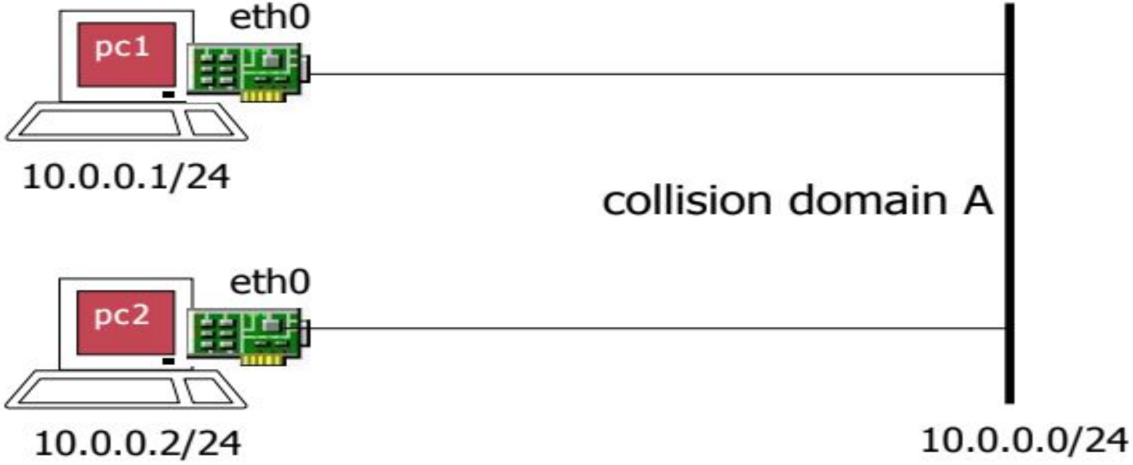
Lab 01

CT106H - Computer network

Exercise 1

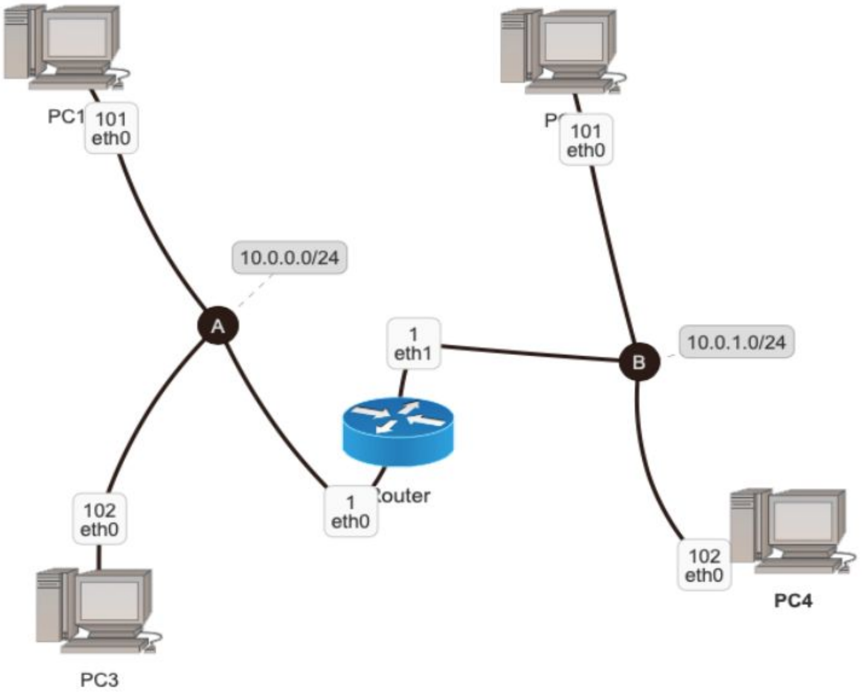
Construct a simple network with two hosts connected to the same collision domain

Solution: 003-kathara-lab_two-hosts.pdf

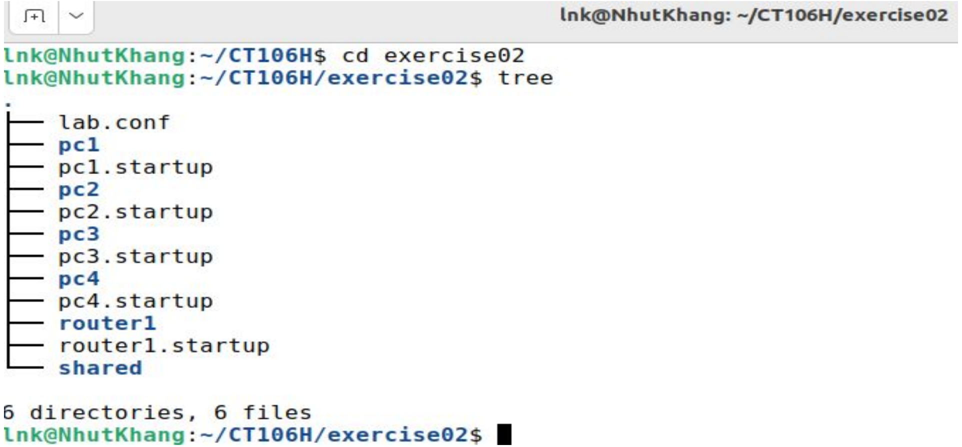


Exercise 2

Construct the following network

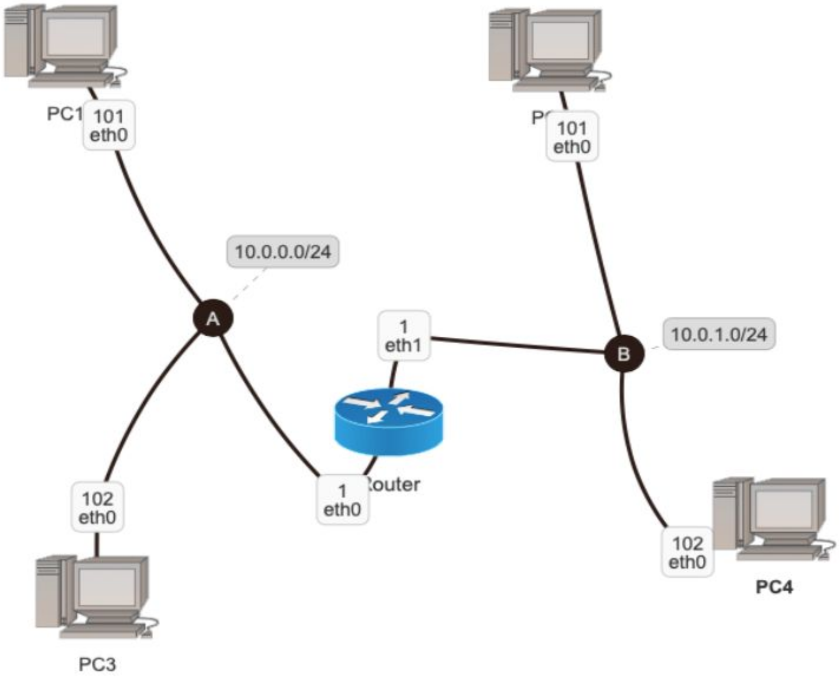


Exercise 2 (solution)

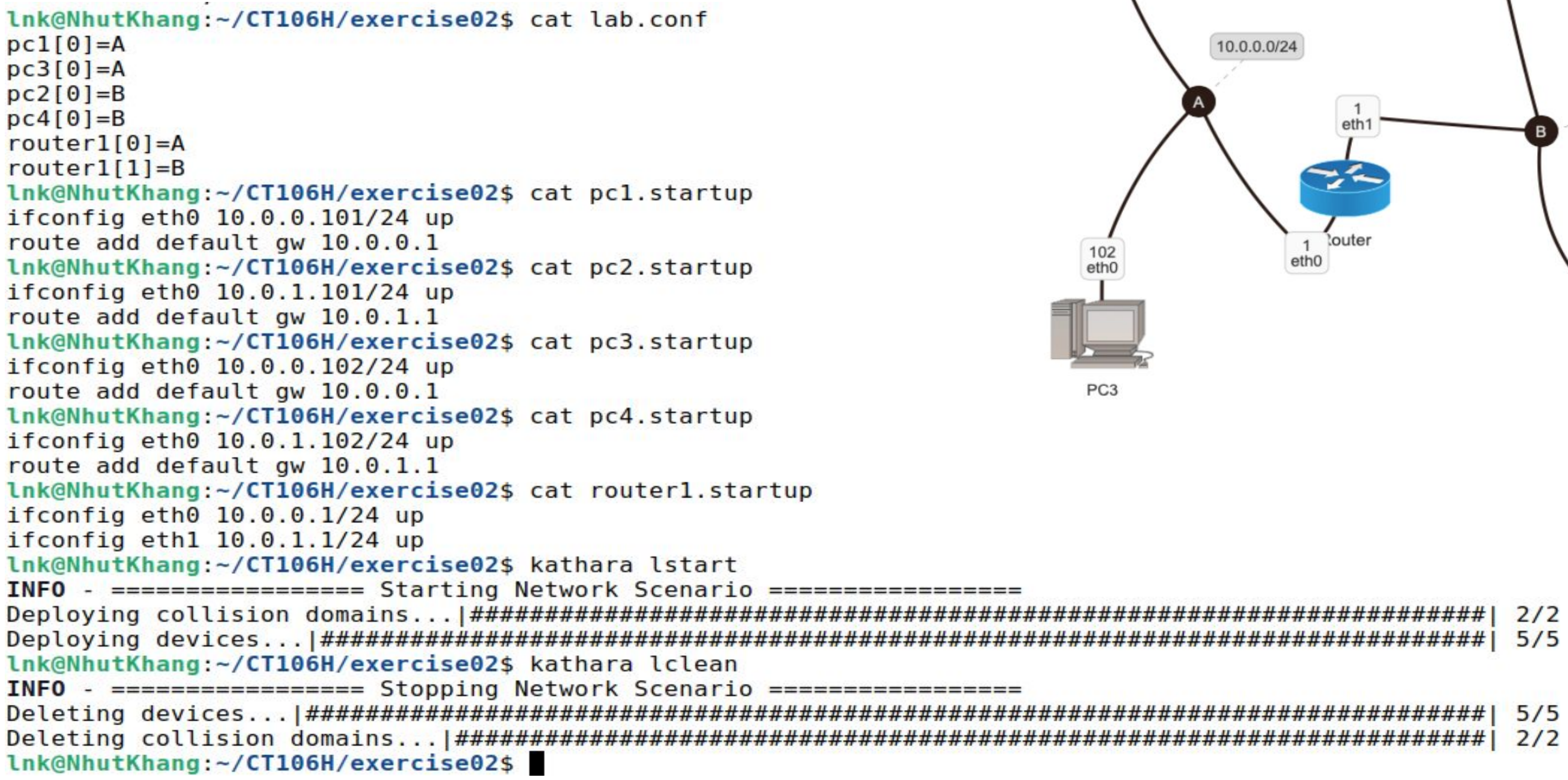


lnk@NhutKhang: ~/CT106H/exercise02

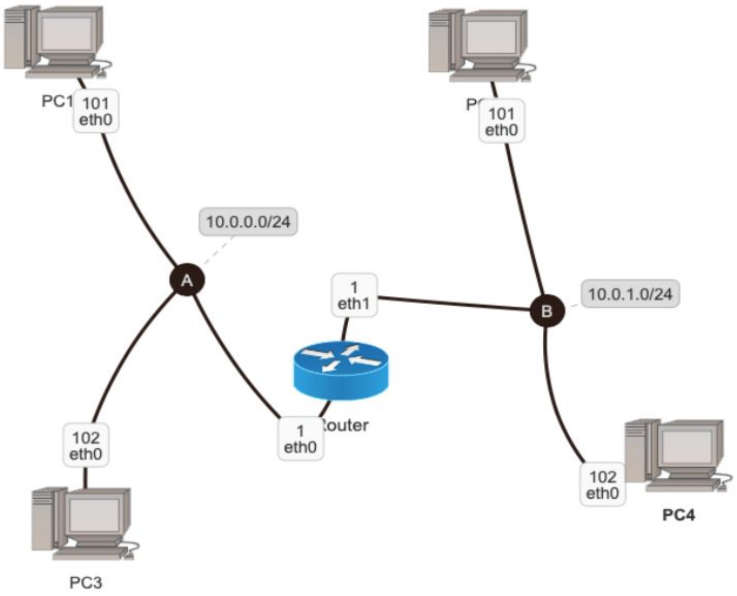
```
lnk@NhutKhang:~/CT106H$ cd exercise02
lnk@NhutKhang:~/CT106H/exercise02$ tree
.
├── lab.conf
├── pc1
├── pc1.startup
├── pc2
├── pc2.startup
├── pc3
├── pc3.startup
├── pc4
├── pc4.startup
├── router1
├── router1.startup
└── shared

6 directories, 6 files
lnk@NhutKhang:~/CT106H/exercise02$ 
```



Exercise 2 (solution)



