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

Submitted By:

Siddharth Samber

110124156

Submission Date:

31 January 2024

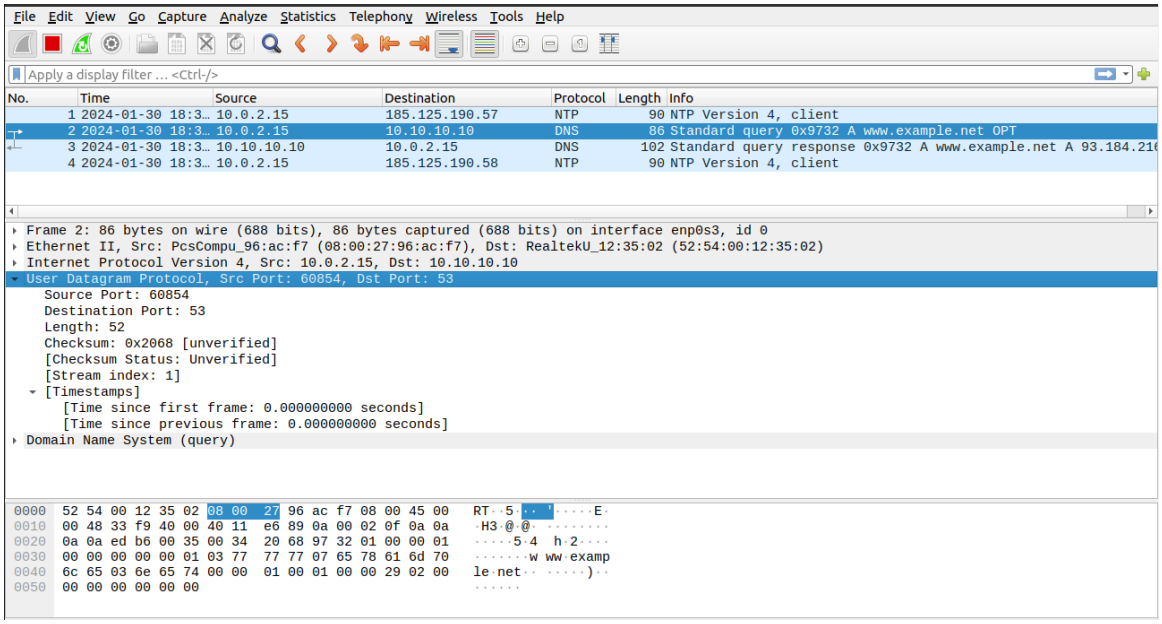
Question 1

```
[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

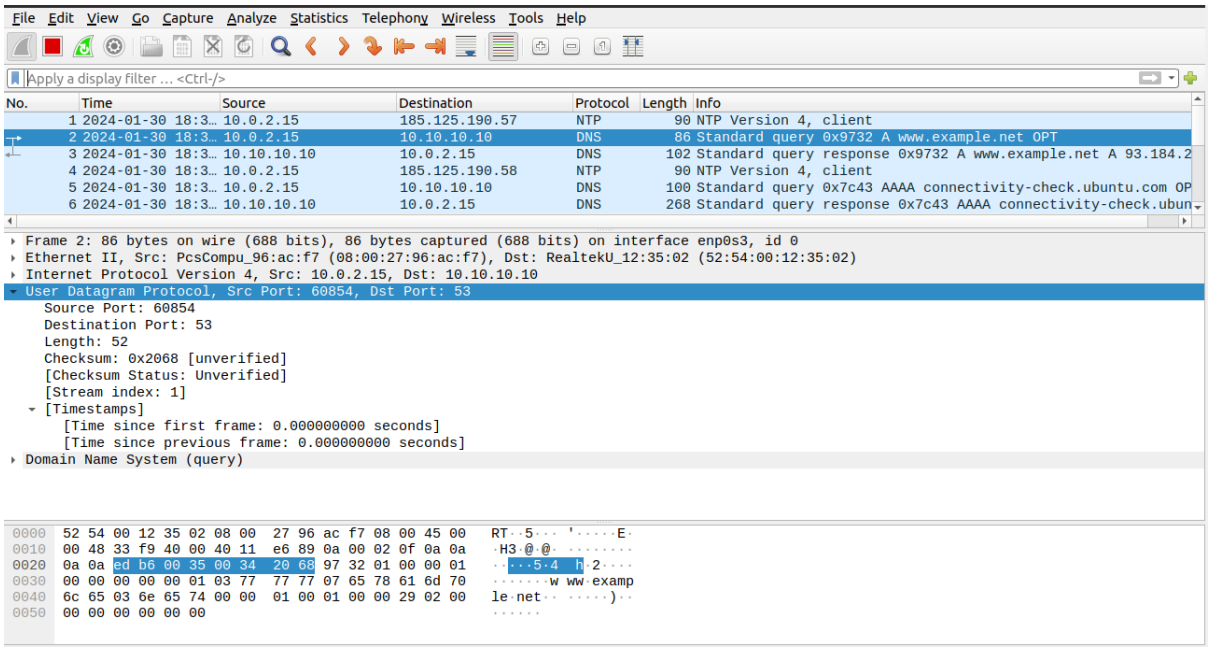


It can be observed that DNS request packet has UDP as its transport layer protocol.

