COMP8677: Networking and Data Security

Lab - 3

Submitted By: Shivam Sunil Bhosale (110090402)

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?

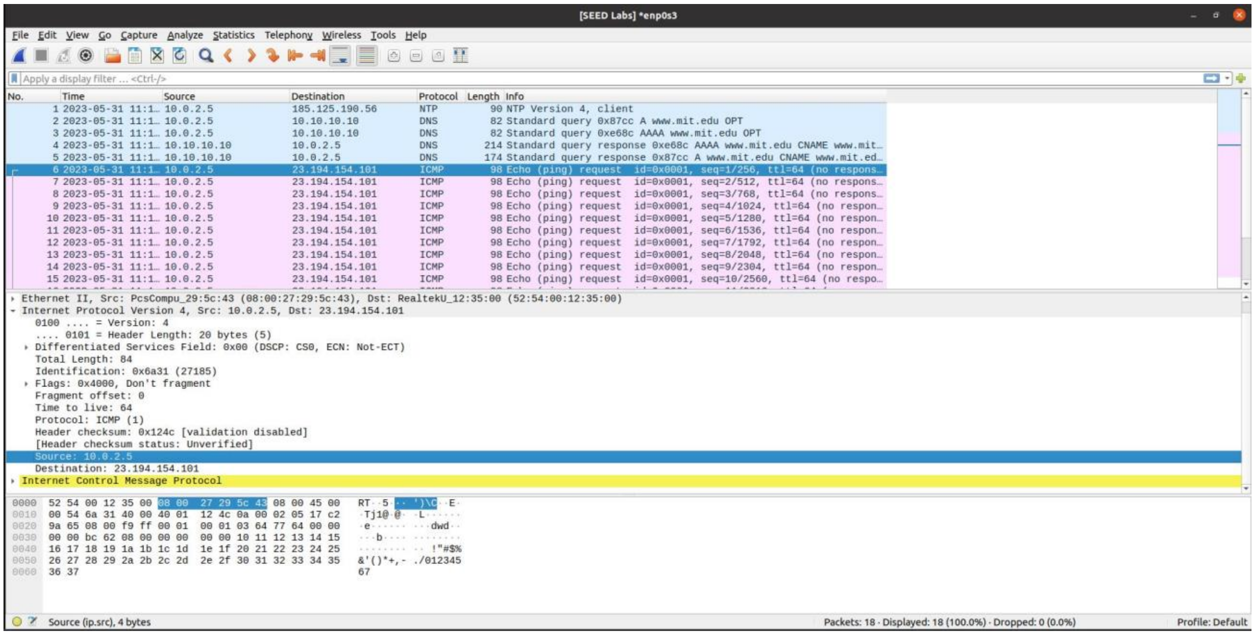
c. what is the ip header length?

d. Calculate the payload length for ip packet. This is totallength - headerlegnth.

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.

(a) So, the Source IP: 10.0.2.5 and Destination IP: 23.194.154.101

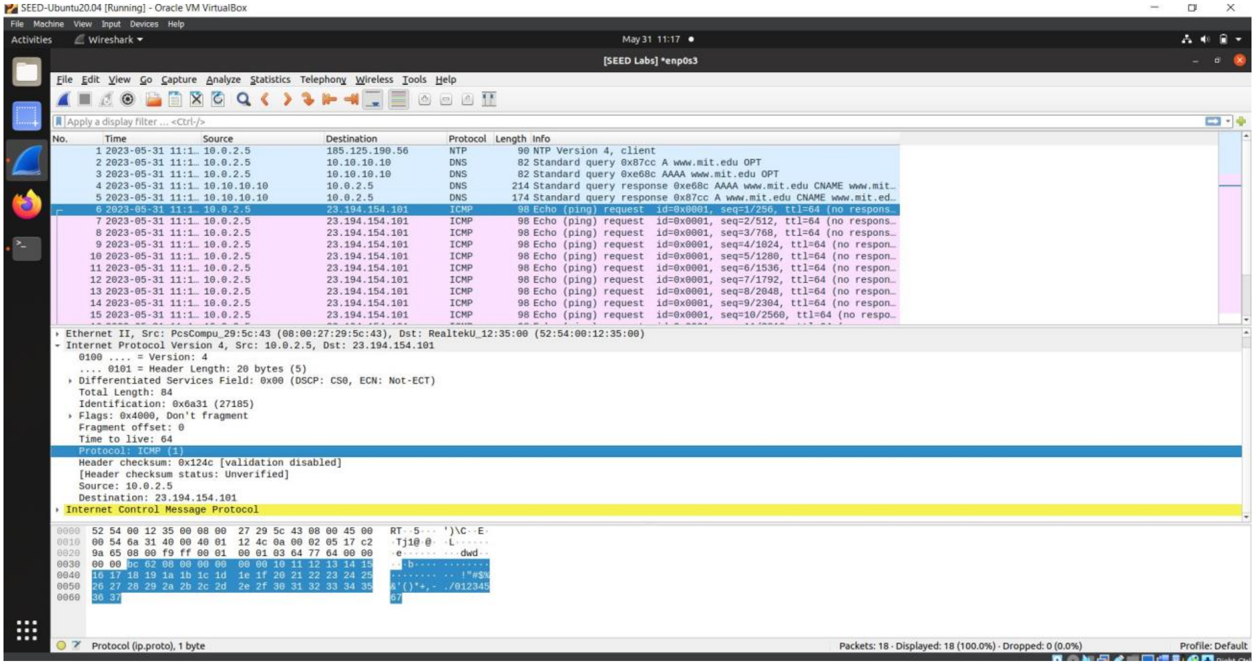

[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time              Source         Destination      Protocol Length Info
    1 2023-05-31 11:1… 10.0.2.5       185.125.190.56   NTP        90 NTP Version 4, client
    2 2023-05-31 11:1… 10.0.2.5       10.10.10.10      DNS        82 Standard query 0x87cc A www.mit.edu OPT
    3 2023-05-31 11:1… 10.0.2.5       10.10.10.10      DNS        82 Standard query 0xe68c AAAA www.mit.edu OPT
    4 2023-05-31 11:1… 10.10.10.10    10.0.2.5         DNS       214 Standard query response 0xe68c AAAA www.mit.edu CNAME www.mit…
    5 2023-05-31 11:1… 10.10.10.10    10.0.2.5         DNS       174 Standard query response 0x87cc A www.mit.edu CNAME www.mit.ed…
    6 2023-05-31 11:1… 10.0.2.5       23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no respons…
    7 2023-05-31 11:1… 10.0.2.5       23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (no respons…
    8 2023-05-31 11:1… 10.0.2.5       23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (no respons…
    9 2023-05-31 11:1… 10.0.2.5       23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=4/1024, ttl=64 (no respon…
   10 2023-05-31 11:1… 10.0.2.5       23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=5/1280, ttl=64 (no respon…
   11 2023-05-31 11:1… 10.0.2.5       23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=6/1536, ttl=64 (no respon…
   12 2023-05-31 11:1… 10.0.2.5       23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=7/1792, ttl=64 (no respon…
   13 2023-05-31 11:1… 10.0.2.5       23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=8/2048, ttl=64 (no respon…
   14 2023-05-31 11:1… 10.0.2.5       23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=9/2304, ttl=64 (no respon…
   15 2023-05-31 11:1… 10.0.2.5       23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=10/2560, ttl=64 (no respo…
```

```
▸ Ethernet II, Src: PcsCompu_29:5c:43 (08:00:27:29:5c:43), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▾ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 23.194.154.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x6a31 (27185)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x124c [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.5
    Destination: 23.194.154.101
▸ Internet Control Message Protocol
```

```
0000  52 54 00 12 35 00 08 00  27 29 5c 43 08 00 45 00   RT··5···')\C··E·
0010  00 54 6a 31 40 00 40 01  12 4c 0a 00 02 05 17 c2   ·Tj1@·@··L······
0020  9a 65 08 00 f9 ff 00 01  00 01 03 64 77 64 00 00   ·e·········dwd··
0030  00 00 bc 62 08 00 00 00  00 00 10 11 12 13 14 15   ···b············
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ·········· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37                                              67
```

(b) The upper layer protocol in IP header is ICMP.



SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark ▾ May 31 11:17

[SEED Labs] *enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter … <Ctrl-/>

```
No.  Time                Source       Destination      Protocol Length Info
   1 2023-05-31 11:1…  10.0.2.5     185.125.190.56   NTP        90 NTP Version 4, client
   2 2023-05-31 11:1…  10.0.2.5     10.10.10.10      DNS        82 Standard query 0x87cc A www.mit.edu OPT
   3 2023-05-31 11:1…  10.0.2.5     10.10.10.10      DNS        82 Standard query 0xe68c AAAA www.mit.edu OPT
   4 2023-05-31 11:1…  10.10.10.10  10.0.2.5         DNS       214 Standard query response 0xe68c AAAA www.mit.edu CNAME www.mit…
   5 2023-05-31 11:1…  10.10.10.10  10.0.2.5         DNS       174 Standard query response 0x87cc A www.mit.edu CNAME www.mit.ed…
   6 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no respons…
   7 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (no respons…
   8 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (no respons…
   9 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=4/1024, ttl=64 (no respon…
  10 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=5/1280, ttl=64 (no respon…
  11 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=6/1536, ttl=64 (no respon…
  12 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=7/1792, ttl=64 (no respon…
  13 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=8/2048, ttl=64 (no respon…
  14 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=9/2304, ttl=64 (no respon…
  15 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=10/2560, ttl=64 (no respo…
```

