



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

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	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...

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\$

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\$

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

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...

Packets: 21 - Displayed: 21 (100.0%) - Dropped: 0 (0.0%) Profile: Default

64°F Cloudy

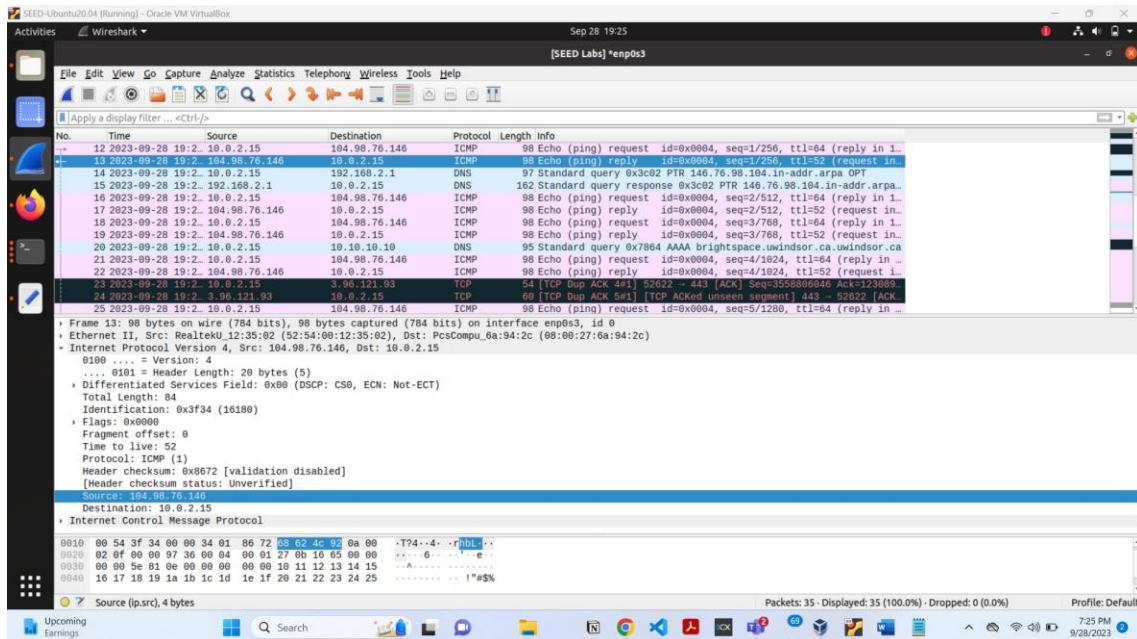
Search

12:41 PM 9/28/2023

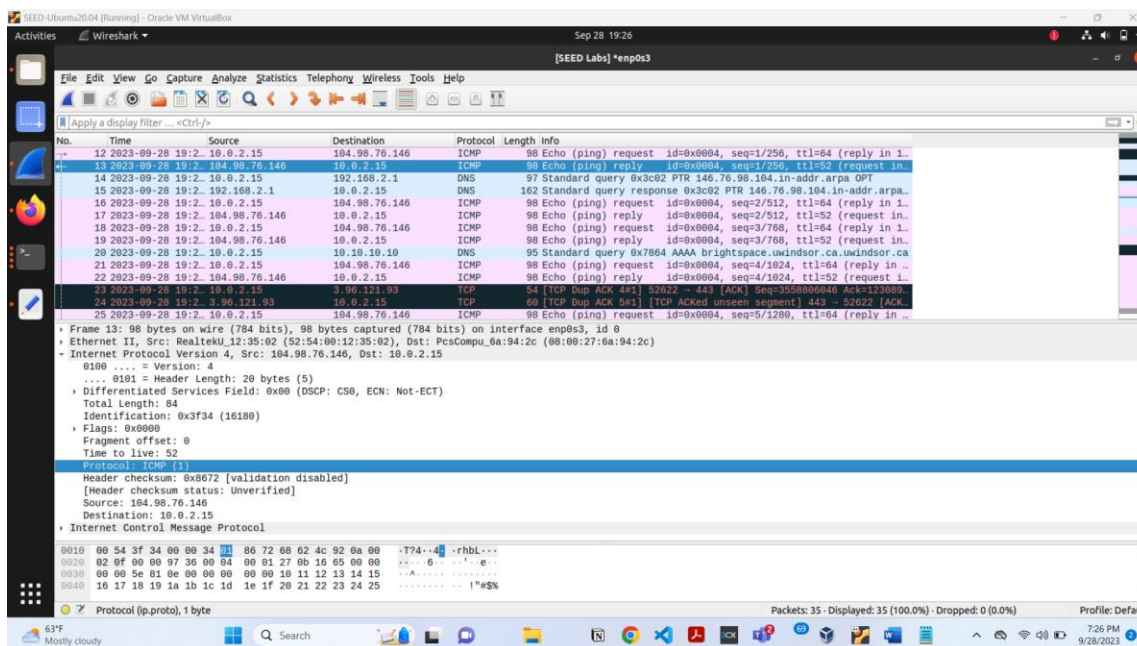
Lab: 3

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?



The screenshot shows the Wireshark interface with a packet capture of an ICMP Echo (ping) request. The packet list on the left shows a request from 10.0.2.15 to 104.98.76.146. The packet details pane on the right shows the ICMP Echo (ping) request structure, including the header and data. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

The screenshot displays a Kali Linux desktop environment. The top panel shows the system is running 'SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox' at 9:27 PM on 9/28/2023. The main window is Wireshark, capturing traffic on the 'eth0' interface. The packet list shows a series of ICMP Echo (ping) requests and responses. The selected packet is an ICMP Echo (ping) request from 10.0.2.15 to 104.98.76.146. The packet details pane shows the ICMP Echo (ping) request structure, including the header and data. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
