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 3

Master of Applied Computing

Networking & Data Security

COMP 8677

University of Windsor

Submitted By:

Siddharth Samber

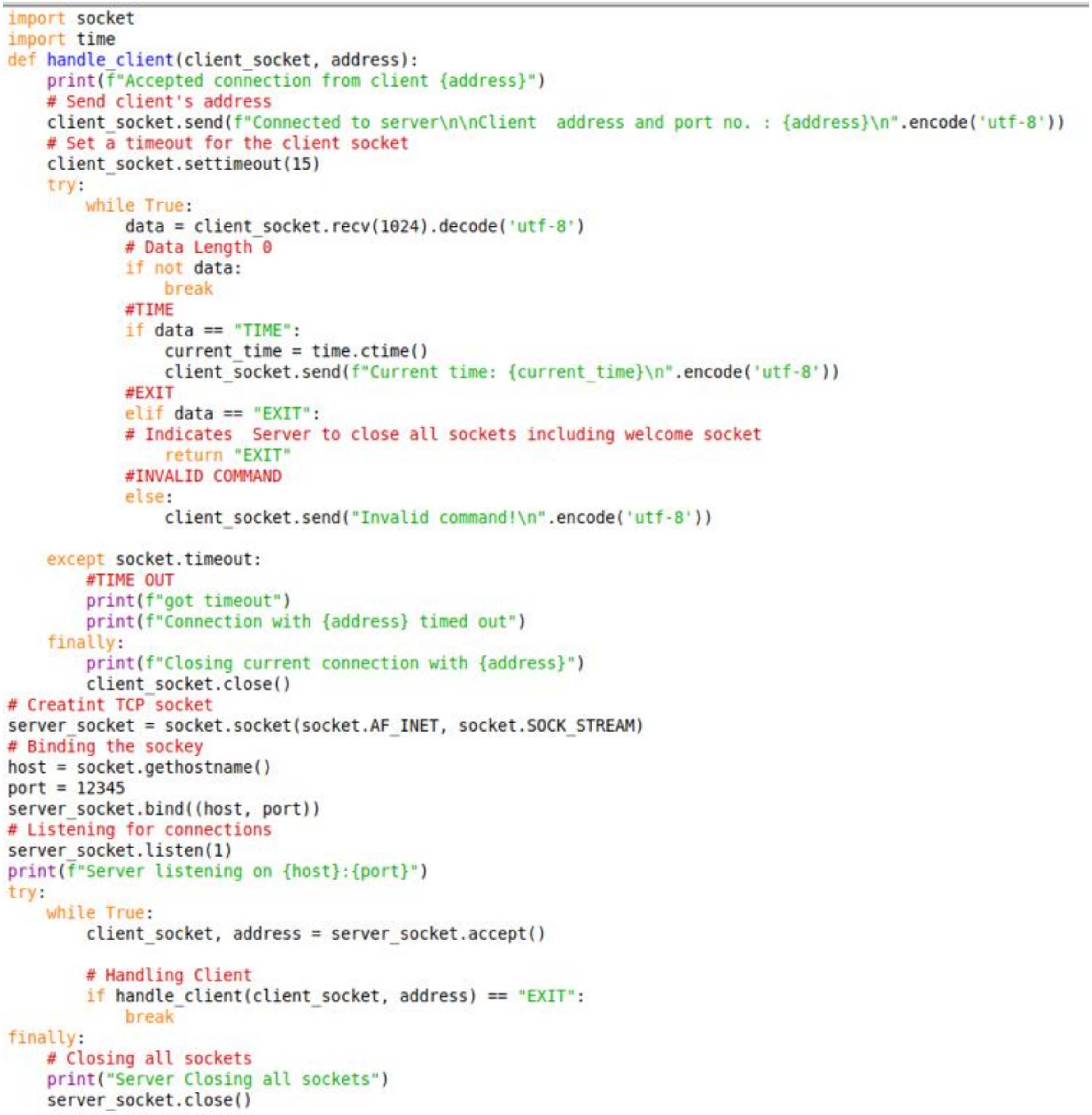
110124156

Submission Date:

11 February 2024

LAB 2 QUESTION 4

SERVER CODE (PORT 12345)



```
import socket
import time
def handle_client(client_socket, address):
    print(f"Accepted connection from client {address}")
    # Send client's address
    client_socket.send(f"Connected to server\n\nClient  address and port no. : {address}\n".encode('utf-8'))
    # Set a timeout for the client socket
    client_socket.settimeout(15)
    try:
        while True:
            data = client_socket.recv(1024).decode('utf-8')
            # Data Length 0
            if not data:
                break
            #TIME
            if data == "TIME":
                current_time = time.ctime()
                client_socket.send(f"Current time: {current_time}\n".encode('utf-8'))
            #EXIT
            elif data == "EXIT":
            # Indicates  Server to close all sockets including welcome socket
                return "EXIT"
            #INVALID COMMAND
            else:
                client_socket.send("Invalid command!\n".encode('utf-8'))

    except socket.timeout:
        #TIME OUT
        print(f"got timeout")
        print(f"Connection with {address} timed out")
    finally:
        print(f"Closing current connection with {address}")
        client_socket.close()
# Creatint TCP socket
server_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
# Binding the sockey
host = socket.gethostname()
port = 12345
server_socket.bind((host, port))
# Listening for connections
server_socket.listen(1)
print(f"Server listening on {host}:{port}")
try:
    while True:
        client_socket, address = server_socket.accept()

        # Handling Client
        if handle_client(client_socket, address) == "EXIT":
            break
finally:
    # Closing all sockets
    print("Server Closing all sockets")
    server_socket.close()
```