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

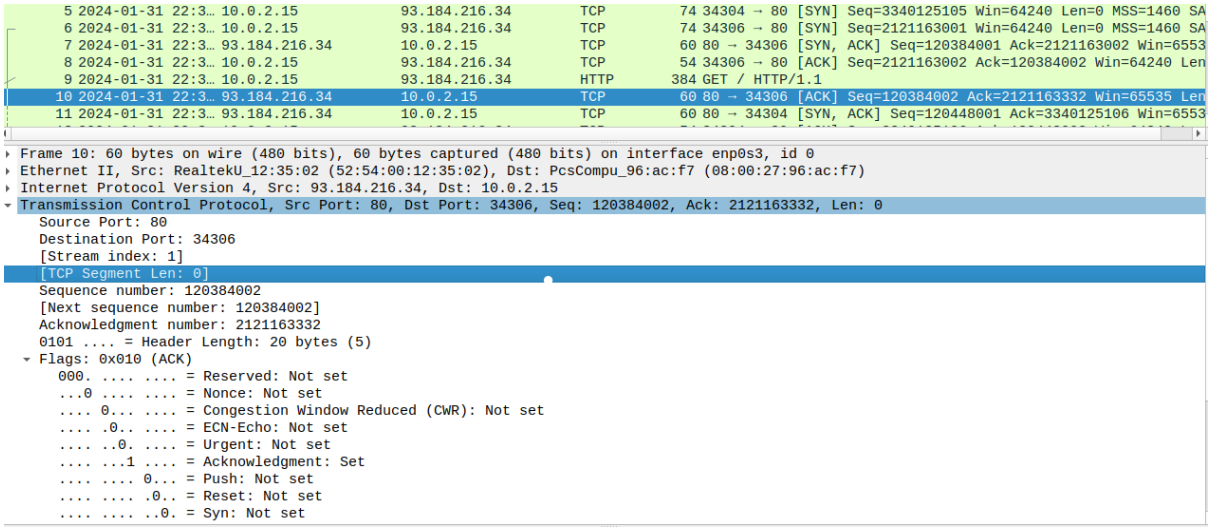
PART C



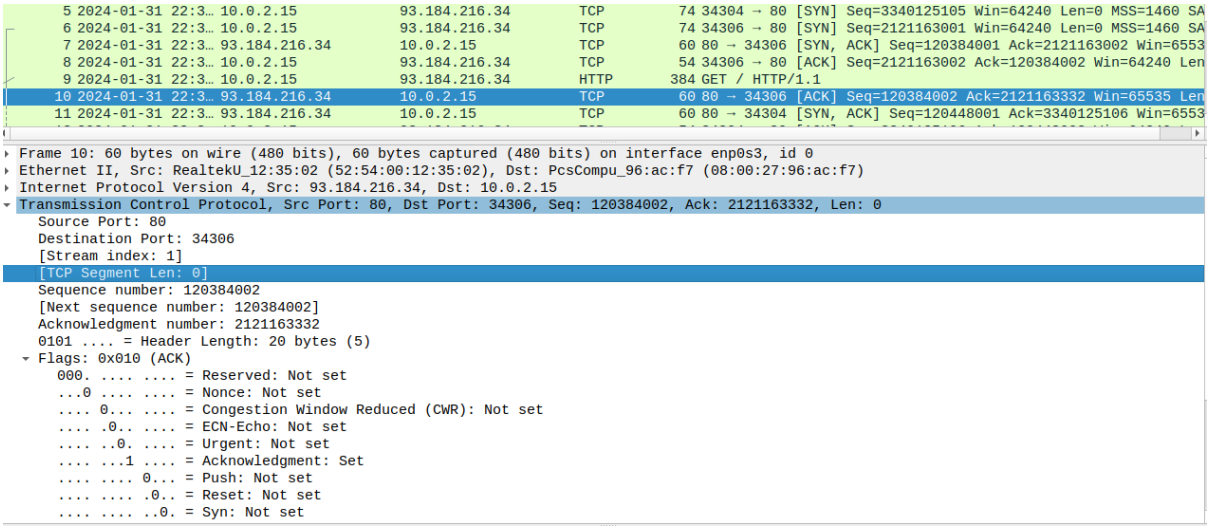
1. DNS server's IP address: 10.10.10.10 (it is also destination IP of DNS request packet)
2. It can be seen from the above screenshot that there is no exchange of any packets between DNS and virtual machine prior to DNS request packet.

