

Computer Networks Lab 8

Name: Vaibhav Chaudhari

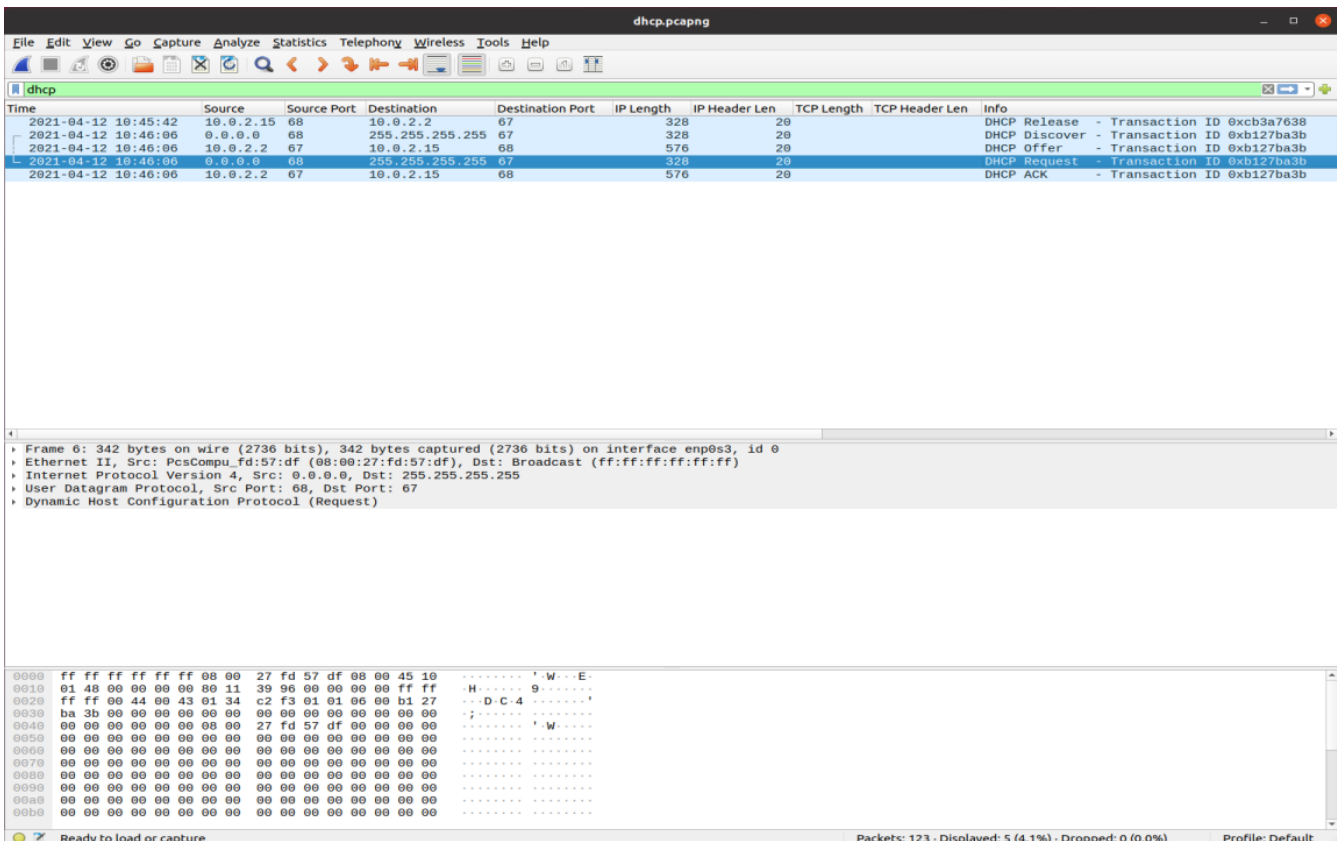
ID: 2017B5A70834G

Use Wireshark to capture packets in your LAN.

