University of Windsor

Lab 3 & 2.4

Course: Networking and Data Security

COMP8677-1-R-2023F

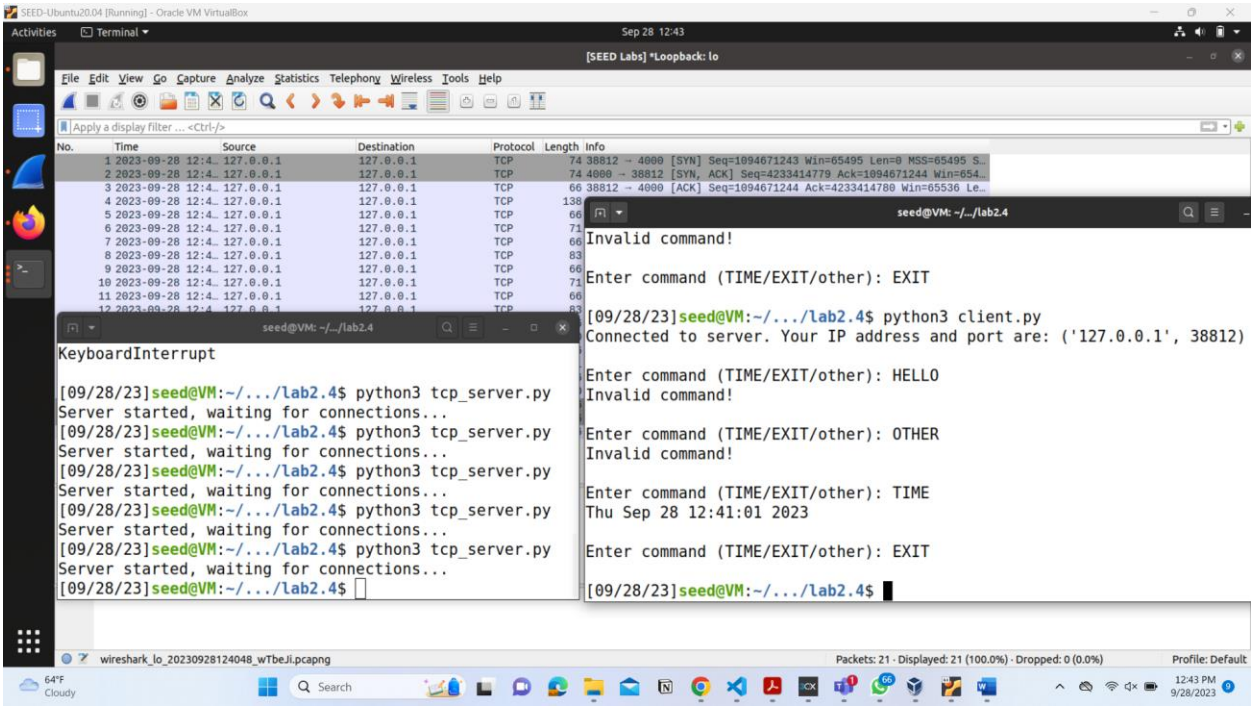
Professor: Dr. Shaoquan Jiang

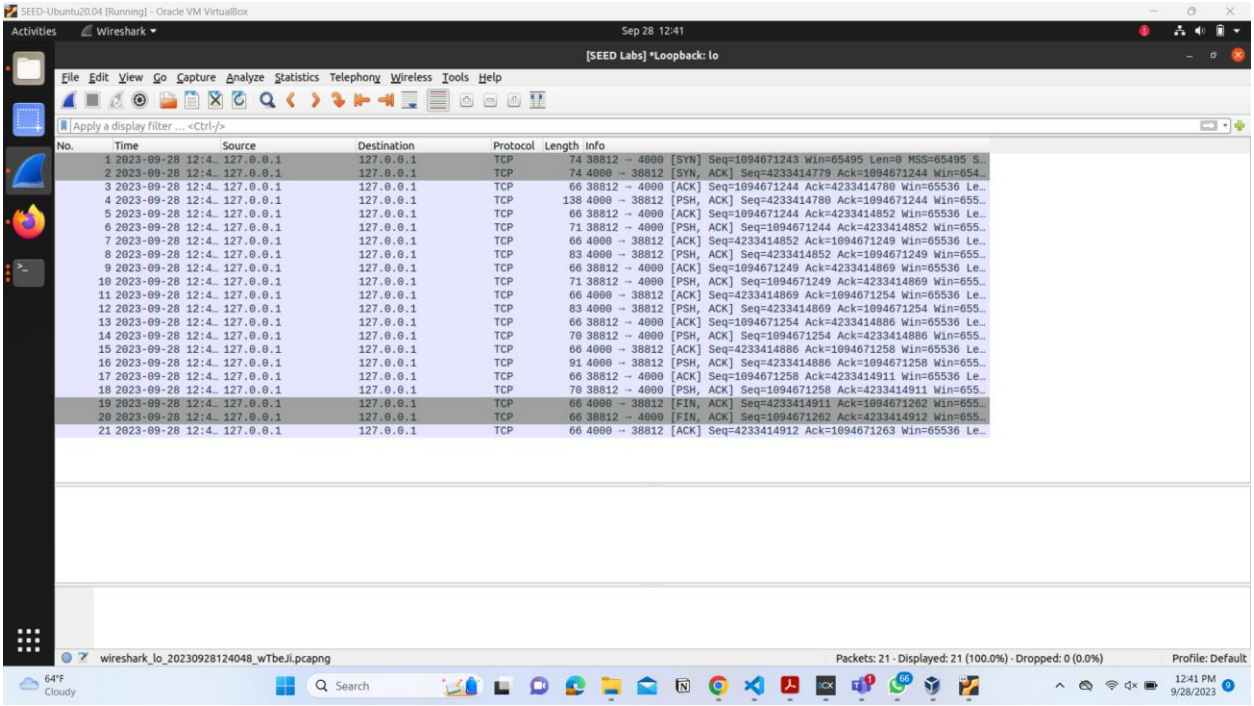
Prepared by

Harshil Hitendrabhai Panchal (110096129)