```
▸ Ethernet II, Src: PcsCompu_29:5c:43 (08:00:27:29:5c:43), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▾ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 23.194.154.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x6a31 (27185)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x124c [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.5
    Destination: 23.194.154.101
▸ Internet Control Message Protocol
```

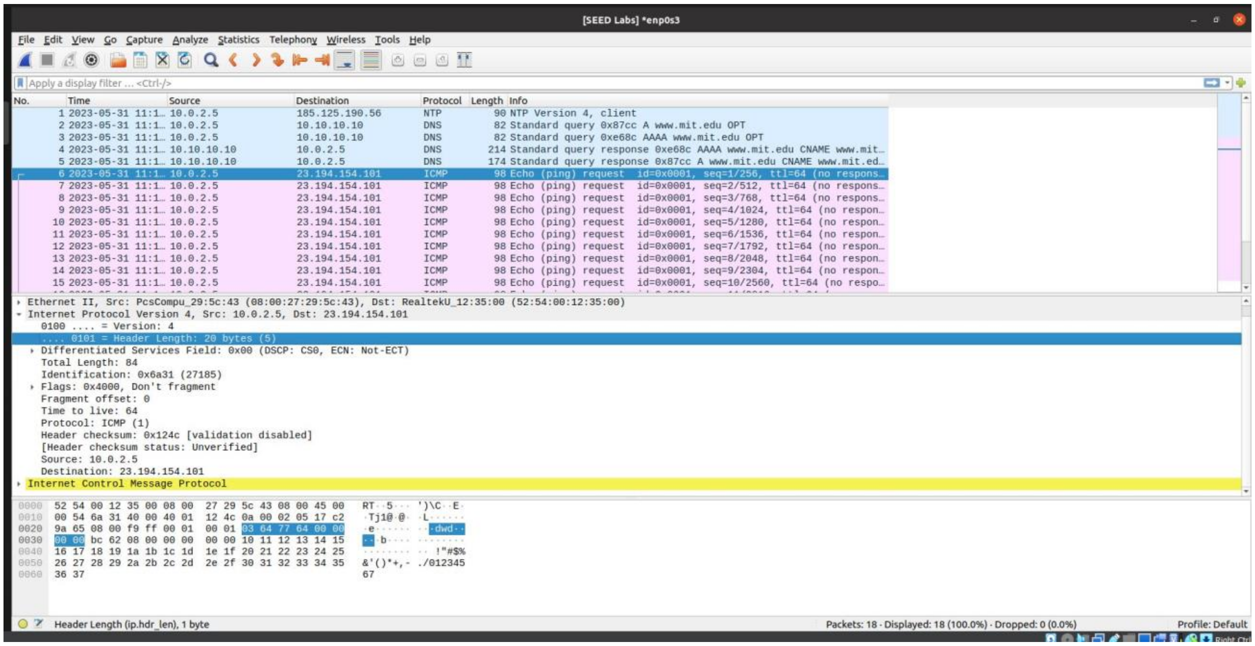
```
0000  52 54 00 12 35 00 08 00  27 29 5c 43 08 00 45 00   RT··5··· ')\C··E·
0010  00 54 6a 31 40 00 40 01  12 4c 0a 00 02 05 17 c2   ·Tj1@·@· ·L······
0020  9a 65 08 00 f9 ff 00 01  00 01 03 64 77 64 00 00   ·e······ ···dwd··
0030  00 00 bc 62 08 00 00 00  00 00 10 11 12 13 14 15   ···b···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Protocol (ip.proto), 1 byte

Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

(c) The IP header length is 20 bytes



[SEED Labs] *enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter … <Ctrl-/>

```
No.  Time                Source       Destination      Protocol Length Info
   1 2023-05-31 11:1…  10.0.2.5     185.125.190.56   NTP        90 NTP Version 4, client
   2 2023-05-31 11:1…  10.0.2.5     10.10.10.10      DNS        82 Standard query 0x87cc A www.mit.edu OPT
   3 2023-05-31 11:1…  10.0.2.5     10.10.10.10      DNS        82 Standard query 0xe68c AAAA www.mit.edu OPT
   4 2023-05-31 11:1…  10.10.10.10  10.0.2.5         DNS       214 Standard query response 0xe68c AAAA www.mit.edu CNAME www.mit…
   5 2023-05-31 11:1…  10.10.10.10  10.0.2.5         DNS       174 Standard query response 0x87cc A www.mit.edu CNAME www.mit.ed…
   6 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no respons…
   7 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (no respons…
   8 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (no respons…
   9 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=4/1024, ttl=64 (no respon…
  10 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=5/1280, ttl=64 (no respon…
  11 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=6/1536, ttl=64 (no respon…
  12 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=7/1792, ttl=64 (no respon…
  13 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=8/2048, ttl=64 (no respon…
  14 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=9/2304, ttl=64 (no respon…
  15 2023-05-31 11:1…  10.0.2.5     23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=10/2560, ttl=64 (no respo…
```

```
▸ Ethernet II, Src: PcsCompu_29:5c:43 (08:00:27:29:5c:43), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▾ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 23.194.154.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x6a31 (27185)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x124c [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.5
    Destination: 23.194.154.101
▸ Internet Control Message Protocol
```

```
0000  52 54 00 12 35 00 08 00  27 29 5c 43 08 00 45 00   RT··5··· ')\C··E·
0010  00 54 6a 31 40 00 40 01  12 4c 0a 00 02 05 17 c2   ·Tj1@·@· ·L······
0020  9a 65 08 00 f9 ff 00 01  00 01 03 64 77 64 00 00   ·e······ ···dwd··
0030  00 00 bc 62 08 00 00 00  00 00 10 11 12 13 14 15   ···b···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

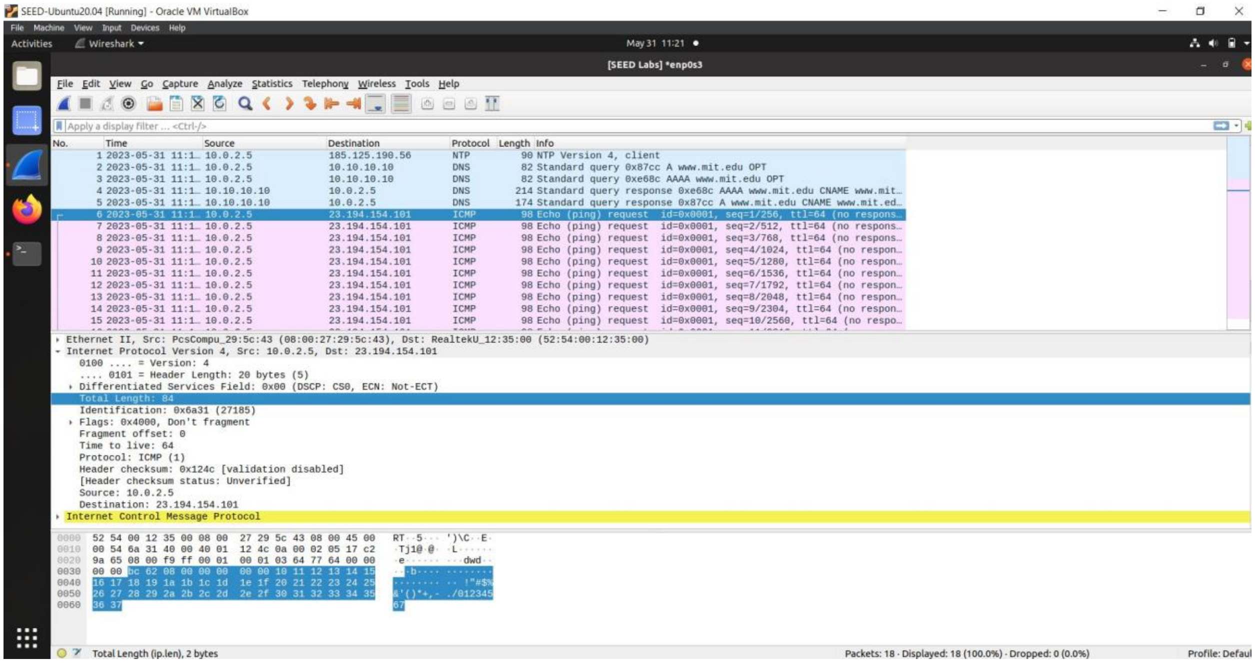
Header Length (ip.hdr_len), 1 byte

Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

(d) payload length for IP packet. This is total length – header length.

Here, total length = 84 and header length = 20. So, pay load length = 84 – 20 = 64.



SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Wireshark
May 31 11:21
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

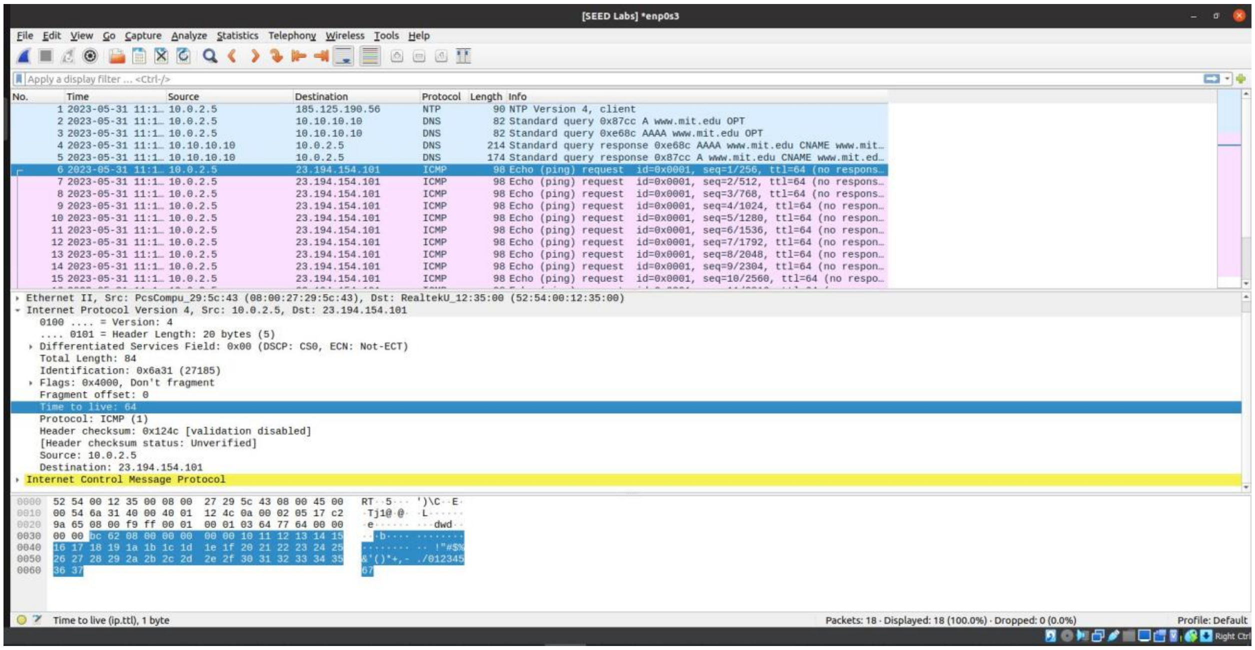
```
No.  Time             Source        Destination      Protocol Length Info
   1 2023-05-31 11:1… 10.0.2.5      185.125.190.56   NTP        90 NTP Version 4, client
   2 2023-05-31 11:1… 10.0.2.5      10.10.10.10      DNS        82 Standard query 0x87cc A www.mit.edu OPT
   3 2023-05-31 11:1… 10.0.2.5      10.10.10.10      DNS        82 Standard query 0xe68c AAAA www.mit.edu OPT
   4 2023-05-31 11:1… 10.10.10.10   10.0.2.5         DNS       214 Standard query response 0xe68c AAAA www.mit.edu CNAME www.mit…
   5 2023-05-31 11:1… 10.10.10.10   10.0.2.5         DNS       174 Standard query response 0x87cc A www.mit.edu CNAME www.mit.ed…
   6 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no respons…
   7 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (no respons…
   8 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (no respons…
   9 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=4/1024, ttl=64 (no respon…
  10 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=5/1280, ttl=64 (no respon…
  11 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=6/1536, ttl=64 (no respon…
  12 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=7/1792, ttl=64 (no respon…
  13 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=8/2048, ttl=64 (no respon…
  14 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=9/2304, ttl=64 (no respon…
  15 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=10/2560, ttl=64 (no respo…
```