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

Question 2



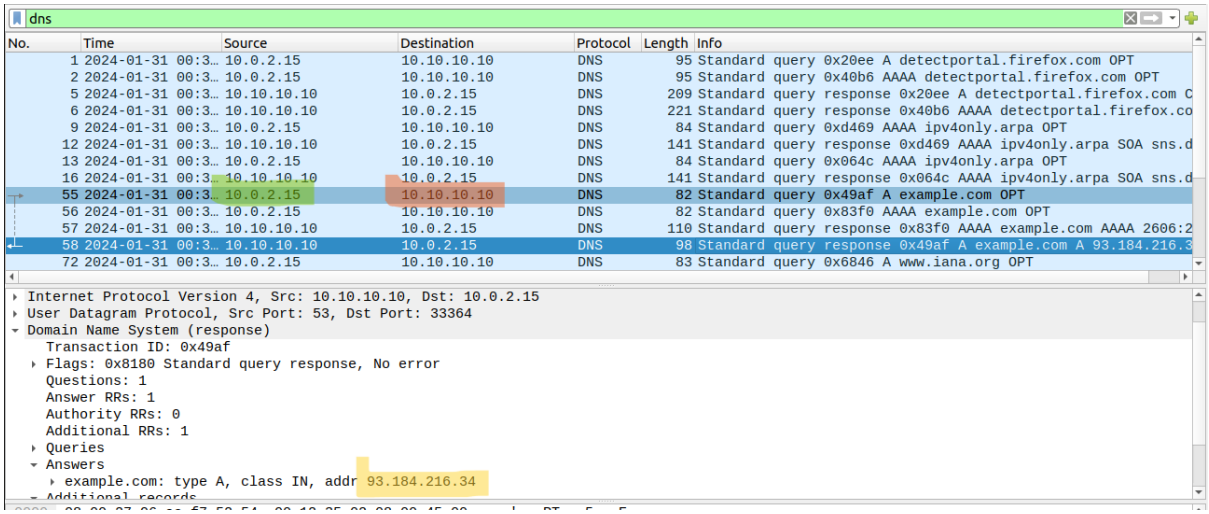
1. It can be seen from packet number 6-8 are SYN ,SYN-ACK and ACK packet in the respective order which is used for 3-way handshake for stream index 1.
2. It can also be observed TCP is used as transporation layer protocol for these packets.