SEQUENCE OF COMMANDS FROM CLIENT SIDES

FIRST CLIENT

TIME

HELLO

SECURITY

SLEEP FOR 2 SECONDS

TIME

SLEEP FOR 20 SECONDS

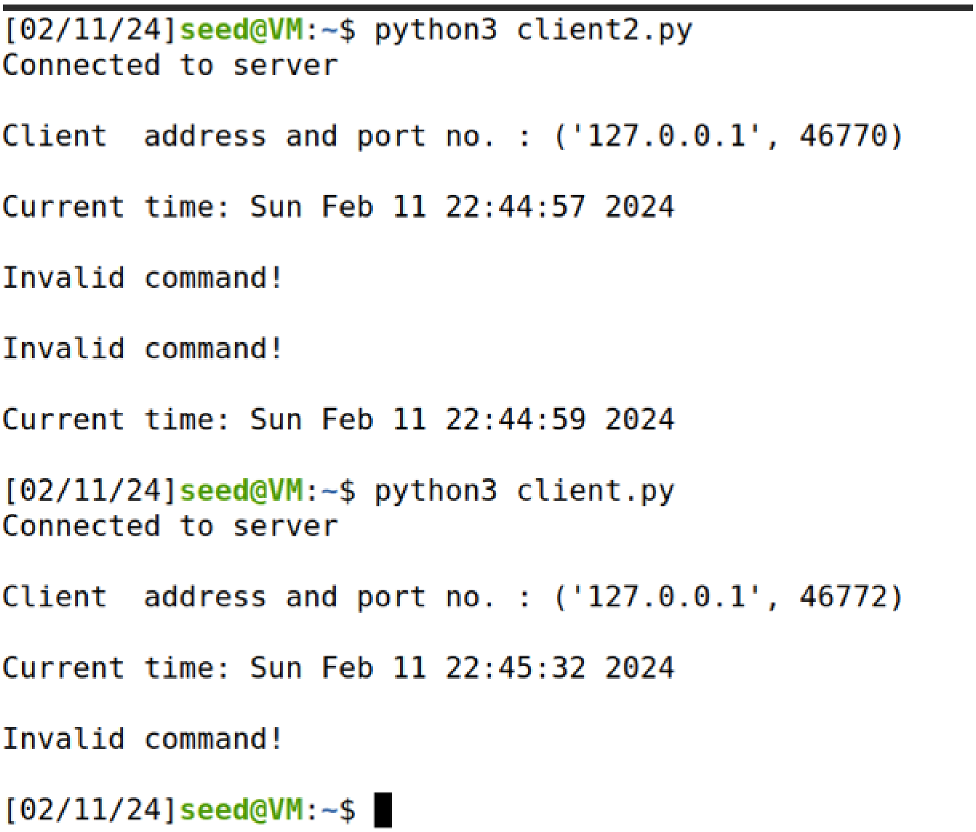
SECOND CLIENT

TIME

HELLO

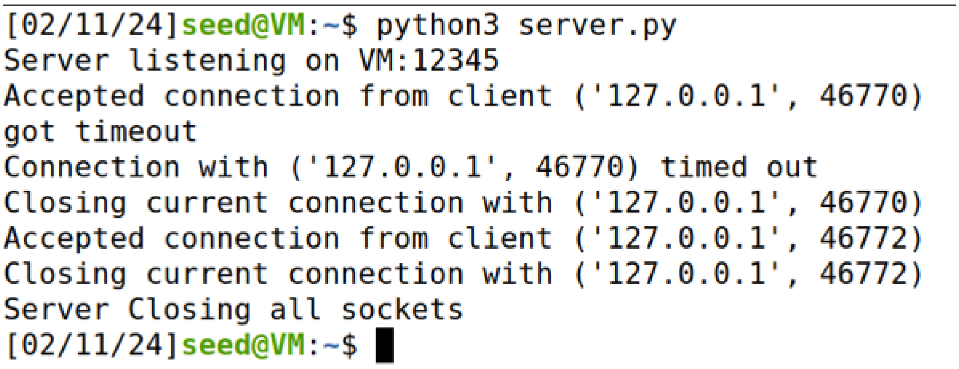
EXIT

RUNNING RESULTS AT CLIENT SIDE



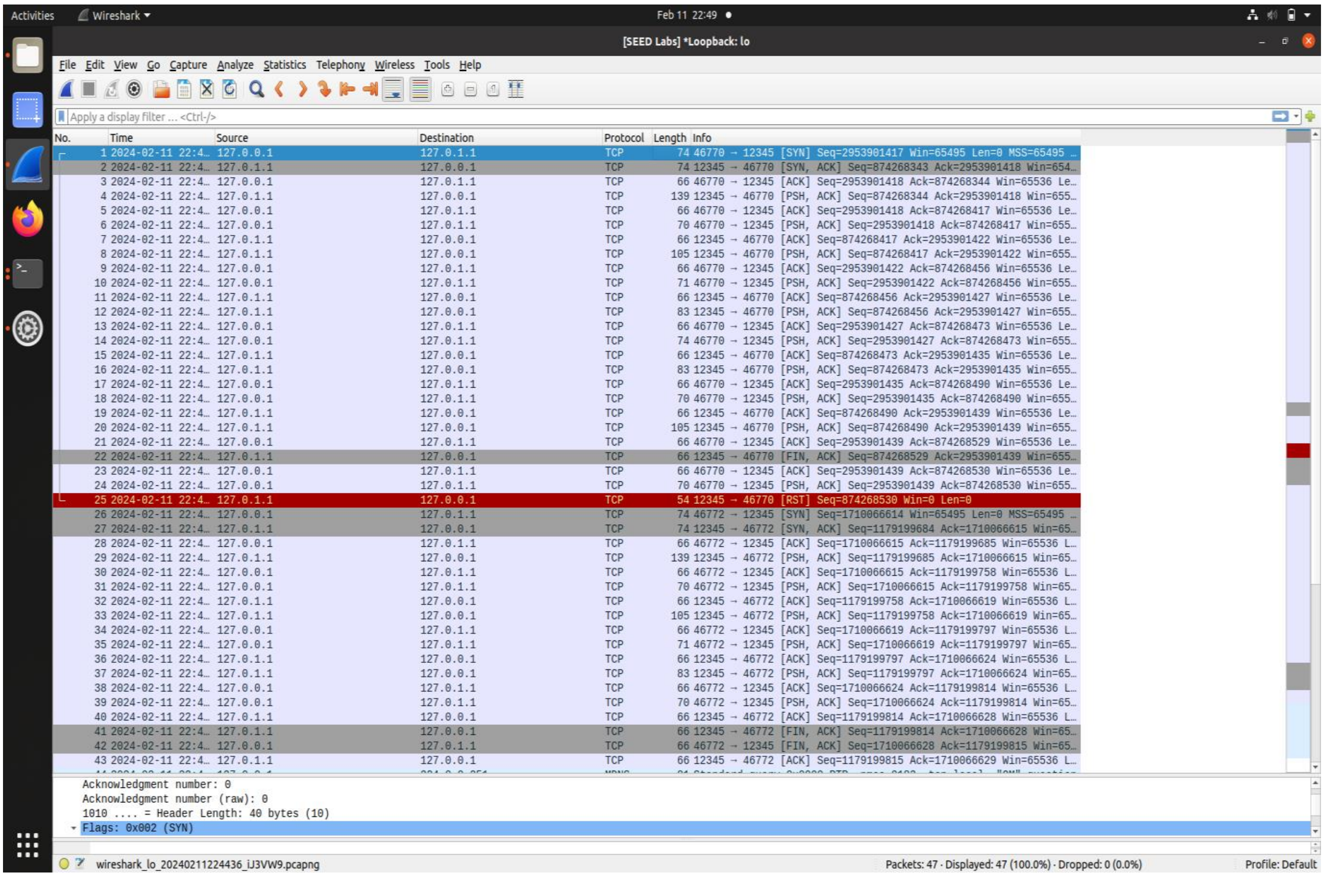
```
[02/11/24]seed@VM:~$ python3 client2.py
Connected to server

Client  address and port no. : ('127.0.0.1', 46770)

Current time: Sun Feb 11 22:44:57 2024

Invalid command!

Invalid command!

Current time: Sun Feb 11 22:44:59 2024

[02/11/24]seed@VM:~$ python3 client.py
Connected to server

Client  address and port no. : ('127.0.0.1', 46772)

Current time: Sun Feb 11 22:45:32 2024

Invalid command!

[02/11/24]seed@VM:~$ █
```

RUNNING RESULTS AT SERVER SIDE



```
[02/11/24]seed@VM:~$ python3 server.py
Server listening on VM:12345
Accepted connection from client ('127.0.0.1', 46770)
got timeout
Connection with ('127.0.0.1', 46770) timed out
Closing current connection with ('127.0.0.1', 46770)
Accepted connection from client ('127.0.0.1', 46772)
Closing current connection with ('127.0.0.1', 46772)
Server Closing all sockets
[02/11/24]seed@VM:~$ █
```

PACKET LIST BETWEEN SERVER AND CLIENT (LOOPBACK INTERFACE USED)



Activities
Wireshark
Feb 11 22:49
[SEED Labs] *Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