12	2023-09-28 19:2:10.0.2.15	104.98.76.146	ICMP	98	Echo (ping) request id=0x0004, seq=1/256, ttl=64 (reply in 1..)	
13	2023-09-28 19:2:10.0.2.15	104.98.76.146	ICMP	98	Echo (ping) request id=0x0004, seq=2/256, ttl=64 (reply in 1..)	
14	2023-09-28 19:2:10.0.2.15	192.168.2.1	DNS	97	Standard query 0x3c02 PTR 146.76.98.104.in-addr.arpa OPT	
15	2023-09-28 19:2:10.0.2.15	104.98.76.146	DNS	162	Standard query response 0x3c02 PTR 146.76.98.104.in-addr.arpa	
16	2023-09-28 19:2:10.0.2.15	104.98.76.146	ICMP	98	Echo (ping) request id=0x0004, seq=2/512, ttl=64 (reply in 1..)	
17	2023-09-28 19:2:10.0.2.15	104.98.76.146	ICMP	98	Echo (ping) request id=0x0004, seq=2/512, ttl=52 (request in 1..)	
18	2023-09-28 19:2:10.0.2.15	104.98.76.146	ICMP	98	Echo (ping) request id=0x0004, seq=3/768, ttl=64 (reply in 1..)	
19	2023-09-28 19:2:10.0.2.15	104.98.76.146	ICMP	98	Echo (ping) request id=0x0004, seq=3/768, ttl=52 (request in 1..)	
20	2023-09-28 19:2:10.0.2.15	10.10.10.10	DNS	95	Standard query 0x7064 AAAA brightspace.uwindsor.ca.uwindsor.ca	
21	2023-09-28 19:2:10.0.2.15	104.98.76.146	ICMP	98	Echo (ping) request id=0x0004, seq=4/1024, ttl=64 (reply in 1..)	
22	2023-09-28 19:2:10.0.2.15	104.98.76.146	ICMP	98	Echo (ping) request id=0x0004, seq=4/1024, ttl=52 (request in 1..)	
23	2023-09-28 19:2:10.0.2.15	3.96.121.93	TCP	54	[TCP Dup ACK #41] 52622 → 443 [ACK] Seq=35580000040 Ack=123089	
24	2023-09-28 19:2:3.96.121.93	10.0.2.15	TCP	60	[TCP Dup ACK #41] [TCP ACKed unseen segment] 443 → 52622 [ACK]	
25	2023-09-28 19:2:10.0.2.15	104.98.76.146	ICMP	98	Echo (ping) request id=0x0004, seq=5/1280, ttl=64 (reply in 1..)	