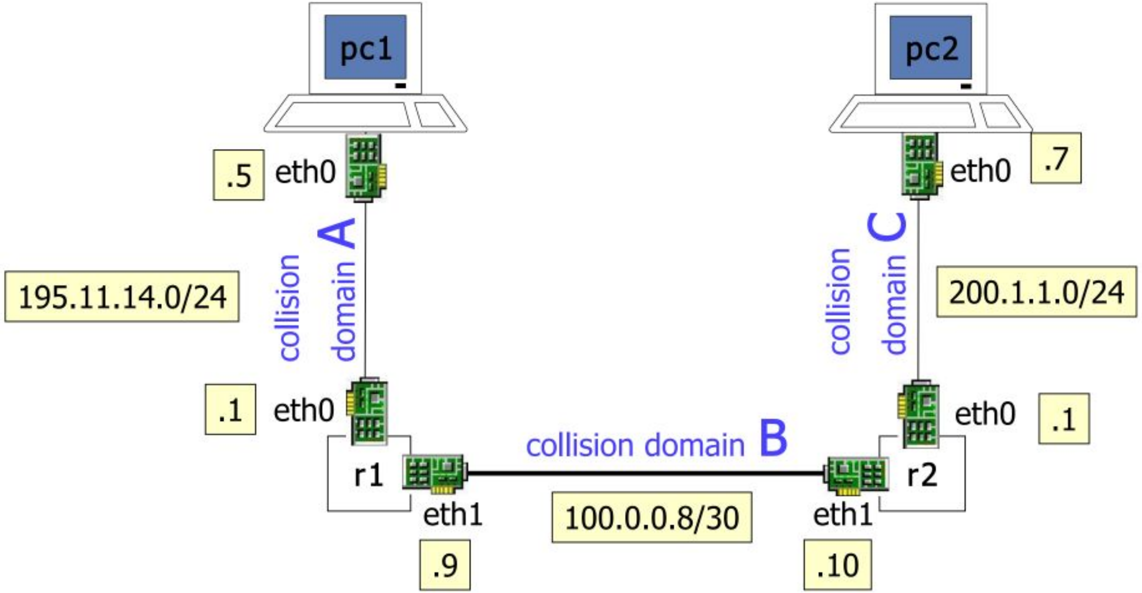
```
lnk@NhutKhang:~/CT106H/exercise02$ cat lab.conf
pc1[0]=A
pc3[0]=A
pc2[0]=B
pc4[0]=B
router1[0]=A
router1[1]=B
lnk@NhutKhang:~/CT106H/exercise02$ cat pc1.startup
ifconfig eth0 10.0.0.101/24 up
route add default gw 10.0.0.1
lnk@NhutKhang:~/CT106H/exercise02$ cat pc2.startup
ifconfig eth0 10.0.1.101/24 up
route add default gw 10.0.1.1
lnk@NhutKhang:~/CT106H/exercise02$ cat pc3.startup
ifconfig eth0 10.0.0.102/24 up
route add default gw 10.0.0.1
lnk@NhutKhang:~/CT106H/exercise02$ cat pc4.startup
ifconfig eth0 10.0.1.102/24 up
route add default gw 10.0.1.1
lnk@NhutKhang:~/CT106H/exercise02$ cat router1.startup
ifconfig eth0 10.0.0.1/24 up
ifconfig eth1 10.0.1.1/24 up
lnk@NhutKhang:~/CT106H/exercise02$ kathara lstart
INFO - ================= Starting Network Scenario =================
Deploying collision domains...|####################################################################| 2/2
Deploying devices...|##############################################################################| 5/5
lnk@NhutKhang:~/CT106H/exercise02$ kathara lclean
INFO - ================= Stopping Network Scenario =================
Deleting devices...|###############################################################################| 5/5
Deleting collision domains...|#####################################################################| 2/2
lnk@NhutKhang:~/CT106H/exercise02$ █
```



Exercise 3

Construct the following network

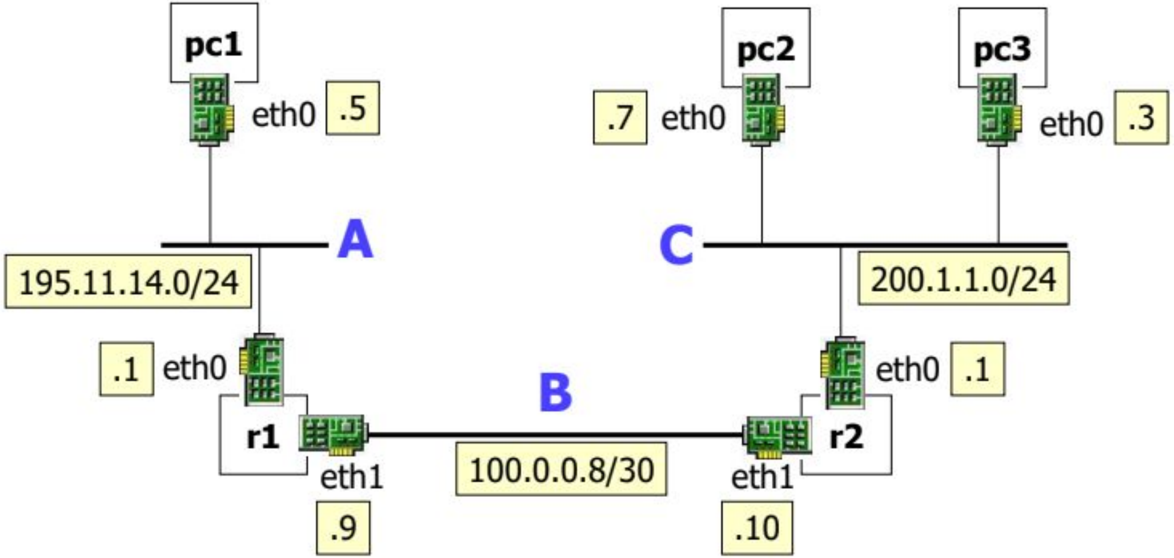
Solution: 004-kathara-lab_static-routing.pdf



Exercise 4

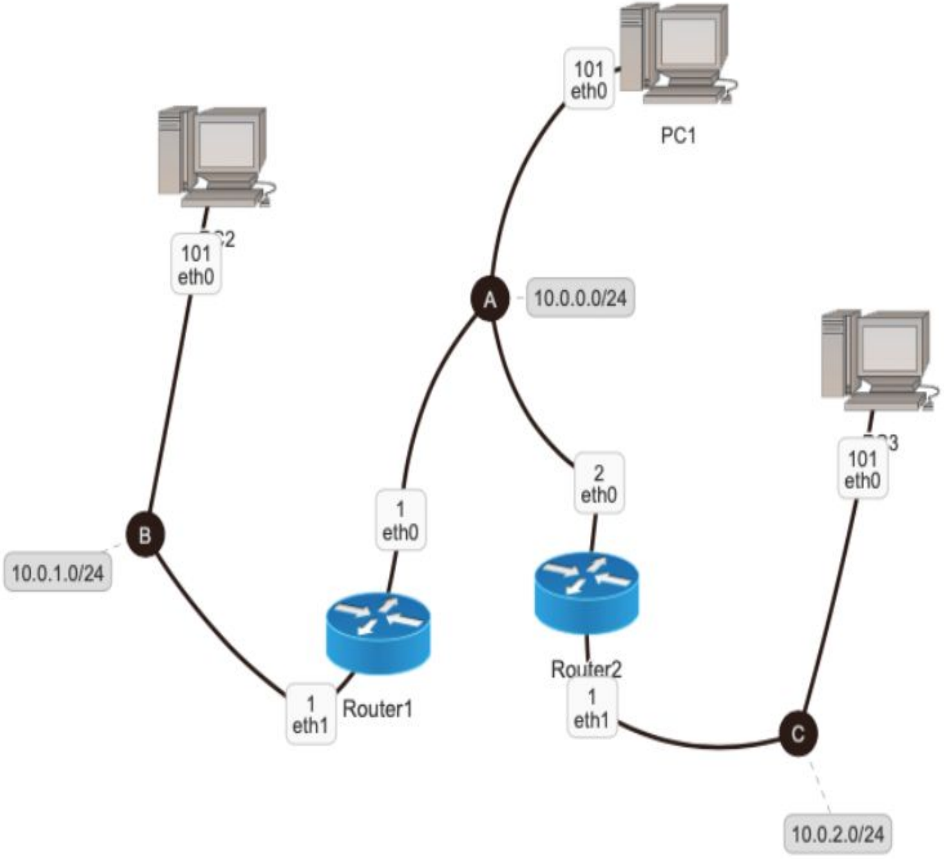
Study arp protocol

Solution: 005-kathara-lab_arp.pdf

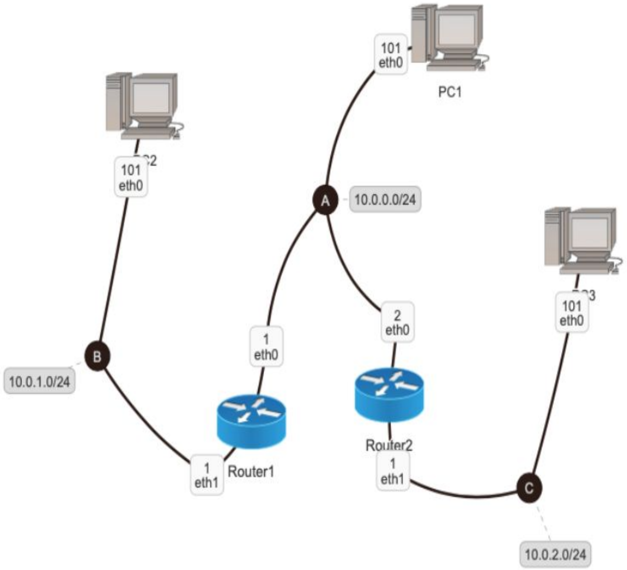


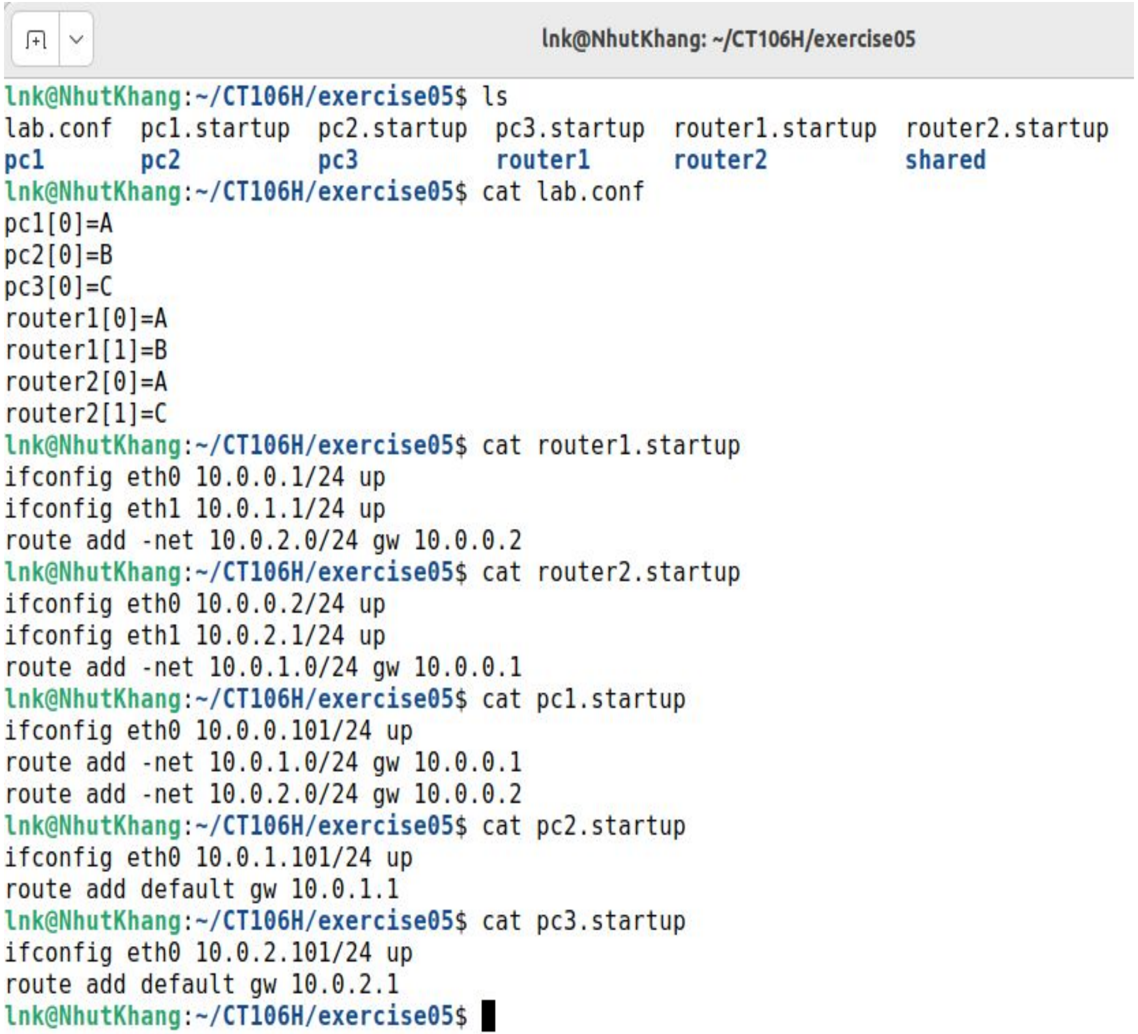
Exercise 5

Construct the following network



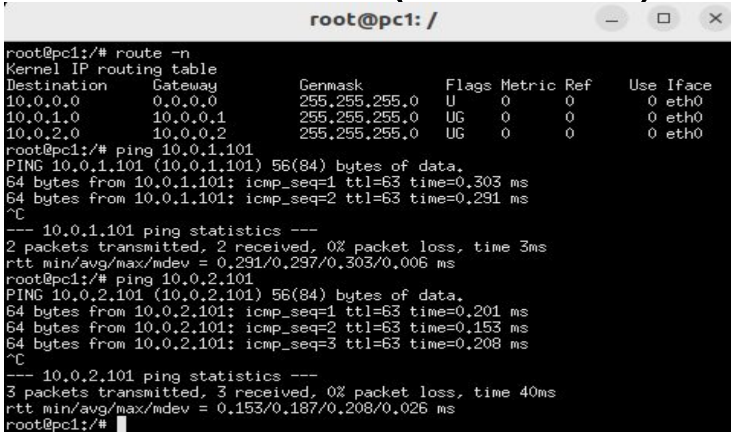
Exercise 5 (solution)





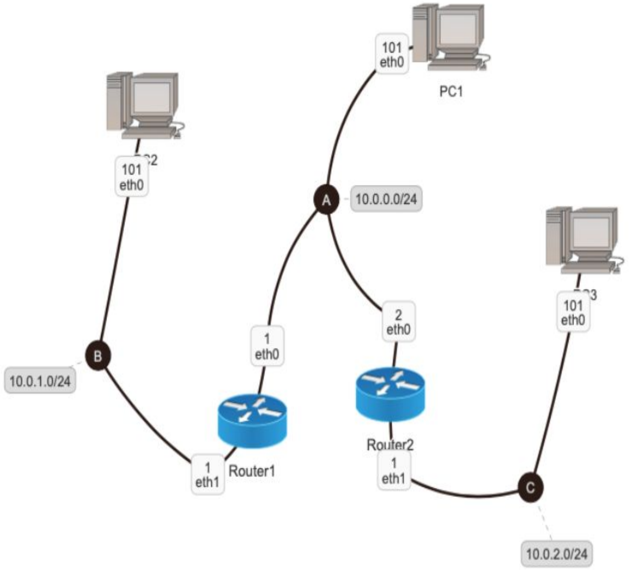
```
lnk@NhutKhang:~/CT106H/exercise05$ ls
lab.conf   pc1.startup   pc2.startup   pc3.startup   router1.startup   router2.startup
pc1        pc2           pc3           router1       router2           shared
lnk@NhutKhang:~/CT106H/exercise05$ cat lab.conf
pc1[0]=A
pc2[0]=B
pc3[0]=C
router1[0]=A
router1[1]=B
router2[0]=A
router2[1]=C
lnk@NhutKhang:~/CT106H/exercise05$ cat router1.startup
ifconfig eth0 10.0.0.1/24 up
ifconfig eth1 10.0.1.1/24 up
route add -net 10.0.2.0/24 gw 10.0.0.2
lnk@NhutKhang:~/CT106H/exercise05$ cat router2.startup
ifconfig eth0 10.0.0.2/24 up
ifconfig eth1 10.0.2.1/24 up
route add -net 10.0.1.0/24 gw 10.0.0.1
lnk@NhutKhang:~/CT106H/exercise05$ cat pc1.startup
ifconfig eth0 10.0.0.101/24 up
route add -net 10.0.1.0/24 gw 10.0.0.1
route add -net 10.0.2.0/24 gw 10.0.0.2
lnk@NhutKhang:~/CT106H/exercise05$ cat pc2.startup
ifconfig eth0 10.0.1.101/24 up
route add default gw 10.0.1.1
lnk@NhutKhang:~/CT106H/exercise05$ cat pc3.startup
ifconfig eth0 10.0.2.101/24 up
route add default gw 10.0.2.1
lnk@NhutKhang:~/CT106H/exercise05$ 
```