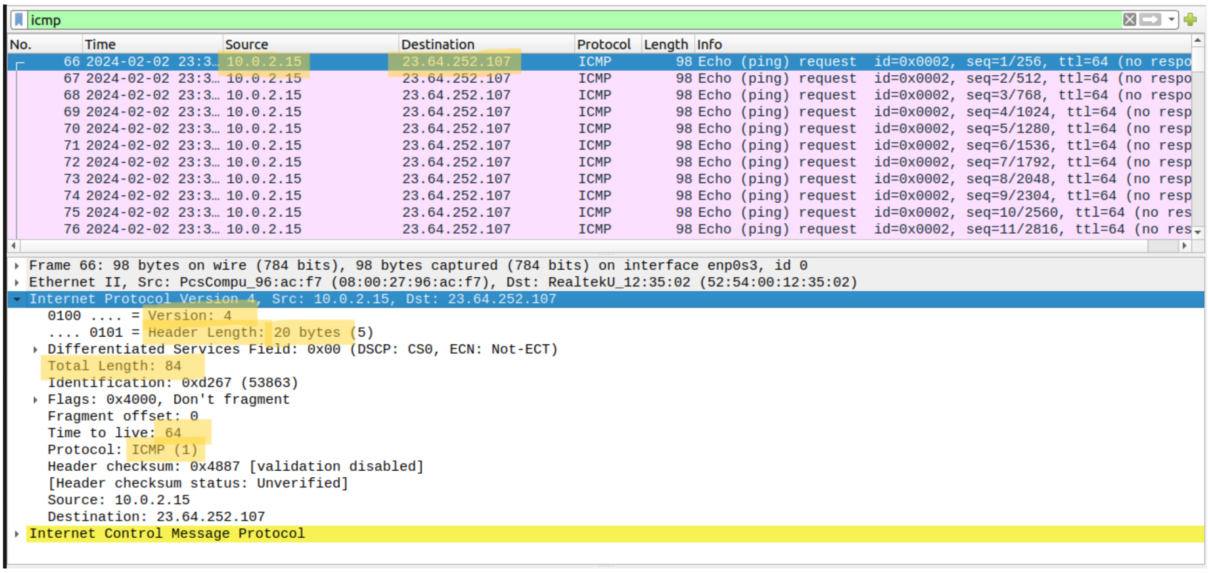
```
No.  Time              Source      Destination  Protocol  Length  Info
  1 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        74 46770 → 12345 [SYN] Seq=2953901417 Win=65495 Len=0 MSS=65495 …
  2 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        74 12345 → 46770 [SYN, ACK] Seq=874268343 Ack=2953901418 Win=654…
  3 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46770 → 12345 [ACK] Seq=2953901418 Ack=874268344 Win=65536 Le…
  4 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP       139 12345 → 46770 [PSH, ACK] Seq=874268344 Ack=2953901418 Win=655…
  5 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46770 → 12345 [ACK] Seq=2953901418 Ack=874268417 Win=65536 Le…
  6 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        70 46770 → 12345 [PSH, ACK] Seq=2953901418 Ack=874268417 Win=655…
  7 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        66 12345 → 46770 [ACK] Seq=874268417 Ack=2953901422 Win=65536 Le…
  8 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP       105 12345 → 46770 [PSH, ACK] Seq=874268417 Ack=2953901422 Win=655…
  9 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46770 → 12345 [ACK] Seq=2953901422 Ack=874268456 Win=65536 Le…
 10 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        71 46770 → 12345 [PSH, ACK] Seq=2953901422 Ack=874268456 Win=655…
 11 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        66 12345 → 46770 [ACK] Seq=874268456 Ack=2953901427 Win=65536 Le…
 12 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        83 12345 → 46770 [PSH, ACK] Seq=874268456 Ack=2953901427 Win=655…
 13 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46770 → 12345 [ACK] Seq=2953901427 Ack=874268473 Win=65536 Le…
 14 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        74 46770 → 12345 [PSH, ACK] Seq=2953901427 Ack=874268473 Win=655…
 15 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        66 12345 → 46770 [ACK] Seq=874268473 Ack=2953901435 Win=65536 Le…
 16 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        83 12345 → 46770 [PSH, ACK] Seq=874268473 Ack=2953901435 Win=655…
 17 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46770 → 12345 [ACK] Seq=2953901435 Ack=874268490 Win=65536 Le…
 18 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        70 46770 → 12345 [PSH, ACK] Seq=2953901435 Ack=874268490 Win=655…
 19 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        66 12345 → 46770 [ACK] Seq=874268490 Ack=2953901439 Win=65536 Le…
 20 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP       105 12345 → 46770 [PSH, ACK] Seq=874268490 Ack=2953901439 Win=655…
 21 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46770 → 12345 [ACK] Seq=2953901439 Ack=874268529 Win=65536 Le…
 22 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        66 12345 → 46770 [FIN, ACK] Seq=874268529 Ack=2953901439 Win=655…
 23 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46770 → 12345 [ACK] Seq=2953901439 Ack=874268530 Win=65536 Le…
 24 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        70 46770 → 12345 [PSH, ACK] Seq=2953901439 Ack=874268530 Win=655…
 25 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        54 12345 → 46770 [RST] Seq=874268530 Win=0 Len=0
 26 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        74 46772 → 12345 [SYN] Seq=1710066614 Win=65495 Len=0 MSS=65495 …
 27 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        74 12345 → 46772 [SYN, ACK] Seq=1179199684 Ack=1710066615 Win=65…
 28 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46772 → 12345 [ACK] Seq=1710066615 Ack=1179199685 Win=65536 L…
 29 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP       139 12345 → 46772 [PSH, ACK] Seq=1179199685 Ack=1710066615 Win=65…
 30 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46772 → 12345 [ACK] Seq=1710066615 Ack=1179199758 Win=65536 L…
 31 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        70 46772 → 12345 [PSH, ACK] Seq=1710066615 Ack=1179199758 Win=65…
 32 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        66 12345 → 46772 [ACK] Seq=1179199758 Ack=1710066619 Win=65536 L…
 33 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP       105 12345 → 46772 [PSH, ACK] Seq=1179199758 Ack=1710066619 Win=65…
 34 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46772 → 12345 [ACK] Seq=1710066619 Ack=1179199797 Win=65536 L…
 35 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        71 46772 → 12345 [PSH, ACK] Seq=1710066619 Ack=1179199797 Win=65…
 36 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        66 12345 → 46772 [ACK] Seq=1179199797 Ack=1710066624 Win=65536 L…
 37 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        83 12345 → 46772 [PSH, ACK] Seq=1179199797 Ack=1710066624 Win=65…
 38 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46772 → 12345 [ACK] Seq=1710066624 Ack=1179199814 Win=65536 L…
 39 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        70 46772 → 12345 [PSH, ACK] Seq=1710066624 Ack=1179199814 Win=65…
 40 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        66 12345 → 46772 [ACK] Seq=1179199814 Ack=1710066628 Win=65536 L…
 41 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        66 12345 → 46772 [FIN, ACK] Seq=1179199814 Ack=1710066628 Win=65…
 42 2024-02-11 22:4…  127.0.0.1   127.0.1.1    TCP        66 46772 → 12345 [FIN, ACK] Seq=1710066628 Ack=1179199815 Win=65…
 43 2024-02-11 22:4…  127.0.1.1   127.0.0.1    TCP        66 12345 → 46772 [ACK] Seq=1179199815 Ack=1710066629 Win=65536 L…
```

```
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  ▾ Flags: 0x002 (SYN)
```

```
wireshark_lo_20240211224436_iJ3VW9.pcapng          Packets: 47 · Displayed: 47 (100.0%) · Dropped: 0 (0.0%)          Profile: Default
```

