

110124156

I confirm that I will keep the content of this Lab confidential. I confirm that I have not received any unauthorized assistance in preparing for or writing this Lab. I acknowledge that a mark of 0 may be assigned for copied work.”

Name: Siddharth Samber

Student number: 110124156

LAB 2

Master of Applied Computing

Networking & Data Security

COMP 8677

University of Windsor



University
of Windsor

Submitted By:

Siddharth Samber

110124156

Submission Date:

31 January 2024

110124156

Question 1

```
[01/30/24]seed@VM:~$ dig www.example.net

;<<<> DiG 9.16.1-Ubuntu <<<> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8005
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

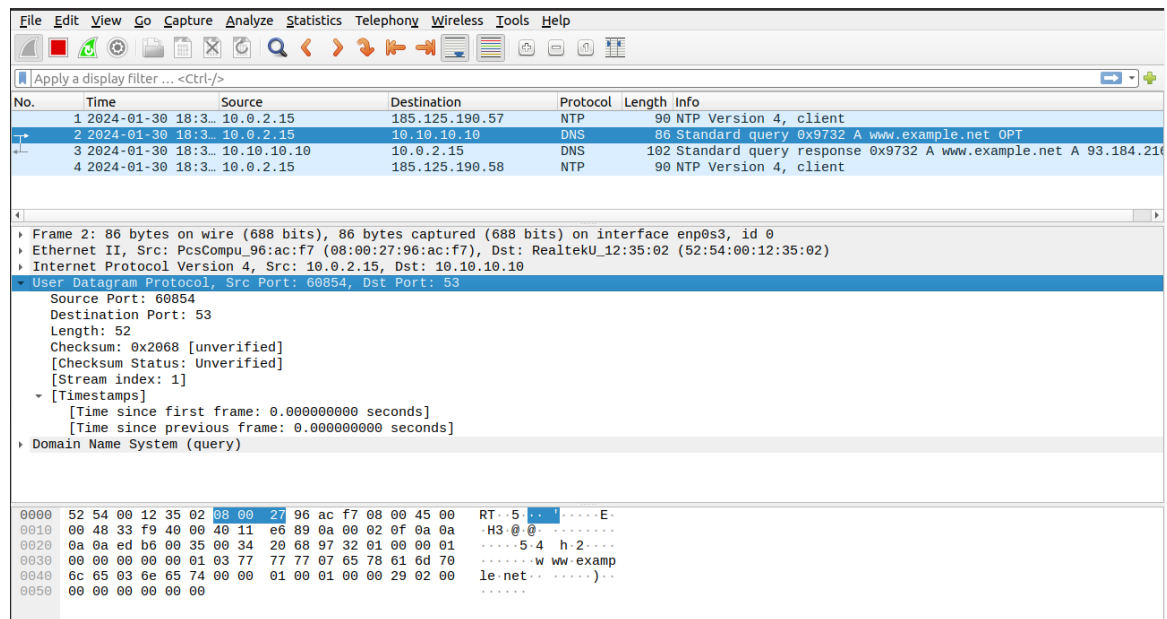
;; ANSWER SECTION:
www.example.net.                600     IN      A      93.184.216.34

;; Query time: 92 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Jan 30 18:33:58 EST 2024
;; MSG SIZE rcvd: 60
```

PART A

DIG command is run on www.example.net which gives its ip address as 93.184.216.34