3. Pakcet 10 is frist 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.

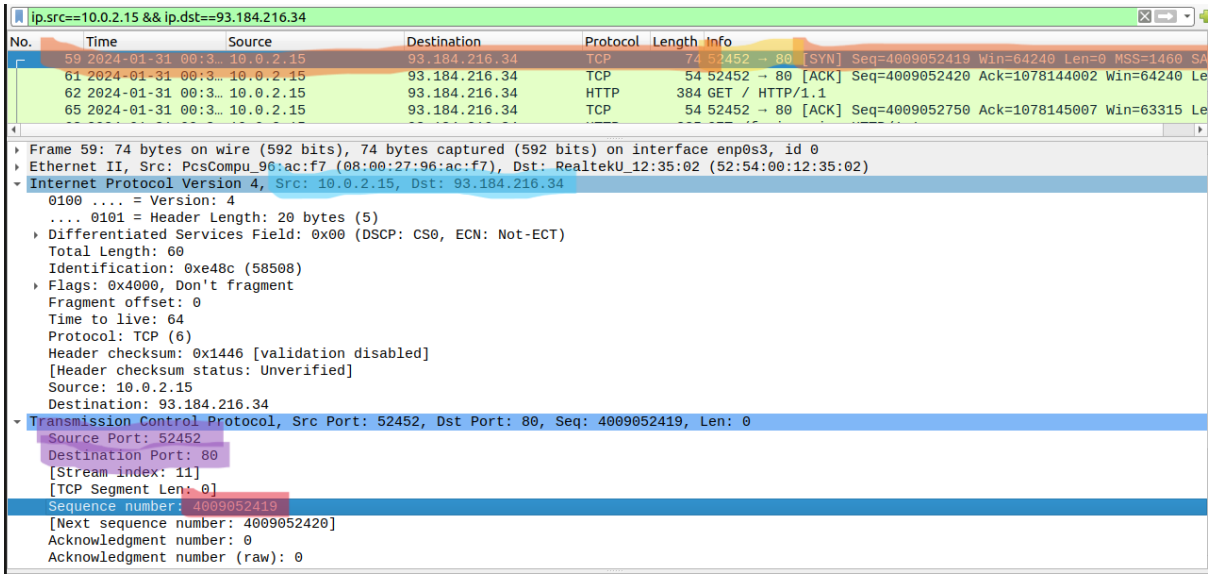
Question 3

INTRO



- 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**)

PART A



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)

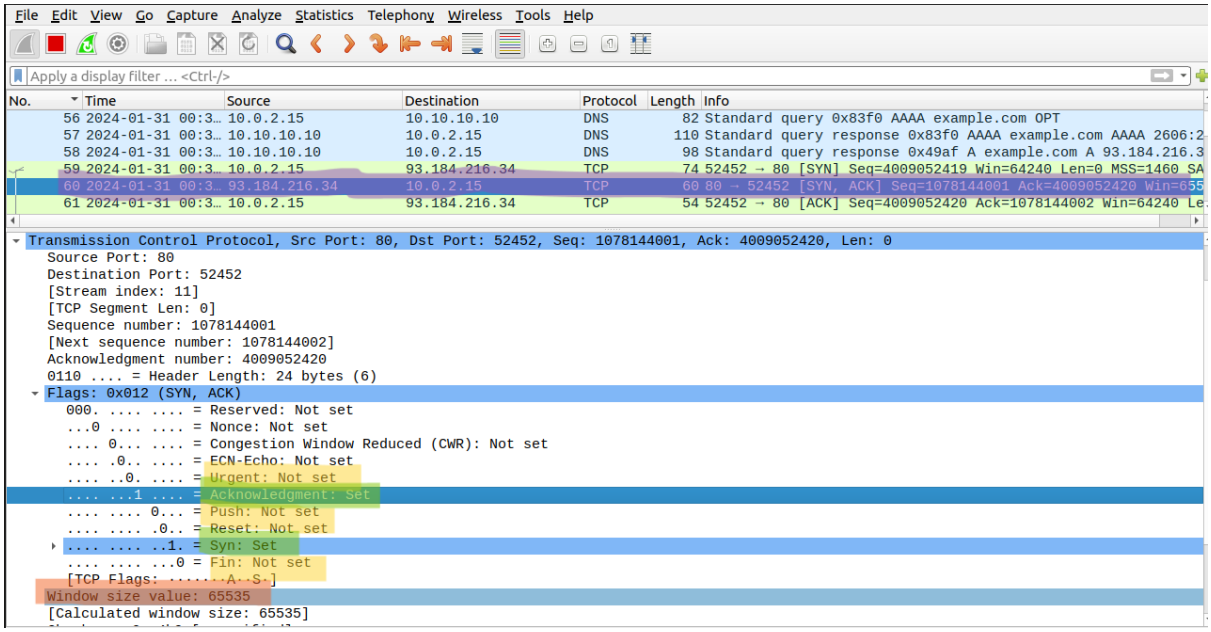
PART B

Procedure:

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