```
▸ Ethernet II, Src: PcsCompu_29:5c:43 (08:00:27:29:5c:43), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▾ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 23.194.154.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x6a31 (27185)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x124c [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.5
    Destination: 23.194.154.101
▸ Internet Control Message Protocol
```

```
0000  52 54 00 12 35 00 08 00  27 29 5c 43 08 00 45 00   RT··5···')\C··E·
0010  00 54 6a 31 40 00 40 01  12 4c 0a 00 02 05 17 c2   ·Tj1@·@··L······
0020  9a 65 08 00 f9 ff 00 01  00 01 03 64 77 64 00 00   ·e·········dwd··
0030  00 00 bc 62 08 00 00 00  00 00 10 11 12 13 14 15   ···b············
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ·········· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37                                              67
```

```
Total Length (ip.len), 2 bytes          Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%)          Profile: Defaul
```

(e) The TTL value is 64. TTL indicates the maximum number of hops (routers) a packet can pass through before being discarded. It prevents packet from endlessly circulating in the network.



[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Right Ctrl

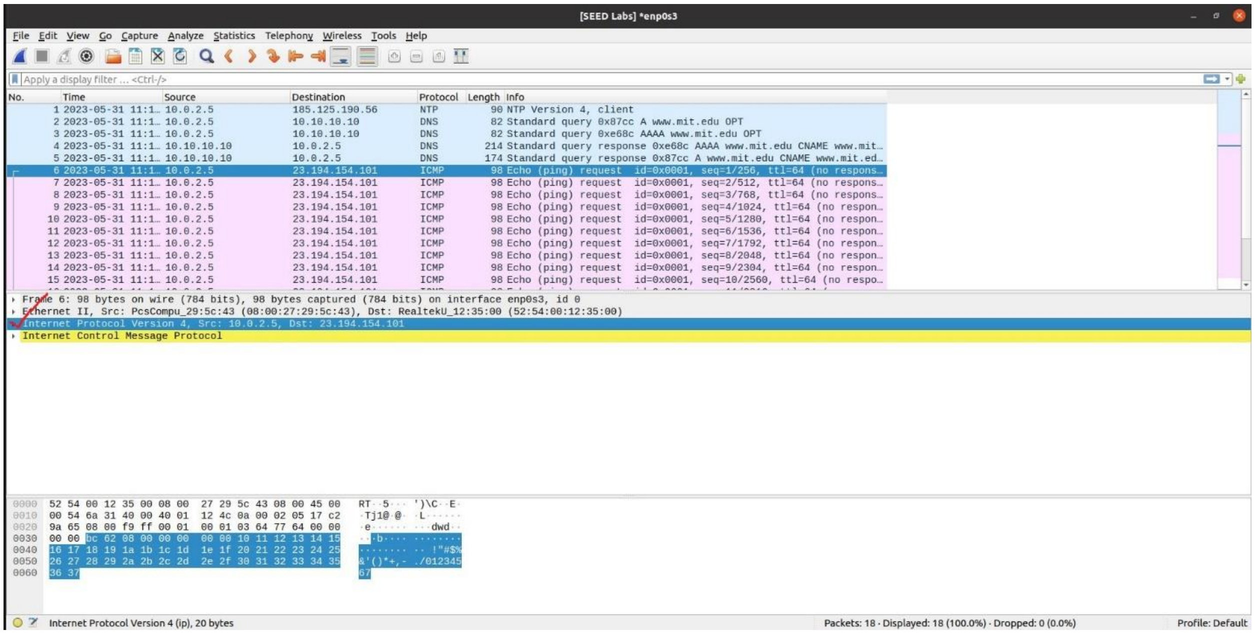
```
No.  Time             Source        Destination      Protocol Length Info
   1 2023-05-31 11:1… 10.0.2.5      185.125.190.56   NTP        90 NTP Version 4, client
   2 2023-05-31 11:1… 10.0.2.5      10.10.10.10      DNS        82 Standard query 0x87cc A www.mit.edu OPT
   3 2023-05-31 11:1… 10.0.2.5      10.10.10.10      DNS        82 Standard query 0xe68c AAAA www.mit.edu OPT
   4 2023-05-31 11:1… 10.10.10.10   10.0.2.5         DNS       214 Standard query response 0xe68c AAAA www.mit.edu CNAME www.mit…
   5 2023-05-31 11:1… 10.10.10.10   10.0.2.5         DNS       174 Standard query response 0x87cc A www.mit.edu CNAME www.mit.ed…
   6 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no respons…
   7 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (no respons…
   8 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (no respons…
   9 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=4/1024, ttl=64 (no respon…
  10 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=5/1280, ttl=64 (no respon…
  11 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=6/1536, ttl=64 (no respon…
  12 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=7/1792, ttl=64 (no respon…
  13 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=8/2048, ttl=64 (no respon…
  14 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=9/2304, ttl=64 (no respon…
  15 2023-05-31 11:1… 10.0.2.5      23.194.154.101   ICMP       98 Echo (ping) request  id=0x0001, seq=10/2560, ttl=64 (no respo…
```