1. Show a round of execution of the DHCP protocol.

```
vaibhav@Jarvis:~$ sudo dhclient -r enp0s3
[sudo] password for vaibhav:
Killed old client process
vaibhav@Jarvis:~$ sudo dhclient -v enp0s3
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:fd:57:df
Sending on LPF/enp0s3/08:00:27:fd:57:df
Sending on Socket/fallback
DHCPDISCOVER on enp0s3 to 255.255.255.255 port 67 interval 3 (xid=0xb127ba3b)
DHCPOFFER of 10.0.2.15 from 10.0.2.2
DHCPREQUEST for 10.0.2.15 on enp0s3 to 255.255.255.255 port 67 (xid=0xbba27b1)
DHCPACK of 10.0.2.15 from 10.0.2.2 (xid=0xb127ba3b)
bound to 10.0.2.15 -- renewal in 41876 seconds.
vaibhav@Jarvis:~$
```



The filter used here is **dhcp** or **udp.port==67**. So we can use any one of them.

Show DHCP Request (2 marks),

The image shows a Wireshark packet capture window titled 'dhcp.pcapng'. The filter bar at the top contains the expression 'dhcp.option.dhcp==1'. The packet list pane shows a single packet at time 2021-04-12 10:46:06, source 0.0.0.0, source port 68, destination 255.255.255.255, destination port 67, and info 'DHCP Discover - Transaction ID 0xb127ba3b'. The packet details pane shows the following structure:

- Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface enp0s3, id 0
- Ethernet II, Src: PcsCompu_fd:57:df (08:00:27:fd:57:df), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Discover)

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII column displays the DHCP message structure: 'W-E', 'H-9', 'D-C-4', 'S', 'W', and several null bytes.

Time	Source	Source Port	Destination	Destination Port	Info
2021-04-12 10:46:06	0.0.0.0	68	255.255.255.255	67	DHCP Discover - Transaction ID 0xb127ba3b

Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface enp0s3, id 0

- Ethernet II, Src: PcsCompu_fd:57:df (08:00:27:fd:57:df), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Discover)

0000 ff ff ff ff ff ff 08 00 27 fd 57 df 08 00 45 10 'W-E-

0010 01 48 00 00 00 00 80 11 39 96 00 00 00 00 ff ff ..H...9.....

0020 ff ff 00 44 00 43 01 34 cb 35 01 01 06 00 b1 27 ...D-C-4-S...

0030 ba 3b 00 00 00 00 00 00 00 00 00 00 00 00 00 ;.....

0040 00 00 00 00 00 00 00 00 27 fd 57 df 00 00 00 00 'W.....

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

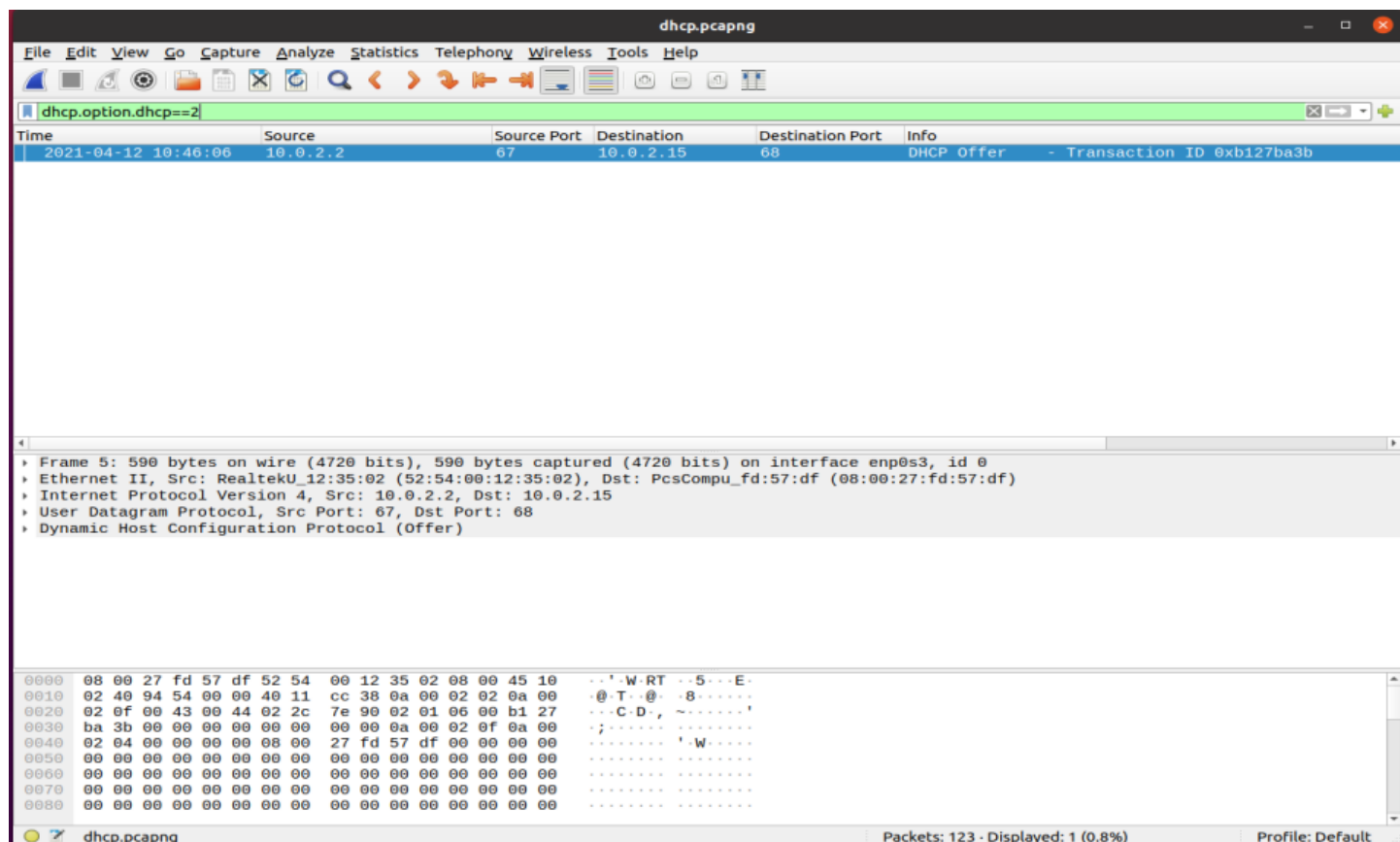
dhcp.pcapng Packets: 123 - Displayed: 1 (0.8%) Profile: Default