Due date: September 28, 2023

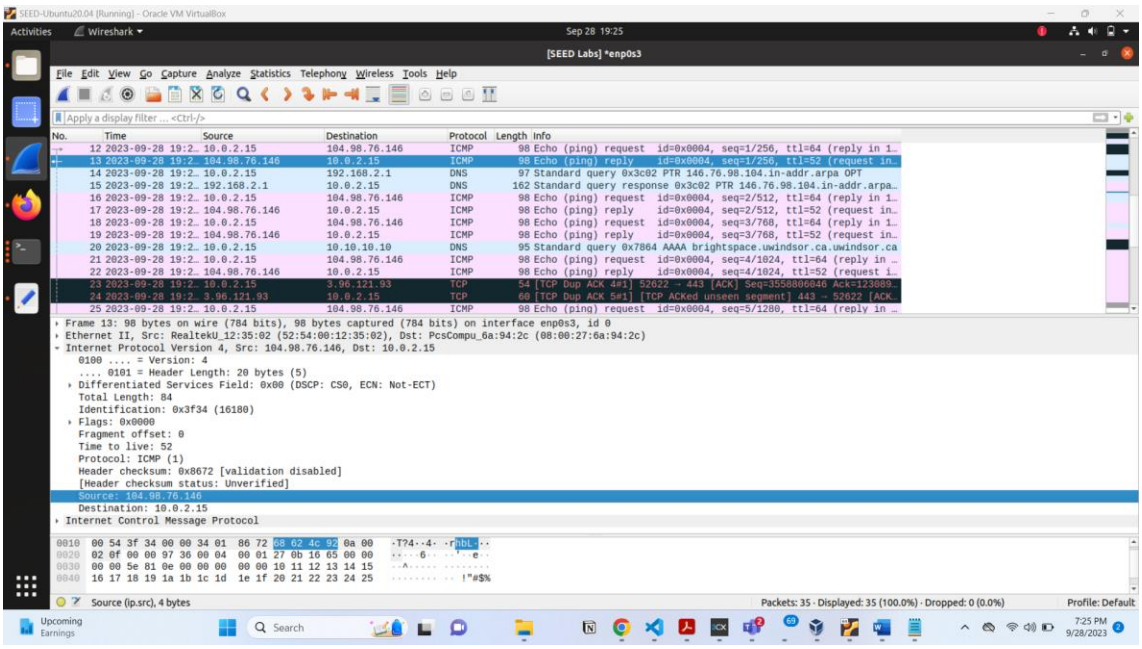
Lab 2.4


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Terminal
Sep 28 12:43
[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 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 74 38812 → 4000 [SYN] Seq=1094671243 Win=65495 Len=0 MSS=65495 S...
2 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 74 4000 → 38812 [SYN, ACK] Seq=4233414779 Ack=1094671244 Win=654...
3 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 38812 → 4000 [ACK] Seq=1094671244 Ack=4233414780 Win=65536 Le...
4 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 138
5 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66
6 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 71
7 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66
8 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 83
9 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66
10 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 71
11 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66
seed@VM: ~/.../lab2.4
KeyboardInterrupt
[09/28/23]seed@VM:~/.../lab2.4$ python3 tcp_server.py
Server started, waiting for connections...
[09/28/23]seed@VM:~/.../lab2.4$ python3 tcp_server.py
Server started, waiting for connections...
[09/28/23]seed@VM:~/.../lab2.4$ python3 tcp_server.py
Server started, waiting for connections...
[09/28/23]seed@VM:~/.../lab2.4$ python3 tcp_server.py
Server started, waiting for connections...
[09/28/23]seed@VM:~/.../lab2.4$ python3 tcp_server.py
Server started, waiting for connections...
[09/28/23]seed@VM:~/.../lab2.4$
seed@VM: ~/.../lab2.4
Invalid command!
Enter command (TIME/EXIT/other): EXIT
[09/28/23]seed@VM:~/.../lab2.4$ python3 client.py
Connected to server. Your IP address and port are: ('127.0.0.1', 38812)
Enter command (TIME/EXIT/other): HELLO
Invalid command!
Enter command (TIME/EXIT/other): OTHER
Invalid command!
Enter command (TIME/EXIT/other): TIME
Thu Sep 28 12:41:01 2023
Enter command (TIME/EXIT/other): EXIT
[09/28/23]seed@VM:~/.../lab2.4$
wireshark_lo_20230928124048_wTbeJi.pcapng
Packets: 21 · Displayed: 21 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
64°F Cloudy
Search
12:43 PM 9/28/2023