Packet Details:

- Frame 13: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
- Ethernet II, Src: RealtekU (52:54:00:12:35:62), Dst: PcsCompu, 0a:94:2c:08:00:27:6a:94:2c)
 - Internet Protocol Version 4, Src: 104.98.76.146, Dst: 10.0.2.15
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 84
 - Identification: 0x3f34 (16180)
 - Flags: 0x0000
 - Fragment offset: 0
 - Time to live: 52
 - Protocol: ICMP (1)
 - Header checksum: 0x8672 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 104.98.76.146
 - Destination: 10.0.2.15
 - Internet Control Message Protocol

Packet Bytes:

```

0010 00 50 3f 34 00 00 34 01 86 72 68 62 4c 92 0a 00 7f4-4-..rhl...
0020 82 0f 00 00 97 36 00 04 00 01 27 0b 16 65 00 00 ....6-...
0030 00 00 5e 81 0e 00 00 00 00 00 11 12 13 14 15 ....A.....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 00 .....!#$%
  
```

Summary:

- Total Length (p.len): 2 bytes
- Packets: 35 · Displayed: 35 (100.0%) · Dropped: 0 (0.0%)
- Profile: Default

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

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

The screenshot shows a Wireshark packet capture of an ICMP Echo (ping) request. The packet list on the left shows packet 12 at 12:23:09.28, source 192.168.2.1, destination 10.0.2.15, protocol ICMP, length 98. The packet details pane on the right shows the following structure:

- Frame 13: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
- Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_6a:94:2c (08:00:27:6a:94:2c)
- Internet Protocol Version 4, Src: 104.98.76.146, Dst: 10.0.2.15
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 84
 - Identification: 0x3f34 (16180)
 - Flags: 0x0000
 - Fragment offset: 0
 - Time to live: 64
 - Protocol: ICMP (1)
 - Header checksum: 0xb672 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 104.98.76.146
 - Destination: 10.0.2.15
- Internet Control Message Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII. The TTL value of 64 is highlighted in the details pane.