The filter is **dhcp.option.dhcp==1**

Here 1 is for Discover.

Here Discover=Request

Reply (2 marks),



The filter is **dhcp.option.dhcp==2**

Here 2 for offer.

Here Offer =Reply

ACK messages (2 marks) in that round.

dhcpcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcpcapng

Time	Source	Source Port	Destination	Destination Port	Info
2021-04-12 10:46:06	10.0.2.2	67	10.0.2.15	68	DHCP ACK - Transaction ID 0xb127ba3b

Frame 7: 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_fd:57:df (08:00:27:fd:57:df)

Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.15

User Datagram Protocol, Src Port: 67, Dst Port: 68

Dynamic Host Configuration Protocol (ACK)

0000 08 00 27 fd 57 df 52 54 00 12 35 02 08 00 45 10 ...W.RT..5..E-

0010 02 40 94 55 00 00 40 11 cc 37 0a 00 02 02 0a 00 ..U..@..7....

0020 02 0f 00 43 00 44 02 2c 6f 81 02 01 06 00 b1 27 ...C.D.,o.....

0030 ba 3b 00 00 00 00 0a 00 02 0f 0a 00 02 0f 0a 00 ;.....'-W....

0040 02 04 00 00 00 00 08 00 27 fd 57 df 00 00 00 00Ub untu 20.

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00Ub untu 20.

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00Ub untu 20.

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00Ub untu 20.

0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00Ub untu 20.

0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00Ub untu 20.

Ethernet (eth), 14 bytes

Packets: 123 - Displayed: 1 (0.8%)

Profile: Default

The filter is **dhcp.option.dhcp==5** where 5 is for acknowledgement.

Find out IP addresses of the DHCP server (2 marks) and client (2 marks). Write the filter and show the output in a screenshot.

Wireshark packet capture showing DHCP traffic. The packet list shows a DHCP Release, Membership Report, DHCP Discover, DHCP Offer, DHCP Request, and DHCP ACK. The packet details pane shows the DHCP Release packet with fields for Server IP (0.0.0.0) and Client IP (10.0.2.15). The packet bytes pane shows the raw data of the DHCP Release packet.