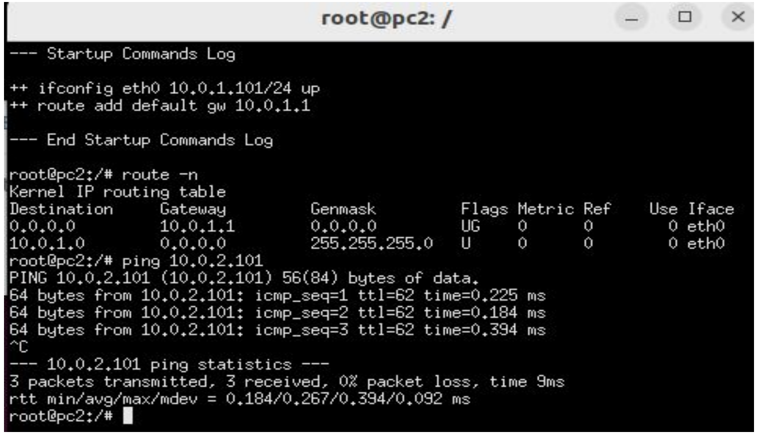
Exercise 5 (solution)



root@pc1: /

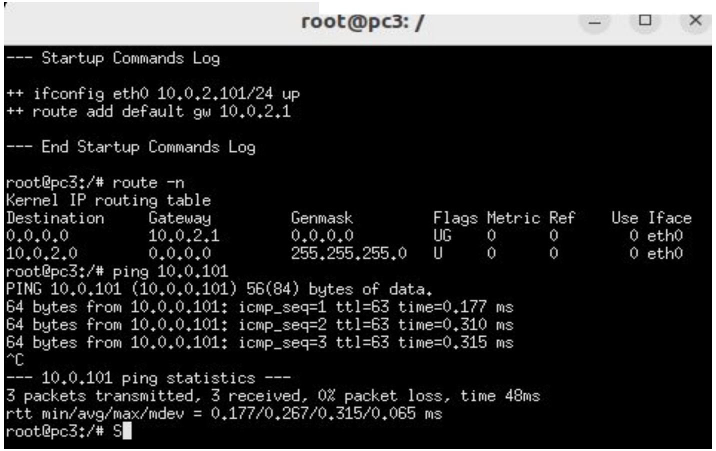
```
root@pc1:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.0.1.0        10.0.0.1        255.255.255.0   UG    0      0        0 eth0
10.0.2.0        10.0.0.2        255.255.255.0   UG    0      0        0 eth0
root@pc1:/# ping 10.0.1.101
PING 10.0.1.101 (10.0.1.101) 56(84) bytes of data.
64 bytes from 10.0.1.101: icmp_seq=1 ttl=63 time=0.303 ms
64 bytes from 10.0.1.101: icmp_seq=2 ttl=63 time=0.291 ms
^C
--- 10.0.1.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 0.291/0.297/0.303/0.006 ms
root@pc1:/# ping 10.0.2.101
PING 10.0.2.101 (10.0.2.101) 56(84) bytes of data.
64 bytes from 10.0.2.101: icmp_seq=1 ttl=63 time=0.201 ms
64 bytes from 10.0.2.101: icmp_seq=2 ttl=63 time=0.153 ms
64 bytes from 10.0.2.101: icmp_seq=3 ttl=63 time=0.208 ms
^C
--- 10.0.2.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 40ms
rtt min/avg/max/mdev = 0.153/0.187/0.208/0.026 ms
root@pc1:/# 
```





root@pc2: /

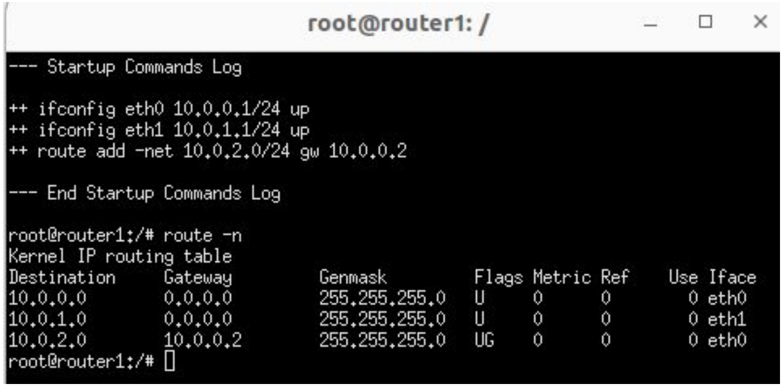
```
--- Startup Commands Log

++ ifconfig eth0 10.0.1.101/24 up
++ route add default gw 10.0.1.1

--- End Startup Commands Log

root@pc2:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.1.1        0.0.0.0         UG    0      0        0 eth0
10.0.1.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
root@pc2:/# ping 10.0.2.101
PING 10.0.2.101 (10.0.2.101) 56(84) bytes of data.
64 bytes from 10.0.2.101: icmp_seq=1 ttl=62 time=0.225 ms
64 bytes from 10.0.2.101: icmp_seq=2 ttl=62 time=0.184 ms
64 bytes from 10.0.2.101: icmp_seq=3 ttl=62 time=0.394 ms
^C
--- 10.0.2.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 9ms
rtt min/avg/max/mdev = 0.184/0.267/0.394/0.092 ms
root@pc2:/# 
```



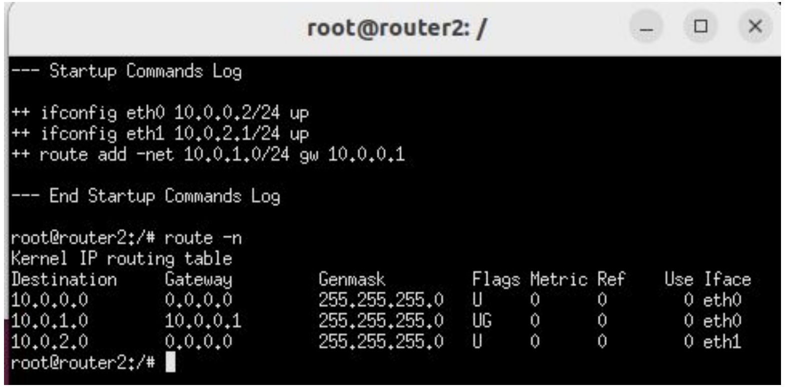
root@pc3: /

```
--- Startup Commands Log

++ ifconfig eth0 10.0.2.101/24 up
++ route add default gw 10.0.2.1

--- End Startup Commands Log

root@pc3:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.1        0.0.0.0         UG    0      0        0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
root@pc3:/# ping 10.0.101
PING 10.0.101 (10.0.0.101) 56(84) bytes of data.
64 bytes from 10.0.0.101: icmp_seq=1 ttl=63 time=0.177 ms
64 bytes from 10.0.0.101: icmp_seq=2 ttl=63 time=0.310 ms
64 bytes from 10.0.0.101: icmp_seq=3 ttl=63 time=0.315 ms
^C
--- 10.0.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 48ms
rtt min/avg/max/mdev = 0.177/0.267/0.315/0.065 ms
root@pc3:/# S
```

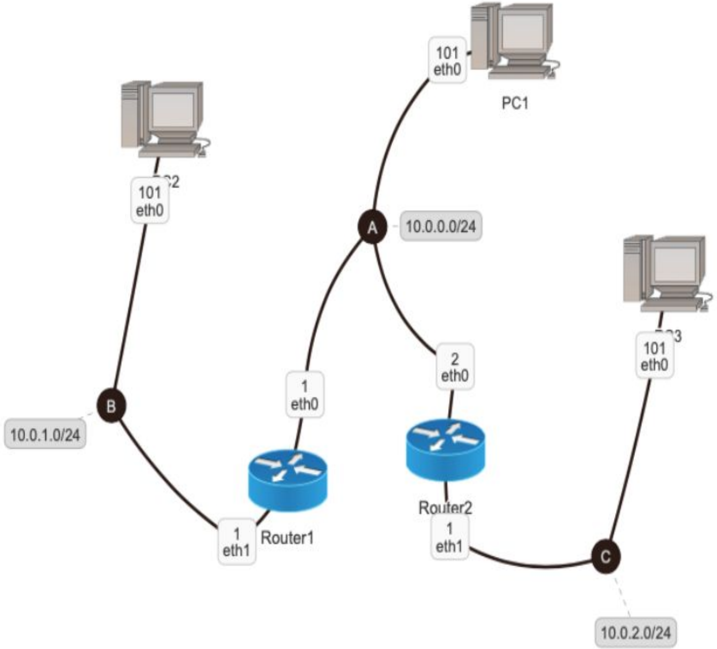
Exercise 5 (solution)



```
--- Startup Commands Log

++ ifconfig eth0 10.0.0.1/24 up
++ ifconfig eth1 10.0.1.1/24 up
++ route add -net 10.0.2.0/24 gw 10.0.0.2

--- End Startup Commands Log

root@router1:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.0.1.0        0.0.0.0         255.255.255.0   U     0      0        0 eth1
10.0.2.0        10.0.0.2        255.255.255.0   UG    0      0        0 eth0
root@router1:/# 
```

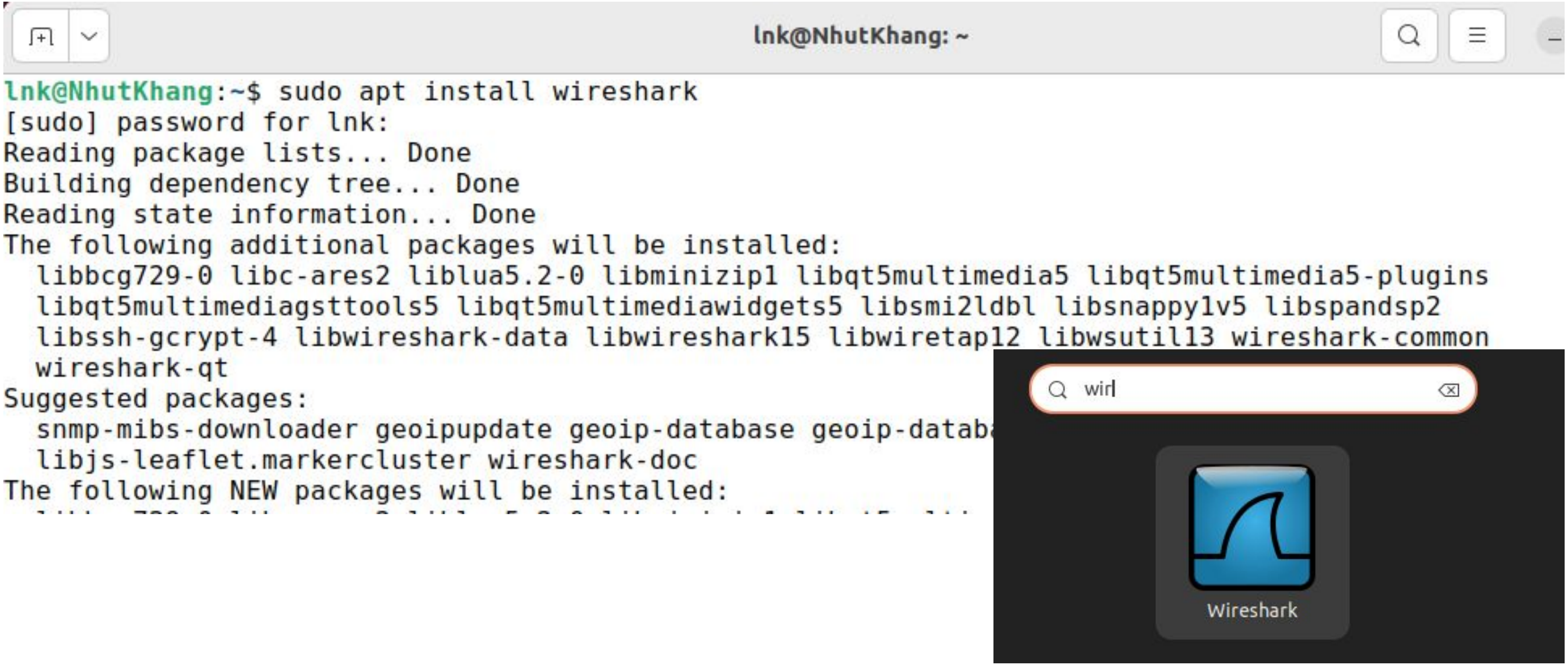


```
--- Startup Commands Log

++ ifconfig eth0 10.0.0.2/24 up
++ ifconfig eth1 10.0.2.1/24 up
++ route add -net 10.0.1.0/24 gw 10.0.0.1

--- End Startup Commands Log

root@router2:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.0.1.0        10.0.0.1        255.255.255.0   UG    0      0        0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 eth1
root@router2:/# 
```