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

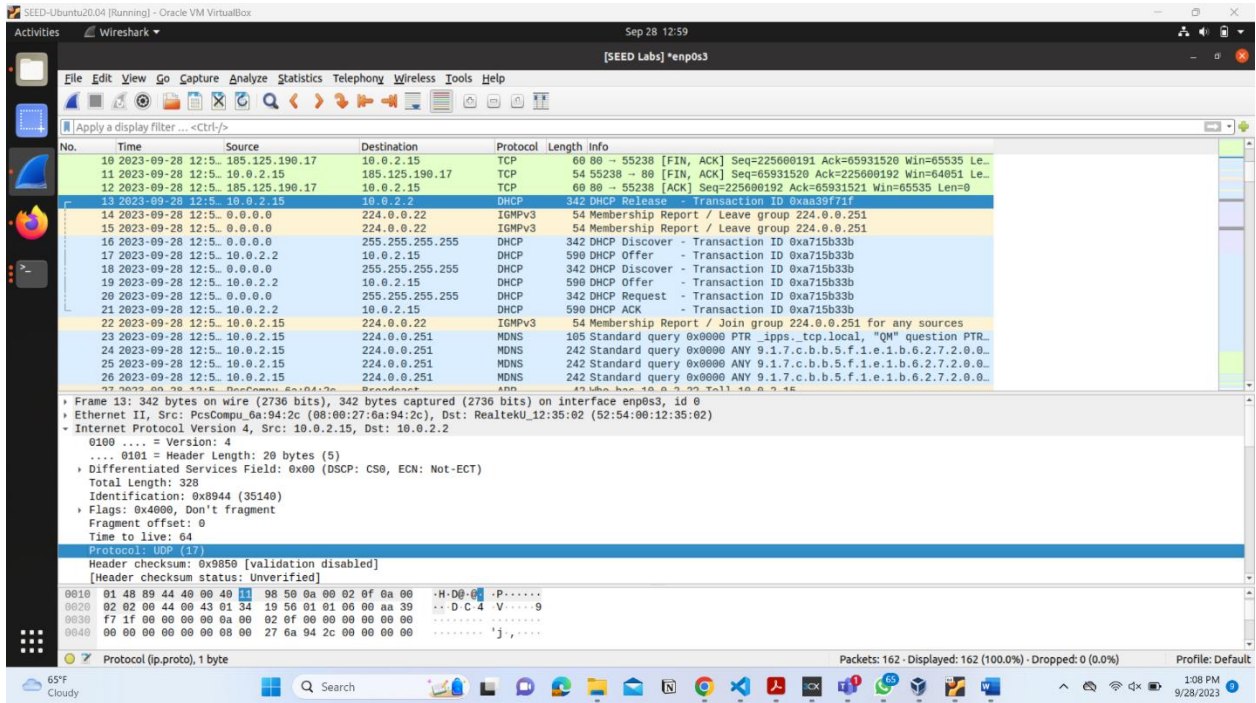
The screenshot shows a Wireshark packet capture of an ICMP Echo (ping) request. The packet list on the left shows packet 12 at 12:23:09.28, source 192.168.2.1, destination 10.0.2.15, protocol ICMP, length 98. The packet details pane on the right shows the following structure:

- Frame 13: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
- Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_6a:94:2c (08:00:27:6a:94:2c)
- Internet Protocol Version 4, Src: 104.98.76.146, Dst: 10.0.2.15
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 84
 - Identification: 0x3f34 (16180)
 - Flags: 0x0000
 - Fragment offset: 0
 - Time to live: 64
 - Protocol: ICMP (1)
 - Header checksum: 0xb672 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 104.98.76.146
 - Destination: 10.0.2.15
- Internet Control Message Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII. The TTL value of 64 is highlighted in the details pane.

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).