Wireshark Preferences dialog box showing the 'Columns' tab. The 'Displayed' column is checked for Time, Source, Source Port, Destination, Destination Port, IP Length, IP Header Len, TCP Length, TCP Header Len, Info, MAC Address, Host, Server Name, Server IP, and Client IP. The 'Fields' column is checked for ip.len, ip.hdr_len, tcp.len, tcp.hdr_len, arp.dst.hw_mac, http.host, tls.handshake.e..., dhcp.ip.server, and dhcp.ip.client.

Filter for IP address of server: **dhcp.ip.server**

Filter for IP address of client: **dhcp.ip.client**

2. Show a round of execution of the ARP protocol.

```
vaibhav@Jarvis: ~  
vaibhav@Jarvis:~$ ping www.google.com -c 4  
PING www.google.com (142.250.194.196) 56(84) bytes of data.  
64 bytes from del12s07-in-f4.1e100.net (142.250.194.196): icmp_seq=1 ttl=110 time=56.7 ms  
64 bytes from del12s07-in-f4.1e100.net (142.250.194.196): icmp_seq=2 ttl=110 time=47.8 ms  
64 bytes from del12s07-in-f4.1e100.net (142.250.194.196): icmp_seq=3 ttl=110 time=44.7 ms  
64 bytes from del12s07-in-f4.1e100.net (142.250.194.196): icmp_seq=4 ttl=110 time=53.9 ms  
  
--- www.google.com ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3024ms  
rtt min/avg/max/mdev = 44.702/50.759/56.654/4.741 ms  
vaibhav@Jarvis:~$ arp -a  
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3  
vaibhav@Jarvis:~$
```

The image shows a Wireshark packet capture window titled 'arp.pcapng'. The filter bar at the top is set to 'arp'. The packet list pane shows two packets:

Time	Source	Source Port	Destination	Destination Port	Info	MAC Address	Opcode
2021-04-12 11:34:28	PcsCompu_fd:57:df		RealtekU_12:35:02		who has 10.0.2.2? Tell 10.0.2.15	08:00:00:00:00:00	request
2021-04-12 11:34:28	RealtekU_12:35:02		PcsCompu_fd:57:df		10.0.2.2 is at 52:54:00:12:35:02	08:00:27:fd:57:df	reply

The packet details pane for the selected packet (Frame 15) shows:

- Frame 15: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s3, id 0
- Ethernet II, Src: PcsCompu_fd:57:df (08:00:27:fd:57:df), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
- Address Resolution Protocol (request)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  52 54 00 12 35 02 08 00 27 fd 57 df 08 06 00 01  RT...S...W....  
0010  08 00 06 04 00 01 08 00 27 fd 57 df 0a 00 02 0f  ....W....  
0020  00 00 00 00 00 00 0a 00 02 02  ....
```

The status bar at the bottom indicates: Address Resolution Protocol: Protocol, Packets: 18 - Displayed: 2 (11.1%), Profile: Default.

The filter used here is **arp** to filter It out.

Show ARP Request (2 marks)

The screenshot shows a Wireshark capture of an ARP request packet. The filter bar at the top is set to `arp.opcode==1`. The packet list shows a single packet at time 2021-04-12 11:34:28. The packet details pane shows the following structure:

- Frame 15: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s3, id 0
- Ethernet II, Src: PcsCompu_fd:57:df (08:00:27:fd:57:df), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
- Address Resolution Protocol (request)

The packet bytes pane shows the raw data of the ARP request:

```
0000  52 54 00 12 35 02 08 00 27 fd 57 df 08 06 00 01  RT--5... :W-----
0010  08 00 06 04 00 01 08 00 27 fd 57 df 0a 00 02 0f  .... RT--5... :W-----
0020  00 00 00 00 00 00 0a 00 02 02  .... :W-----
```

The filter is `arp.opcode==1` for request

Reply (2 marks) messages in that round.

The screenshot shows a Wireshark capture of an ARP reply packet. The filter bar at the top is set to `arp.opcode==2`. The packet list shows a single packet at time 2021-04-12 11:34:28. The packet details pane shows the following structure:

- Frame 16: 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_fd:57:df (08:00:27:fd:57:df)
- Address Resolution Protocol (reply)

The packet bytes pane shows the raw data of the ARP reply:

```
0000  08 00 27 fd 57 df 52 54 00 12 35 02 08 06 00 01  ..-W-RT--5-----
0010  08 00 06 04 00 02 52 54 00 12 35 02 0a 00 02 02  .... RT--5-----
0020  08 00 27 fd 57 df 0a 00 02 0f 00 00 00 00 00 00 00  ..-W-----
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
```

The filter is `arp.opcode==2` for reply

Find the MAC address of the replier (2 marks). Write the filter and show the output in a screenshot.

arp

Time	Source	Source Port	Destination	Destination Port	Info	MAC Address	Opcode
2021-04-12 11:34:28	PcsCompu_fd:57:df		RealtekU_12:35:02		who has 10.0.2.2? Tell 10.0.2.15	00:00:00:00:00:00	request
2021-04-12 11:34:28	RealtekU_12:35:02		PcsCompu_fd:57:df		10.0.2.2 is at 52:54:00:12:35:02	08:00:27:fd:57:df	reply

Frame 16: 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_fd:57:df (08:00:27:fd:57:df)
 Address Resolution Protocol (reply)

0000 08 00 27 fd 57 df 52 54 00 12 35 02 08 06 00 01 ...W RT --5--
 0010 08 00 06 04 00 02 52 54 00 12 35 02 0a 00 02 02 ...RT --5--
 0020 08 00 27 fd 57 df 0a 00 02 0f 00 00 00 00 00 00 ...W--
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Address Resolution Protocol: Protocol Packets: 18 - Displayed: 2 (11.1%) Profile: Default

Wireshark - Preferences

Displayed	Title	Type	Fields	Field
<input checked="" type="checkbox"/>	Time	UTC date, as YYYY-MM-DD, and time		
<input checked="" type="checkbox"/>	Source	Source address		
<input checked="" type="checkbox"/>	Source Port	Src port (unresolved)		
<input checked="" type="checkbox"/>	Destination	Destination address		
<input checked="" type="checkbox"/>	Destination Port	Dest port (unresolved)		
<input type="checkbox"/>	IP Length	Custom	ip.len	0
<input type="checkbox"/>	IP Header Len	Custom	ip.hdr_len	0
<input type="checkbox"/>	TCP Length	Custom	tcp.len	0
<input type="checkbox"/>	TCP Header Len	Custom	tcp.hdr_len	0
<input checked="" type="checkbox"/>	Info	Information		
<input checked="" type="checkbox"/>	MAC Address	Custom	arp.dst.hw_mac	0
<input type="checkbox"/>	Host	Custom	http.host	0
<input type="checkbox"/>	Server Name	Custom	tls.handshake....	0
<input type="checkbox"/>	Server IP	Custom	dhcp.ip.server	0
<input type="checkbox"/>	Client IP	Custom	dhcp.ip.client	0
<input checked="" type="checkbox"/>	Opcode	Custom	arp.opcode	0

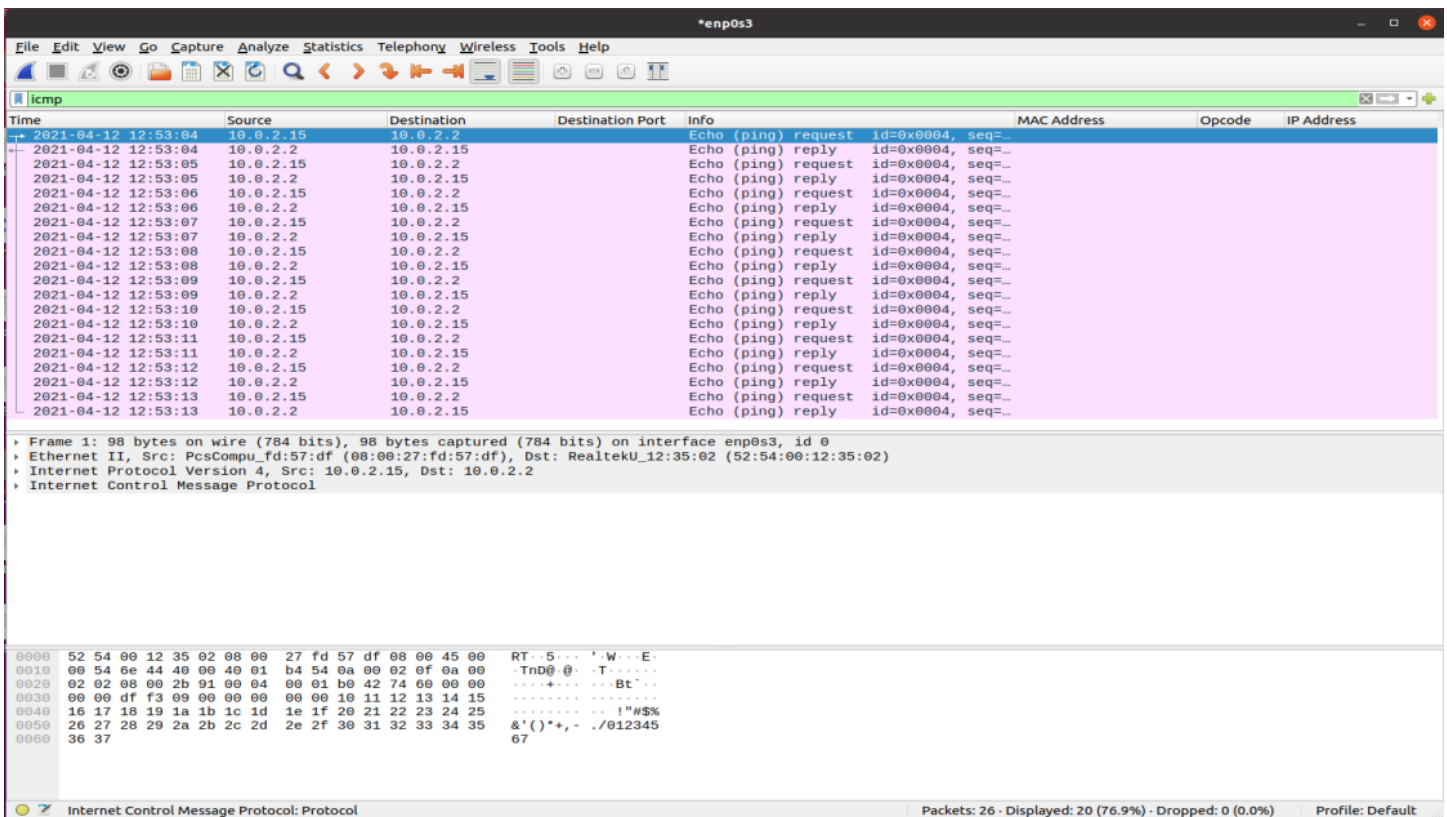
☒ Show displayed columns only

Help Cancel OK

The filter for the MAC address is **arp.dst.hw_mac**. I have added a column to get the MAC Addresses.

3. Find the MAC address and the IP address of the Gateway router (2 marks).
Write the filter and show the output in a screenshot.