PART B



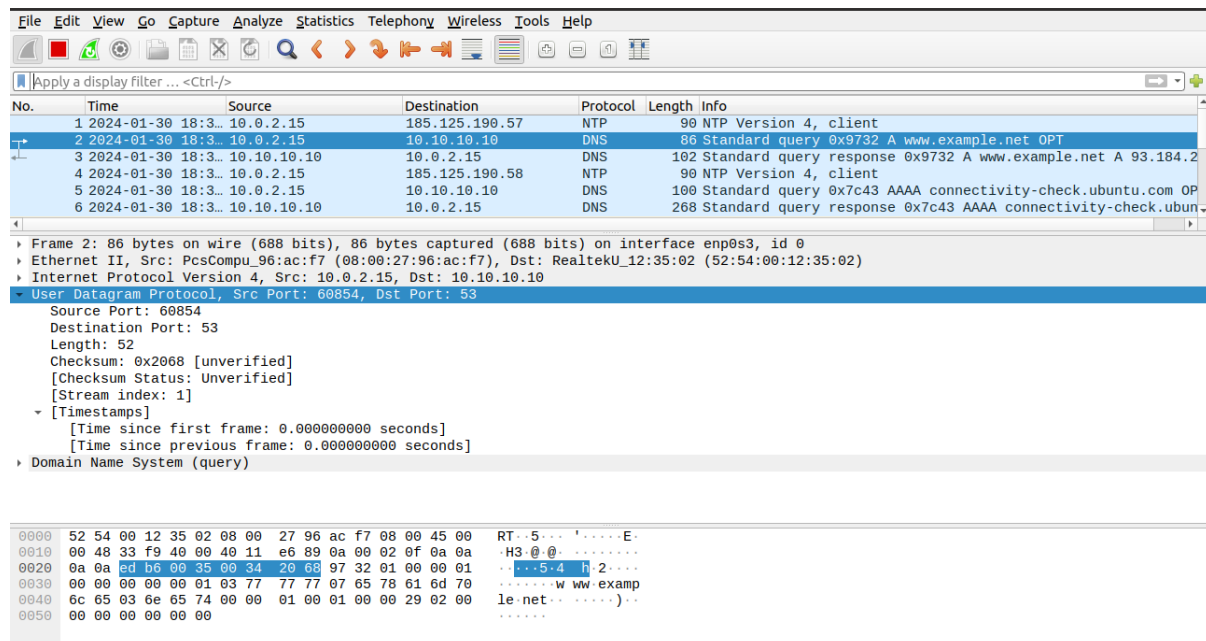
It can be observed that DNS request packet has UDP as its transport layer protocol.

UDP header Field values

1. Source port : 60854
2. Destination port : 53
3. Length (length of entire UDP datagram): 52
4. Checksum (For error checking) : 0x2068

110124156

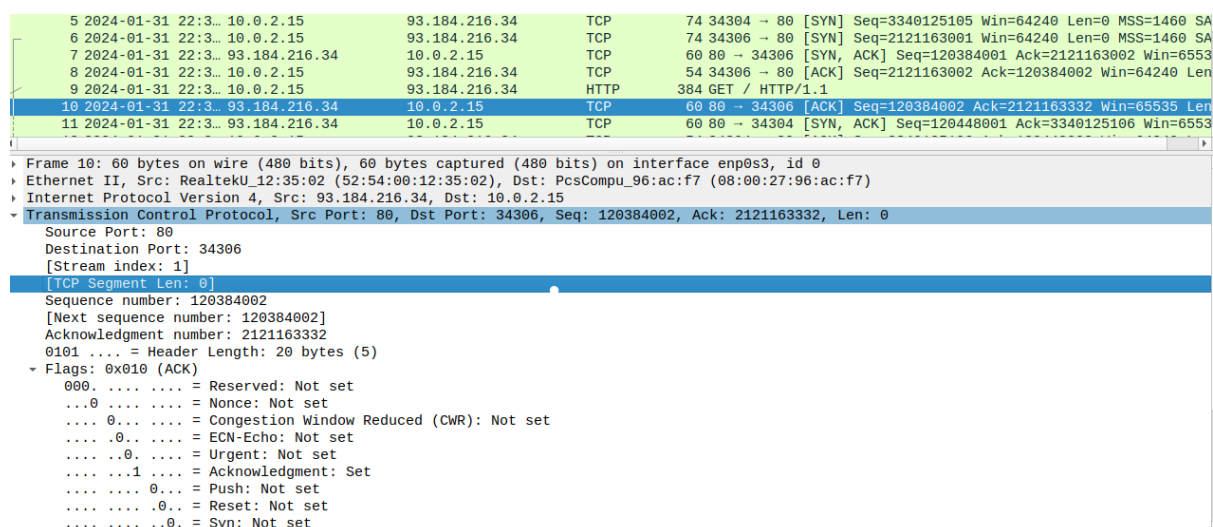
PART C



1. DNS server's IP address: 10.10.10.10 (it is also destination IP of DNS request packet)
2. It can be seen from the above screenshot that there is no exchange of any packets between DNS and virtual machine prior to DNS request packet.