```
▸ Ethernet II, Src: PcsCompu_29:5c:43 (08:00:27:29:5c:43), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▾ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 23.194.154.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x6a31 (27185)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x124c [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.5
    Destination: 23.194.154.101
▸ Internet Control Message Protocol
```

```
0000  52 54 00 12 35 00 08 00  27 29 5c 43 08 00 45 00   RT··5···')\C··E·
0010  00 54 6a 31 40 00 40 01  12 4c 0a 00 02 05 17 c2   ·Tj1@·@··L······
0020  9a 65 08 00 f9 ff 00 01  00 01 03 64 77 64 00 00   ·e·········dwd··
0030  00 00 bc 62 08 00 00 00  00 00 10 11 12 13 14 15   ···b············
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ·········· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37                                              67
```

```
Time to live (ip.ttl), 1 byte          Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%)          Profile: Default
```

(f) The highlighted field in the below Screenshot shows the IP header is in ipv4.



[SEED Labs] *enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time               Source          Destination       Protocol Length Info
    1 2023-05-31 11:1… 10.0.2.5        185.125.190.56    NTP         90 NTP Version 4, client
    2 2023-05-31 11:1… 10.0.2.5        10.10.10.10       DNS         82 Standard query 0x87cc A www.mit.edu OPT
    3 2023-05-31 11:1… 10.0.2.5        10.10.10.10       DNS         82 Standard query 0xe68c AAAA www.mit.edu OPT
    4 2023-05-31 11:1… 10.10.10.10     10.0.2.5          DNS        214 Standard query response 0xe68c AAAA www.mit.edu CNAME www.mit…
    5 2023-05-31 11:1… 10.10.10.10     10.0.2.5          DNS        174 Standard query response 0x87cc A www.mit.edu CNAME www.mit.ed…
    6 2023-05-31 11:1… 10.0.2.5        23.194.154.101    ICMP        98 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no respons…
    7 2023-05-31 11:1… 10.0.2.5        23.194.154.101    ICMP        98 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (no respons…
    8 2023-05-31 11:1… 10.0.2.5        23.194.154.101    ICMP        98 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (no respons…
    9 2023-05-31 11:1… 10.0.2.5        23.194.154.101    ICMP        98 Echo (ping) request  id=0x0001, seq=4/1024, ttl=64 (no respon…
   10 2023-05-31 11:1… 10.0.2.5        23.194.154.101    ICMP        98 Echo (ping) request  id=0x0001, seq=5/1280, ttl=64 (no respon…
   11 2023-05-31 11:1… 10.0.2.5        23.194.154.101    ICMP        98 Echo (ping) request  id=0x0001, seq=6/1536, ttl=64 (no respon…
   12 2023-05-31 11:1… 10.0.2.5        23.194.154.101    ICMP        98 Echo (ping) request  id=0x0001, seq=7/1792, ttl=64 (no respon…
   13 2023-05-31 11:1… 10.0.2.5        23.194.154.101    ICMP        98 Echo (ping) request  id=0x0001, seq=8/2048, ttl=64 (no respon…
   14 2023-05-31 11:1… 10.0.2.5        23.194.154.101    ICMP        98 Echo (ping) request  id=0x0001, seq=9/2304, ttl=64 (no respon…
   15 2023-05-31 11:1… 10.0.2.5        23.194.154.101    ICMP        98 Echo (ping) request  id=0x0001, seq=10/2560, ttl=64 (no respo…
```

```
› Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
› Ethernet II, Src: PcsCompu_29:5c:43 (08:00:27:29:5c:43), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
› Internet Protocol Version 4, Src: 10.0.2.5, Dst: 23.194.154.101
› Internet Control Message Protocol
```

```
0000  52 54 00 12 35 00 08 00  27 29 5c 43 08 00 45 00   RT··5···  ')\C··E·
0010  00 54 6a 31 40 00 40 01  12 4c 0a 00 02 05 17 c2   ·Tj1@·@·  ·L······
0020  9a 65 08 00 f9 ff 00 01  00 01 03 64 77 64 00 00   ·e······  ···dwd··
0030  00 00 bc 62 08 00 00 00  00 00 10 11 12 13 14 15   ···b····  ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········  ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,-  ./012345
0060  36 37                                              67
```

Internet Protocol Version 4 (ip), 20 bytes

Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

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. In addition to offer the ip address to your computer, DHCP can in fact provide you more useful configuration. Check DHCP offer packet to find out the following information.

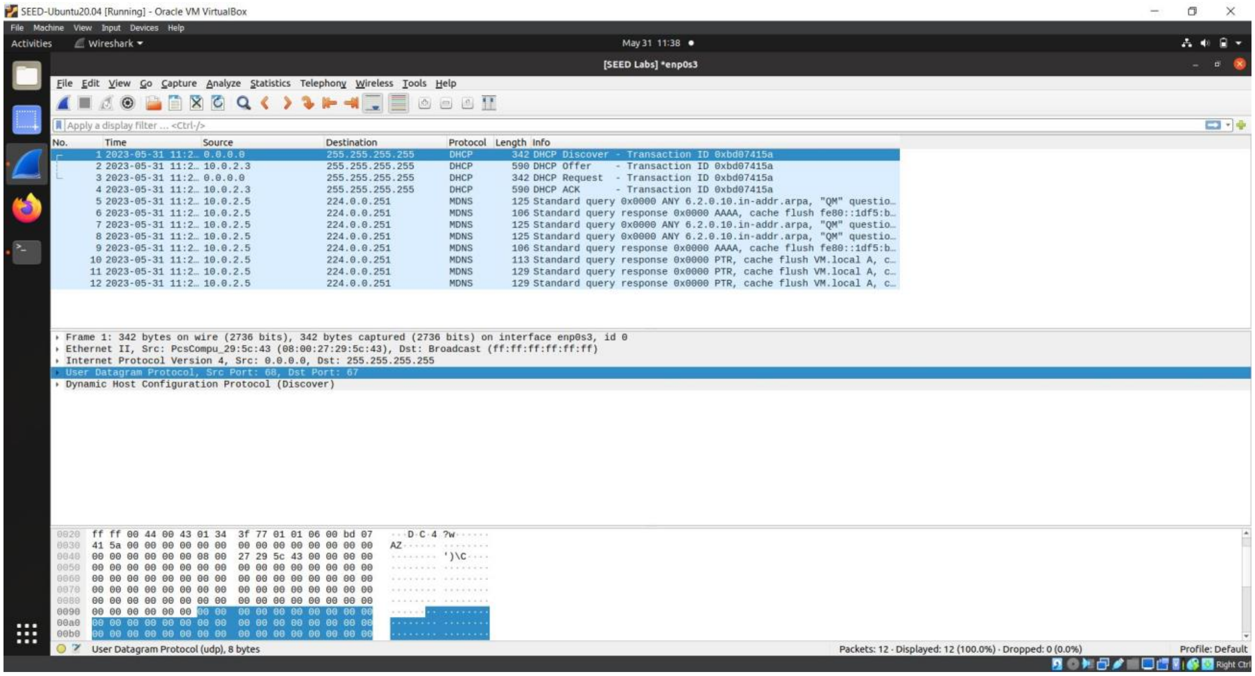
DHCP server IP: you need this to extend your time to use the current IP address.

Subnet mask: this tells you the subnet type.

Router IP: That is the ip address your outgoing packet will first go to.

DNS IP: this is the ip address of the DNS server that you will request to resolve your DNS query. That is, this is your local DNS server.

(a)The below screenshot proves that the transport layer protocol of DHCP protocol is UDP. UDP is a connectionless and lightweight transport protocol that does not require establishing a connection before sending data while TCP uses 3- way handshake to establish connection before sending messages. That's why USP is suitable for protocols like DHCP, which prioritize simplicity and efficiency over the reliability and sequencing provided by TCP.