LAB 3

QUESTION 1



```
No.  Time              Source       Destination   Protocol Length Info
  66 2024-02-02 23:3… 10.0.2.15    23.64.252.107 ICMP         98 Echo (ping) request  id=0x0002, seq=1/256, ttl=64 (no respo
  67 2024-02-02 23:3… 10.0.2.15    23.64.252.107 ICMP         98 Echo (ping) request  id=0x0002, seq=2/512, ttl=64 (no respo
  68 2024-02-02 23:3… 10.0.2.15    23.64.252.107 ICMP         98 Echo (ping) request  id=0x0002, seq=3/768, ttl=64 (no respo
  69 2024-02-02 23:3… 10.0.2.15    23.64.252.107 ICMP         98 Echo (ping) request  id=0x0002, seq=4/1024, ttl=64 (no resp
  70 2024-02-02 23:3… 10.0.2.15    23.64.252.107 ICMP         98 Echo (ping) request  id=0x0002, seq=5/1280, ttl=64 (no resp
  71 2024-02-02 23:3… 10.0.2.15    23.64.252.107 ICMP         98 Echo (ping) request  id=0x0002, seq=6/1536, ttl=64 (no resp
  72 2024-02-02 23:3… 10.0.2.15    23.64.252.107 ICMP         98 Echo (ping) request  id=0x0002, seq=7/1792, ttl=64 (no resp
  73 2024-02-02 23:3… 10.0.2.15    23.64.252.107 ICMP         98 Echo (ping) request  id=0x0002, seq=8/2048, ttl=64 (no resp
  74 2024-02-02 23:3… 10.0.2.15    23.64.252.107 ICMP         98 Echo (ping) request  id=0x0002, seq=9/2304, ttl=64 (no resp
  75 2024-02-02 23:3… 10.0.2.15    23.64.252.107 ICMP         98 Echo (ping) request  id=0x0002, seq=10/2560, ttl=64 (no res
  76 2024-02-02 23:3… 10.0.2.15    23.64.252.107 ICMP         98 Echo (ping) request  id=0x0002, seq=11/2816, ttl=64 (no res
```

```
▸ Frame 66: 98 bytes on wire (784 bits), 98 bytes captured (784 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: 23.64.252.107
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xd267 (53863)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x4887 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.15
    Destination: 23.64.252.107
▸ Internet Control Message Protocol
```

PART A

Source IP address : 10.0.2.15

Destination IP address : 23.64.252.107

PART B

Upper Layer Protocol : ICMP

PART C

IP header Length : 20 bytes

PART D

Payload Length : 84 – 20 = 60 bytes

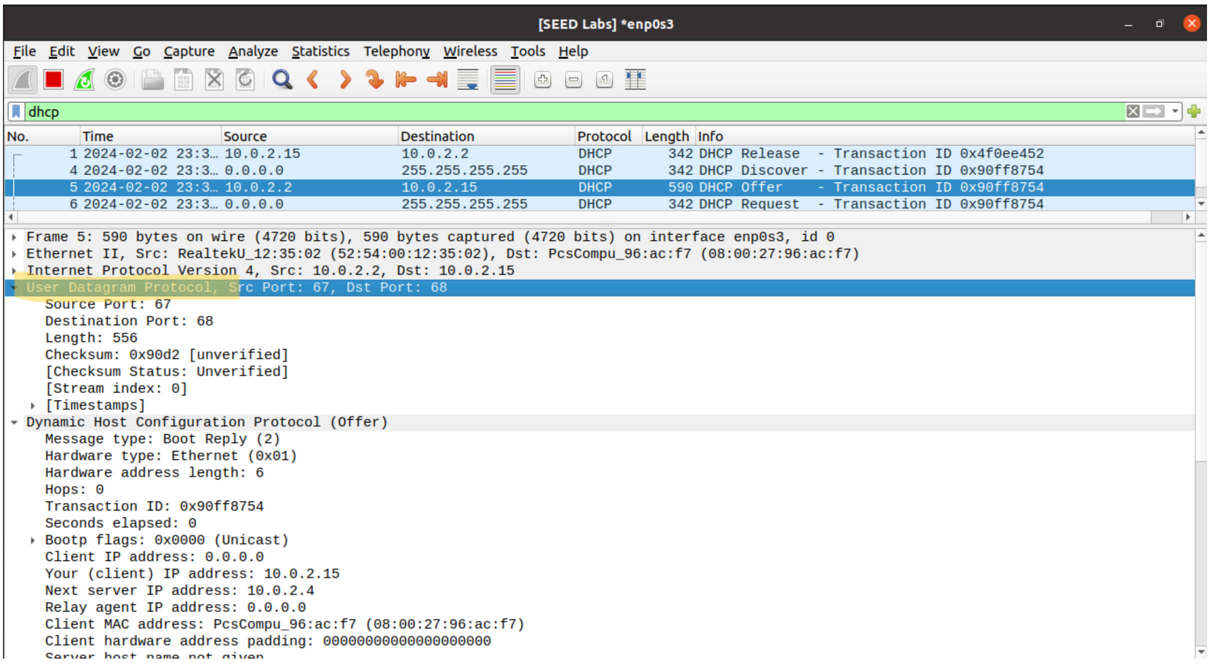
PART E

TTL value: 64

It means after 64 hops this packet will be discarded

QUESTION 2

PART A



[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dhcp
```

```
No.   Time              Source      Destination      Protocol Length Info
    1 2024-02-02 23:3… 10.0.2.15   10.0.2.2         DHCP      342 DHCP Release  - Transaction ID 0x4f0ee452
    4 2024-02-02 23:3… 0.0.0.0     255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x90ff8754
    5 2024-02-02 23:3… 10.0.2.2    10.0.2.15        DHCP      590 DHCP Offer    - Transaction ID 0x90ff8754
    6 2024-02-02 23:3… 0.0.0.0     255.255.255.255  DHCP      342 DHCP Request  - Transaction ID 0x90ff8754
```