Note: 1st packet captured in wireshark is packet which is send from virtual machine to somewhere else and not to DNS server.

Question 2



1. It can be seen from packet number 6-8 are SYN ,SYN-ACK and ACK packet in the respective order which is used for 3-way handshake for stream index 1.
2. It can also be observed TCP is used as transporation layer protocol for these packets.

110124156

5	2024-01-31 22:3...	10.0.2.15	93.184.216.34	TCP	74	34304 → 80 [SYN]	Seq=3340125105 Win=64240 Len=0 MSS=1460 SA
6	2024-01-31 22:3...	10.0.2.15	93.184.216.34	TCP	74	34306 → 80 [SYN]	Seq=2121163001 Win=64240 Len=0 MSS=1460 SA
7	2024-01-31 22:3...	93.184.216.34	10.0.2.15	TCP	60	80 → 34306 [SYN, ACK]	Seq=120384001 Ack=2121163002 Win=6553
8	2024-01-31 22:3...	10.0.2.15	93.184.216.34	TCP	54	34306 → 80 [ACK]	Seq=2121163002 Ack=120384002 Win=64240 Len
9	2024-01-31 22:3...	10.0.2.15	93.184.216.34	HTTP	384	GET / HTTP/1.1	
10	2024-01-31 22:3...	93.184.216.34	10.0.2.15	TCP	60	80 → 34306 [ACK]	Seq=120384002 Ack=2121163332 Win=65535 Len
11	2024-01-31 22:3...	93.184.216.34	10.0.2.15	TCP	60	80 → 34304 [SYN, ACK]	Seq=120448001 Ack=3340125106 Win=6553

Frame 10: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s3, id 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7)
Internet Protocol Version 4, Src: 93.184.216.34, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 34306, Seq: 120384002, Ack: 2121163332, Len: 0
Source Port: 80
Destination Port: 34306
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 120384002
[Next sequence number: 120384002]
Acknowledgment number: 2121163332
0101 = Header Length: 20 bytes (5)
Flags: 0x010 (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
...1 = Acknowledgment: Set
...0 = Push: Not set
...0 = Reset: Not set
...0 = Syn: Not set

3. Paket 10 is first acknowledgement packet when message exchange starts and it's acknowledgement bit is set to 1.
4. Packet 10 does not contain any data as TCP segment len is 0.

Question 3

INTRO

No.	Time	Source	Destination	Protocol	Length	Info
1	2024-01-31 00:3...	10.0.2.15	10.10.10.10	DNS	95	Standard query 0x20ee A detectportal.firefox.com OPT
2	2024-01-31 00:3...	10.0.2.15	10.10.10.10	DNS	95	Standard query 0x40b6 AAAA detectportal.firefox.com OPT
5	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	209	Standard query response 0x20ee A detectportal.firefox.com C
6	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	221	Standard query response 0x40b6 AAAA detectportal.firefox.co
9	2024-01-31 00:3...	10.0.2.15	10.10.10.10	DNS	84	Standard query 0xd469 AAAA ipv4only.arpa OPT
12	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	141	Standard query response 0xd469 AAAA ipv4only.arpa S0A sns.d
13	2024-01-31 00:3...	10.0.2.15	10.10.10.10	DNS	84	Standard query 0x064c AAAA ipv4only.arpa OPT
16	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	141	Standard query response 0x064c AAAA ipv4only.arpa S0A sns.d
55	2024-01-31 00:3...	10.0.2.15	10.10.10.10	DNS	82	Standard query 0x49af A example.com OPT
56	2024-01-31 00:3...	10.0.2.15	10.10.10.10	DNS	82	Standard query 0x83f0 AAAA example.com OPT
57	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	110	Standard query response 0x83f0 AAAA example.com AAAA 2606:2
58	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	98	Standard query response 0x49af A example.com A 93.184.216.3
72	2024-01-31 00:3...	10.0.2.15	10.10.10.10	DNS	83	Standard query 0x6846 A www.iana.org OPT

Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 33364
Domain Name System (response)
Transaction ID: 0x49af
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1
Queries
Answers
example.com: type A, class IN, addr 93.184.216.34
Additional records