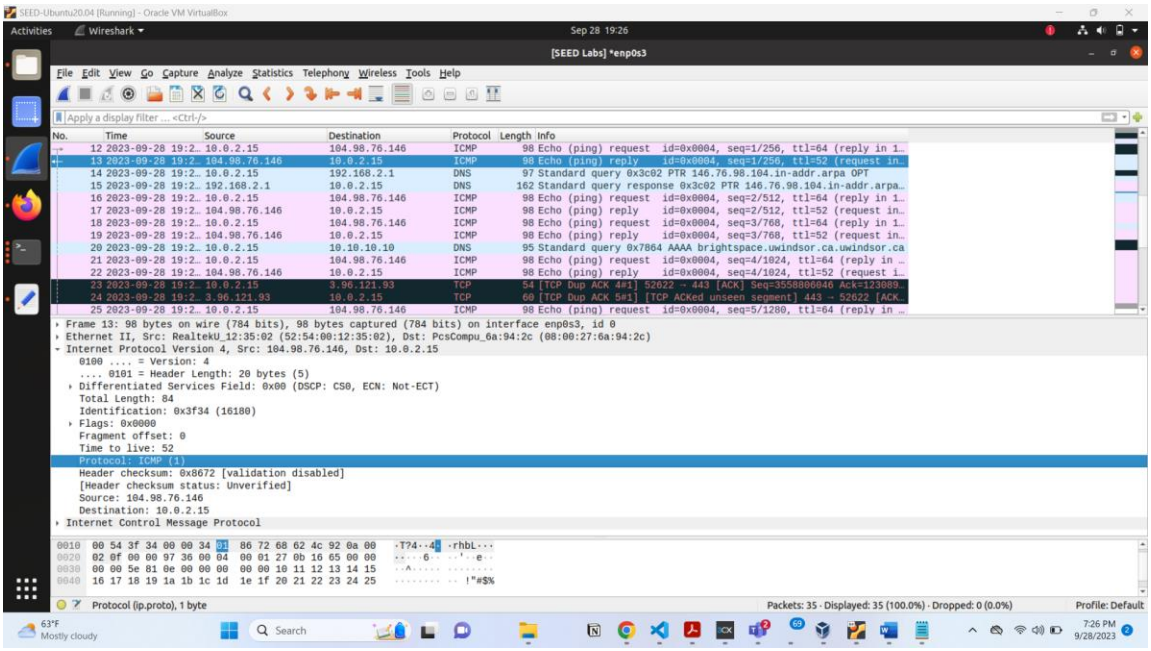

SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 28 12:41
[SEED Labs] *Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 74 38812 → 4000 [SYN] Seq=1094671243 Win=65495 Len=0 MSS=65495 S...
2 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 74 4000 → 38812 [SYN, ACK] Seq=4233414779 Ack=1094671244 Win=654...
3 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 38812 → 4000 [ACK] Seq=1094671244 Ack=4233414780 Win=65536 Le...
4 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 138 4000 → 38812 [PSH, ACK] Seq=4233414780 Ack=1094671244 Win=655...
5 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 38812 → 4000 [ACK] Seq=1094671244 Ack=4233414852 Win=65536 Le...
6 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 71 38812 → 4000 [PSH, ACK] Seq=1094671244 Ack=4233414852 Win=655...
7 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 4000 → 38812 [ACK] Seq=4233414852 Ack=1094671249 Win=65536 Le...
8 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 83 4000 → 38812 [PSH, ACK] Seq=4233414852 Ack=1094671249 Win=655...
9 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 38812 → 4000 [ACK] Seq=1094671249 Ack=4233414869 Win=65536 Le...
10 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 71 38812 → 4000 [PSH, ACK] Seq=1094671249 Ack=4233414869 Win=655...
11 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 4000 → 38812 [ACK] Seq=4233414869 Ack=1094671254 Win=65536 Le...
12 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 83 4000 → 38812 [PSH, ACK] Seq=4233414869 Ack=1094671254 Win=655...
13 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 38812 → 4000 [ACK] Seq=1094671254 Ack=4233414886 Win=65536 Le...
14 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 70 38812 → 4000 [PSH, ACK] Seq=1094671254 Ack=4233414886 Win=655...
15 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 4000 → 38812 [ACK] Seq=4233414886 Ack=1094671258 Win=65536 Le...
16 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 91 4000 → 38812 [PSH, ACK] Seq=4233414886 Ack=1094671258 Win=655...
17 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 38812 → 4000 [ACK] Seq=1094671258 Ack=4233414911 Win=65536 Le...
18 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 70 38812 → 4000 [PSH, ACK] Seq=1094671258 Ack=4233414911 Win=655...
19 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 4000 → 38812 [FIN, ACK] Seq=4233414911 Ack=1094671262 Win=655...
20 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 38812 → 4000 [FIN, ACK] Seq=1094671262 Ack=4233414912 Win=655...
21 2023-09-28 12:4... 127.0.0.1 127.0.0.1 TCP 66 4000 → 38812 [ACK] Seq=4233414912 Ack=1094671263 Win=65536 Le...
wireshark_lo_20230928124048_wTbeJi.pcapng
Packets: 21 · Displayed: 21 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
64°F Cloudy
Search
12:41 PM 9/28/2023