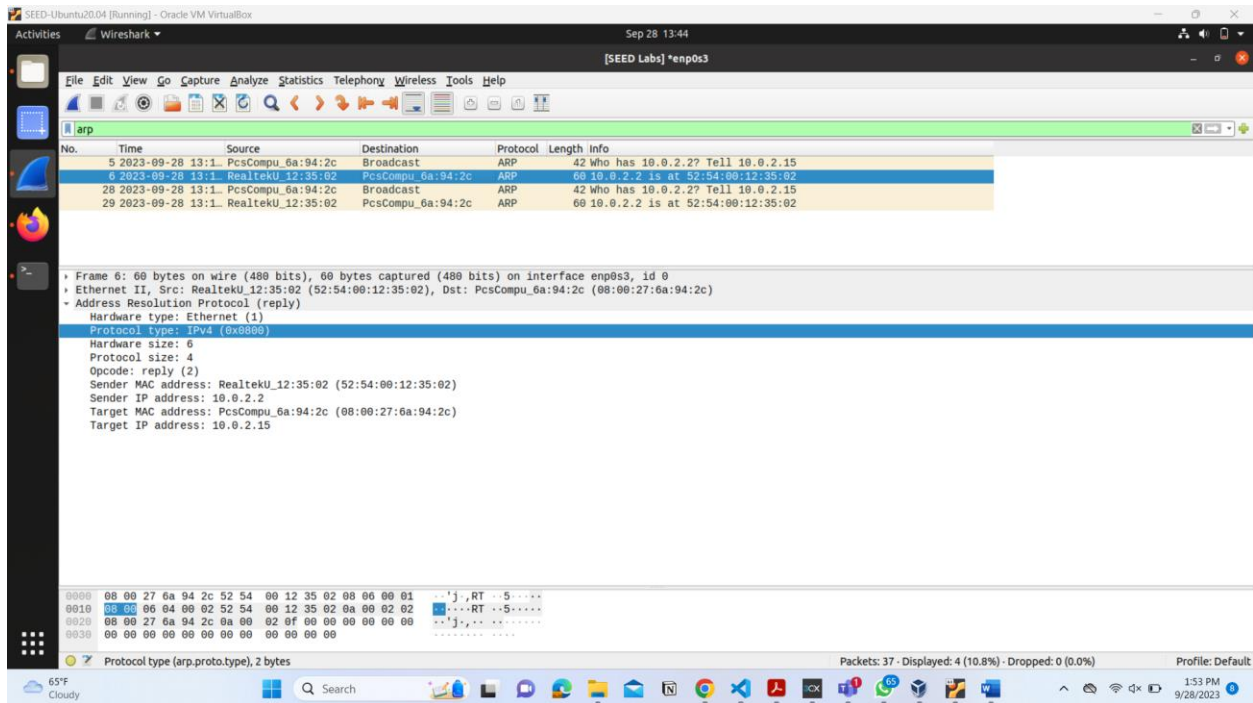


b. DHCP server IP: 10.0.2.2
Subnet mask: 255.255.255.0
Router IP: 10.0.2.2
DNS IP: 10.10.10.10

- 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.

[SEED Labs] *enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 93.184.216.34

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-09-28 19:4	10.0.2.15	10.10.10.10	DNS	95	Standard query 0x39f7 A detectportal.firefox.com OPT
2	2023-09-28 19:4	10.0.2.15	10.10.10.10	DNS	95	Standard query 0xac48 AAAA detectportal.firefox.com OPT
3	2023-09-28 19:4	10.10.10.10	10.0.2.15	DNS	221	Standard query response 0xac48 AAAA detectportal.firefox.com ...
4	2023-09-28 19:4	10.10.10.10	10.0.2.15	DNS	209	Standard query response 0x39f7 A detectportal.firefox.com CNAME
5	2023-09-28 19:4	10.0.2.15	34.107.221.82	TCP	74	55292 → 80 [SYN] Seq=2432448509 Win=64240 Len=0 MSS=1408 SACK_
6	2023-09-28 19:4	34.107.221.82	10.0.2.15	TCP	60	80 → 55292 [SYN, ACK] Seq=24128001 Ack=2432448510 Win=65535 L_
7	2023-09-28 19:4	10.0.2.15	34.107.221.82	TCP	54	55292 → 80 [ACK] Seq=2432448510 Ack=24128002 Win=64240 Len=0
8	2023-09-28 19:4	10.0.2.15	34.107.221.82	HTTP	350	GET /success.txt HTTP/1.1
9	2023-09-28 19:4	34.107.221.82	10.0.2.15	TCP	60	80 → 55292 [ACK] Seq=24128002 Ack=2432448006 Win=65535 Len=0
10	2023-09-28 19:4	34.107.221.82	10.0.2.15	HTTP	278	HTTP/1.1 200 OK (text/plain)
11	2023-09-28 19:4	10.0.2.15	34.107.221.82	TCP	54	55292 → 80 [ACK] Seq=2432448006 Ack=24128218 Win=64024 Len=0
12	2023-09-28 19:4	10.0.2.15	10.10.10.10	DNS	95	Standard query 0xcfab A www.googletagmanager.com OPT
13	2023-09-28 19:4	10.0.2.15	10.10.10.10	DNS	95	Standard query 0x3d1d AAAA www.googletagmanager.com OPT