- IP address of example.com is 93.184.216.34 (Highlighted in yellow)
- IP address of DNS server is 10.10.10.10 (Highlighted in orange)
- IP address of virtual machine is 10.0.2.15 (Highlighted in green)

110124156

PART A

ip.src==10.0.2.15 && ip.dst==93.184.216.34						
No.	Time	Source	Destination	Protocol	Length	Info
59	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	74	52452 → 80 [SYN] Seq=4009052419 Win=64240 Len=0 MSS=1460 SA
61	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54	52452 → 80 [ACK] Seq=4009052420 Ack=1078144002 Win=64240 Le
62	2024-01-31 00:3...	10.0.2.15	93.184.216.34	HTTP	384	GET / HTTP/1.1
65	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54	52452 → 80 [ACK] Seq=4009052750 Ack=1078145007 Win=63315 Le

Frame 59: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 93.184.216.34
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0xe48c (58508)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x1446 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.15
Destination: 93.184.216.34
Transmission Control Protocol, Src Port: 52452, Dst Port: 80, Seq: 4009052419, Len: 0
Source Port: 52452
Destination Port: 80
[Stream index: 11]
[TCP Segment Len: 0]
Sequence number: 4009052419
[Next sequence number: 4009052420]
Acknowledgment number: 0
Acknowledgment number (raw): 0

Procedure:

1. Got IP address of our virtual machine and example.org from above.
2. Used filter ip.src==10.0.2.15 && ip.dst==93.184.216.34 to find the first packet from VM to example.net. (Packet no. 50)

RESULTS

1. First packet from VM to example.net is SYN packet as displayed in the info. SYN packet (Highlighted in orange)
2. Source port no. is 52452 and destination port number is 80 in SYN packet. (Highlighted in yellow)
3. In TCP header also port number for source is 52452 and for destination is 80 same as depicted in SYN packet. (Highlighted in Purple)
4. Source IP address is 10.0.2.15 and destination IP address is 93.184.216.34.
5. In IP header also source IP address is 10.0.2.15 and destination IP address is 93.184.216.34 same as in SYN packet (Highlighted in blue)

PART B

Procedure:

1. Note down the sequence number in TCP header
2. Repeating the experiment suggest sequence number is randomly generated

RESULTS

SYN packet has sequence number 4009052419 which is a random number as running experiment again give different values of sequence number. (Highlighted in red)

110124156

No.	Time	Source	Destination	Protocol	Length	Info
56	2024-01-31 00:3...	10.0.2.15	10.10.10.10	DNS	82	Standard query 0x83f0 AAAA example.com OPT
57	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	110	Standard query response 0x83f0 AAAA example.com AAAA 2606:2
58	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	98	Standard query response 0x49af A example.com A 93.184.216.3
59	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	74	52452 → 80 [SYN] Seq=4009052419 Win=64240 Len=0 MSS=1460 SA
60	2024-01-31 00:3...	93.184.216.34	10.0.2.15	TCP	60	80 → 52452 [SYN, ACK] Seq=1078144001 Ack=4009052420 Win=655
61	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54	52452 → 80 [ACK] Seq=4009052420 Ack=1078144002 Win=64240 Le

Transmission Control Protocol, Src Port: 80, Dst Port: 52452, Seq: 1078144001, Ack: 4009052420, Len: 0
Source Port: 80
Destination Port: 52452
[Stream index: 11]
[TCP Segment Len: 0]
Sequence number: 1078144001
[Next sequence number: 1078144002]
Acknowledgment number: 4009052420
0110 = Header Length: 24 bytes (6)
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
...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: 65535
[Calculated window size: 65535]

PART C

RESULTS

1. [SYN ACK] packet is sent after SYN packet (Highlighted in purple)
2. The flag bits UAPRSF are shown under flags in TCP header. SYN and Acknowledgement flag bits are set while other Urgent Push Reset Fin flag bits are unset in [SYN ACK] packet (Set bits in Green & unset bits in Yellow)
3. SYN ACK packet receiver buffer size is 65535 (Highlighted in orange)

