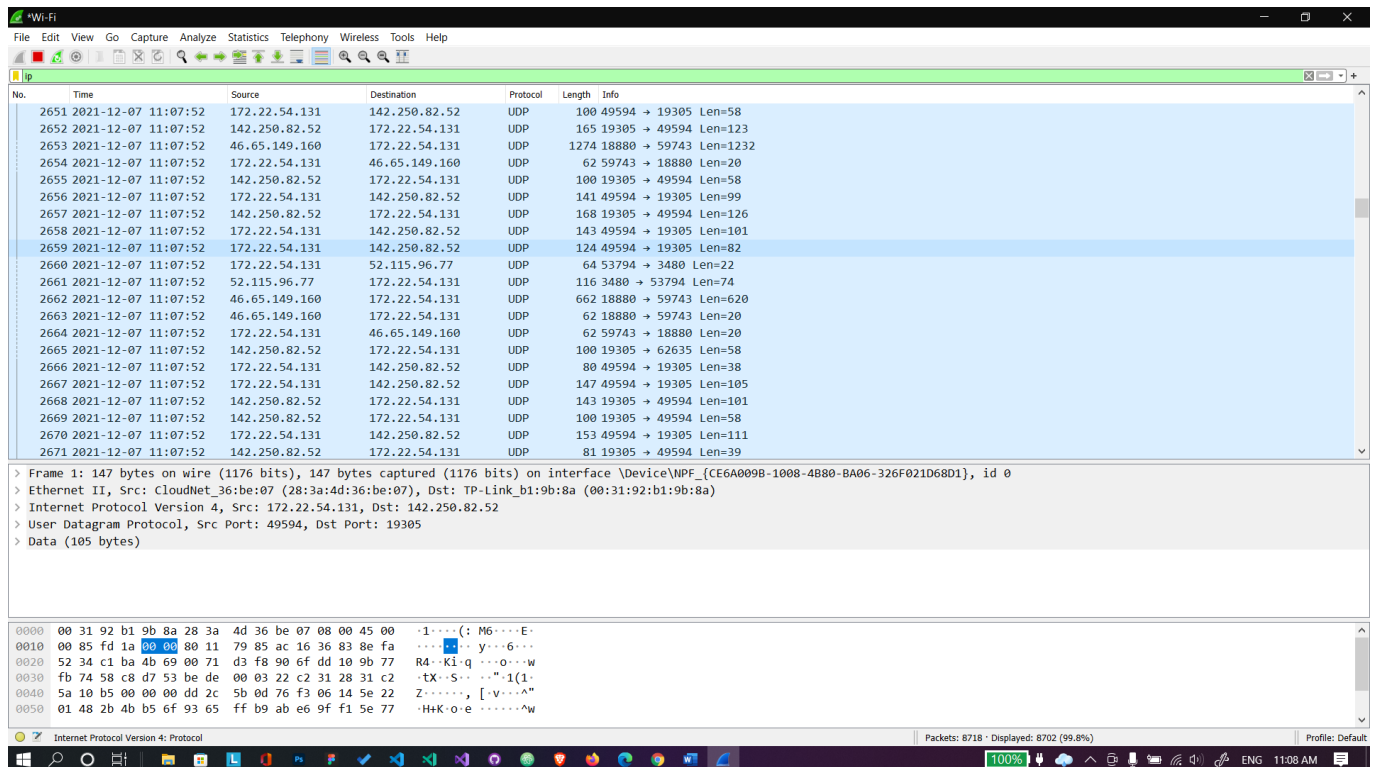
(a)



2. (a) I'm showing the screenshots of following 5 protocols: -

IP, TCP, HTTP, UDP, DNS

IP:



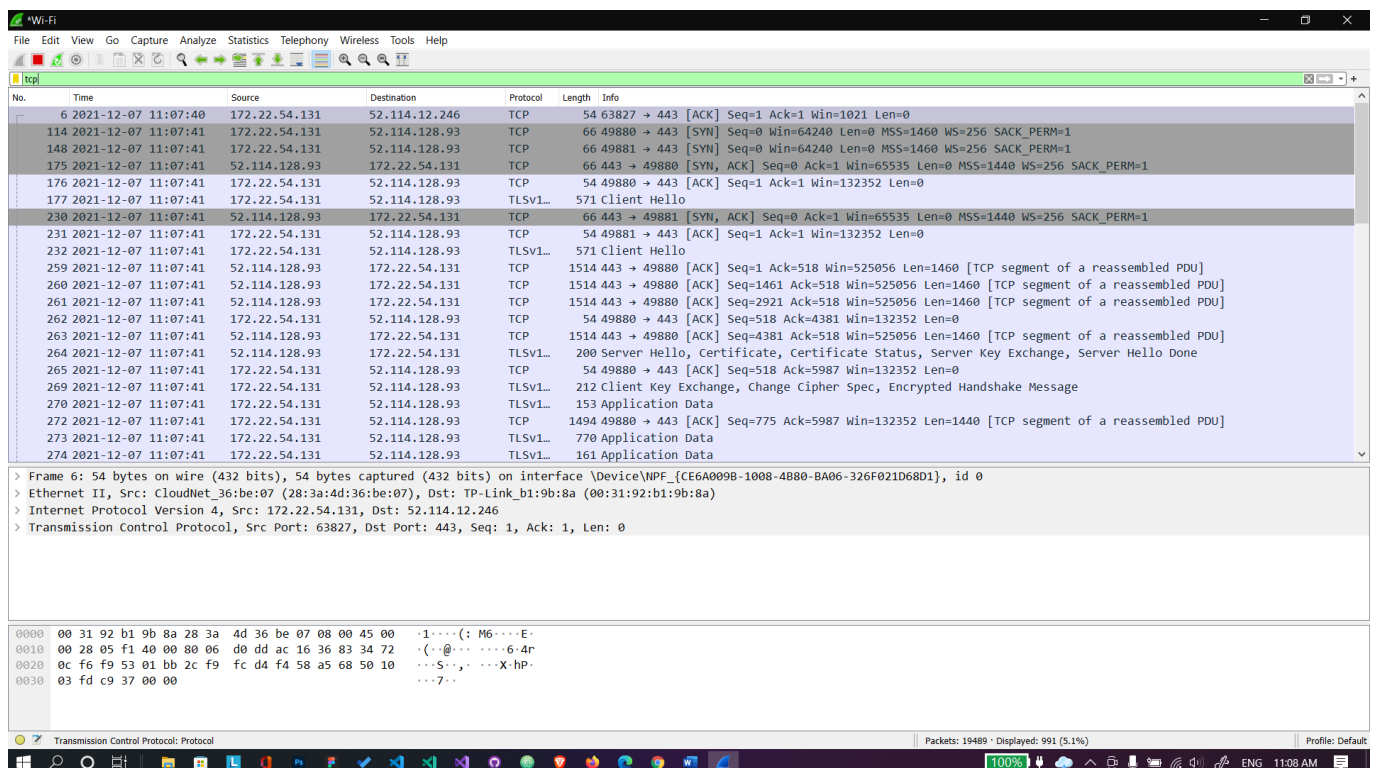
The image shows a Wireshark capture of a UDP packet. The packet list pane shows a single packet (No. 2651) at time 2021-12-07 11:07:52, source 172.22.54.131, destination 142.250.82.52, protocol UDP, length 100, and info 49594 → 19305 Len=58. The packet details pane shows the frame structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (105 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2651	2021-12-07 11:07:52	172.22.54.131	142.250.82.52	UDP	100	49594 → 19305 Len=58

> Frame 1: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface \Device\NPF_{CE6A009B-1008-4880-BA06-326F021D68D1}, id 0
> Ethernet II, Src: CloudNet_36:be:07 (28:3a:4d:36:be:07), Dst: TP-Link_b1:9b:8a (00:31:92:b1:9b:8a)
> Internet Protocol Version 4, Src: 172.22.54.131, Dst: 142.250.82.52
> User Datagram Protocol, Src Port: 49594, Dst Port: 19305
> Data (105 bytes)