Use Wireshark

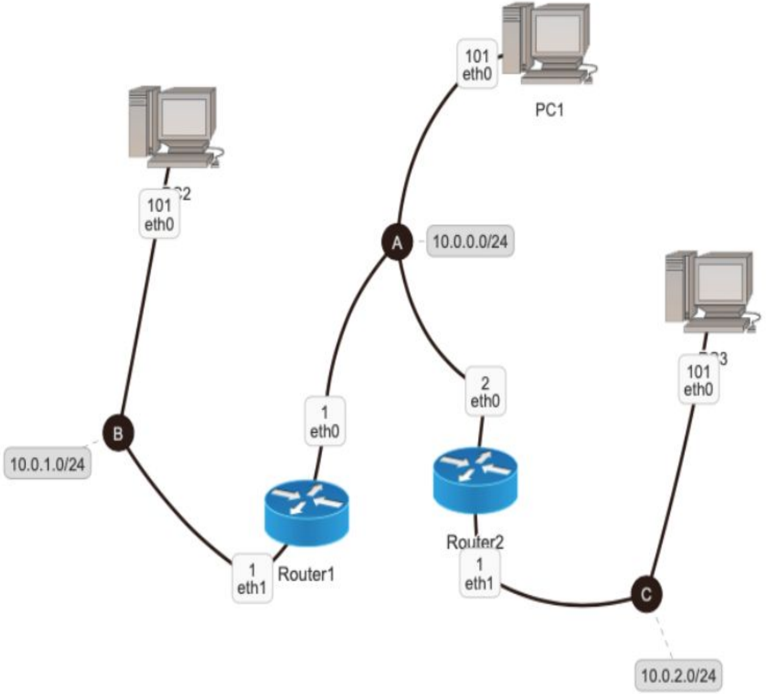
Install Wireshark



```
lnk@NhutKhang:~$ sudo apt install wireshark
[sudo] password for lnk:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbcg729-0 libc-ares2 liblua5.2-0 libminizip1 libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimediagsttools5 libqt5multimediawidgets5 libsmi2ldbl libsnappy1v5 libspandsp2
  libssh-gcrypt-4 libwireshark-data libwireshark15 libwiretap12 libwsutil13 wireshark-common
  wireshark-qt
Suggested packages:
  snmp-mibs-downloader geoipupdate geoip-database geoip-databa
  libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
```

Reuse the network of Exercise 5 :)

Please lstart the network



On pc2, type: `tcpdump -s 1536 -w /hostlab/Ex5_pc2.pcap`

On router1, type: `tcpdump -s 1536 -w /hostlab/BT5_router1.pcap`

On router2, type: `tcpdump -s 1536 -w /hostlab/BT5_router2.pcap`

→ All packets are save in .pcap files which are in the /shared folder

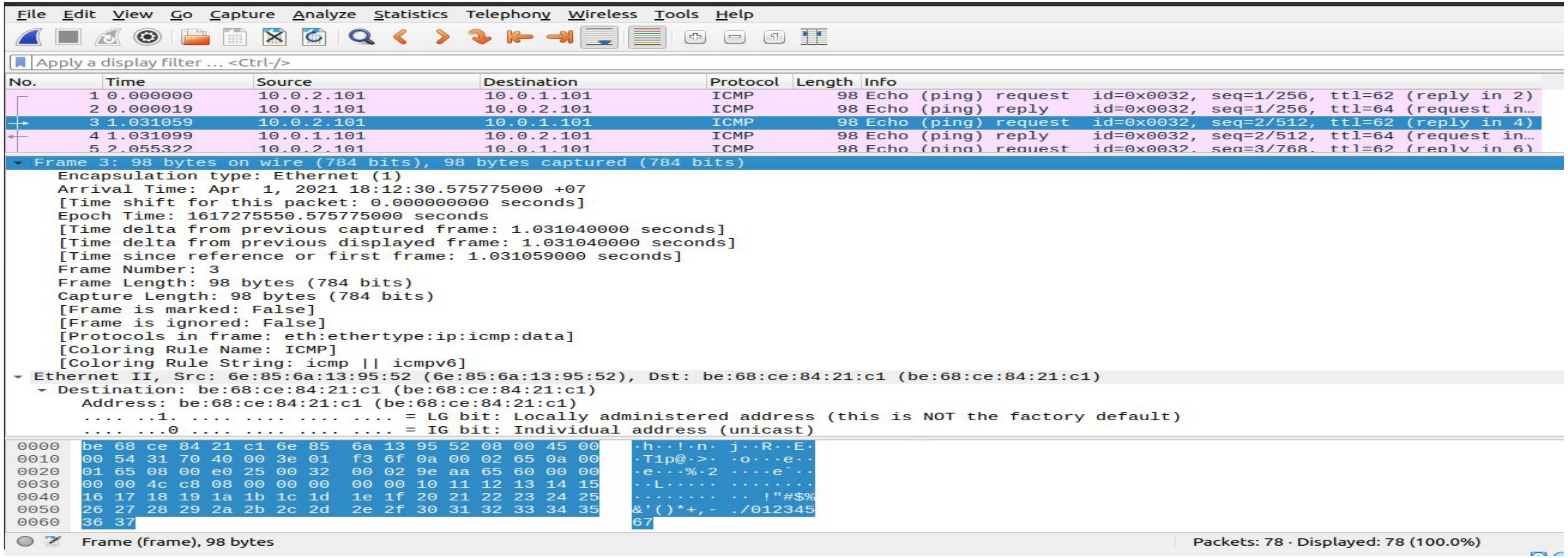
On pc3, send packets to pc2 using the command `ping 10.0.1.101`, wait for about 10 seconds and:

- Stop the `ping` command
- Stop the `tcpdump` on pc2, router1 and router2

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

- Size of frame in bytes?



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

```
No.   Time        Source        Destination   Protocol Length Info
    1 0.000000    10.0.2.101    10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=1/256, ttl=62 (reply in 2)
    2 0.000019    10.0.1.101    10.0.2.101    ICMP         98 Echo (ping) reply    id=0x0032, seq=1/256, ttl=64 (request in…
    3 1.031059    10.0.2.101    10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=2/512, ttl=62 (reply in 4)
    4 1.031099    10.0.1.101    10.0.2.101    ICMP         98 Echo (ping) reply    id=0x0032, seq=2/512, ttl=64 (request in…
    5 2.055322    10.0.2.101    10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=3/768, ttl=62 (reply in 6)
```

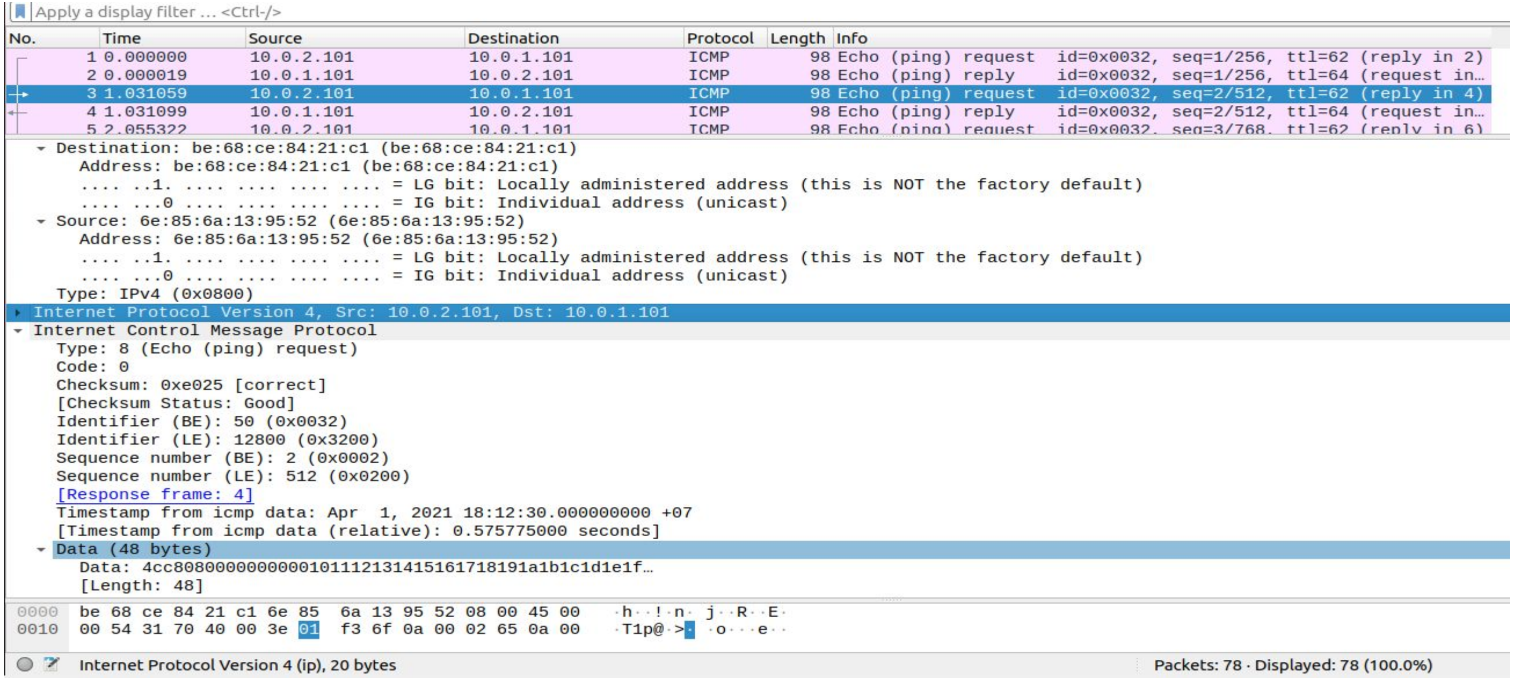
```
▾ Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr  1, 2021 18:12:30.575775000 +07
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1617275550.575775000 seconds
    [Time delta from previous captured frame: 1.031040000 seconds]
    [Time delta from previous displayed frame: 1.031040000 seconds]
    [Time since reference or first frame: 1.031059000 seconds]
    Frame Number: 3
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
▾ Ethernet II, Src: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52), Dst: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
  ▾ Destination: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
      Address: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

```
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```

```
Frame (frame), 98 bytes                                  Packets: 78 · Displayed: 78 (100.0%)
```

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

- Select Header Internet Control Message Protocol → which protocol is using? On which layer of the OSI model does this protocol operate? What is the content of the message? How long is this message in bytes?



```
No.   Time         Source       Destination   Protocol Length Info
    1 0.000000     10.0.2.101   10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=1/256, ttl=62 (reply in 2)
    2 0.000019     10.0.1.101   10.0.2.101    ICMP         98 Echo (ping) reply    id=0x0032, seq=1/256, ttl=64 (request in…
    3 1.031059     10.0.2.101   10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=2/512, ttl=62 (reply in 4)
    4 1.031099     10.0.1.101   10.0.2.101    ICMP         98 Echo (ping) reply    id=0x0032, seq=2/512, ttl=64 (request in…
    5 2.055322     10.0.2.101   10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=3/768, ttl=62 (reply in 6)
```

```
  ▾ Destination: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
      Address: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe025 [correct]
    [Checksum Status: Good]
    Identifier (BE): 50 (0x0032)
    Identifier (LE): 12800 (0x3200)
    Sequence number (BE): 2 (0x0002)
    Sequence number (LE): 512 (0x0200)
    [Response frame: 4]
    Timestamp from icmp data: Apr  1, 2021 18:12:30.000000000 +07
    [Timestamp from icmp data (relative): 0.575775000 seconds]
  ▾ Data (48 bytes)
      Data: 4cc80800000000000101112131415161718191a1b1c1d1e1f…
      [Length: 48]
```

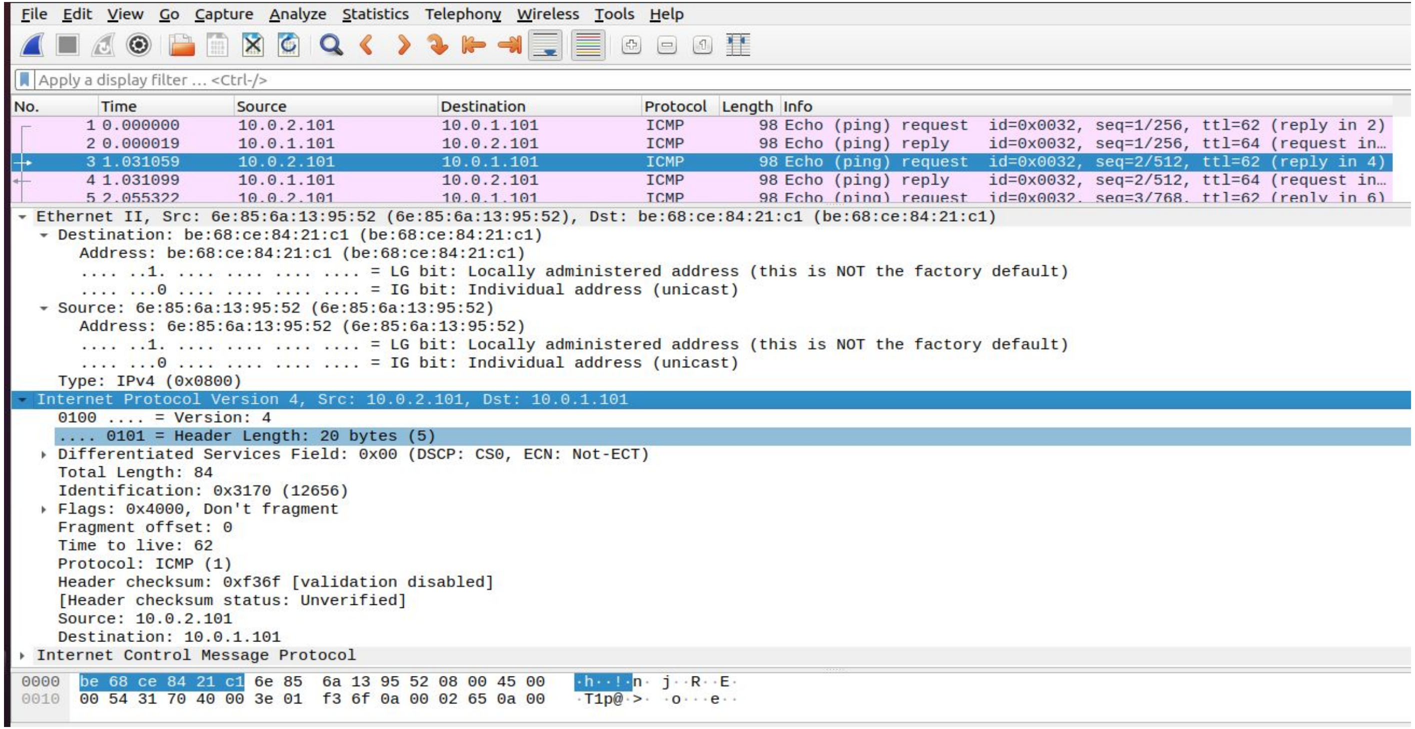
```
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
```

Internet Protocol Version 4 (ip), 20 bytes

Packets: 78 · Displayed: 78 (100.0%)

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

- Select Header Internet Protocol Version 4 → what are the IP addresses of the source and destination hosts?