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Wireshark
May 31 11:38
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Profile: Default

```
No.  Time             Source     Destination      Protocol Length Info
   1 2023-05-31 11:2… 0.0.0.0    255.255.255.255  DHCP     342 DHCP Discover - Transaction ID 0xbd07415a
   2 2023-05-31 11:2… 10.0.2.3   255.255.255.255  DHCP     590 DHCP Offer    - Transaction ID 0xbd07415a
   3 2023-05-31 11:2… 0.0.0.0    255.255.255.255  DHCP     342 DHCP Request  - Transaction ID 0xbd07415a
   4 2023-05-31 11:2… 10.0.2.3   255.255.255.255  DHCP     590 DHCP ACK      - Transaction ID 0xbd07415a
   5 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   6 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     106 Standard query response 0x0000 AAAA, cache flush fe80::1df5:b…
   7 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   8 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   9 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     106 Standard query response 0x0000 AAAA, cache flush fe80::1df5:b…
  10 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     113 Standard query response 0x0000 PTR, cache flush VM.local A, c…
  11 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     129 Standard query response 0x0000 PTR, cache flush VM.local A, c…
  12 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     129 Standard query response 0x0000 PTR, cache flush VM.local A, c…
```

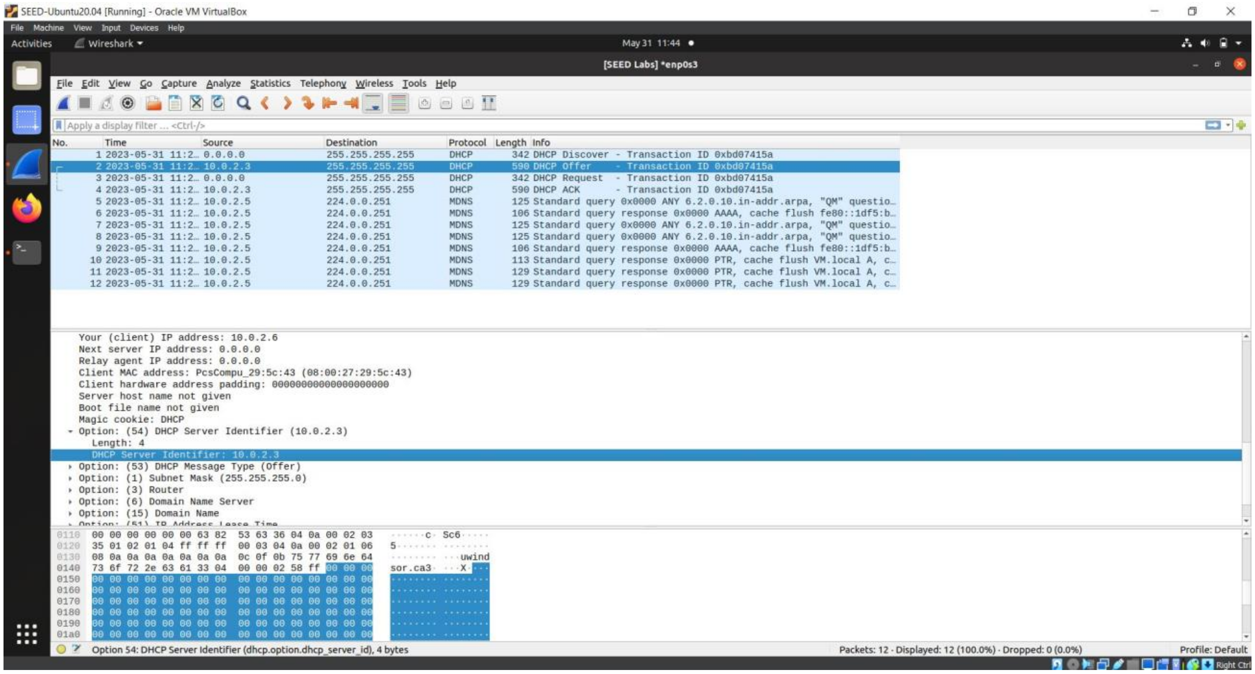
```
› Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface enp0s3, id 0
› Ethernet II, Src: PcsCompu_29:5c:43 (08:00:27:29:5c:43), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
› User Datagram Protocol, Src Port: 68, Dst Port: 67
› Dynamic Host Configuration Protocol (Discover)
```

```
0020  ff ff 00 44 00 43 01 34  3f 77 01 01 06 00 bd 07   ···D·C·4 ?w······
0030  41 5a 00 00 00 00 00 00  00 00 00 00 00 00 00 00   AZ······ ········
0040  00 00 00 00 00 00 08 00  27 29 5c 43 00 00 00 00   ········ ')\C····
0050  00 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 00   ········ ········
0070  00 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 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

User Datagram Protocol (udp), 8 bytes

Packets: 12 · Displayed: 12 (100.0%) · Dropped: 0 (0.0%)

(b) **DHCP server IP: 10.0.2.3**


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Wireshark
May 31 11:44
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Profile: Default

```
No.  Time             Source     Destination      Protocol Length Info
   1 2023-05-31 11:2… 0.0.0.0    255.255.255.255  DHCP     342 DHCP Discover - Transaction ID 0xbd07415a
   2 2023-05-31 11:2… 10.0.2.3   255.255.255.255  DHCP     590 DHCP Offer    - Transaction ID 0xbd07415a
   3 2023-05-31 11:2… 0.0.0.0    255.255.255.255  DHCP     342 DHCP Request  - Transaction ID 0xbd07415a
   4 2023-05-31 11:2… 10.0.2.3   255.255.255.255  DHCP     590 DHCP ACK      - Transaction ID 0xbd07415a
   5 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   6 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     106 Standard query response 0x0000 AAAA, cache flush fe80::1df5:b…
   7 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   8 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   9 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     106 Standard query response 0x0000 AAAA, cache flush fe80::1df5:b…
  10 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     113 Standard query response 0x0000 PTR, cache flush VM.local A, c…
  11 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     129 Standard query response 0x0000 PTR, cache flush VM.local A, c…
  12 2023-05-31 11:2… 10.0.2.5   224.0.0.251      MDNS     129 Standard query response 0x0000 PTR, cache flush VM.local A, c…
```

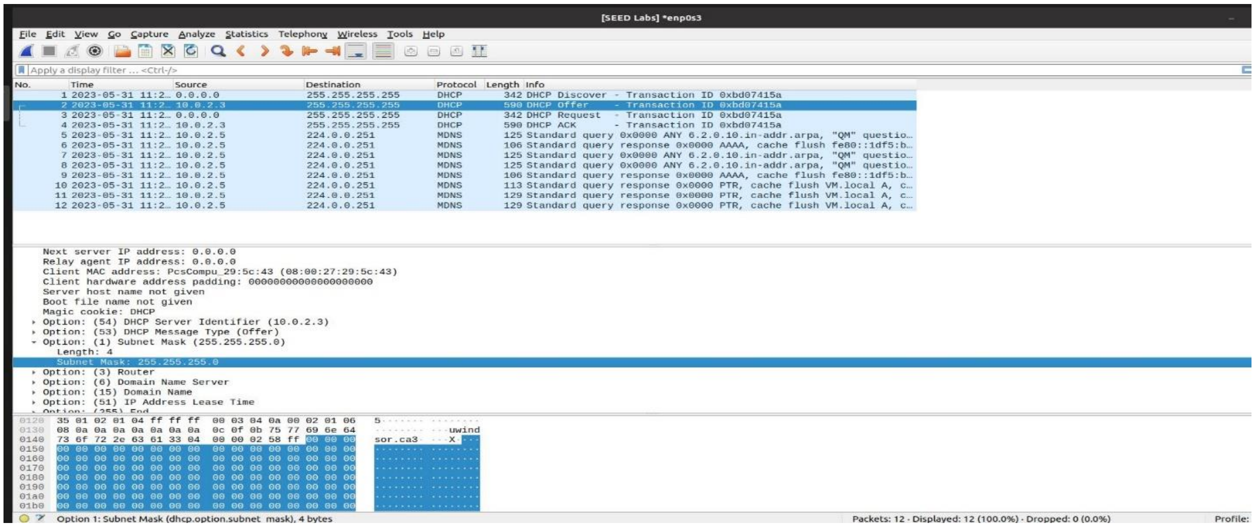
```
    Your (client) IP address: 10.0.2.6
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▾ Option: (54) DHCP Server Identifier (10.0.2.3)
      Length: 4
      DHCP Server Identifier: 10.0.2.3
  › Option: (53) DHCP Message Type (Offer)
  › Option: (1) Subnet Mask (255.255.255.0)
  › Option: (3) Router
  › Option: (6) Domain Name Server
  › Option: (15) Domain Name
  › Option: (51) IP Address Lease Time
```

```
0110  00 00 00 00 00 00 63 82  53 63 36 04 0a 00 02 03   ······c· Sc6·····
0120  35 01 02 01 04 ff ff ff  00 03 04 0a 00 02 01 06   5······· ········
0130  08 0a 0a 0a 0a 0a 0a 0a  0c 0f 0b 75 77 69 6e 64   ········ ···uwind
0140  73 6f 72 2e 63 61 33 04  00 00 02 58 ff 00 00 00   sor.ca3· ···X····
0150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
01a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Option 54: DHCP Server Identifier (dhcp.option.dhcp_server_id), 4 bytes

Packets: 12 · Displayed: 12 (100.0%) · Dropped: 0 (0.0%)