0000 00 31 92 b1 9b 8a 28 3a 4d 36 be 07 08 00 45 00 :1....(: M6....E-
0010 00 85 fd 1a 00 00 80 11 79 85 ac 16 36 83 8e fa y...6...
0020 52 34 c1 ba 4b 69 00 71 d3 f8 90 6f dd 10 9b 77 R4...K!q ...o...w
0030 fb 74 58 c8 d7 53 be de 00 03 22 c2 31 28 31 c2 :tX..S...^1(1-
0040 5a 10 b5 00 00 00 dd 2c 5b 0d 76 f3 06 14 5e 22 Z..... [v...^"
0050 01 48 2b 4b b5 6f 93 65 ff b9 ab e6 9f f1 5e 77 :H+K..o.ew

TCP:



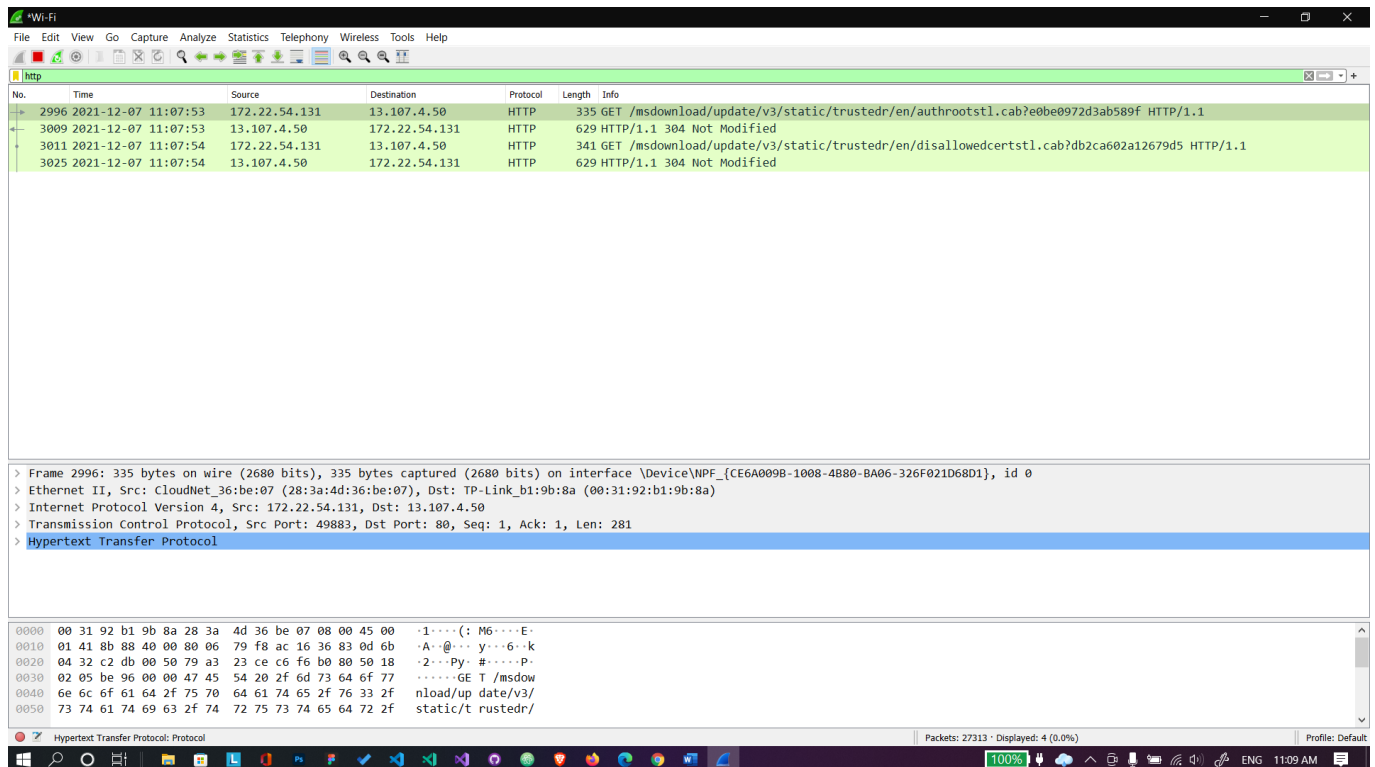
The image shows a Wireshark capture of a TCP connection. The packet list pane shows a sequence of packets (No. 6 to 274) at time 2021-12-07 11:07:40 to 11:07:41, source 172.22.54.131, destination 52.114.12.246, protocol TCP, and various info fields. The packet details pane shows the frame structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Application Data. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
6	2021-12-07 11:07:40	172.22.54.131	52.114.12.246	TCP	54	63827 → 443 [ACK] Seq=1 Ack=1 Win=1021 Len=0
114	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TCP	66	49880 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
148	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TCP	66	49881 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
175	2021-12-07 11:07:41	52.114.128.93	172.22.54.131	TCP	66	443 → 49880 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
176	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TCP	54	49880 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
177	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TLSV1..	571	Client Hello
230	2021-12-07 11:07:41	52.114.128.93	172.22.54.131	TCP	66	443 → 49881 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