No.	Time	Source	Destination	Protocol	Length	Info
59	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	74	52452 → 80 [SYN] Seq=4009052419 Win=64240 Len=0 MSS=1460 SA
60	2024-01-31 00:3...	93.184.216.34	10.0.2.15	TCP	60	80 → 52452 [SYN, ACK] Seq=1078144001 Ack=4009052420 Win=655
61	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54	52452 → 80 [ACK] Seq=4009052420 Ack=1078144002 Win=64240 Le
62	2024-01-31 00:3...	10.0.2.15	93.184.216.34	HTTP	384	GET / HTTP/1.1
63	2024-01-31 00:3...	93.184.216.34	10.0.2.15	TCP	60	80 → 52452 [ACK] Seq=1078144002 Ack=4009052750 Win=65535 Le
64	2024-01-31 00:3...	93.184.216.34	10.0.2.15	HTTP	1059	HTTP/1.1 200 OK (text/html)
65	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54	52452 → 80 [ACK] Seq=4009052750 Ack=1078145007 Win=63315 Le

[Next sequence number: 1078145007]
Acknowledgment number: 4009052750
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, 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
...1 = Acknowledgment: Set
...1 = Push: Set
...0 = Reset: Not set
...0 = Syn: Not set
...0 = Fin: Not set
[TCP Flags:AP..]
Window size value: 65535
[Calculated window size: 65535]
[Window size scaling factor: -2 (no window scaling used)]

PART D

RESULTS

1. SYN ACK packet receiver buffer size is 65535 (Highlighted in orange)
2. HTTP repose packet is highlighted in red
3. HTTP response packet receiver buffer size is 65535 (Highlighted in orange)
4. Observation: Both HTTP repose packet SYN ACK packet buffer size are same

PART E

56	2024-01-31 00:3...	10.0.2.15	10.10.10.10	DNS	82 Standard query 0x83f0 AAAA example.com OPT
57	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	110 Standard query response 0x83f0 AAAA example.com AAAA 2606:2
58	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	98 Standard query response 0x49af A example.com A 93.184.216.3
59	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	74 52452 → 80 [SYN] Seq=4009052419 Win=64240 Len=0 MSS=1460 SA
60	2024-01-31 00:3...	93.184.216.34	10.0.2.15	TCP	60 80 → 52452 [SYN, ACK] Seq=1078144001 Ack=4009052420 Win=655
61	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54 52452 → 80 [ACK] Seq=4009052420 Ack=1078144002 Win=64240 Le
62	2024-01-31 00:3...	10.0.2.15	93.184.216.34	HTTP	384 GET / HTTP/1.1
63	2024-01-31 00:3...	93.184.216.34	10.0.2.15	TCP	60 80 → 52452 [ACK] Seq=1078144002 Ack=4009052750 Win=65535 Le
64	2024-01-31 00:3...	93.184.216.34	10.0.2.15	HTTP	1059 HTTP/1.1 200 OK (text/html)
65	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54 52452 → 80 [ACK] Seq=4009052750 Ack=1078145007 Win=63315 Le

Ethernet II, Src: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 93.184.216.34
 Transmission Control Protocol, Src Port: 52452, Dst Port: 80, Seq: 4009052420, Ack: 1078144002, Len: 330
 Source Port: 52452
 Destination Port: 80
 [Stream index: 11]
 [TCP Segment Len: 330]
 Sequence number: 4009052420
 [Next sequence number: 4009052750]
 Acknowledgment number: 1078144002
 0101 = Header Length: 20 bytes (5)
 Flags: 0x018 (PSH, ACK)

1. HTTP request packet is packet number 62 (Highlighted in yellow).
2. Payload size or segment length is 330 (Highlighted in green)
3. Sequence number is which is 4009052420. (Highlighted in red)
4. Next sequence number is 4009052750. (Highlighted in orange)
5. Observation : $4009052420 + 330 = 4009052750$