```
Frame 5: 590 bytes on wire (4720 bits), 590 bytes captured (4720 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: 10.0.2.2, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 67, Dst Port: 68
  Source Port: 67
  Destination Port: 68
  Length: 556
  Checksum: 0x90d2 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Timestamps]
Dynamic Host Configuration Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x90ff8754
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.0.2.15
  Next server IP address: 10.0.2.4
  Relay agent IP address: 0.0.0.0
  Client MAC address: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7)
  Client hardware address padding: 00000000000000000000
  Server host name not given
```

Transport Layer protocol is UDP.

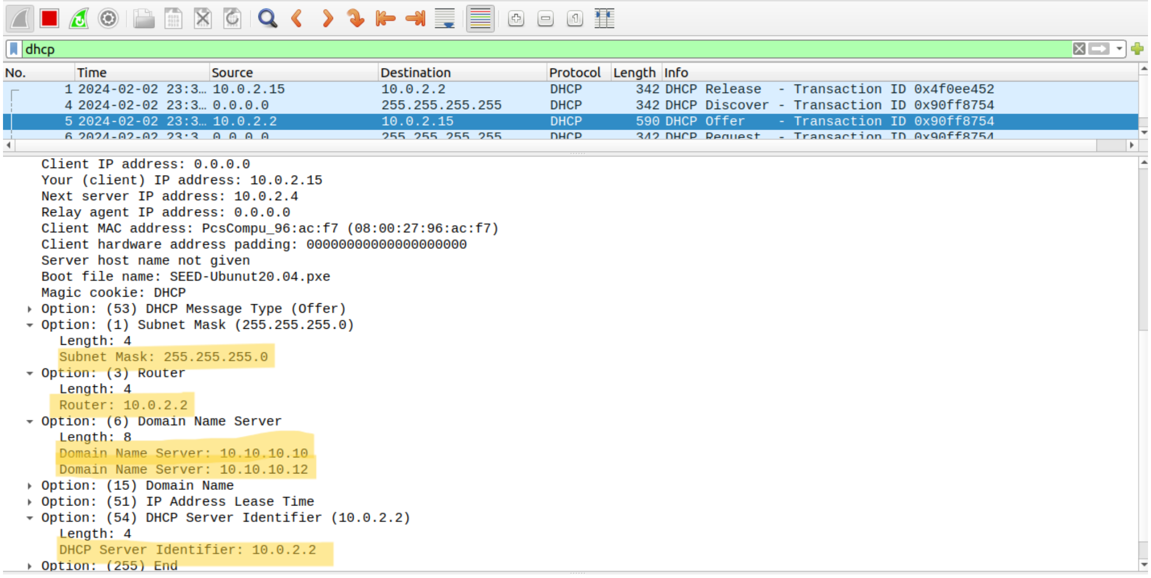
Explanation:

Connection Oriented (TCP): TCP has Connection requirement of 3-way handshake for which it requires IP address, however device requesting IP address has not any IP yet.

Connectionless (UDP) : No connection requirement hence UDP is suitable.

It is UDP and not TCP as there will be overhead in establishing connection for TCP and DHCP interactions are stateless.

PART B

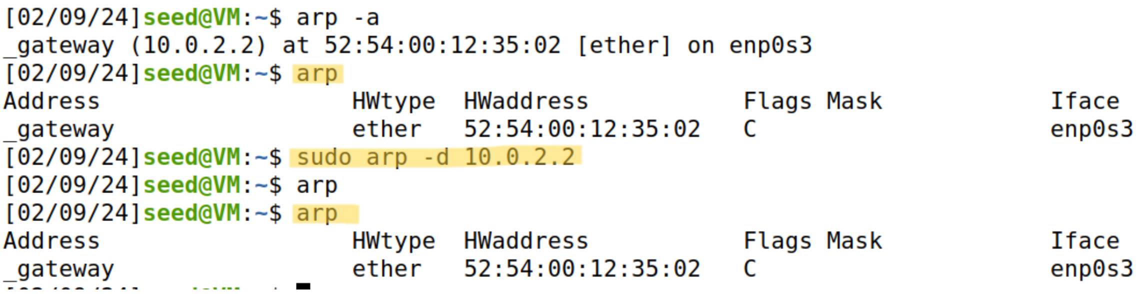


```
No.   Time                Source       Destination        Protocol  Length  Info
    1 2024-02-02 23:3…    10.0.2.15    10.0.2.2           DHCP         342  DHCP Release  - Transaction ID 0x4f0ee452
    4 2024-02-02 23:3…    0.0.0.0      255.255.255.255    DHCP         342  DHCP Discover - Transaction ID 0x90ff8754
    5 2024-02-02 23:3…    10.0.2.2     10.0.2.15          DHCP         590  DHCP Offer    - Transaction ID 0x90ff8754
    6 2024-02-02 23:3     0.0.0.0      255.255.255.255    DHCP         342  DHCP Request  - Transaction ID 0x90ff8754
```