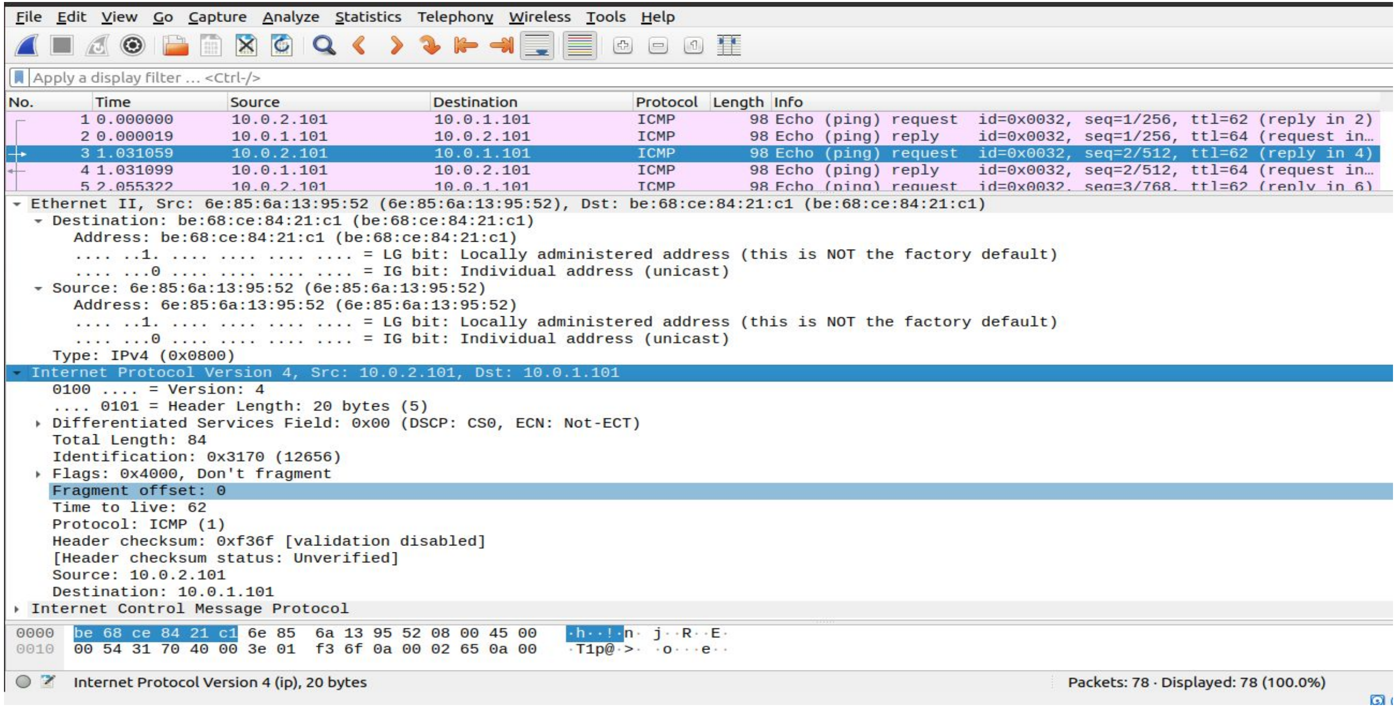
```
No.   Time        Source       Destination   Protocol Length Info
    1 0.000000    10.0.2.101   10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=1/256, ttl=62 (reply in 2)
    2 0.000019    10.0.1.101   10.0.2.101    ICMP         98 Echo (ping) reply    id=0x0032, seq=1/256, ttl=64 (request in…
    3 1.031059    10.0.2.101   10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=2/512, ttl=62 (reply in 4)
    4 1.031099    10.0.1.101   10.0.2.101    ICMP         98 Echo (ping) reply    id=0x0032, seq=2/512, ttl=64 (request in…
    5 2.055322    10.0.2.101   10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=3/768, ttl=62 (reply in 6)
```

```
▾ Ethernet II, Src: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52), Dst: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
  ▾ Destination: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
      Address: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x3170 (12656)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 62
    Protocol: ICMP (1)
    Header checksum: 0xf36f [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.101
    Destination: 10.0.1.101
▸ Internet Control Message Protocol
```

```
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
```

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

- Select Header Internet Protocol Version 4 → What is the length of the IP packet header? What fields does the Header include? How long is each field (Bytes)


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

```
No.   Time        Source       Destination  Protocol Length Info
    1 0.000000    10.0.2.101   10.0.1.101   ICMP       98 Echo (ping) request  id=0x0032, seq=1/256, ttl=62 (reply in 2)
    2 0.000019    10.0.1.101   10.0.2.101   ICMP       98 Echo (ping) reply    id=0x0032, seq=1/256, ttl=64 (request in…
    3 1.031059    10.0.2.101   10.0.1.101   ICMP       98 Echo (ping) request  id=0x0032, seq=2/512, ttl=62 (reply in 4)
    4 1.031099    10.0.1.101   10.0.2.101   ICMP       98 Echo (ping) reply    id=0x0032, seq=2/512, ttl=64 (request in…
    5 2.055322    10.0.2.101   10.0.1.101   ICMP       98 Echo (ping) request  id=0x0032, seq=3/768, ttl=62 (reply in 6)
```

```
Ethernet II, Src: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52), Dst: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
  Destination: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
    Address: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
    Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x3170 (12656)
  Flags: 0x4000, Don't fragment
  Fragment offset: 0
  Time to live: 62
  Protocol: ICMP (1)
  Header checksum: 0xf36f [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.0.2.101
  Destination: 10.0.1.101
Internet Control Message Protocol
```

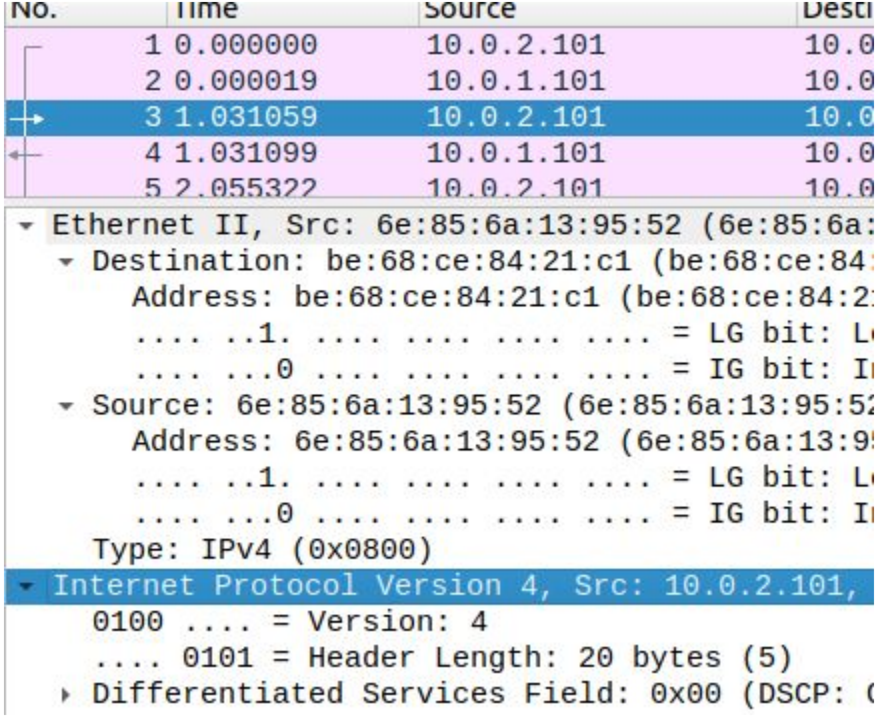
```
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
```

Internet Protocol Version 4 (ip), 20 bytes

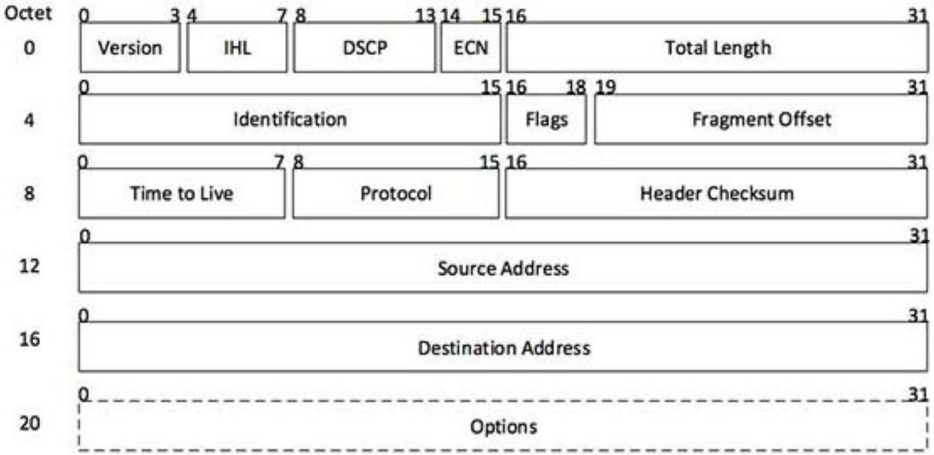
Packets: 78 · Displayed: 78 (100.0%)

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

- Select Header Internet Protocol Version 4 → What is the length of the IP packet header? What fields does the Header include? How long is each field (Bytes)



```
No.        Time          Source          Desti
         1 0.000000      10.0.2.101      10.0
         2 0.000019      10.0.1.101      10.0
         3 1.031059      10.0.2.101      10.0
         4 1.031099      10.0.1.101      10.0
         5 2.055322      10.0.2.101      10.0
▾ Ethernet II, Src: 6e:85:6a:13:95:52 (6e:85:6a:
  ▾ Destination: be:68:ce:84:21:c1 (be:68:ce:84
      Address: be:68:ce:84:21:c1 (be:68:ce:84:2
      .... ..1. .... .... .... .... = LG bit: L
      .... ...0 .... .... .... .... = IG bit: I
  ▾ Source: 6e:85:6a:13:95:52 (6e:85:6a:13:95:5
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:9
      .... ..1. .... .... .... .... = LG bit: L
      .... ...0 .... .... .... .... = IG bit: I
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.101,
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: (
```



Octet

0: Version (0–3), IHL (4–7), DSCP (8–13), ECN (14–15), Total Length (16–31)

4: Identification (0–15), Flags (16–18), Fragment Offset (19–31)

8: Time to Live (0–7), Protocol (8–15), Header Checksum (16–31)

12: Source Address (0–31)

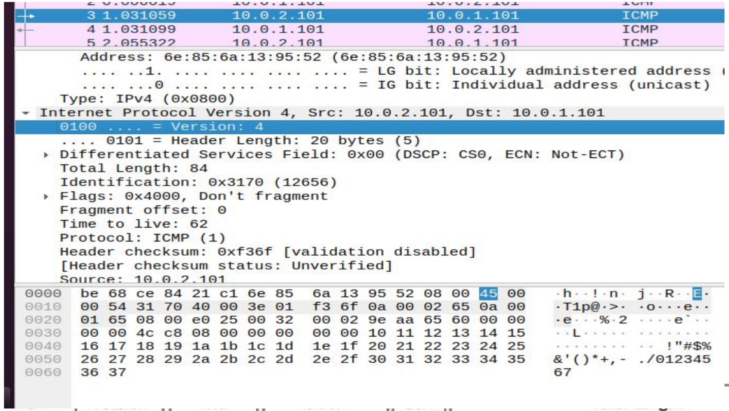
16: Destination Address (0–31)

20: Options (0–31)

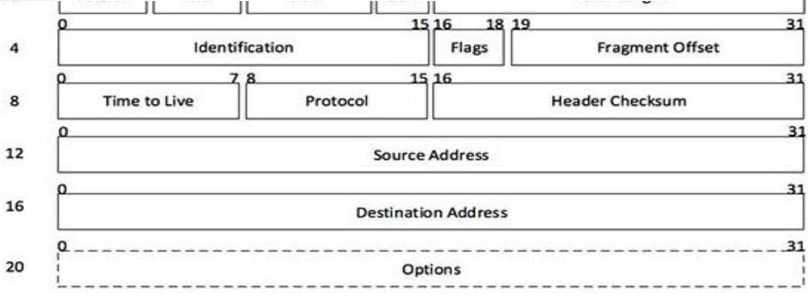
[Image: IP Header]