Lab: 3

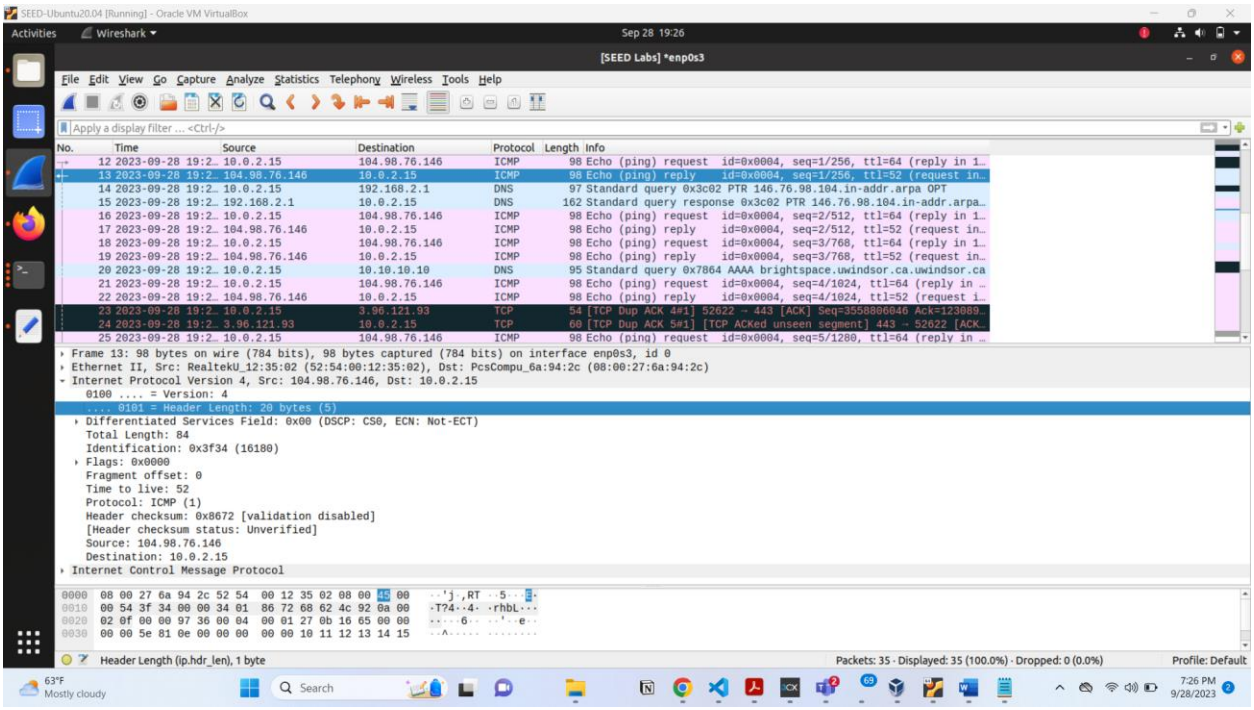
1. **In this problem, you will get familiar with ip format. Start the Wireshark and run ping www.mit.edu and then stop Wireshark. Ping www.mit.edu is to send an icmp packet. Check the first echo request packet in the Wireshark window and answer the following questions.**
    a. **Look at the ip header, what is the source and destination ip address?**



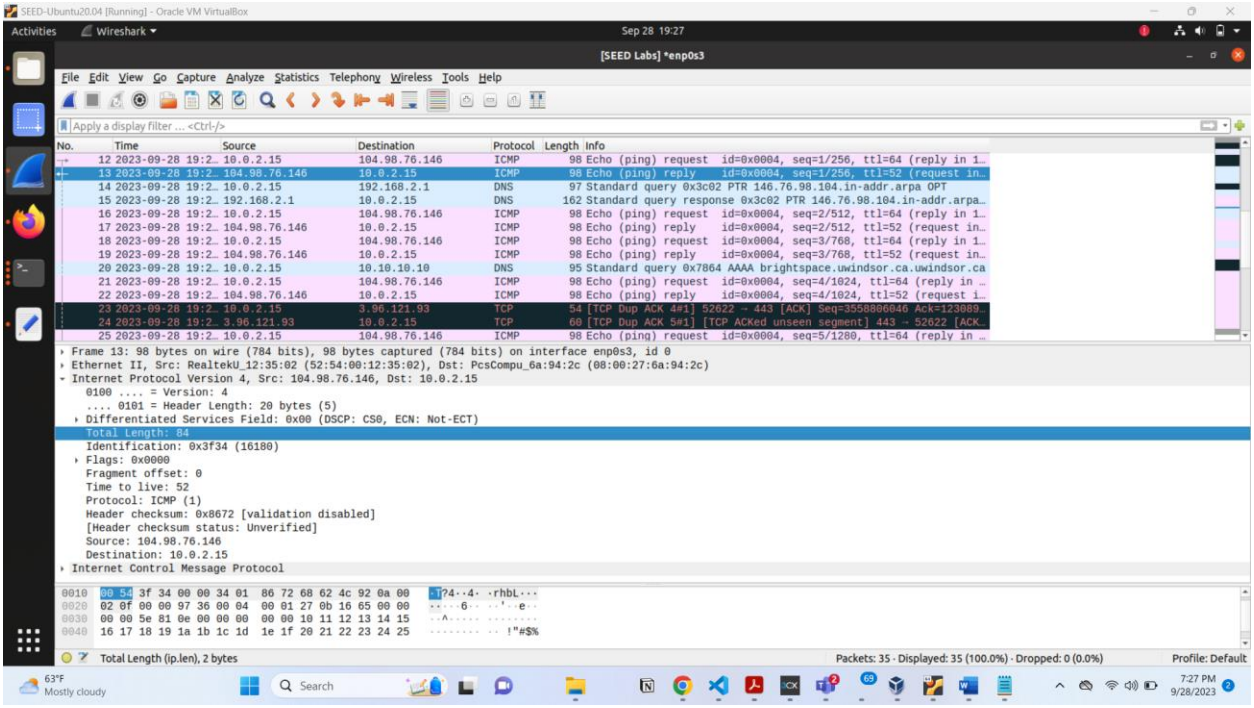
    b. **What is the upper layer protocol in ip header?**