```
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.0.2.15
    Next server IP address: 10.0.2.4
    Relay agent IP address: 0.0.0.0
    Client MAC address: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name: SEED-Ubunut20.04.pxe
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Offer)
  ▾ Option: (1) Subnet Mask (255.255.255.0)
      Length: 4
      Subnet Mask: 255.255.255.0
  ▾ Option: (3) Router
      Length: 4
      Router: 10.0.2.2
  ▾ Option: (6) Domain Name Server
      Length: 8
      Domain Name Server: 10.10.10.10
      Domain Name Server: 10.10.10.12
  ▸ Option: (15) Domain Name
  ▸ Option: (51) IP Address Lease Time
  ▾ Option: (54) DHCP Server Identifier (10.0.2.2)
      Length: 4
      DHCP Server Identifier: 10.0.2.2
  ▸ Option: (255) End
```

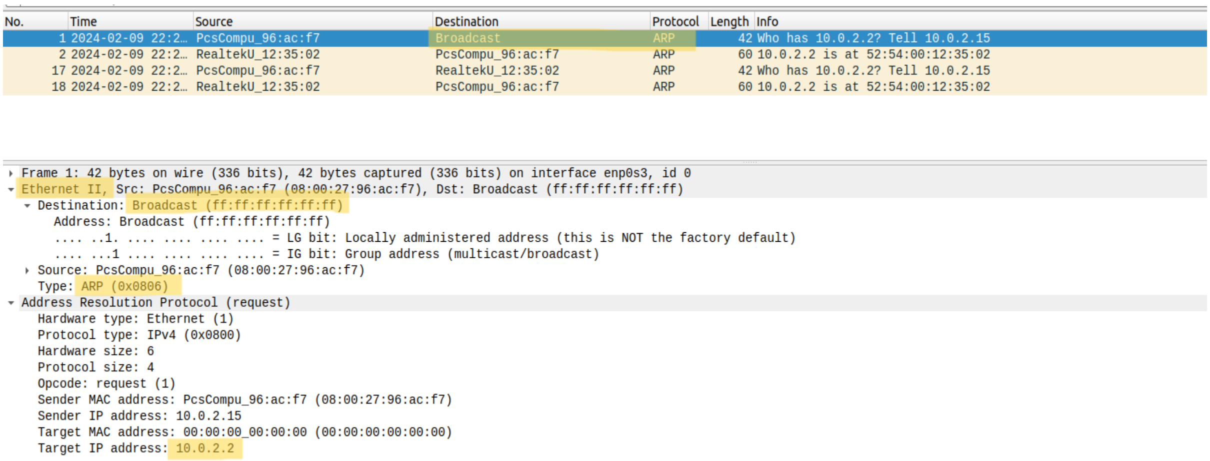
1) DHCP server IP : 10.0.2.2
2) Subnet Mask : 255.255.255.0
3) Router IP : 10.0.2.2
4) DNS IP : 10.10.10.1.0 and 10.0.2.2

QUESTION 3



```
[02/09/24]seed@VM:~$ arp -a
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
[02/09/24]seed@VM:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   52:54:00:12:35:02   C                     enp0s3
[02/09/24]seed@VM:~$ sudo arp -d 10.0.2.2
[02/09/24]seed@VM:~$ arp
[02/09/24]seed@VM:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   52:54:00:12:35:02   C                     enp0s3
[02/09/24]seed@VM:~$
```

PART A



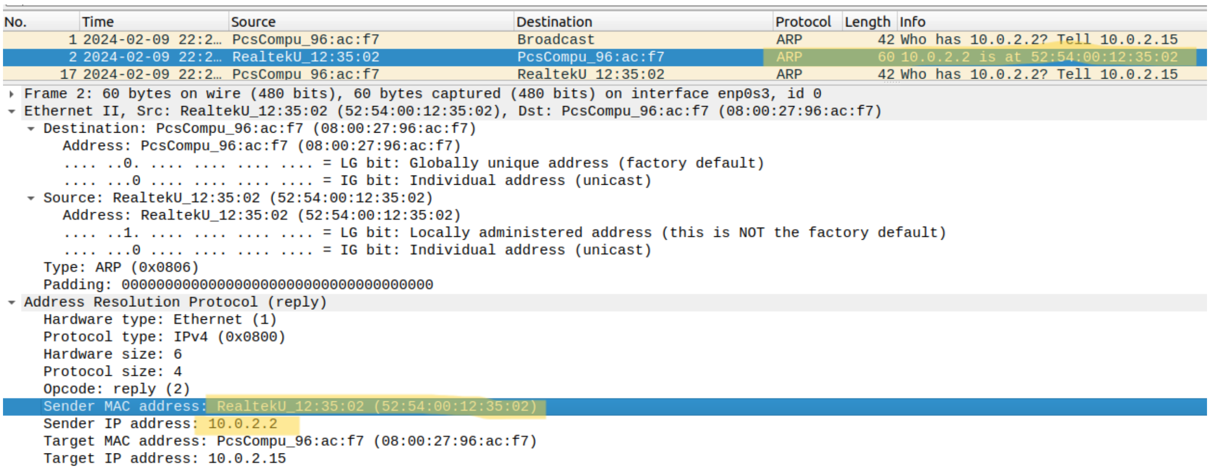
```
No.   Time                Source              Destination         Protocol  Length  Info
    1 2024-02-09 22:2…    PcsCompu_96:ac:f7   Broadcast           ARP           42  Who has 10.0.2.2? Tell 10.0.2.15
    2 2024-02-09 22:2…    RealtekU_12:35:02   PcsCompu_96:ac:f7   ARP           60  10.0.2.2 is at 52:54:00:12:35:02
   17 2024-02-09 22:2…    PcsCompu_96:ac:f7   RealtekU_12:35:02   ARP           42  Who has 10.0.2.2? Tell 10.0.2.15
   18 2024-02-09 22:2…    RealtekU_12:35:02   PcsCompu_96:ac:f7   ARP           60  10.0.2.2 is at 52:54:00:12:35:02
```