56	2024-01-31 00:3...	10.0.2.15	10.10.10.10	DNS	82 Standard query 0x83f0 AAAA example.com OPT
57	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	110 Standard query response 0x83f0 AAAA example.com AAAA 2606:2
58	2024-01-31 00:3...	10.10.10.10	10.0.2.15	DNS	98 Standard query response 0x49af A example.com A 93.184.216.3
59	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	74 52452 → 80 [SYN] Seq=4009052419 Win=64240 Len=0 MSS=1460 SA
60	2024-01-31 00:3...	93.184.216.34	10.0.2.15	TCP	60 80 → 52452 [SYN, ACK] Seq=1078144001 Ack=4009052420 Win=655
61	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54 52452 → 80 [ACK] Seq=4009052420 Ack=1078144002 Win=64240 Le
62	2024-01-31 00:3...	10.0.2.15	93.184.216.34	HTTP	384 GET / HTTP/1.1
63	2024-01-31 00:3...	93.184.216.34	10.0.2.15	TCP	60 80 → 52452 [ACK] Seq=1078144002 Ack=4009052750 Win=65535 Le
64	2024-01-31 00:3...	93.184.216.34	10.0.2.15	HTTP	1059 HTTP/1.1 200 OK (text/html)
65	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54 52452 → 80 [ACK] Seq=4009052750 Ack=1078145007 Win=63315 Le

Ethernet II, Src: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 93.184.216.34
 Transmission Control Protocol, Src Port: 52452, Dst Port: 80, Seq: 4009052750, Ack: 1078145007, Len: 0
 Source Port: 52452
 Destination Port: 80
 [Stream index: 11]
 [TCP Segment Len: 0]
 Sequence number: 4009052750
 [Next sequence number: 4009052750]
 Acknowledgment number: 1078145007
 0101 = Header Length: 20 bytes (5)

1. Next packet sent by VM is Acknowledgment packet which is packet number 65 (Highlighted in yellow).
2. Next packet's Sequence number is 4009052750, which is same as next sequence number of HTTP request packet sent by VM initially (Highlighted in green)

PART F

59	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	74 52452 → 80 [SYN] Seq=4009052419 Win=64240 Len=0 MSS=1460 SA
60	2024-01-31 00:3...	93.184.216.34	10.0.2.15	TCP	60 80 → 52452 [SYN, ACK] Seq=1078144001 Ack=4009052420 Win=655
61	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54 52452 → 80 [ACK] Seq=4009052420 Ack=1078144002 Win=64240 Le
62	2024-01-31 00:3...	10.0.2.15	93.184.216.34	HTTP	384 GET / HTTP/1.1
63	2024-01-31 00:3...	93.184.216.34	10.0.2.15	TCP	60 80 → 52452 [ACK] Seq=1078144002 Ack=4009052750 Win=65535 Le
64	2024-01-31 00:3...	93.184.216.34	10.0.2.15	HTTP	1059 HTTP/1.1 200 OK (text/html)
65	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54 52452 → 80 [ACK] Seq=4009052750 Ack=1078145007 Win=63315 Le
66	2024-01-31 00:3...	10.0.2.15	142.251.41.67	TCP	54 [TCP Dup ACK 33#1] 57626 → 80 [ACK] Seq=1975842907 Ack=1069
67	2024-01-31 00:3...	10.0.2.15	142.251.41.67	TCP	60 [TCP Dup ACK 34#1] [TCP ACKed unseen segment] 80 → 57626 [A

Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7)
 Internet Protocol Version 4, Src: 93.184.216.34, Dst: 10.0.2.15
 Transmission Control Protocol, Src Port: 80, Dst Port: 52452, Seq: 1078144002, Ack: 4009052750, Len: 1005
 Source Port: 80
 Destination Port: 52452
 [Stream index: 11]
 [TCP Segment Len: 1005]
 Sequence number: 1078144002
 [Next sequence number: 1078145007]
 Acknowledgment number: 4009052750
 0101 = Header Length: 20 bytes (5)

1. Http response packet is packet number 64 (Highlighted in green)

2. It has acknowledgement number of 4009052750 (Highlighted in yellow)

59	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	74	52452 → 80 [SYN]	Seq=4009052419 Win=64240 Len=0 MSS=1460 SA
60	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	60	80 → 52452 [SYN, ACK]	Seq=1078144001 Ack=4009052420 Win=655
61	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54	52452 → 80 [ACK]	Seq=4009052420 Ack=1078144002 Win=64240 Le
62	2024-01-31 00:3...	10.0.2.15	93.184.216.34	HTTP	384	GET / HTTP/1.1	
63	2024-01-31 00:3...	93.184.216.34	10.0.2.15	TCP	60	80 → 52452 [ACK]	Seq=1078144002 Ack=4009052750 Win=65535 Le
64	2024-01-31 00:3...	93.184.216.34	10.0.2.15	HTTP	1059	HTTP/1.1 200 OK (text/html)	
65	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54	52452 → 80 [ACK]	Seq=4009052750 Ack=1078145007 Win=63315 Le
66	2024-01-31 00:3...	10.0.2.15	142.251.41.67	TCP	54	[TCP Dup ACK 33#1] 57626 → 80 [ACK]	Seq=1975842907 Ack=1069
67	2024-01-31 00:3...	142.251.41.67	10.0.2.15	TCP	60	[TCP Dup ACK 34#1] [TCP ACKed unseen segment] 80 → 57626 [A	