Subnet mask: 255.255.255.0


[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

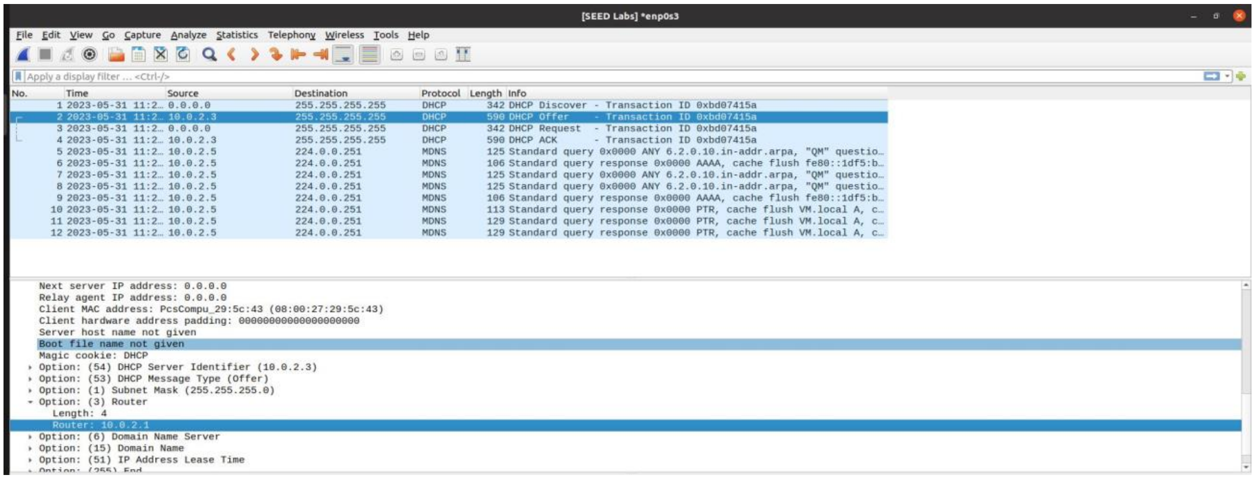
```
No.  Time             Source      Destination       Protocol Length Info
   1 2023-05-31 11:2… 0.0.0.0     255.255.255.255   DHCP     342 DHCP Discover  - Transaction ID 0xbd07415a
   2 2023-05-31 11:2… 10.0.2.3    255.255.255.255   DHCP     590 DHCP Offer     - Transaction ID 0xbd07415a
   3 2023-05-31 11:2… 0.0.0.0     255.255.255.255   DHCP     342 DHCP Request   - Transaction ID 0xbd07415a
   4 2023-05-31 11:2… 10.0.2.3    255.255.255.255   DHCP     590 DHCP ACK       - Transaction ID 0xbd07415a
   5 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   6 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     106 Standard query response 0x0000 AAAA, cache flush fe80::1df5:b…
   7 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   8 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   9 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     106 Standard query response 0x0000 AAAA, cache flush fe80::1df5:b…
  10 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     113 Standard query response 0x0000 PTR, cache flush VM.local A, c…
  11 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     129 Standard query response 0x0000 PTR, cache flush VM.local A, c…
  12 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     129 Standard query response 0x0000 PTR, cache flush VM.local A, c…
```

```
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (54) DHCP Server Identifier (10.0.2.3)
  ▸ 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
  ▸ Option: (6) Domain Name Server
  ▸ Option: (15) Domain Name
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (255) End
```

```
0120  35 01 02 01 04 ff ff ff  00 03 04 0a 00 02 01 06   5······· ········
0130  08 0a 0a 0a 0a 0a 0a 0a  0c 0f 0b 75 77 69 6e 64   ········ ···uwind
0140  73 6f 72 2e 63 61 33 04  00 00 02 58 ff 00 00 00   sor.ca3· ···X····
0150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
01a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
01b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

```
Option 1: Subnet Mask (dhcp.option.subnet_mask), 4 bytes     Packets: 12 · Displayed: 12 (100.0%) · Dropped: 0 (0.0%)     Profile:
```

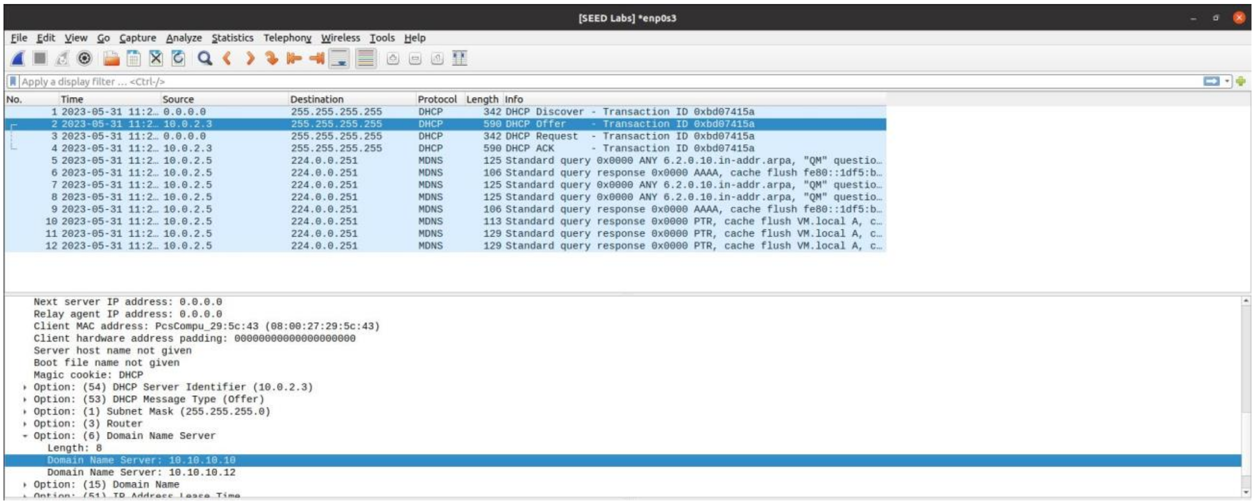
Router IP: 10.0.2.1


[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time             Source      Destination       Protocol Length Info
   1 2023-05-31 11:2… 0.0.0.0     255.255.255.255   DHCP     342 DHCP Discover  - Transaction ID 0xbd07415a
   2 2023-05-31 11:2… 10.0.2.3    255.255.255.255   DHCP     590 DHCP Offer     - Transaction ID 0xbd07415a
   3 2023-05-31 11:2… 0.0.0.0     255.255.255.255   DHCP     342 DHCP Request   - Transaction ID 0xbd07415a
   4 2023-05-31 11:2… 10.0.2.3    255.255.255.255   DHCP     590 DHCP ACK       - Transaction ID 0xbd07415a
   5 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   6 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     106 Standard query response 0x0000 AAAA, cache flush fe80::1df5:b…
   7 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   8 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   9 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     106 Standard query response 0x0000 AAAA, cache flush fe80::1df5:b…
  10 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     113 Standard query response 0x0000 PTR, cache flush VM.local A, c…
  11 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     129 Standard query response 0x0000 PTR, cache flush VM.local A, c…
  12 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     129 Standard query response 0x0000 PTR, cache flush VM.local A, c…
```

```
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (54) DHCP Server Identifier (10.0.2.3)
  ▸ Option: (53) DHCP Message Type (Offer)
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▾ Option: (3) Router
      Length: 4
      Router: 10.0.2.1
  ▸ Option: (6) Domain Name Server
  ▸ Option: (15) Domain Name
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (255) End
```