```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s3, id 0
▾ Ethernet II, Src: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▸ Source: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7)
    Type: ARP (0x0806)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7)
    Sender IP address: 10.0.2.15
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.2.2
```

In link Layer Header (Enthernet II header)

1) Upper layer protocol -> ARP (0x0806)
2) Broadcast MAC Address: ff:ff:ff:ff:ff:ff
3) Target IP address : 10.0.2.2
   (Target IP address is is the ip address for which broadcast message is inteded to find out the MAC address)

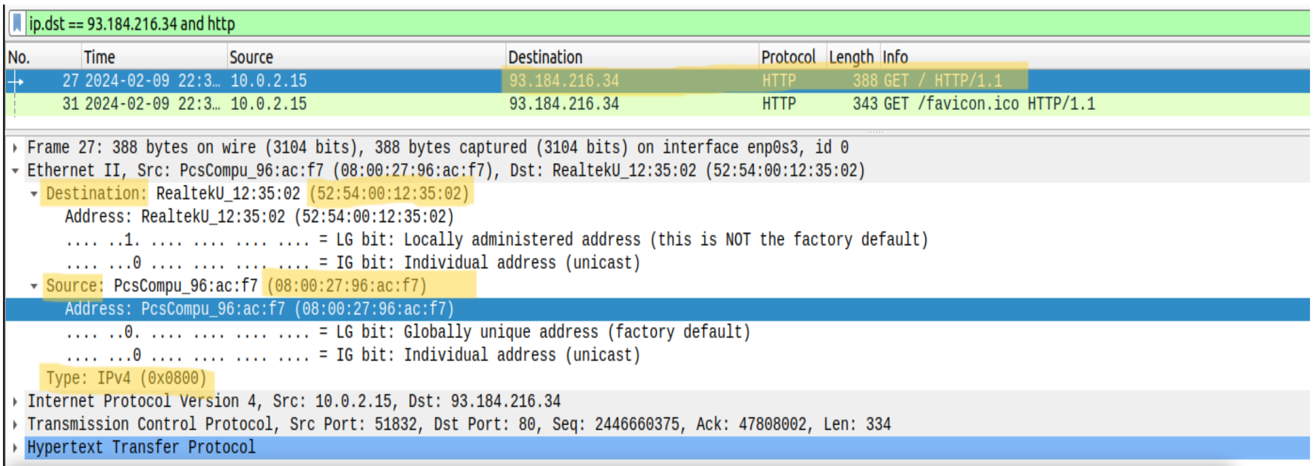
PART B



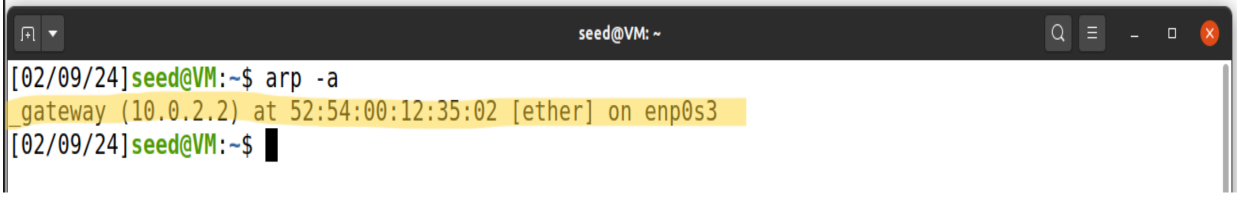
```
No.   Time              Source              Destination         Protocol Length Info
    1 2024-02-09 22:2…  PcsCompu_96:ac:f7   Broadcast           ARP         42 Who has 10.0.2.2? Tell 10.0.2.15
    2 2024-02-09 22:2…  RealtekU_12:35:02   PcsCompu_96:ac:f7   ARP         60 10.0.2.2 is at 52:54:00:12:35:02
   17 2024-02-09 22:2…  PcsCompu_96:ac:f7   RealtekU_12:35:02   ARP         42 Who has 10.0.2.2? Tell 10.0.2.15

▸ Frame 2: 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)
  ▾ Destination: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7)
      Address: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: RealtekU_12:35:02 (52:54:00:12:35:02)
      Address: RealtekU_12:35:02 (52:54:00:12:35:02)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: RealtekU_12:35:02 (52:54:00:12:35:02)
    Sender IP address: 10.0.2.2
    Target MAC address: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7)
    Target IP address: 10.0.2.15
```

1) Sender IP address : 10.0.2.2 (Gateway router IP)
2) Sneder MAC address : 52:54:00:12:35:02 (Gateway router MAC)

QUESTION 4



```
ip.dst == 93.184.216.34 and http

No.   Time              Source      Destination     Protocol Length Info
   27 2024-02-09 22:3…  10.0.2.15   93.184.216.34   HTTP        388 GET / HTTP/1.1
   31 2024-02-09 22:3…  10.0.2.15   93.184.216.34   HTTP        343 GET /favicon.ico HTTP/1.1

▸ Frame 27: 388 bytes on wire (3104 bits), 388 bytes captured (3104 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)
  ▾ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
      Address: RealtekU_12:35:02 (52:54:00:12:35:02)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7)
      Address: PcsCompu_96:ac:f7 (08:00:27:96:ac:f7)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 93.184.216.34
▸ Transmission Control Protocol, Src Port: 51832, Dst Port: 80, Seq: 2446660375, Ack: 47808002, Len: 334
▸ Hypertext Transfer Protocol
```



```
[02/09/24]seed@VM:~$ arp -a
gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
[02/09/24]seed@VM:~$ 
```

PART A

1) Source MAC address: 08:00:27:96:ac:f7
2) Source MAC address -> MAC of our VM

3) Destination MAC address: 52:54:00:12:35:02
4) Destination MAC address -> MAC of our Gateway Router

PART B

Yes, Destination MAC address listed in arp command

Explantion : Destination MAC address 53:54:00:12:35:02 is associated with ip address 10.0.2.2 which is gateway router's IP and not 93.184.216.34

PART C

In link layer header (Ehternet II)

1) Upper protocol field value -> 0x0800
2) 0x0800 Represents IPV4 protocol.