RESULTS

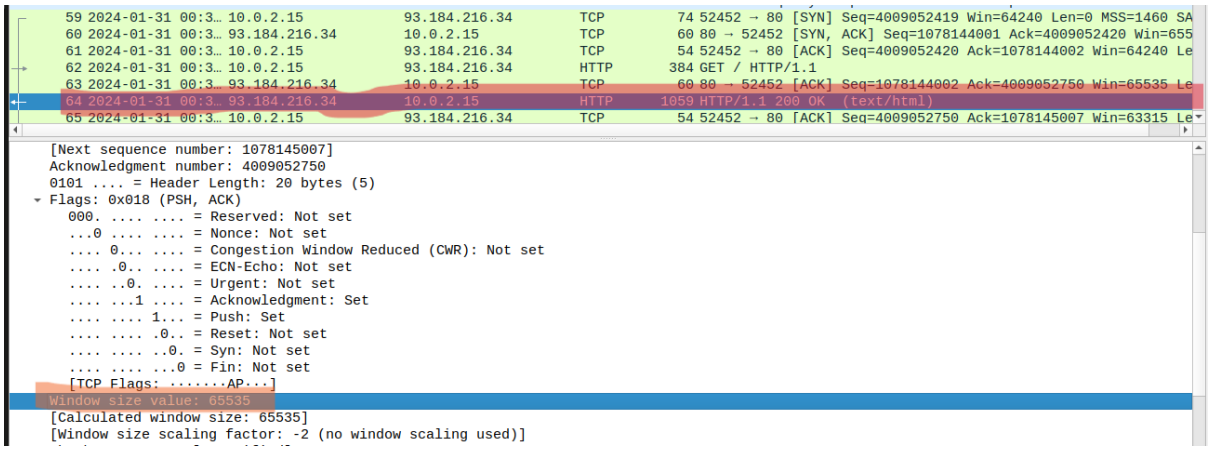
SYN packet has sequence number 4009052419 which is a random number as running experiment again give different values of sequence number. (Highlighted in red)



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)

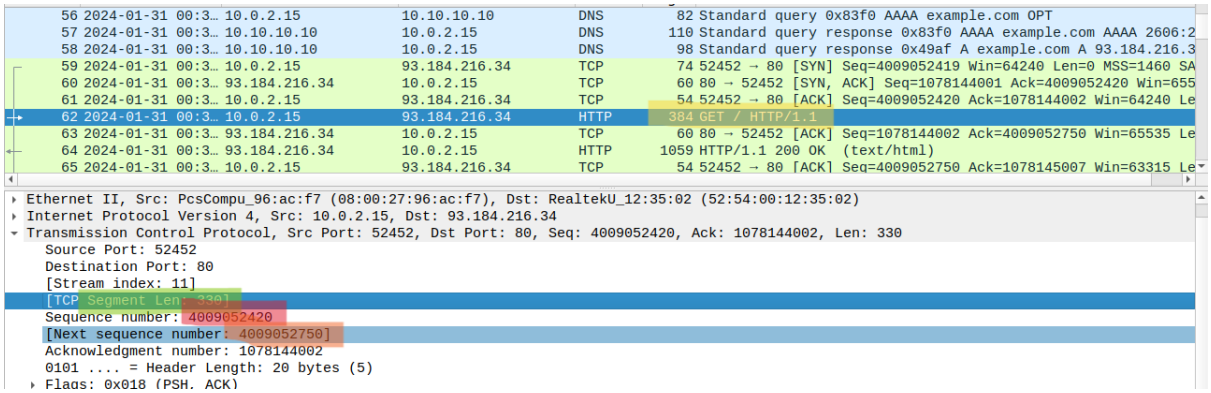


PART D

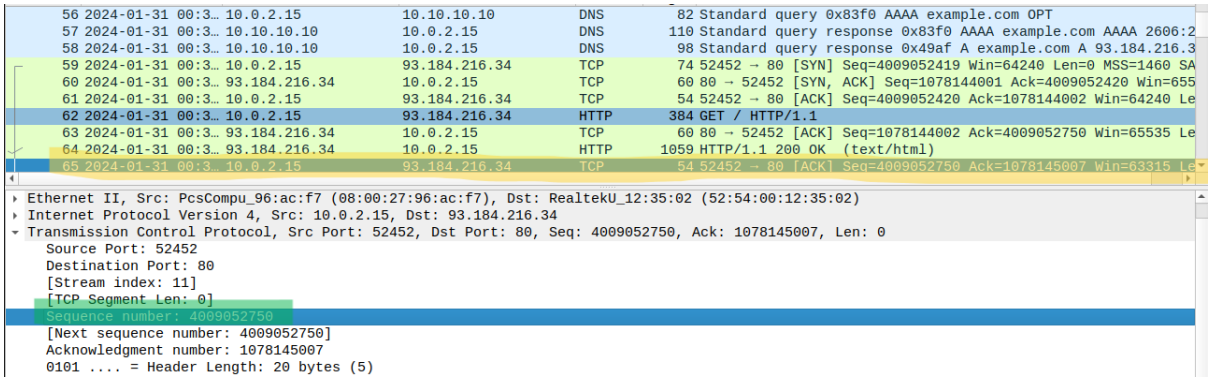
RESULTS