DNS IP: 10.10.10.10


[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time             Source      Destination       Protocol Length Info
   1 2023-05-31 11:2… 0.0.0.0     255.255.255.255   DHCP     342 DHCP Discover  - Transaction ID 0xbd07415a
   2 2023-05-31 11:2… 10.0.2.3    255.255.255.255   DHCP     590 DHCP Offer     - Transaction ID 0xbd07415a
   3 2023-05-31 11:2… 0.0.0.0     255.255.255.255   DHCP     342 DHCP Request   - Transaction ID 0xbd07415a
   4 2023-05-31 11:2… 10.0.2.3    255.255.255.255   DHCP     590 DHCP ACK       - Transaction ID 0xbd07415a
   5 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   6 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     106 Standard query response 0x0000 AAAA, cache flush fe80::1df5:b…
   7 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   8 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     125 Standard query 0x0000 ANY 6.2.0.10.in-addr.arpa, "QM" questio…
   9 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     106 Standard query response 0x0000 AAAA, cache flush fe80::1df5:b…
  10 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     113 Standard query response 0x0000 PTR, cache flush VM.local A, c…
  11 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     129 Standard query response 0x0000 PTR, cache flush VM.local A, c…
  12 2023-05-31 11:2… 10.0.2.5    224.0.0.251       MDNS     129 Standard query response 0x0000 PTR, cache flush VM.local A, c…
```

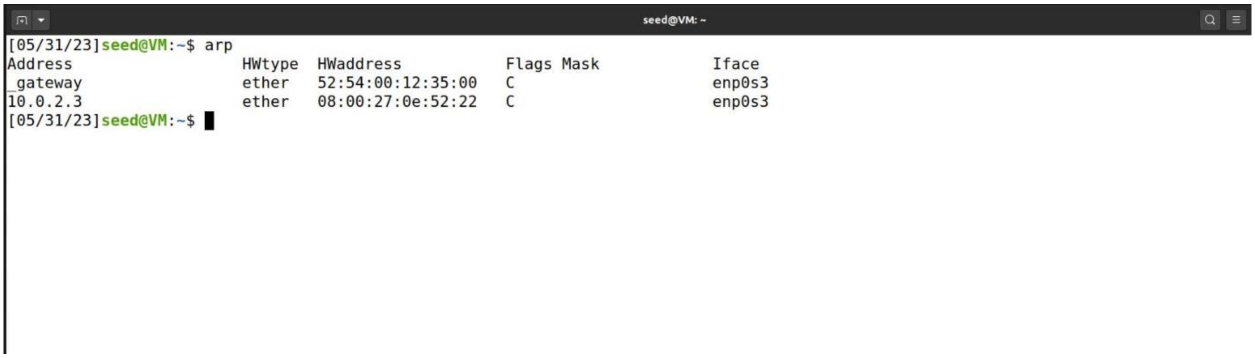
```
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (54) DHCP Server Identifier (10.0.2.3)
  ▸ Option: (53) DHCP Message Type (Offer)
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (3) Router
  ▾ 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
```

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?

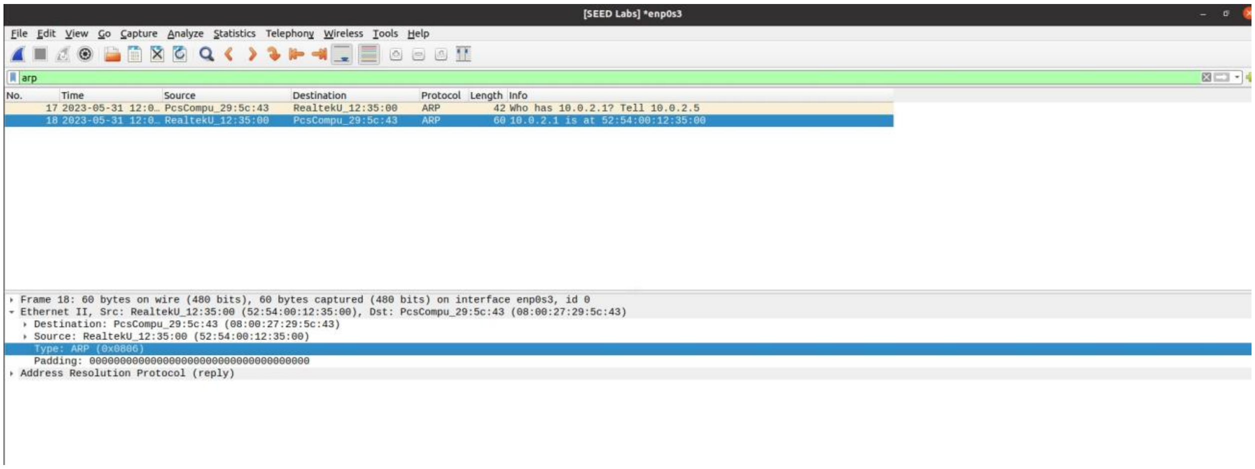
b. look at the response packet for the ARP query. What is the ip address of the sender? What is its MAC address?

ARP Table:



```
[05/31/23]seed@VM:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   52:54:00:12:35:00   C                     enp0s3
10.0.2.3                 ether   08:00:27:0e:52:22   C                     enp0s3
[05/31/23]seed@VM:~$ 
```

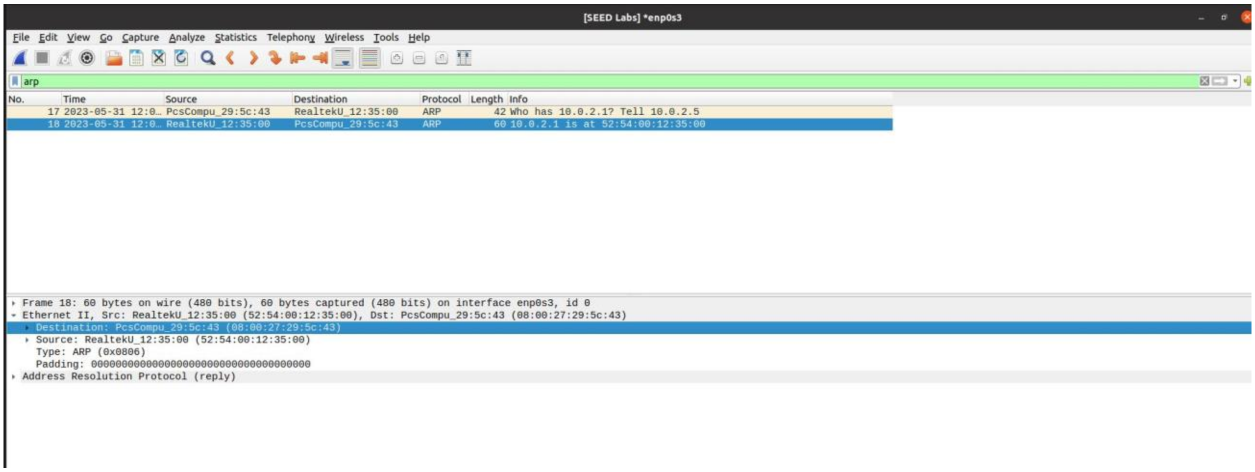
(a) The upper layer protocol in the link layer header is ARP (Address Resolution Protocol).



```
arp
No.     Time              Source              Destination         Protocol Length Info
     17 2023-05-31 12:0… PcsCompu_29:5c:43   RealtekU_12:35:00   ARP          42 Who has 10.0.2.1? Tell 10.0.2.5
     18 2023-05-31 12:0… RealtekU_12:35:00   PcsCompu_29:5c:43   ARP          60 10.0.2.1 is at 52:54:00:12:35:00
```

```
› Frame 18: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s3, id 0
⌄ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
  › Destination: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
  › Source: RealtekU_12:35:00 (52:54:00:12:35:00)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
› Address Resolution Protocol (reply)
```

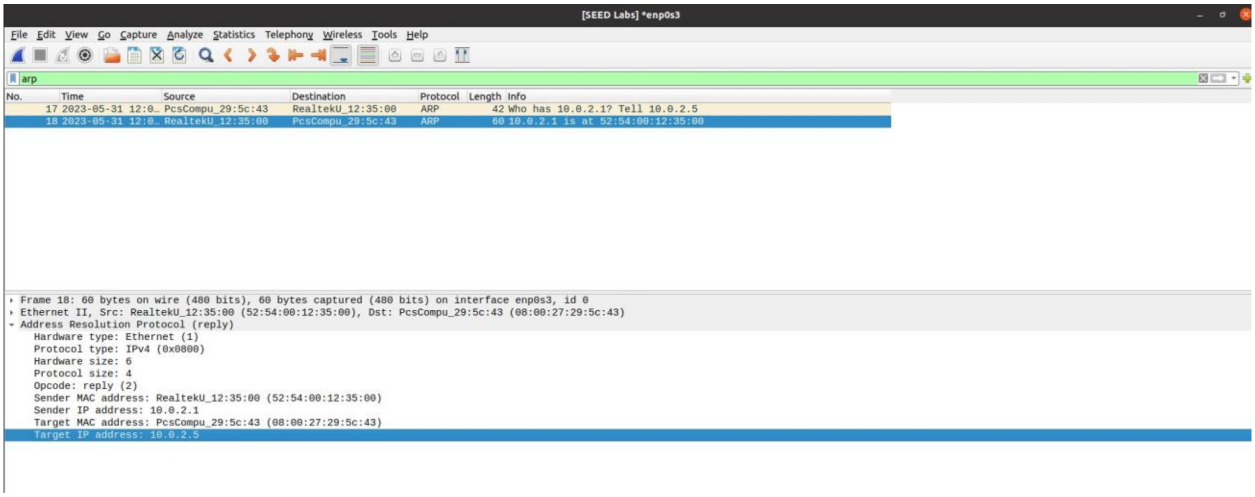
The broadcast MAC address is 08:00:27:29:5c:43


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

```
No.   Time               Source                Destination           Protocol  Length  Info
   17 2023-05-31 12:0… PcsCompu_29:5c:43    RealtekU_12:35:00     ARP          42 Who has 10.0.2.1? Tell 10.0.2.5
   18 2023-05-31 12:0… RealtekU_12:35:00    PcsCompu_29:5c:43     ARP          60 10.0.2.1 is at 52:54:00:12:35:00
```

```
▸ Frame 18: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s3, id 0
▾ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
  ▸ Destination: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
  ▸ Source: RealtekU_12:35:00 (52:54:00:12:35:00)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▸ Address Resolution Protocol (reply)
```

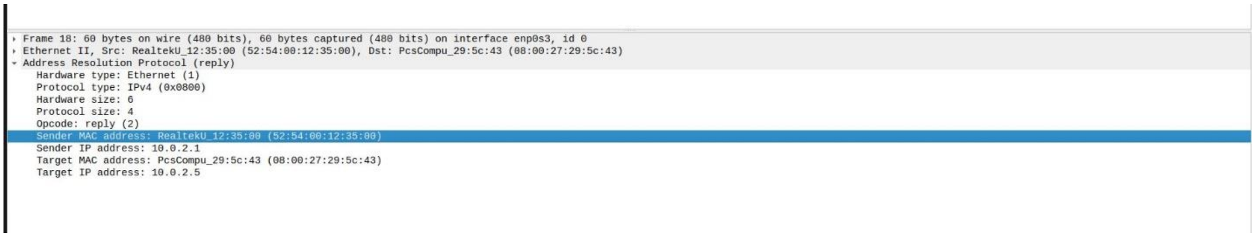
The IP address for which broadcast message is intended to is 10.0.2.5


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