Frame 8: 350 bytes on wire (2800 bits): 350 bytes captured (2800 bits) on interface enp0s3, id 0

Ethernet II, Src: PcsCompu_36:33:4f (08:00:27:36:33:4f), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

Destination: RealtekU_12:35:02 (52:54:00:12:35:02)

Source: PcsCompu_36:33:4f (08:00:27:36:33:4f)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.221.82

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 336

Identification: 0x7d72 (32114)

Flags: 0x0000, Don't fragment

Fragment offset: 0

Time to live: 64

0000 52 54 00 12 35 02 00 00 27 36 33 4f 00 00 45 00 RT 5 ... '630' B

0010 05 50 7d 72 40 00 40 00 00 00 00 00 00 00 00 00 Prio 0 - 0x0000

0020 05 50 7d 72 40 00 40 00 00 00 00 00 00 00 00 00 Prio 0 - 0x0000

0030 7a f0 0d 0f 00 00 47 45 54 20 2f 73 75 63 63 65 ... GE T /succe

0040 73 73 2e 74 78 74 20 48 54 54 50 2f 31 2e 31 0d ss.txt H TTP/1.1

0050 0a 48 0f 73 74 3a 20 64 05 74 05 63 74 70 6f 72 -Host: d detectpor

0060 74 61 6c 2e 66 69 72 65 66 6f 78 2e 63 6f 6d 0d tal.fire fox.com

0070 0a 55 73 65 72 2d 41 67 05 6e 74 3a 20 4d 6f 7a -User-Ag ent: Moz

0080 69 6c 6c 6f 2f 35 2e 30 20 28 50 31 31 30 20 55 illa/5.0 (X11; U

0090 62 75 6e 74 75 3b 20 4c 69 6e 75 70 20 78 30 30 buntu; L linux x86

00a0 5f 36 34 3b 20 72 76 3a 38 33 2e 30 29 20 47 65 _64; rv: 83.0) Ge

00b0 63 06 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 cko/2010 0101 Fir

00c0 65 06 6f 78 2f 30 33 2e 30 6d 0a 41 63 63 65 70 efox/83.0 Accp

00d0 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c t: /* - Accept-L

Internet Protocol Version 4 (IP), 20 bytes

Packets: 254 · Displayed: 254 (100.0%) · Dropped: 0 (0.0%)

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.

[SEED Labs] *enp0s3

seed@VM: ~

```
[09/28/23]seed@VM:~$ arp
```

No.	Address	HWtype	HWaddress	Flags	Mask	Iface
	gateway	ether	52:54:00:12:35:02	C		enp0s3

```
[09/28/23]seed@VM:~$ arp
```

No.	Address	HWtype	HWaddress	Flags	Mask	Iface
	gateway	ether	52:54:00:12:35:02	C		enp0s3

```
[09/28/23]seed@VM:~$
```

0000 74 61 6c 07 66 69 72 65 66 6f 78 03 63 6f 6d 00 tal.fire fox.com

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

[REED Labs] *enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 93.184.216.34