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

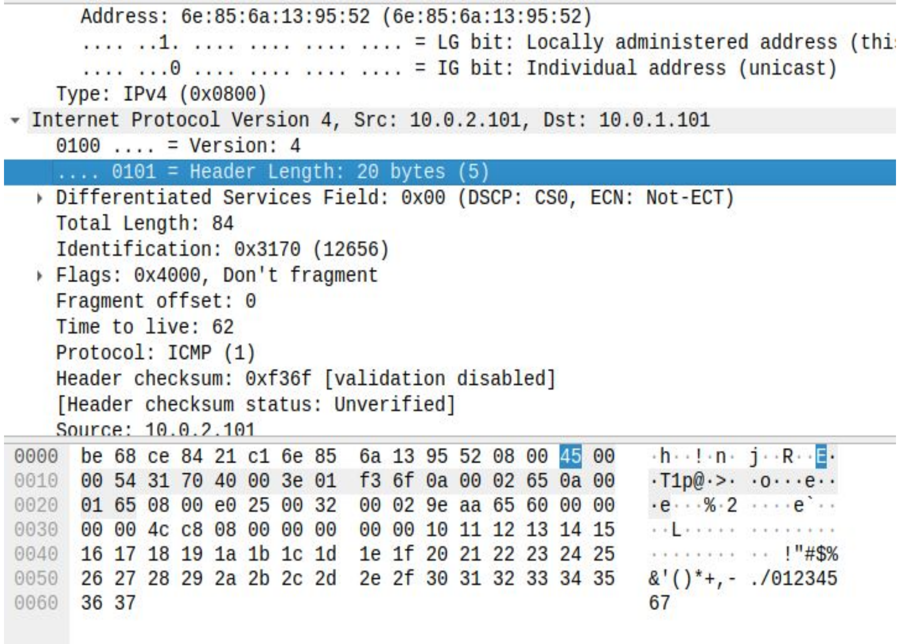
- Select Header Internet Protocol Version 4 → What is the length of the IP packet header? What fields does the Header include? How long is each field (Bytes)



```
3 1.031059   10.0.2.101   10.0.1.101   ICMP
4 1.031099   10.0.1.101   10.0.2.101   ICMP
5 2.055322   10.0.2.101   10.0.1.101   ICMP
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 84
   Identification: 0x3170 (12656)
 ▸ Flags: 0x4000, Don't fragment
   Fragment offset: 0
   Time to live: 62
   Protocol: ICMP (1)
   Header checksum: 0xf36f [validation disabled]
   [Header checksum status: Unverified]
   Source: 10.0.2.101
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```



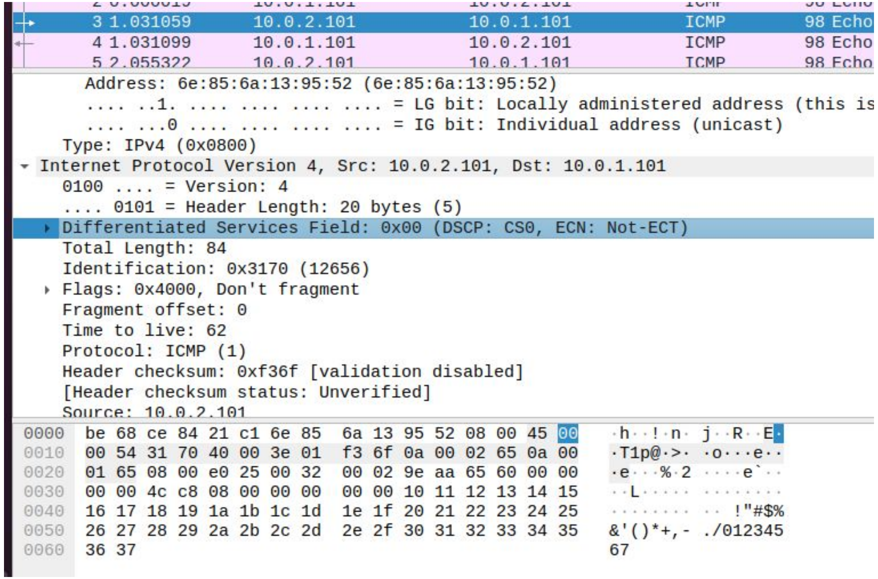
[Image: IP Header]



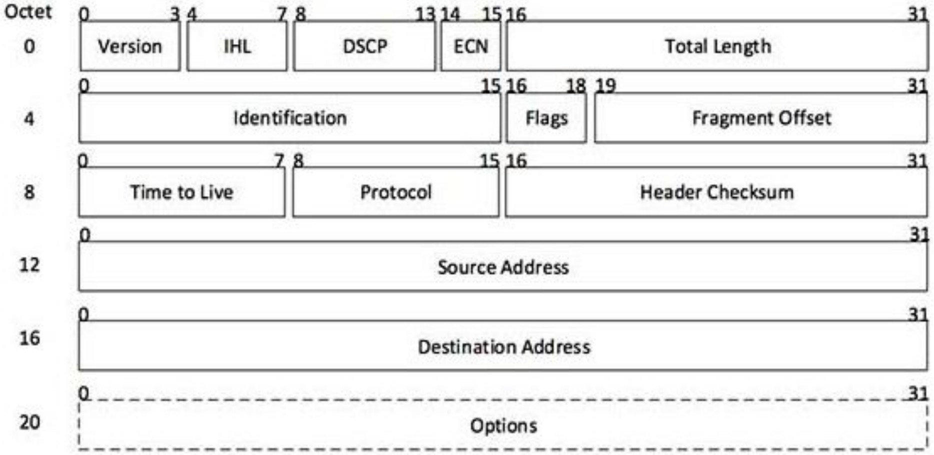
```
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (thi
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 84
   Identification: 0x3170 (12656)
 ▸ Flags: 0x4000, Don't fragment
   Fragment offset: 0
   Time to live: 62
   Protocol: ICMP (1)
   Header checksum: 0xf36f [validation disabled]
   [Header checksum status: Unverified]
   Source: 10.0.2.101
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

- Select Header Internet Protocol Version 4 → What is the length of the IP packet header? What fields does the Header include? How long is each field (Bytes)



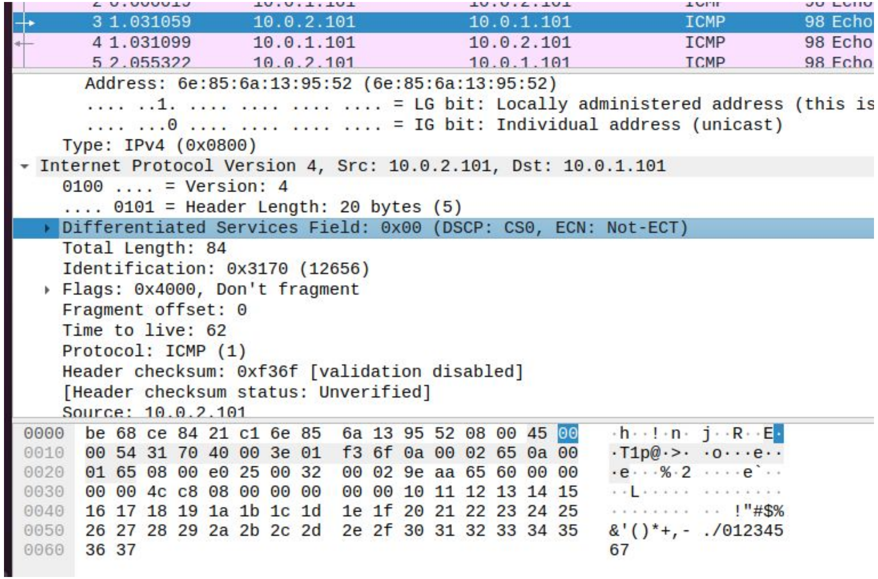
```
     2 0.000015      10.0.1.101         10.0.2.101         ICMP       98 Echo
     3 1.031059      10.0.2.101         10.0.1.101         ICMP       98 Echo
     4 1.031099      10.0.1.101         10.0.2.101         ICMP       98 Echo
     5 2.055322      10.0.2.101         10.0.1.101         ICMP       98 Echo
        Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x3170 (12656)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 62
    Protocol: ICMP (1)
    Header checksum: 0xf36f [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.101

0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```



[Image: IP Header]

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

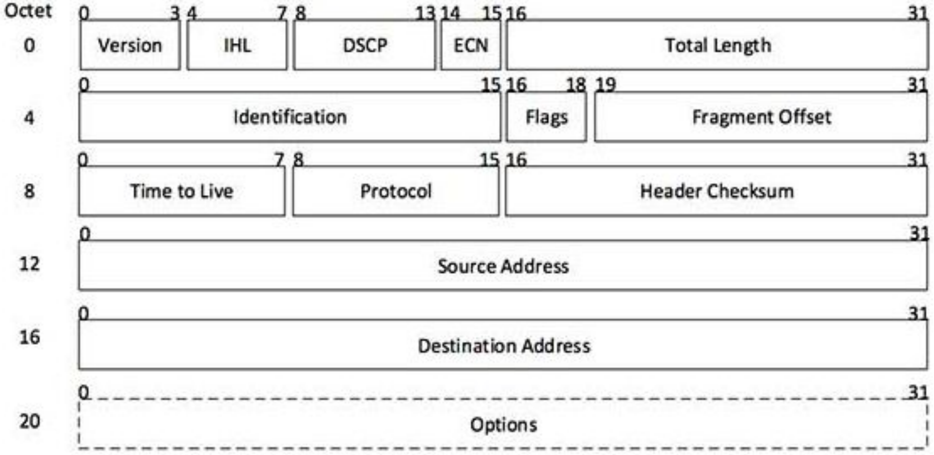
- Select Header Internet Protocol Version 4 → What is the length of the IP packet header? What fields does the Header include? How long is each field (Bytes)



```
    3 1.031059     10.0.2.101        10.0.1.101        ICMP     98 Echo
    4 1.031099     10.0.1.101        10.0.2.101        ICMP     98 Echo
    5 2.055322     10.0.2.101        10.0.1.101        ICMP     98 Echo
```

```
        Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 84
      Identification: 0x3170 (12656)
    Flags: 0x4000, Don't fragment
      Fragment offset: 0
      Time to live: 62
      Protocol: ICMP (1)
      Header checksum: 0xf36f [validation disabled]
      [Header checksum status: Unverified]
      Source: 10.0.2.101
```

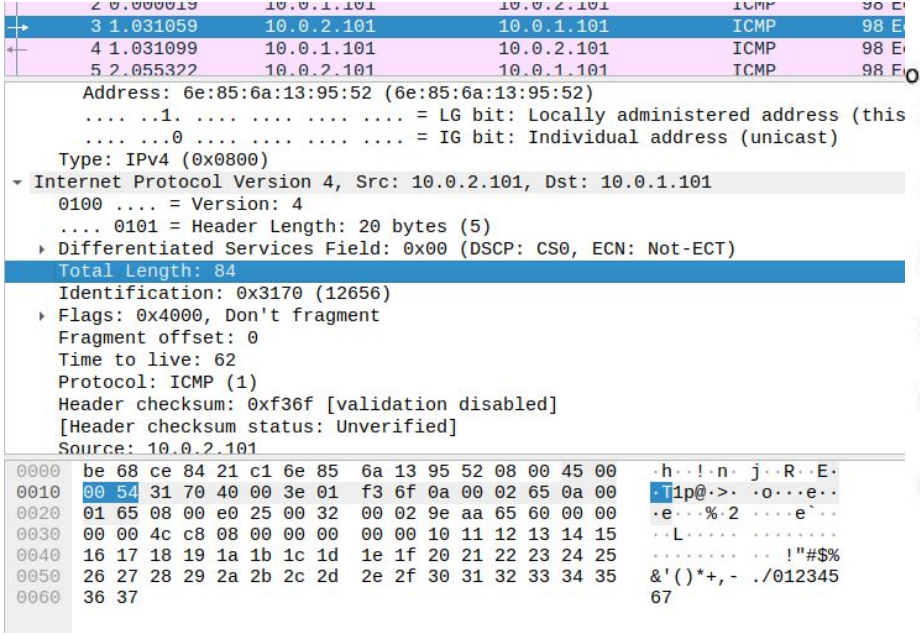
```
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```



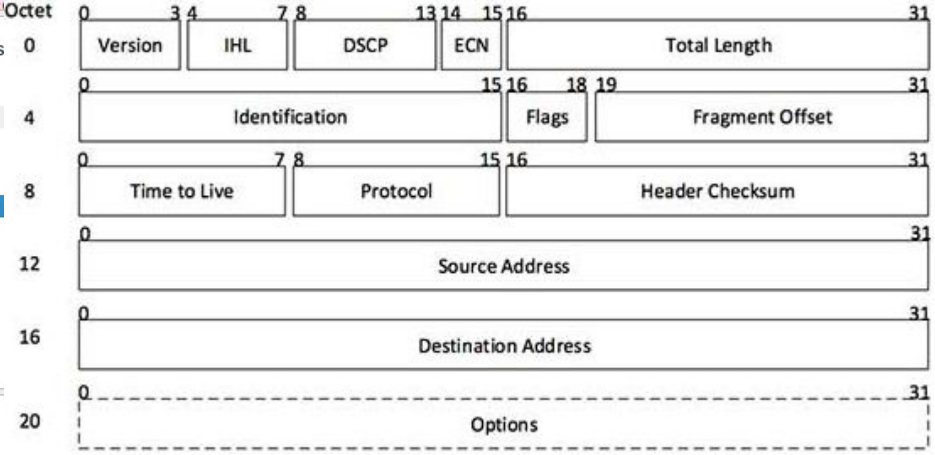
[Image: IP Header]

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

- Select Header Internet Protocol Version 4 → What is the length of the IP packet header? What fields does the Header include? How long is each field (Bytes)



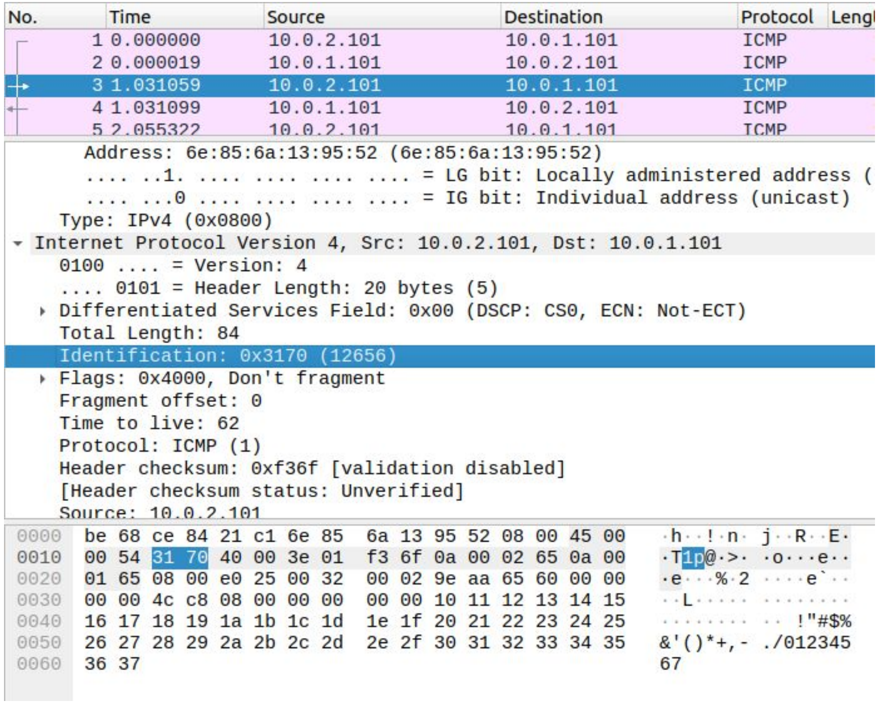
```
  2 0.000019    10.0.1.101     10.0.2.101     ICMP    98 E
  3 1.031059    10.0.2.101     10.0.1.101     ICMP    98 E
  4 1.031099    10.0.1.101     10.0.2.101     ICMP    98 E
  5 2.055322    10.0.2.101     10.0.1.101     ICMP    98 E
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x3170 (12656)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 62
    Protocol: ICMP (1)
    Header checksum: 0xf36f [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.101

0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```



[Image: IP Header]

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

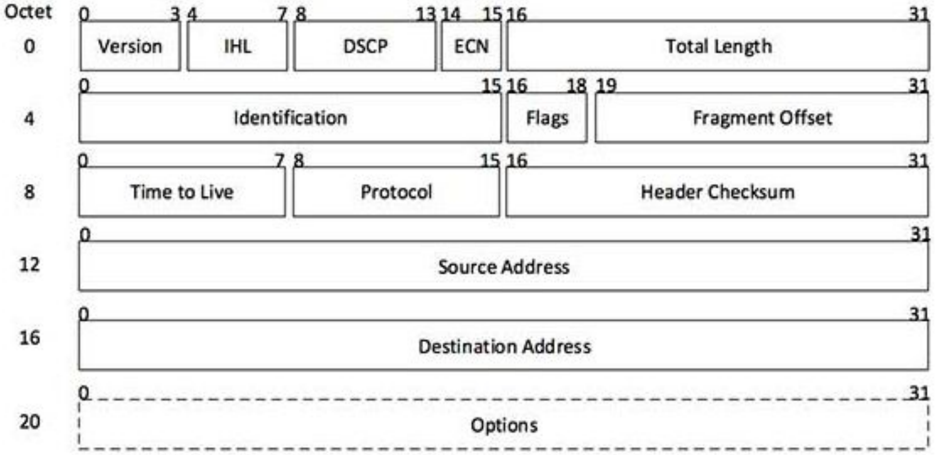
- Select Header Internet Protocol Version 4 → What is the length of the IP packet header? What fields does the Header include? How long is each field (Bytes)