c. **What is the ip header length?**

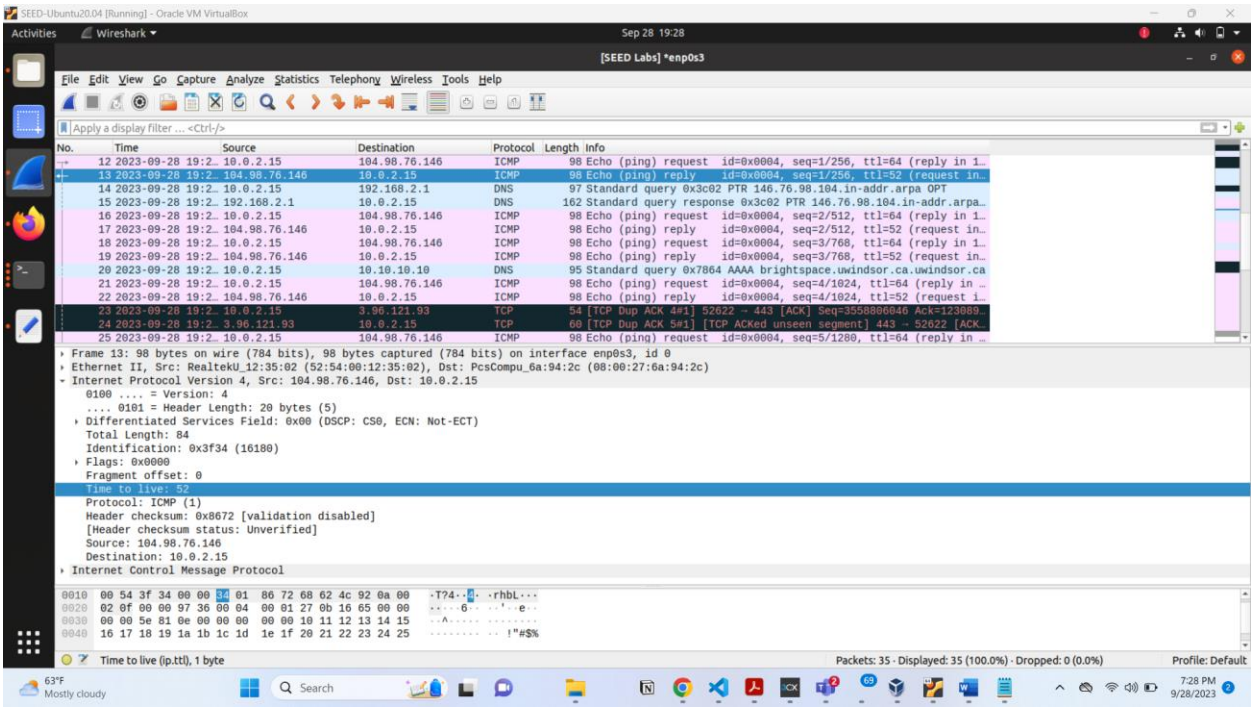


d. **Calculate the payload length for ip packet. This is total length – header length**