```
No.   Time               Source                Destination           Protocol  Length  Info
   17 2023-05-31 12:0… PcsCompu_29:5c:43    RealtekU_12:35:00     ARP          42 Who has 10.0.2.1? Tell 10.0.2.5
   18 2023-05-31 12:0… RealtekU_12:35:00    PcsCompu_29:5c:43     ARP          60 10.0.2.1 is at 52:54:00:12:35:00
```

```
▸ Frame 18: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
▾ 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_12:35:00 (52:54:00:12:35:00)
    Sender IP address: 10.0.2.1
    Target MAC address: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
    Target IP address: 10.0.2.5
```

The IP address of the sender is 10.0.2.1 and MAC address of the sender is 52:54:00:12:35:00



```
▸ Frame 18: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
▾ 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_12:35:00 (52:54:00:12:35:00)
    Sender IP address: 10.0.2.1
    Target MAC address: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
    Target IP address: 10.0.2.5
```

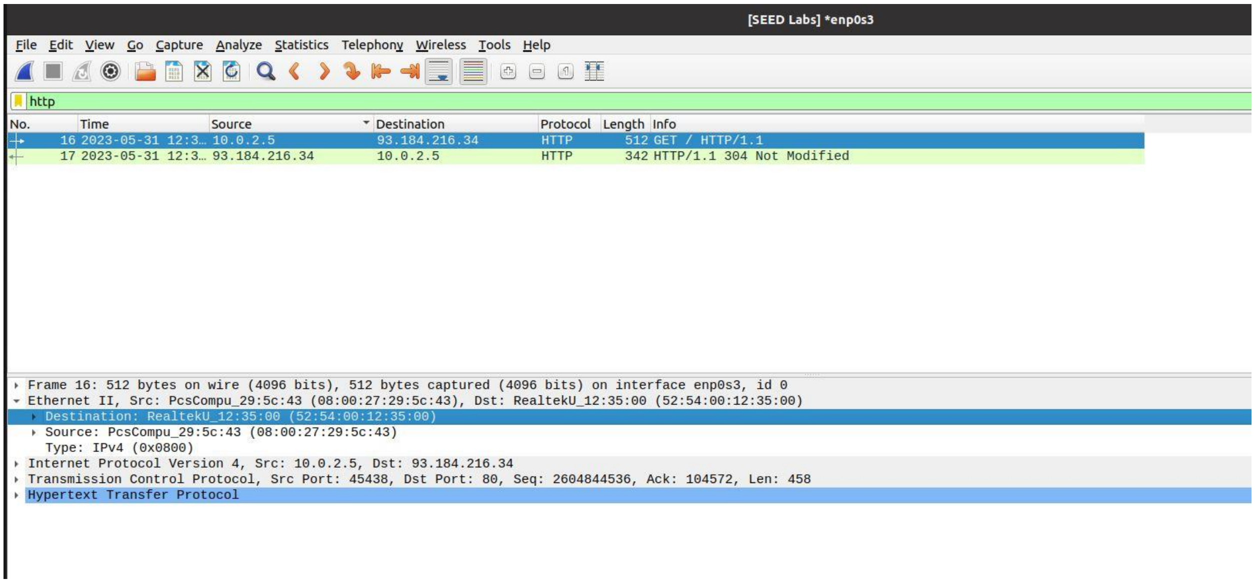
4. Run wireshark and access www.example.com and stop Wireshark. Answer the following questions.

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?

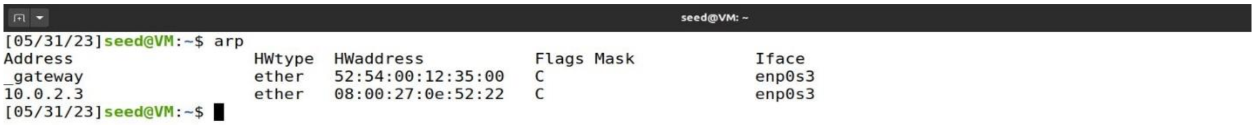
(a) The source MAC is 08:00:27:29:5c:43 and the destination MAC is 52:54:00:12:35:00


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

No.	Time	Source	Destination	Protocol	Length	Info
16	2023-05-31 12:3…	10.0.2.5	93.184.216.34	HTTP	512	GET / HTTP/1.1
17	2023-05-31 12:3…	93.184.216.34	10.0.2.5	HTTP	342	HTTP/1.1 304 Not Modified

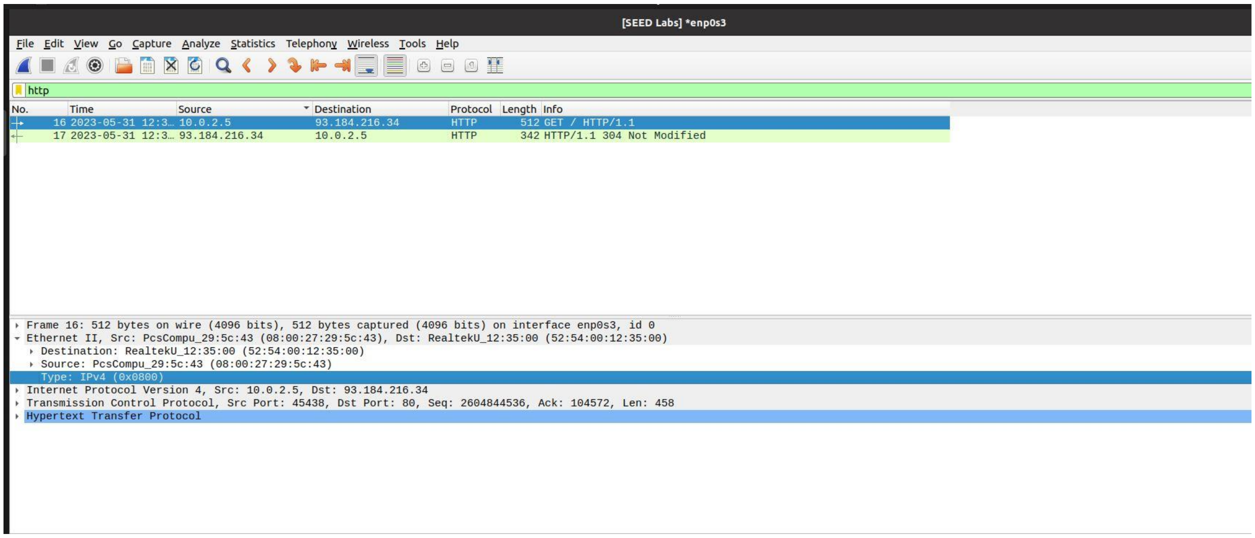
```
Frame 16: 512 bytes on wire (4096 bits), 512 bytes captured (4096 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_29:5c:43 (08:00:27:29:5c:43), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
  Destination: RealtekU_12:35:00 (52:54:00:12:35:00)
  Source: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.5, Dst: 93.184.216.34
Transmission Control Protocol, Src Port: 45438, Dst Port: 80, Seq: 2604844536, Ack: 104572, Len: 458
Hypertext Transfer Protocol
```

(b) In the ARP table we can see the Destination MAC which is 52:54:00:12:35:00 is present but this is doesnot belong to 93.184.216.34. Because we can clearly notice on the Screenshot that the MAC address belongs to the Gateway(router).



```
[05/31/23]seed@VM:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   52:54:00:12:35:00   C                     enp0s3
10.0.2.3                 ether   08:00:27:0e:52:22   C                     enp0s3
[05/31/23]seed@VM:~$
```

(C) The value in the upper protocol field of link layer header of your HTTP request packet is 0x0800. The value represents IPV4.



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

```
No.   Time              Source           Destination      Protocol Length Info
   16 2023-05-31 12:3… 10.0.2.5         93.184.216.34    HTTP        512 GET / HTTP/1.1
   17 2023-05-31 12:3… 93.184.216.34    10.0.2.5         HTTP        342 HTTP/1.1 304 Not Modified
```

```
Frame 16: 512 bytes on wire (4096 bits), 512 bytes captured (4096 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_29:5c:43 (08:00:27:29:5c:43), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
  Destination: RealtekU_12:35:00 (52:54:00:12:35:00)
  Source: PcsCompu_29:5c:43 (08:00:27:29:5c:43)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.5, Dst: 93.184.216.34
Transmission Control Protocol, Src Port: 45438, Dst Port: 80, Seq: 2604844536, Ack: 104572, Len: 458
Hypertext Transfer Protocol
```