Ethernet II, Src: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 93.184.216.34

Transmission Control Protocol, Src Port: 52452, Dst Port: 80, Seq: 4009052420, Ack: 1078144002, Len: 330

Source Port: 52452

Destination Port: 80

[Stream index: 11]

[TCP Segment Len: 330]

Sequence number: 4009052420

[Next sequence number: 4009052750]

Acknowledgment number: 1078144002

0101 = Header Length: 20 bytes (5)

3. It can be observed that it is same as next sequence number of HTTP request packet which is also 4009052750.

PART G

61	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54	52452 → 80 [ACK]	Seq=4009052420 Ack=1078144002 Win=64240 Le
62	2024-01-31 00:3...	10.0.2.15	93.184.216.34	HTTP	384	GET / HTTP/1.1	
63	2024-01-31 00:3...	93.184.216.34	10.0.2.15	TCP	60	80 → 52452 [ACK]	Seq=1078144002 Ack=4009052750 Win=65535 Le
64	2024-01-31 00:3...	93.184.216.34	10.0.2.15	HTTP	1059	HTTP/1.1 200 OK (text/html)	
65	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54	52452 → 80 [ACK]	Seq=4009052750 Ack=1078145007 Win=63315 Le
66	2024-01-31 00:3...	10.0.2.15	142.251.41.67	TCP	54	[TCP Dup ACK 33#1] 57626 → 80 [ACK]	Seq=1975842907 Ack=1069
67	2024-01-31 00:3...	142.251.41.67	10.0.2.15	TCP	60	[TCP Dup ACK 34#1] [TCP ACKed unseen segment] 80 → 57626 [A	

[TCP Segment Len: 1005]

Sequence number: 1078144002

[Next sequence number: 1078145007]

Acknowledgment number: 4009052750

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, 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

....1... = Acknowledgment: Set

....1... = Push: Set

....0... = Reset: Not set

....0... = Syn: Not set

....0... = Fin: Not set

[TCP Flags:AP...]

Window size value: 65535

1. Flag bits in HTTP response packet is Acknowledgement and Push bit are set to 1 other flag bits Urgent, Reset, Syn and Fin are unset.

PART H

Time	Source	Destination	Protocol	Length	Info
59	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	74 52452 → 80 [SYN] Seq=4009052419 Win=64240 Len=0 MSS=1460 SACK...
61	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54 52452 → 80 [ACK] Seq=4009052420 Ack=1078144002 Win=64240 Len=0
62	2024-01-31 00:3...	10.0.2.15	93.184.216.34	HTTP	384 GET / HTTP/1.1
65	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54 52452 → 80 [ACK] Seq=4009052750 Ack=1078145007 Win=63315 Len=0
68	2024-01-31 00:3...	10.0.2.15	93.184.216.34	HTTP	335 GET /favicon.ico HTTP/1.1
70	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54 52452 → 80 [FIN, ACK] Seq=4009053031 Ack=1078145007 Win=63315...
75	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54 52452 → 80 [RST] Seq=4009053032 Win=0 Len=0
77	2024-01-31 00:3...	10.0.2.15	93.184.216.34	TCP	54 52452 → 80 [RST] Seq=4009053032 Win=0 Len=0

Flags: 0x011 (FIN, 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
....1... = Acknowledgment: Set
....0... = Push: Not set
....0... = Reset: Not set
....0... = Syn: Not set
....1... = Fin: Set
[TCP Flags:AF...]
Window size value: 63315
[Calculated window size: 63315]

1. VM sent FIN ACK packet to terminate TCP connection

110124156

2. Fin and acknowledgement bits are set to 1 other flag bits Urgent ,Reset, Syn and push are unset .