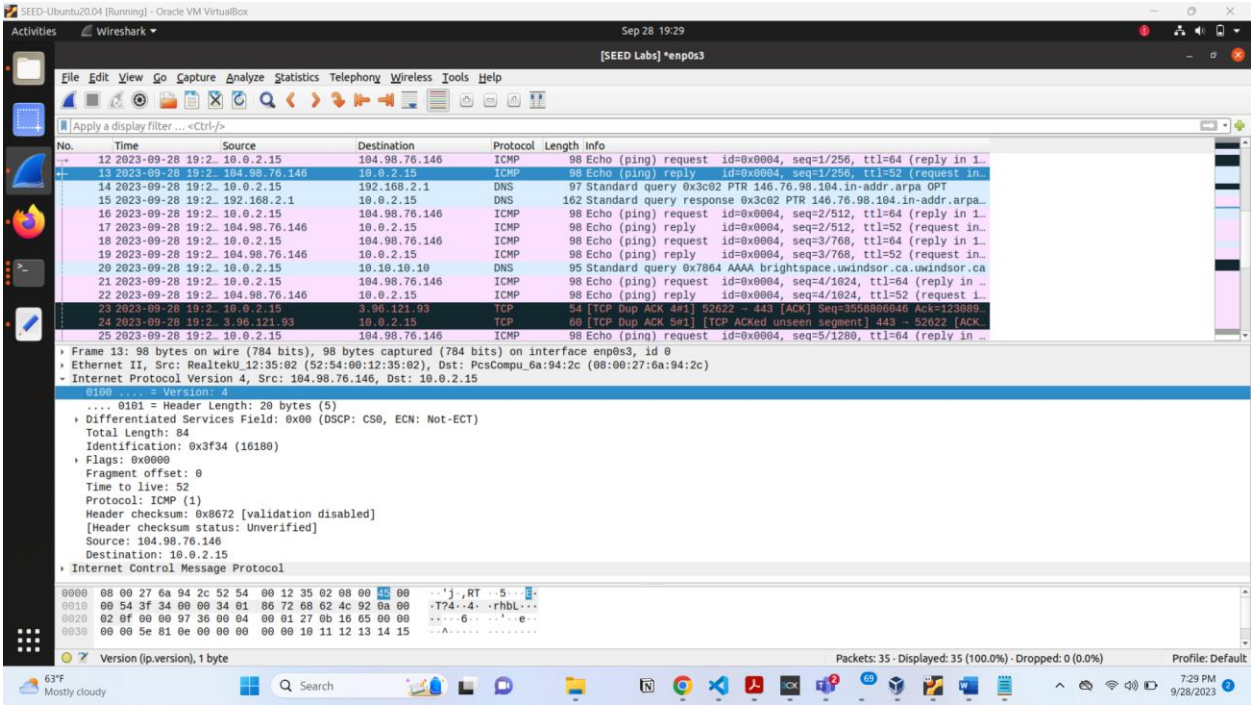


Payload length = total length - header length = 84 – 20 = 60

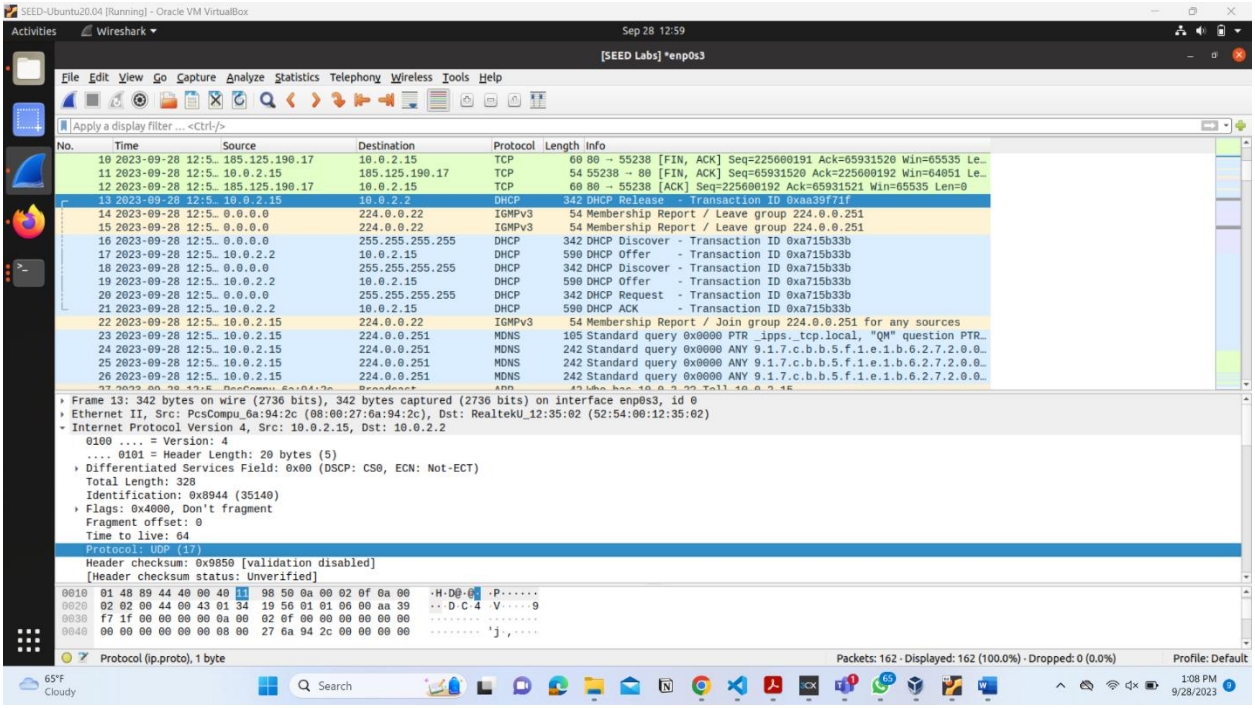
e. **What is the TTL value and what is its meaning?**



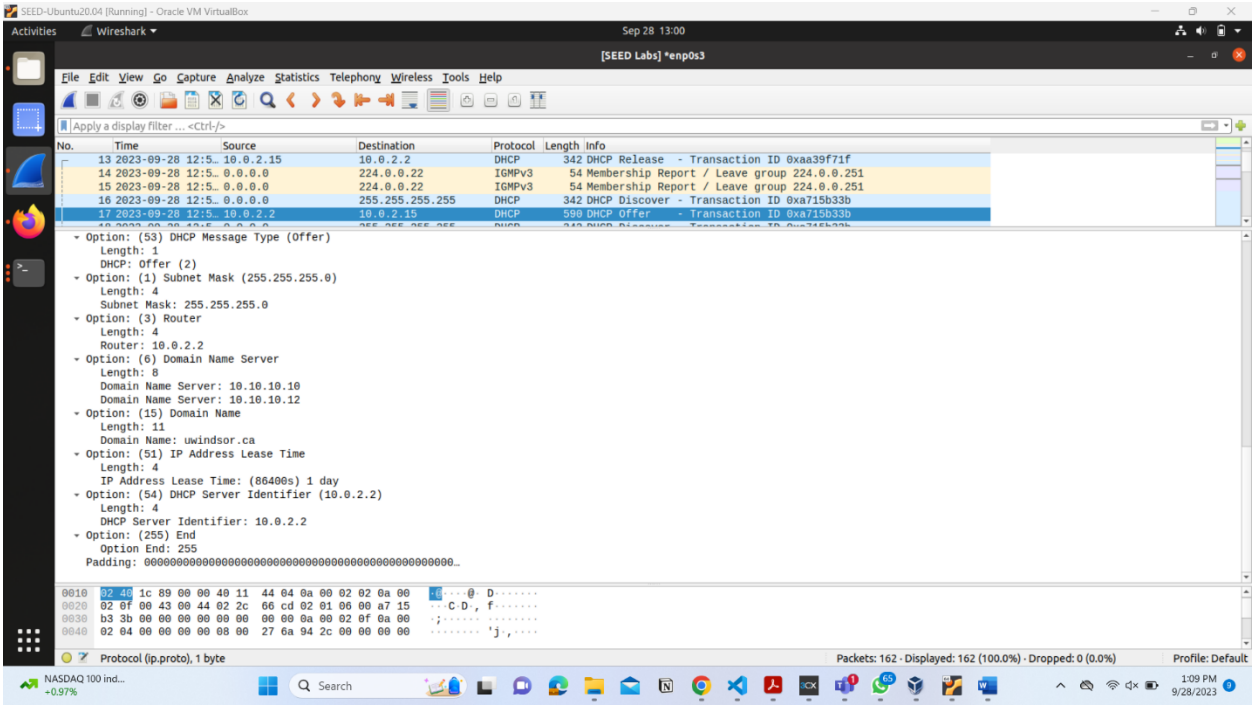
f. **Find out which field shows the ip header is in ipv4 or ipv6 format.**