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-09-28 19:4.10.0.2.15	10.10.10.10	10.10.10.10	DNS	95	Standard query 0x39f7 A detectportal.firefox.com OPT
2	2023-09-28 19:4.10.0.2.15	10.10.10.10	10.10.10.10	DNS	95	Standard query 0xac48 AAAA detectportal.firefox.com OPT
3	2023-09-28 19:4.10.10.10.10	10.0.2.15	10.0.2.15	DNS	221	Standard query response 0xac48 AAAA detectportal.firefox.com ...
4	2023-09-28 19:4.10.10.10.10	10.0.2.15	10.0.2.15	DNS	209	Standard query response 0x39f7 A detectportal.firefox.com CNA...
5	2023-09-28 19:4.10.0.2.15	34.107.221.82	10.0.2.15	TCP	74	55292 → 80 [SYN] Seq=2432440509 Win=64240 Len=0 MSS=1400 SACK...
6	2023-09-28 19:4.34.107.221.82	10.0.2.15	34.107.221.82	TCP	60	80 → 55292 [SYN, ACK] Seq=24128001 Ack=2432440510 Win=65535 L...
7	2023-09-28 19:4.10.0.2.15	34.107.221.82	10.0.2.15	TCP	54	55292 → 80 [ACK] Seq=2432440510 Ack=24128002 Win=64240 Len=0
8	2023-09-28 19:4.10.0.2.15	34.107.221.82	10.0.2.15	HTTP	350	GET /success.txt HTTP/1.1
9	2023-09-28 19:4.34.107.221.82	10.0.2.15	34.107.221.82	TCP	60	80 → 55292 [ACK] Seq=24128002 Ack=2432440806 Win=65535 Len=0
10	2023-09-28 19:4.34.107.221.82	10.0.2.15	34.107.221.82	HTTP	270	HTTP/1.1 200 OK (text/plain)
11	2023-09-28 19:4.10.0.2.15	34.107.221.82	10.0.2.15	TCP	54	55292 → 80 [ACK] Seq=2432440806 Ack=24128218 Win=64024 Len=0
12	2023-09-28 19:4.10.0.2.15	10.10.10.10	10.10.10.10	DNS	95	Standard query 0xcfab A www.googletagmanager.com OPT
13	2023-09-28 19:4.10.0.2.15	10.10.10.10	10.10.10.10	DNS	95	Standard query 0x3d1d AAAA www.googletagmanager.com OPT

Frame 8: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface enp0s3, id 0

Ethernet II, Src: RealtekU12:35:02 (52:54:00:12:35:02), Dst: RealtekU12:35:02 (52:54:00:12:35:02)

Destination: RealtekU12:35:02 (52:54:00:12:35:02)

Source: PcsCompu36:33:4f (08:00:27:36:33:4f)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.221.82

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 336

Identification: 0x7d72 (32114)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 64

0000 52 54 00 12 35 02 08 00 27 36 33 4f 08 00 45 00 RT 5... '630' E

0010 01 50 7d 72 40 00 40 00 b6 69 0a 00 02 0f 22 6b P)R@ - 1... "k

0020 d0 52 07 fc 00 50 90 fc 18 be 01 70 2a 02 50 18 R...P...p*P

0030 fa f0 0d 0f 00 00 47 45 54 20 2f 73 75 03 03 05GE T /succe

0040 73 73 2e 74 78 74 20 48 54 54 50 2f 31 2e 31 0d ss.txt H TTP/1.1-

0050 0a 40 0f 73 7a 20 64 05 74 05 63 74 70 0f 72 Host: d etectpor

0060 74 61 4c 2e 66 69 72 05 66 6f 78 2e 03 6f 6d 0d tal fire fox.com

0070 0a 20 73 65 72 20 41 07 05 0e 74 3a 20 40 0f 7a User-Ag ent: Moz

0080 00 6c 6c 01 2f 30 2e 30 20 20 58 31 31 30 20 55 lile/5.0 (X11; U

0090 02 75 0e 73 75 30 20 4c 00 0e 75 70 20 70 30 34 nant; Linux x86

00a0 5f 30 3a 30 20 72 76 3a 38 33 2e 30 20 20 47 05 ;64; rv: 83.0) G

00b0 63 0b 0f 2f 32 30 31 30 30 31 30 31 20 40 09 72 cko/2010 0101 20f

00c0 00 4b 0f 70 7f 38 33 2e 30 00 0a 41 63 03 05 70 ffox/69.0; Accp

00d0 74 3a 20 2a 2f 2a 0d 0a 41 63 03 05 70 74 2d 4c t: */* Accept-L

Ethernet (eth), 14 bytes

Packets: 254 - Displayed: 254 (100.0%) - Dropped: 0 (0.0%)