231	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TCP	54	49881 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
232	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TLSV1..	571	Client Hello
259	2021-12-07 11:07:41	52.114.128.93	172.22.54.131	TCP	1514	443 → 49880 [ACK] Seq=1 Ack=518 Win=525056 Len=1460 [TCP segment of a reassembled PDU]
260	2021-12-07 11:07:41	52.114.128.93	172.22.54.131	TCP	1514	443 → 49880 [ACK] Seq=1461 Ack=518 Win=525056 Len=1460 [TCP segment of a reassembled PDU]
261	2021-12-07 11:07:41	52.114.128.93	172.22.54.131	TCP	1514	443 → 49880 [ACK] Seq=2921 Ack=518 Win=525056 Len=1460 [TCP segment of a reassembled PDU]
262	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TCP	54	49880 → 443 [ACK] Seq=518 Ack=4381 Win=132352 Len=0
263	2021-12-07 11:07:41	52.114.128.93	172.22.54.131	TCP	1514	443 → 49880 [ACK] Seq=4381 Ack=518 Win=525056 Len=1460 [TCP segment of a reassembled PDU]
264	2021-12-07 11:07:41	52.114.128.93	172.22.54.131	TLSV1..	200	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
265	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TCP	54	49880 → 443 [ACK] Seq=518 Ack=5987 Win=132352 Len=0
269	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TLSV1..	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
270	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TLSV1..	153	Application Data
272	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TCP	1494	49880 → 443 [ACK] Seq=775 Ack=5987 Win=132352 Len=1440 [TCP segment of a reassembled PDU]
273	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TLSV1..	770	Application Data
274	2021-12-07 11:07:41	172.22.54.131	52.114.128.93	TLSV1..	161	Application Data

> Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{CE6A009B-1008-4880-BA06-326F021D68D1}, id 0
> Ethernet II, Src: CloudNet_36:be:07 (28:3a:4d:36:be:07), Dst: TP-Link_b1:9b:8a (00:31:92:b1:9b:8a)
> Internet Protocol Version 4, Src: 172.22.54.131, Dst: 52.114.12.246
> Transmission Control Protocol, Src Port: 63827, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000 00 31 92 b1 9b 8a 28 3a 4d 36 be 07 08 00 45 00 :1....(: M6....E-
0010 00 28 05 f1 40 00 80 06 d0 dd ac 16 36 83 34 72 :(.@.....6.4r
0020 0c f6 f9 53 01 bb 2c f9 fc d4 f4 58 a5 68 50 10 :S... ..X:hP
0030 03 fd c9 37 00 007..

HTTP:

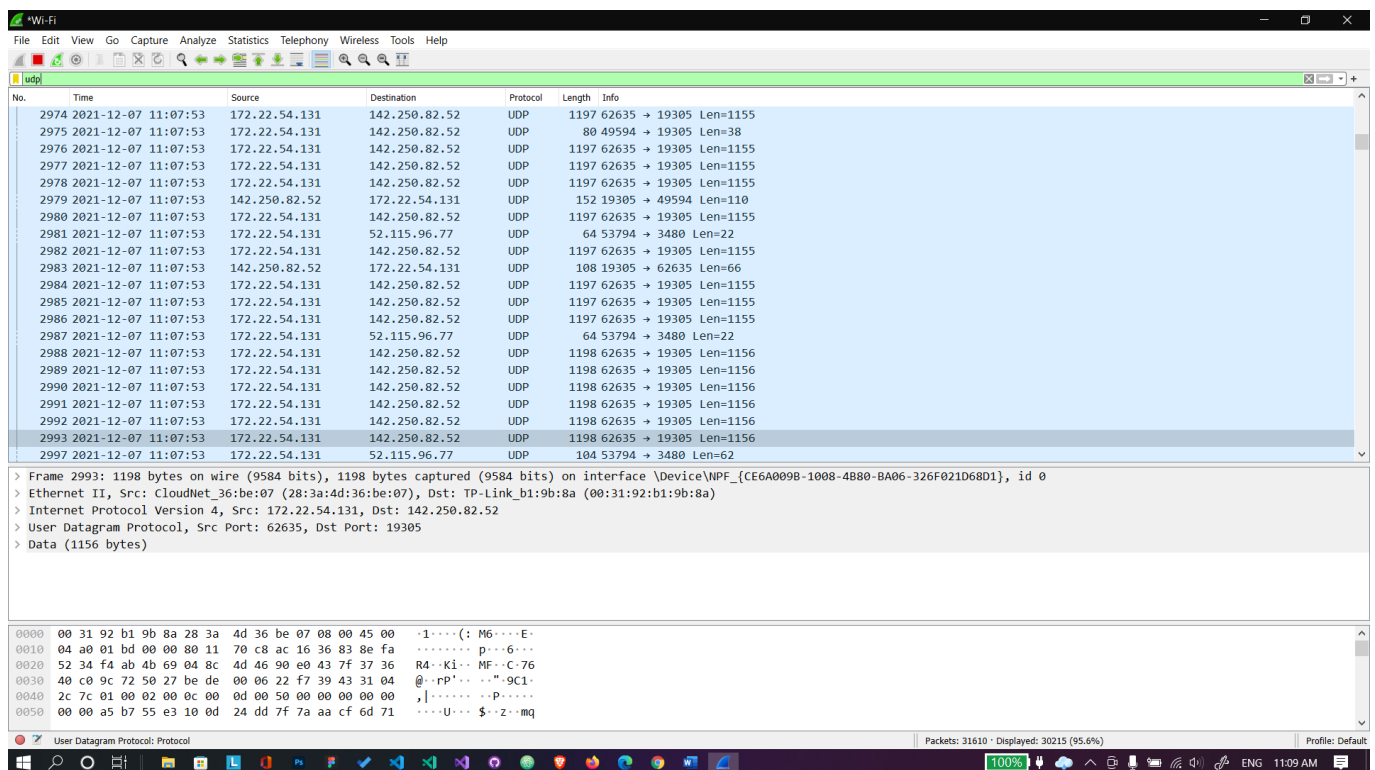


Wireshark capture of HTTP traffic. The packet list shows four packets (2996-3025) from 172.22.54.131 to 13.107.4.50. The packet details pane shows the structure of an HTTP GET request for the path /msdownload/update/v3/static/trusted/en/authrootstl.cab?e0be0972d3ab589f. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2996	2021-12-07 11:07:53	172.22.54.131	13.107.4.50	HTTP	335	GET /msdownload/update/v3/static/trusted/en/authrootstl.cab?e0be0972d3ab589f HTTP/1.1
3009	2021-12-07 11:07:53	13.107.4.50	172.22.54.131	HTTP	629	HTTP/1.1 304 Not Modified
3011	2021-12-07 11:07:54	172.22.54.131	13.107.4.50	HTTP	341	GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?db2ca602a12679d5 HTTP/1.1
3025	2021-12-07 11:07:54	13.107.4.50	172.22.54.131	HTTP	629	HTTP/1.1 304 Not Modified

> Frame 2996: 335 bytes on wire (2680 bits), 335 bytes captured (2680 bits) on interface \Device\NPF_{CE6A009B-1008-4880-BA06-326F021D68D1}, id 0
> Ethernet II, Src: CloudNet_36:be:07 (28:3a:4d:36:be:07), Dst: TP-Link_b1:9b:8a (00:31:92:b1:9b:8a)
> Internet Protocol Version 4, Src: 172.22.54.131, Dst: 13.107.4.50
> Transmission Control Protocol, Src Port: 49883, Dst Port: 80, Seq: 1, Ack: 1, Len: 281
> Hypertext Transfer Protocol

UDP:



Wireshark capture of UDP traffic. The packet list shows 20 packets (2974-2993) from 172.22.54.131 to 142.250.82.52. The packet details pane shows the structure of a User Datagram Protocol (UDP) packet. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2974	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1197	62635 → 19305 Len=1155
2975	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	80	49594 → 19305 Len=38
2976	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1197	62635 → 19305 Len=1155
2977	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1197	62635 → 19305 Len=1155
2978	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1197	62635 → 19305 Len=1155
2979	2021-12-07 11:07:53	142.250.82.52	172.22.54.131	UDP	152	19305 → 49594 Len=110
2980	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1197	62635 → 19305 Len=1155
2981	2021-12-07 11:07:53	172.22.54.131	52.115.96.77	UDP	64	53794 → 3480 Len=22
2982	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1197	62635 → 19305 Len=1155
2983	2021-12-07 11:07:53	142.250.82.52	172.22.54.131	UDP	108	19305 → 62635 Len=66
2984	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1197	62635 → 19305 Len=1155
2985	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1197	62635 → 19305 Len=1155
2986	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1197	62635 → 19305 Len=1155
2987	2021-12-07 11:07:53	172.22.54.131	52.115.96.77	UDP	64	53794 → 3480 Len=22
2988	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1198	62635 → 19305 Len=1156
2989	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1198	62635 → 19305 Len=1156
2990	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1198	62635 → 19305 Len=1156
2991	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1198	62635 → 19305 Len=1156
2992	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1198	62635 → 19305 Len=1156
2993	2021-12-07 11:07:53	172.22.54.131	142.250.82.52	UDP	1198	62635 → 19305 Len=1156
2997	2021-12-07 11:07:53	172.22.54.131	52.115.96.77	UDP	104	53794 → 3480 Len=62

> Frame 2993: 1198 bytes on wire (9584 bits), 1198 bytes captured (9584 bits) on interface \Device\NPF_{CE6A009B-1008-4880-BA06-326F021D68D1}, id 0
> Ethernet II, Src: CloudNet_36:be:07 (28:3a:4d:36:be:07), Dst: TP-Link_b1:9b:8a (00:31:92:b1:9b:8a)
> Internet Protocol Version 4, Src: 172.22.54.131, Dst: 142.250.82.52
> User Datagram Protocol, Src Port: 62635, Dst Port: 19305
> Data (1156 bytes)

DNS:

Wireshark packet capture showing DNS traffic. The packet list shows a series of DNS queries and responses from 172.22.54.1 to 172.22.54.131. The packet details pane shows the structure of a DNS Standard query response, including the question, answer, and authority sections. The packet bytes pane shows the raw data in hexadecimal and ASCII.

(b)

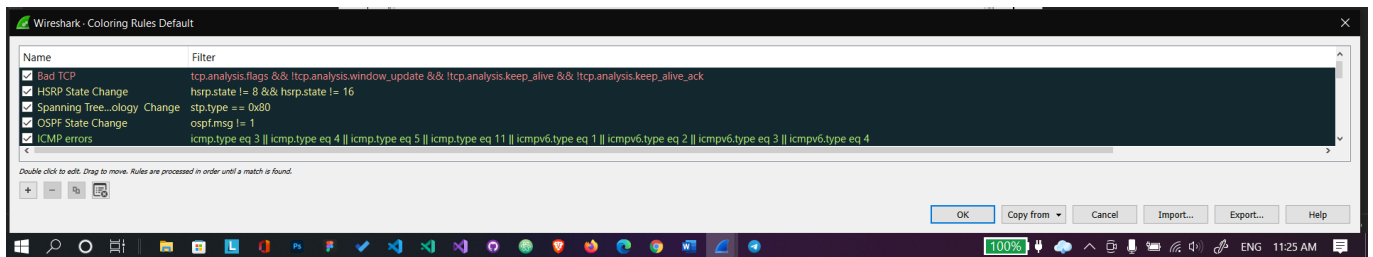
2.

(b)

Wireshark can be setup so that it will colorize packets according to a display filter.

It uses colors to help us identify the types of traffic at a glance.

By default, black colour identifies packets with errors — for example, they could have been delivered out of order.



(c)



2.

(c)

http.request.method == "GET"