```
vaibhav@Jarvis: ~  
vaibhav@Jarvis:~$ ip route  
default via 10.0.2.2 dev enp0s3  
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15  
vaibhav@Jarvis:~$ ping 10.0.2.2 -c 10  
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.  
64 bytes from 10.0.2.2: icmp_seq=1 ttl=64 time=0.442 ms  
64 bytes from 10.0.2.2: icmp_seq=2 ttl=64 time=0.224 ms  
64 bytes from 10.0.2.2: icmp_seq=3 ttl=64 time=0.182 ms  
64 bytes from 10.0.2.2: icmp_seq=4 ttl=64 time=0.269 ms  
64 bytes from 10.0.2.2: icmp_seq=5 ttl=64 time=0.197 ms  
64 bytes from 10.0.2.2: icmp_seq=6 ttl=64 time=0.191 ms  
64 bytes from 10.0.2.2: icmp_seq=7 ttl=64 time=0.373 ms  
64 bytes from 10.0.2.2: icmp_seq=8 ttl=64 time=0.221 ms  
64 bytes from 10.0.2.2: icmp_seq=9 ttl=64 time=0.354 ms  
64 bytes from 10.0.2.2: icmp_seq=10 ttl=64 time=0.210 ms  
  
--- 10.0.2.2 ping statistics ---  
10 packets transmitted, 10 received, 0% packet loss, time 921ms  
rtt min/avg/max/mdev = 0.182/0.266/0.442/0.086 ms
```



The filter is **icmp**.

The IP Address of the Gateway Router is 10.0.2.2 as seen from the image above.

The MAC Address of the Gateway Router is 52:54:00:12:35:02