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

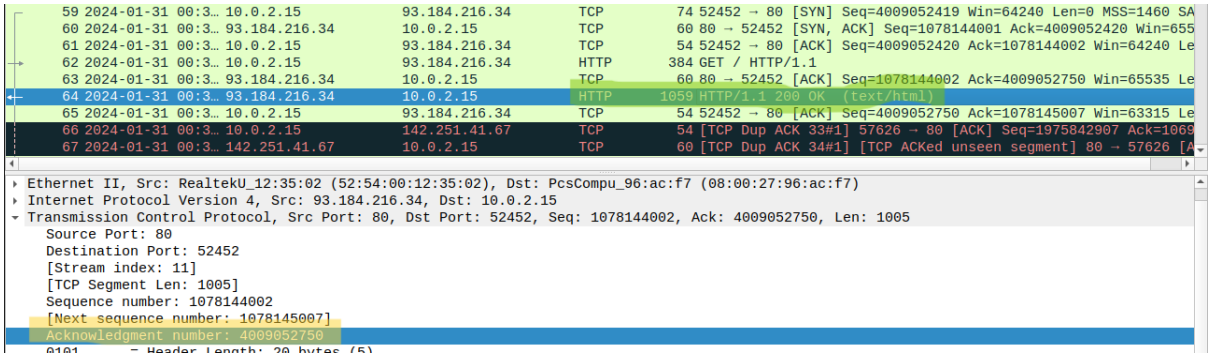


1. HTTP request packet is packet number 62 (Highlighted in yellow).
2. Payload size or segment length is 330 (Highlighted in green)
3. Sequence number is which is 4009052420. (Highlighted in red)
4. Next sequence number is 4009052750. (Highlighted in orange)
5. Observation : 4009052420 + 330 = 4009052750