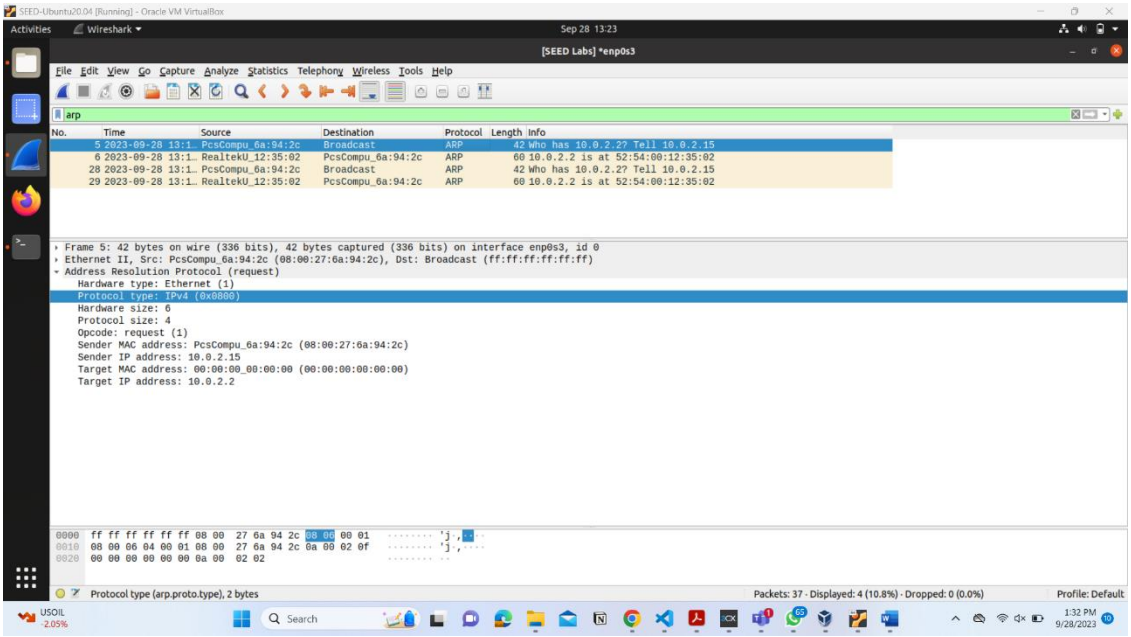
2. **Start Wireshark on your VM. Next, run command sudo dhclient -r -v and then sudo dhclient and finally stop Wireshark. Command sudo dhclient –r –v will release your current ip address. Then sudo dhclient will execute the DHCP protocol. Use packets in Wireshark from executing DHCP to answer the following questions.**
    a. **Confirm that the transport layer protocol of DHCP protocol is UDP. To do this, check a packet with DHCP protocol data and look at the transport layer header. Think about why it is not TCP (recall that TCP needs to establish a connection before exchanging messages).**



    b. **DHCP server IP: 10.0.2.2**
    Subnet mask: 255.255.255.0
    Router IP: 10.0.2.2
    DNS IP: 10.10.10.10



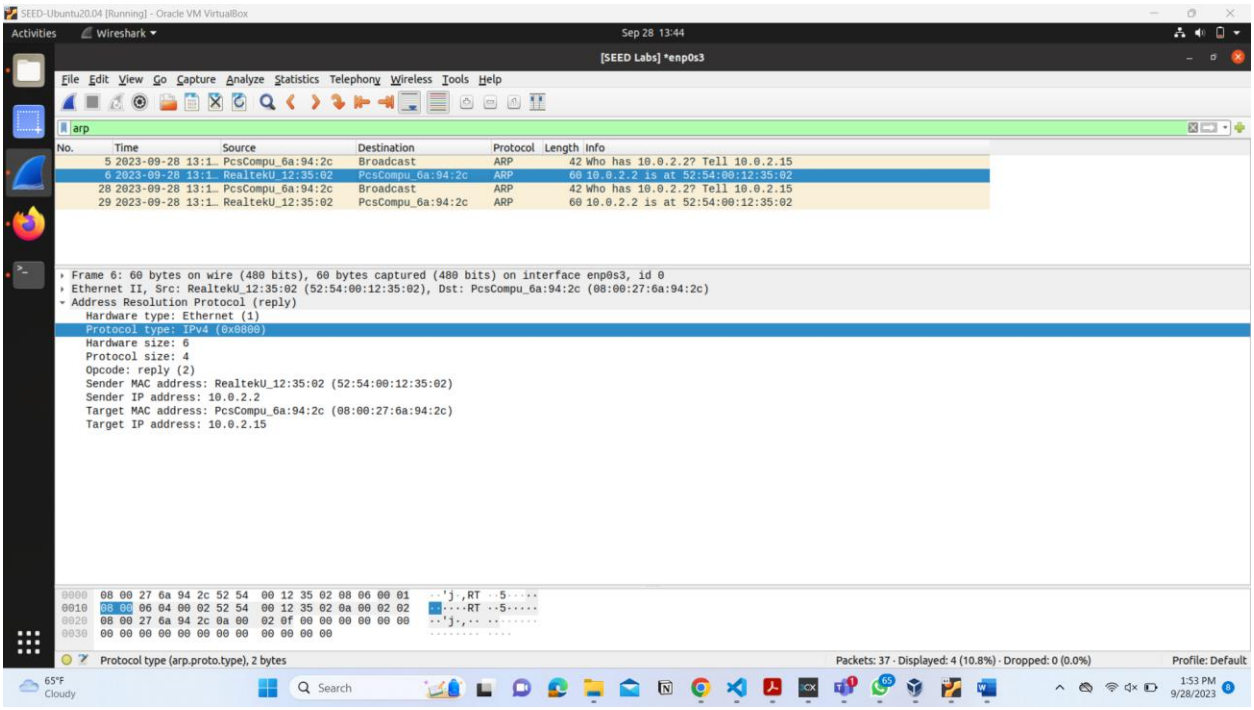
3. **In this exercise, you will look in the arp protocol execution. First, run arp to find out the list of records in the arp table. Next, start your wireshark and run sudo arp -d routerIP to delete the record of routerIP. Here routerIP is the Router IP obtained in the previous DHCP experiment. Then, you should see your VM is now starting to run arp.**
    a. **Find our arp broadcast from your VM. What is the upper layer protocol in the link layer header? What is the broadcast MAC address? What is the ip address for which your broadcast message is intended to find out the MAC address?**