```
No.     Time        Source        Destination   Protocol  Leng
  1 0.000000    10.0.2.101    10.0.1.101    ICMP
  2 0.000019    10.0.1.101    10.0.2.101    ICMP
  3 1.031059    10.0.2.101    10.0.1.101    ICMP
  4 1.031099    10.0.1.101    10.0.2.101    ICMP
  5 2.055322    10.0.2.101    10.0.1.101    ICMP
```

```
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x3170 (12656)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 62
    Protocol: ICMP (1)
    Header checksum: 0xf36f [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.101
```

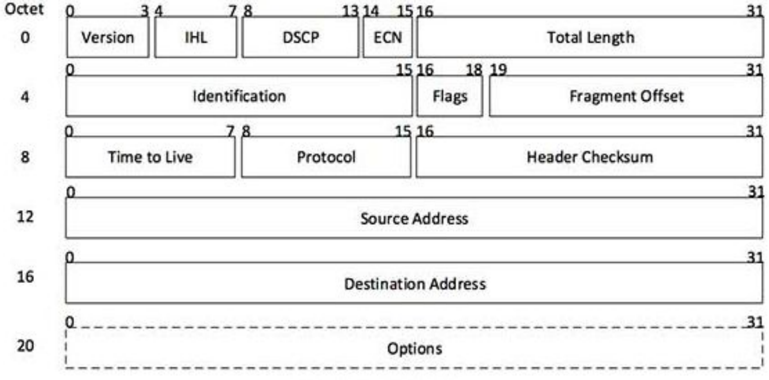
```
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```



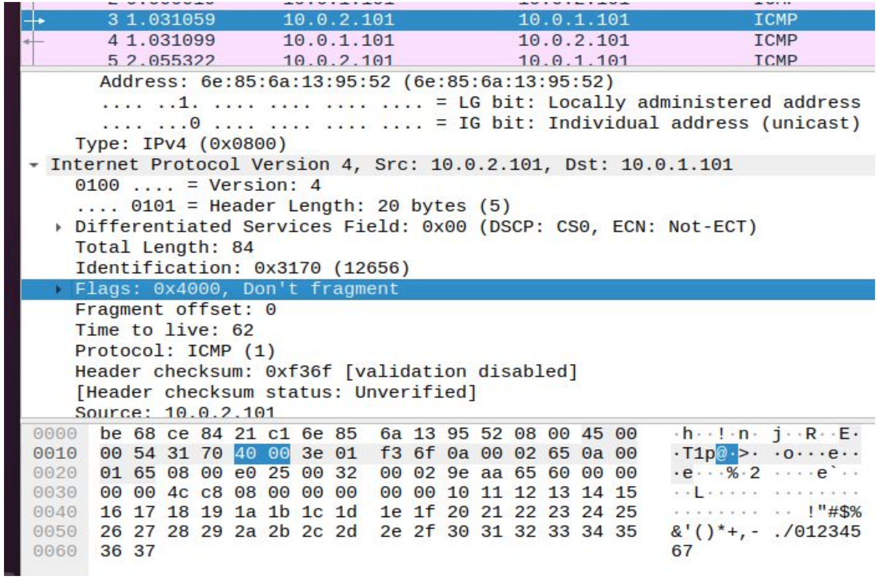
[Image: IP Header]

On the Ubuntu, open Ex5_pc2.pcap using Wireshark,
following questions:

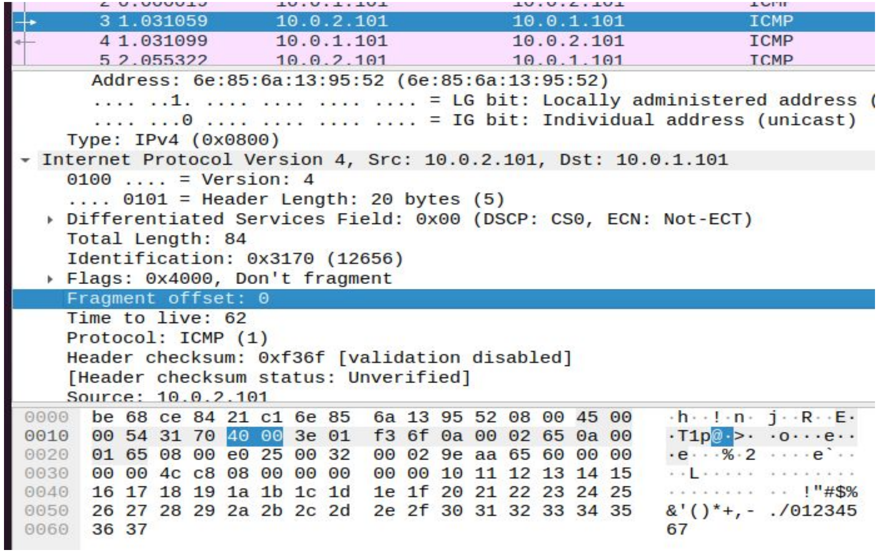
- Select Header Internet Protocol Version 4 → Wh
  header? What fields does the Header include? H



[Image: IP Header]



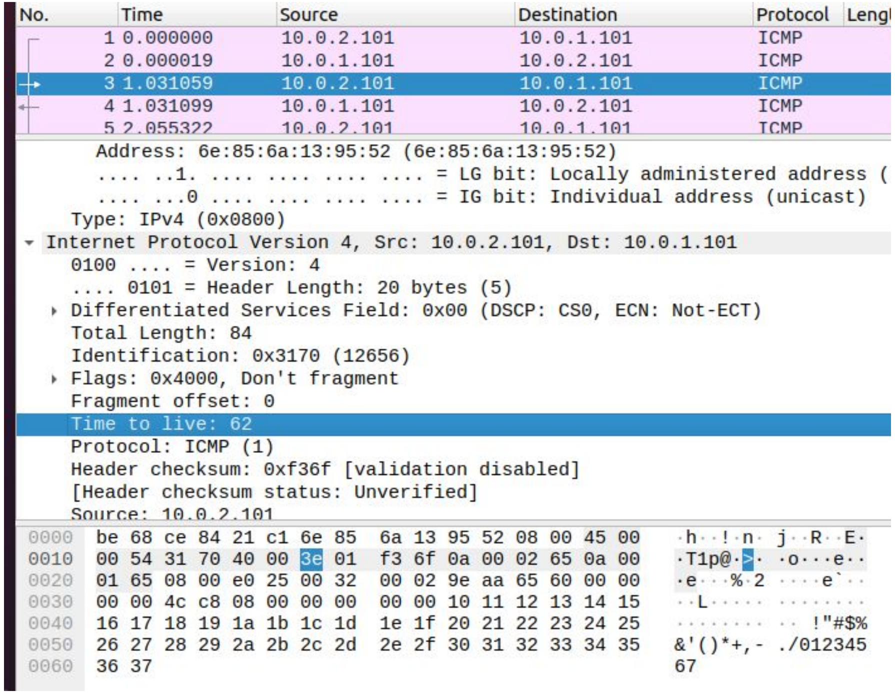
```
  3 1.031059    10.0.2.101        10.0.1.101        ICMP
  4 1.031099    10.0.1.101        10.0.2.101        ICMP
  5 2.055322    10.0.2.101        10.0.1.101        ICMP
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x3170 (12656)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 62
    Protocol: ICMP (1)
    Header checksum: 0xf36f [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.101
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```



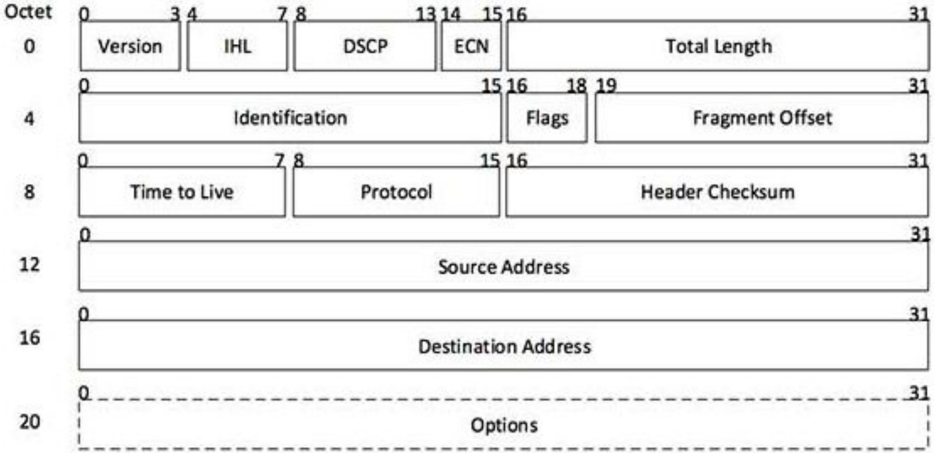
```
  3 1.031059    10.0.2.101        10.0.1.101        ICMP
  4 1.031099    10.0.1.101        10.0.2.101        ICMP
  5 2.055322    10.0.2.101        10.0.1.101        ICMP
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x3170 (12656)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 62
    Protocol: ICMP (1)
    Header checksum: 0xf36f [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.101
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

- Select Header Internet Protocol Version 4 → What is the length of the IP packet header? What fields does the Header include? How long is each field (Bytes)



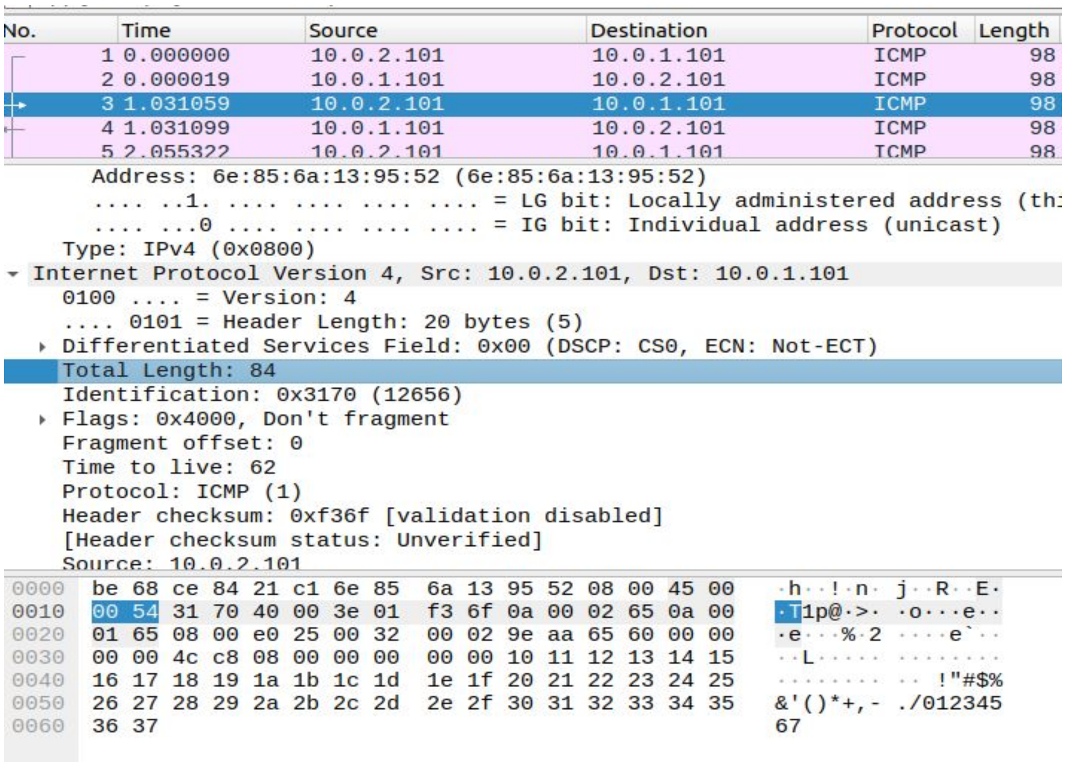
```
No.   Time        Source         Destination    Protocol  Lengt
  1 0.000000    10.0.2.101     10.0.1.101     ICMP
  2 0.000019    10.0.1.101     10.0.2.101     ICMP
  3 1.031059    10.0.2.101     10.0.1.101     ICMP
  4 1.031099    10.0.1.101     10.0.2.101     ICMP
  5 2.055322    10.0.2.101     10.0.1.101     ICMP
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
 ▾ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x3170 (12656)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 62
    Protocol: ICMP (1)
    Header checksum: 0xf36f [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.101
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```



[Image: IP Header]

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

- Select Header Internet Protocol Version 4 → What is the length of the Total Length field (Bytes).



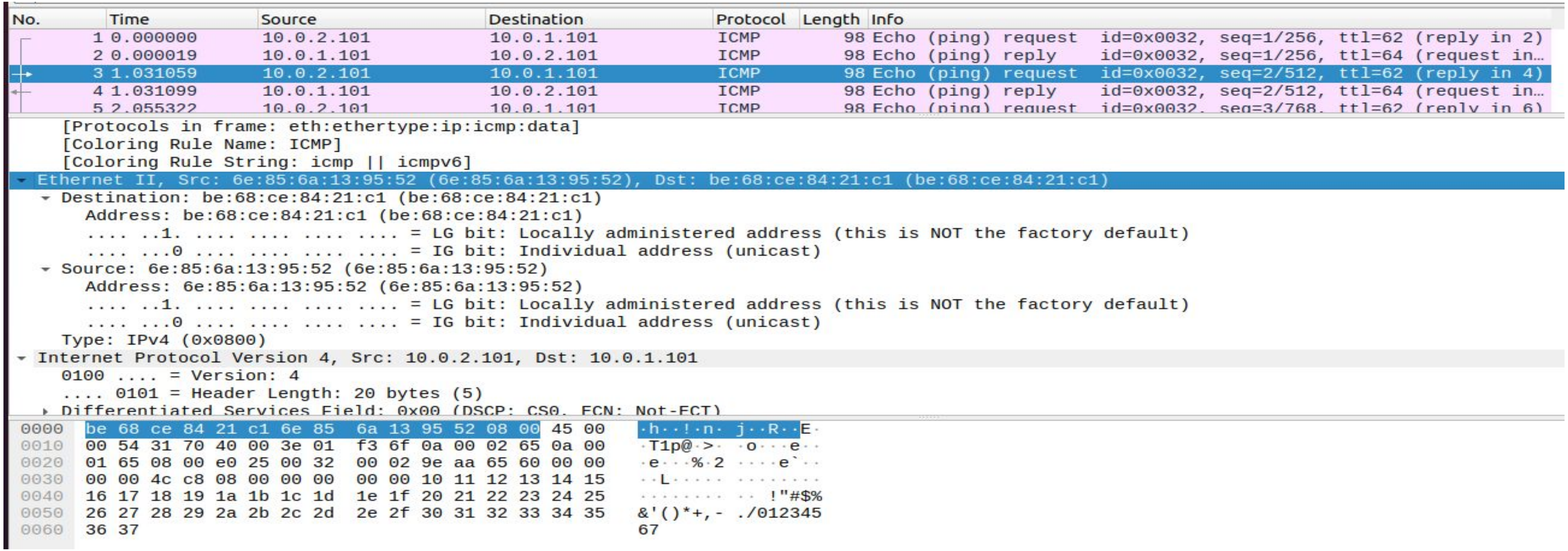
```
No.       Time             Source              Destination          Protocol  Length
        1 0.000000         10.0.2.101          10.0.1.101           ICMP          98
        2 0.000019         10.0.1.101          10.0.2.101           ICMP          98
        3 1.031059         10.0.2.101          10.0.1.101           ICMP          98
        4 1.031099         10.0.1.101          10.0.2.101           ICMP          98
        5 2.055322         10.0.2.101          10.0.1.101           ICMP          98
```

```
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (th
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x3170 (12656)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 62
    Protocol: ICMP (1)
    Header checksum: 0xf36f [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.101
```

```
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

- Select Header Ethernet II → What are the MAC addresses of the source and the destination hosts?