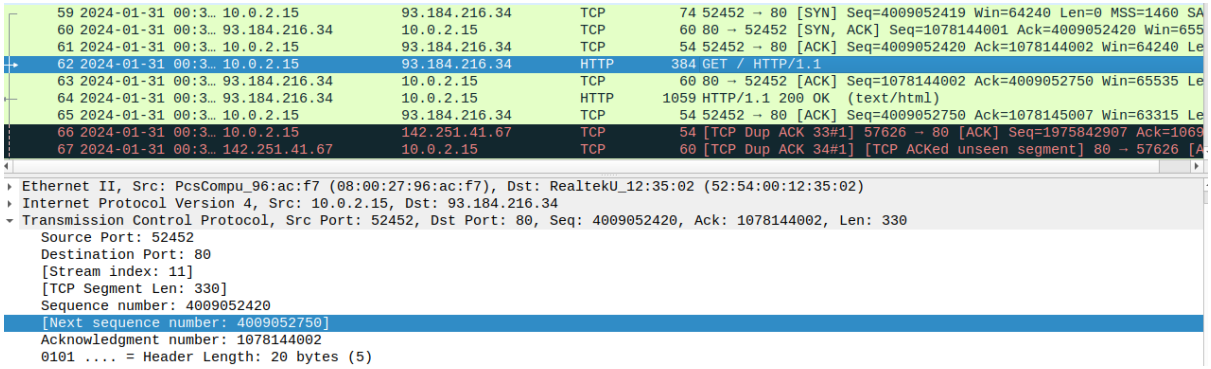
1. Next packet sent by VM is Acknowledgment packet which is packet number 65 (Highlighted in yellow).
2. Next packet's Sequence number is 4009052750 , which is same as next sequence number of HTTP request packet sent by VM initially (Highlighgted in green)

PART F



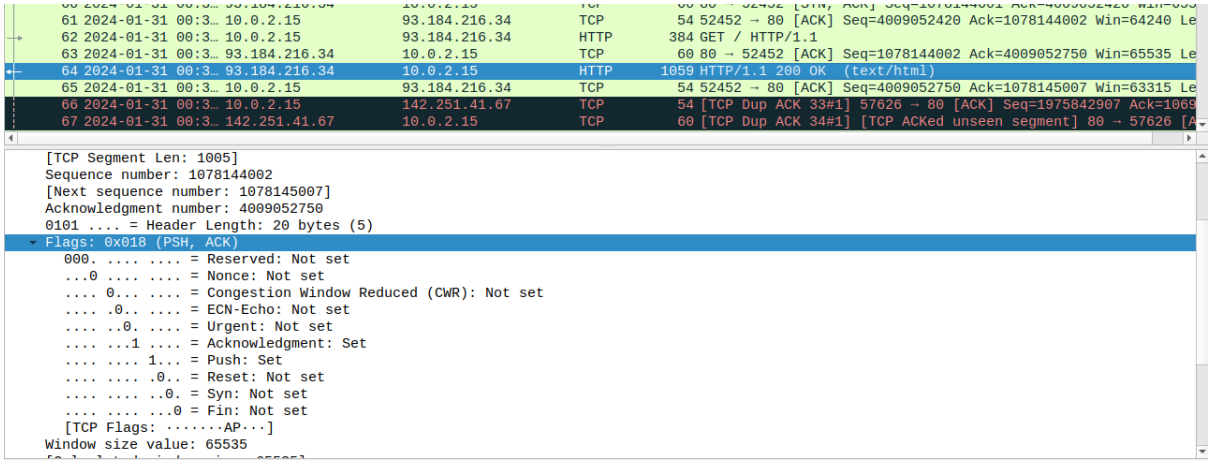
1. Http response packet is packet number 64 (Highlighted in green)

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



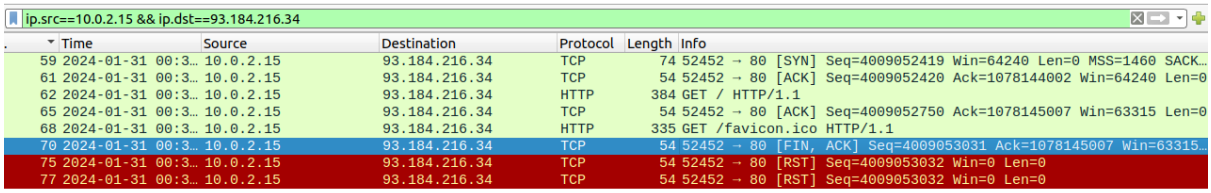
3. It can be observed that it is same as next sequence number of HTTP request packet which is also 4009052750.

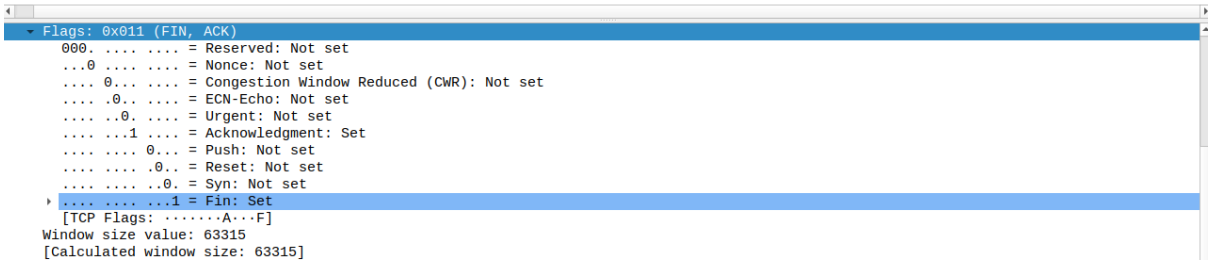
PART G



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





1. VM sent FIN ACK packet to terminate TCP connection

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