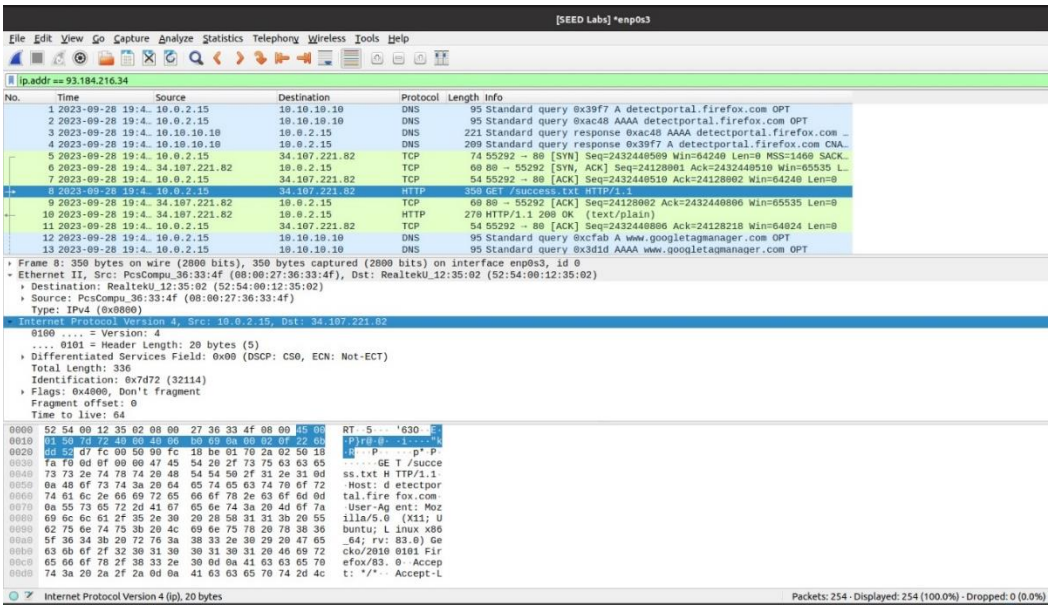
b. **look at the response packet for the ARP query. What is the ip address of the sender? What is its MAC address?**

Mac Address: 52.54.00:12:35:02

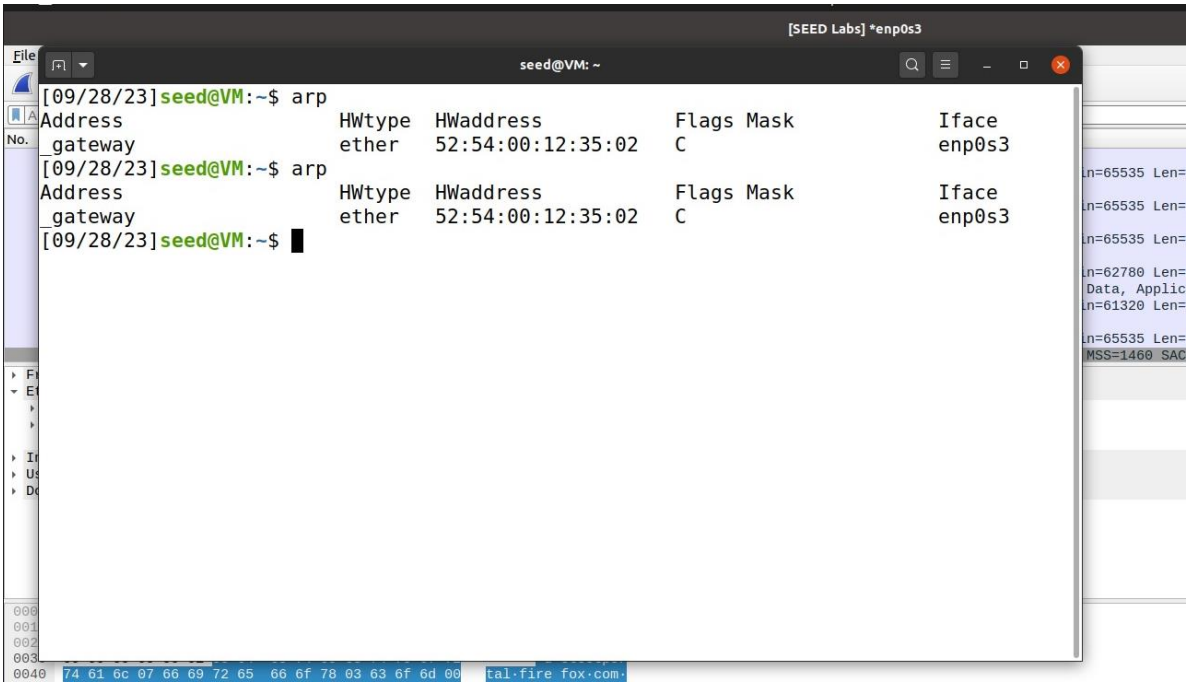
Ip Address: 10.0.2.2



4. **Run wireshark and access www.example.com and stop Wireshark. Answer the following questions.**
    a. **Check the HTTP request packet to 93.184.216.34 (ip of www.example.com). What are the source MAC and destination MAC? You need to check the link layer header in the packet. The source MAC is the MAC of your VM.**



b. Does the destination MAC in a belong to 93.184.216.34? To find out your answer, run command arp to check the arp table of your VM. Is the destination MAC in a listed here? If yes, confirm that this MAC does not belong to 93.184.216.34 and instead belong to your router.



c. **In the upper protocol field of link layer header of your HTTP request packet, what is the value? What protocol does it represent?**