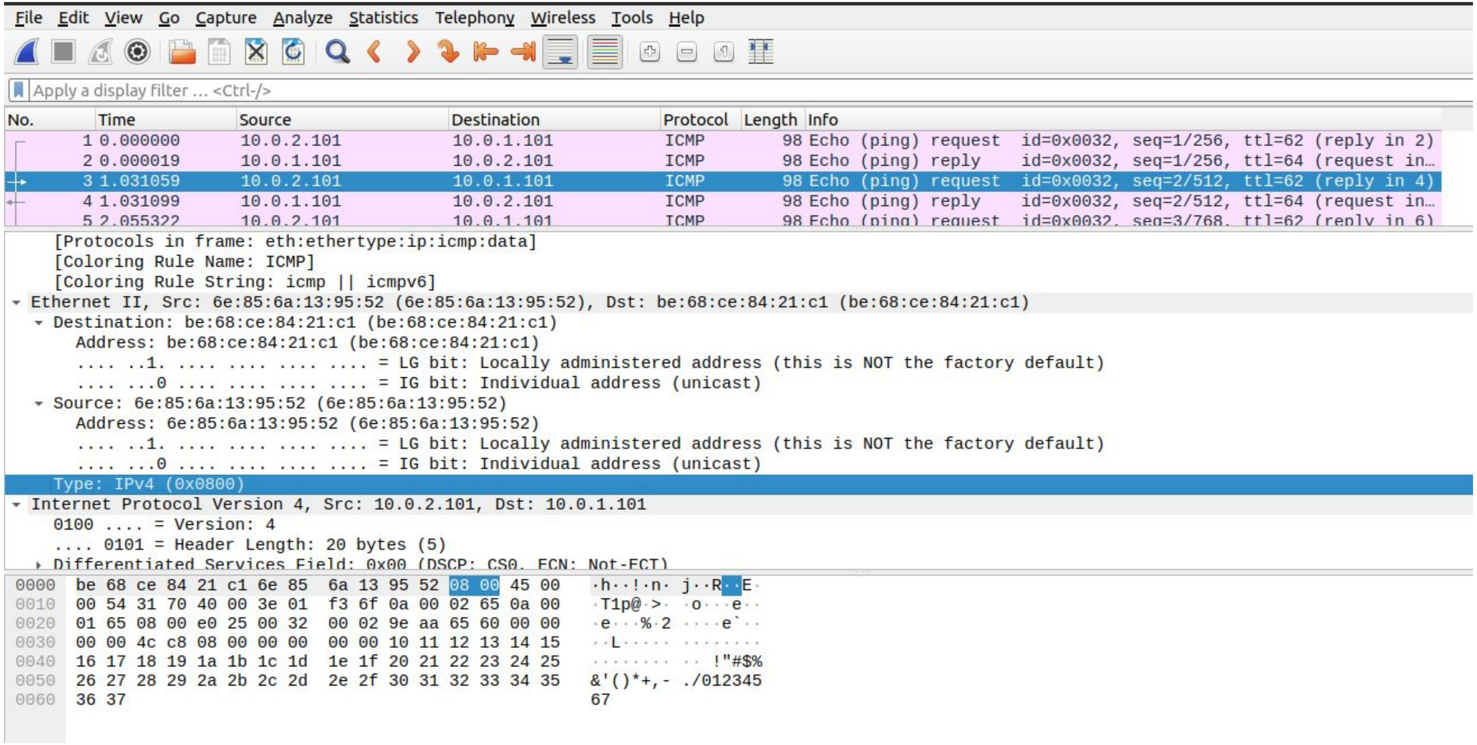
```
No.     Time        Source        Destination   Protocol Length Info
      1 0.000000    10.0.2.101    10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=1/256, ttl=62 (reply in 2)
      2 0.000019    10.0.1.101    10.0.2.101    ICMP         98 Echo (ping) reply    id=0x0032, seq=1/256, ttl=64 (request in…
      3 1.031059    10.0.2.101    10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=2/512, ttl=62 (reply in 4)
      4 1.031099    10.0.1.101    10.0.2.101    ICMP         98 Echo (ping) reply    id=0x0032, seq=2/512, ttl=64 (request in…
      5 2.055322    10.0.2.101    10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=3/768, ttl=62 (reply in 6)
```

```
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
▾ Ethernet II, Src: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52), Dst: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
  ▾ Destination: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
      Address: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

```
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```

On the Ubuntu, open Ex5_pc2.pcap using Wireshark, select the frame #3 and answer the following questions:

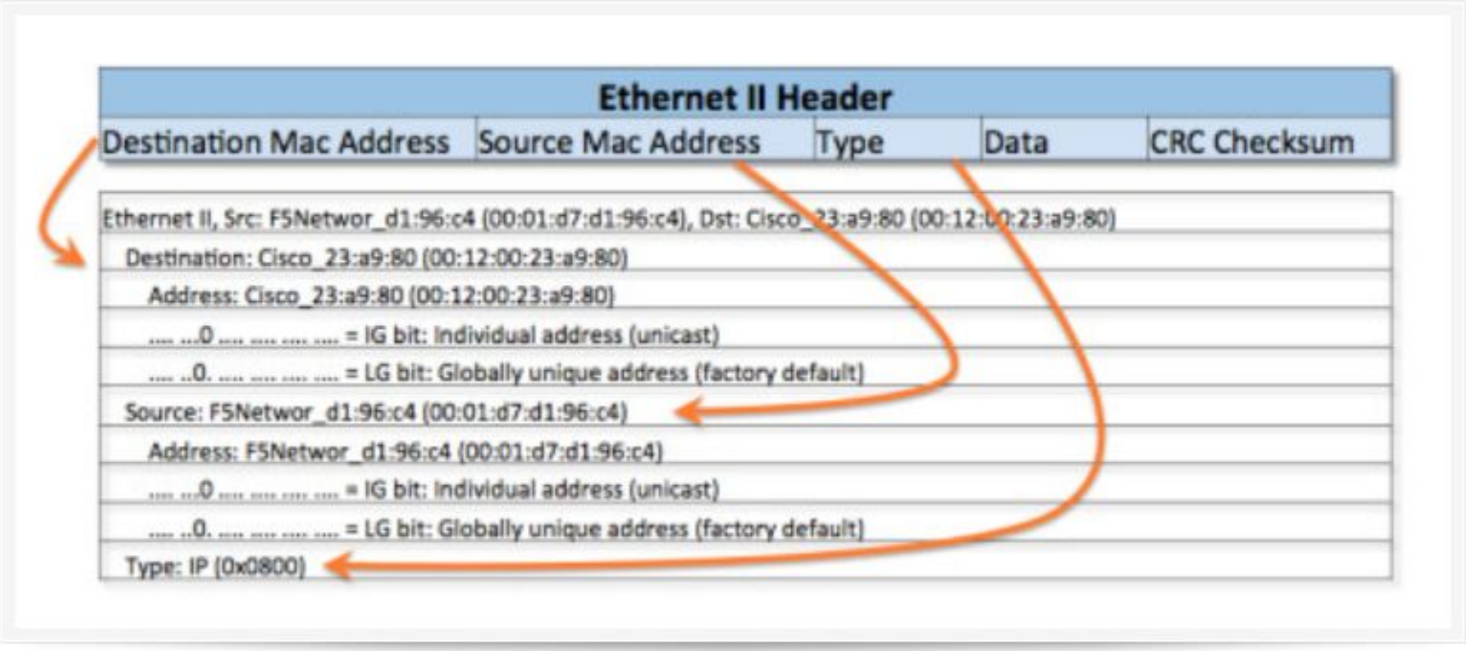
- Select Header Ethernet II → What is the Type value?



```
No.     Time       Source        Destination   Protocol Length Info
      1 0.000000   10.0.2.101    10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=1/256, ttl=62 (reply in 2)
      2 0.000019   10.0.1.101    10.0.2.101    ICMP         98 Echo (ping) reply    id=0x0032, seq=1/256, ttl=64 (request in…
      3 1.031059   10.0.2.101    10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=2/512, ttl=62 (reply in 4)
      4 1.031099   10.0.1.101    10.0.2.101    ICMP         98 Echo (ping) reply    id=0x0032, seq=2/512, ttl=64 (request in…
      5 2.055322   10.0.2.101    10.0.1.101    ICMP         98 Echo (ping) request  id=0x0032, seq=3/768, ttl=62 (reply in 6)
```

```
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
▾ Ethernet II, Src: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52), Dst: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
  ▾ Destination: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
      Address: be:68:ce:84:21:c1 (be:68:ce:84:21:c1)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      Address: 6e:85:6a:13:95:52 (6e:85:6a:13:95:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

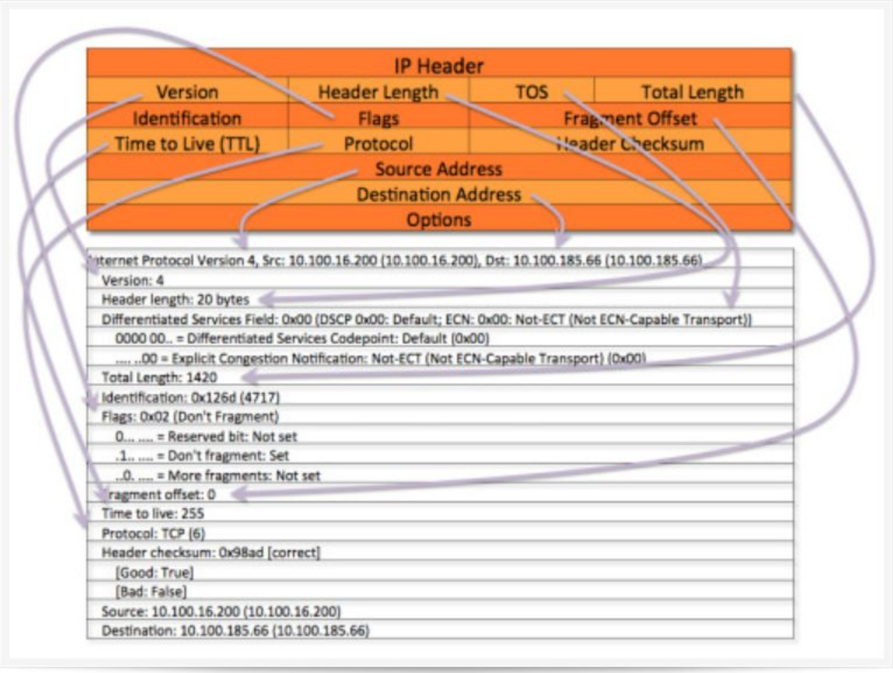
```
0000  be 68 ce 84 21 c1 6e 85  6a 13 95 52 08 00 45 00   ·h··!·n· j··R··E·
0010  00 54 31 70 40 00 3e 01  f3 6f 0a 00 02 65 0a 00   ·T1p@·>· ·o···e··
0020  01 65 08 00 e0 25 00 32  00 02 9e aa 65 60 00 00   ·e···%·2 ····e`··
0030  00 00 4c c8 08 00 00 00  00 00 10 11 12 13 14 15   ··L····· ········
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
```



Ethernet II Header				
Destination Mac Address	Source Mac Address	Type	Data	CRC Checksum

```
Ethernet II, Src: F5Networ_d1:96:c4 (00:01:d7:d1:96:c4), Dst: Cisco_23:a9:80 (00:12:00:23:a9:80)
  Destination: Cisco_23:a9:80 (00:12:00:23:a9:80)
    Address: Cisco_23:a9:80 (00:12:00:23:a9:80)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  Source: F5Networ_d1:96:c4 (00:01:d7:d1:96:c4)
    Address: F5Networ_d1:96:c4 (00:01:d7:d1:96:c4)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  Type: IP (0x0800)
```

Figure 3. Ethernet II (Layer 2) header along with the Wireshark



IP Header			
Version	Header Length	TOS	Total Length
Identification	Flags	Fragment Offset	
Time to Live (TTL)	Protocol	Header Checksum	
Source Address			
Destination Address			
Options			

```
Internet Protocol Version 4, Src: 10.100.16.200 (10.100.16.200), Dst: 10.100.185.66 (10.100.185.66)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 1420
  Identification: 0x126d (4717)
  Flags: 0x02 (Don't Fragment)
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 255
  Protocol: TCP (6)
  Header checksum: 0x98ad [correct]
    [Good: True]
    [Bad: False]
  Source: 10.100.16.200 (10.100.16.200)
  Destination: 10.100.185.66 (10.100.185.66)
```

Figure 4. IP Header (Layer-3)

http://networkstatic.net/what-are-ethernet-ip-and-tcp-headers-in-wireshark-captures/