COMPUTER NETWORKS

LAB – 1

Name: Naga Tharun Makkena

Roll No: SE20UCSE105

Section: CSE-2

1. Wireshark_Intro_v7.0 lab sheet

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

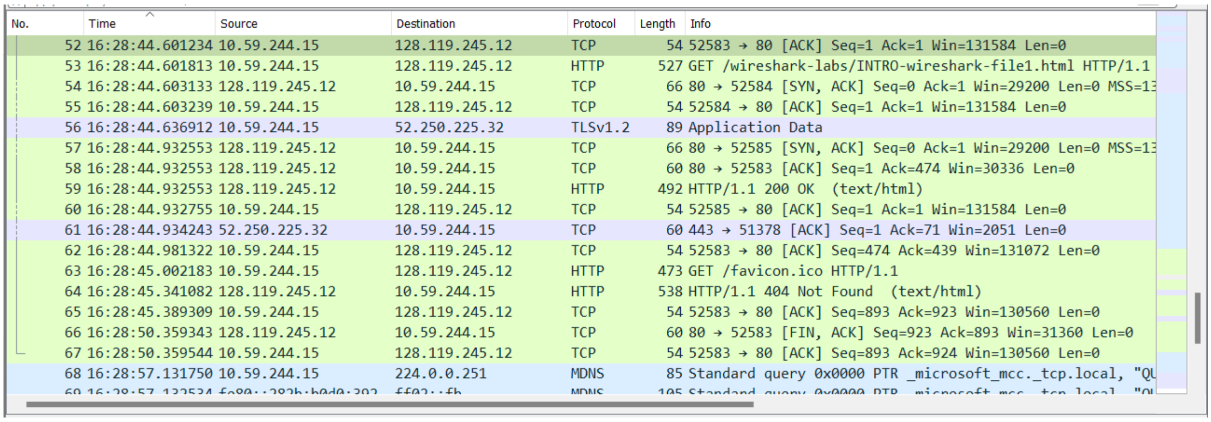
Ans: TCP

HTTP

TLSv1.2

DNS

MDNS



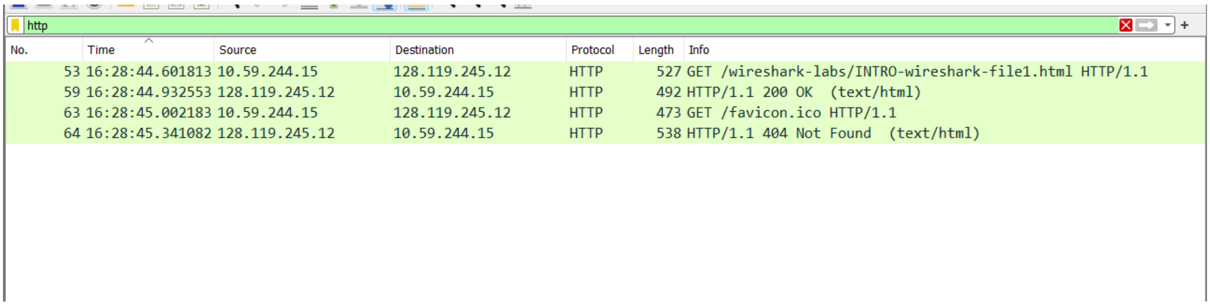
No.	Time	Source	Destination	Protocol	Length	Info
52	16:28:44.601234	10.59.244.15	128.119.245.12	TCP	54	52583 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
53	16:28:44.601813	10.59.244.15	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
54	16:28:44.603133	128.119.245.12	10.59.244.15	TCP	66	80 → 52584 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=13
55	16:28:44.603239	10.59.244.15	128.119.245.12	TCP	54	52584 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
56	16:28:44.636912	10.59.244.15	52.250.225.32	TLSv1.2	89	Application Data
57	16:28:44.932553	128.119.245.12	10.59.244.15	TCP	66	80 → 52585 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=13
58	16:28:44.932553	128.119.245.12	10.59.244.15	TCP	60	80 → 52583 [ACK] Seq=1 Ack=474 Win=30336 Len=0
59	16:28:44.932553	128.119.245.12	10.59.244.15	HTTP	492	HTTP/1.1 200 OK (text/html)
60	16:28:44.932755	10.59.244.15	128.119.245.12	TCP	54	52585 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
61	16:28:44.934243	52.250.225.32	10.59.244.15	TCP	60	443 → 51378 [ACK] Seq=1 Ack=71 Win=2051 Len=0
62	16:28:44.981322	10.59.244.15	128.119.245.12	TCP	54	52583 → 80 [ACK] Seq=474 Ack=439 Win=131072 Len=0
63	16:28:45.002183	10.59.244.15	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
64	16:28:45.341082	128.119.245.12	10.59.244.15	HTTP	538	HTTP/1.1 404 Not Found (text/html)
65	16:28:45.389309	10.59.244.15	128.119.245.12	TCP	54	52583 → 80 [ACK] Seq=893 Ack=923 Win=130560 Len=0
66	16:28:50.359343	128.119.245.12	10.59.244.15	TCP	60	80 → 52583 [FIN, ACK] Seq=923 Ack=893 Win=31360 Len=0
67	16:28:50.359544	10.59.244.15	128.119.245.12	TCP	54	52583 → 80 [ACK] Seq=893 Ack=924 Win=130560 Len=0
68	16:28:57.131750	10.59.244.15	224.0.0.251	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select Time *Display Format*, then select *Time-of-day*.)

Ans: HTTP GET: 16:28:44.601813

HTTP OK: 16:28:44.932553

Time difference: 0.33074 seconds



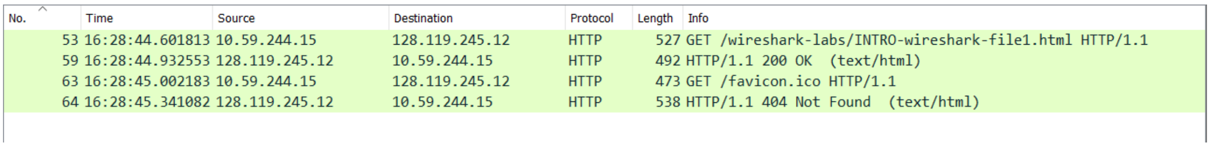
http

No.	Time	Source	Destination	Protocol	Length	Info
53	16:28:44.601813	10.59.244.15	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
59	16:28:44.932553	128.119.245.12	10.59.244.15	HTTP	492	HTTP/1.1 200 OK (text/html)
63	16:28:45.002183	10.59.244.15	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
64	16:28:45.341082	128.119.245.12	10.59.244.15	HTTP	538	HTTP/1.1 404 Not Found (text/html)

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

Ans: Internet address of the gaia.cs.umass.edu: 128.119.245.12

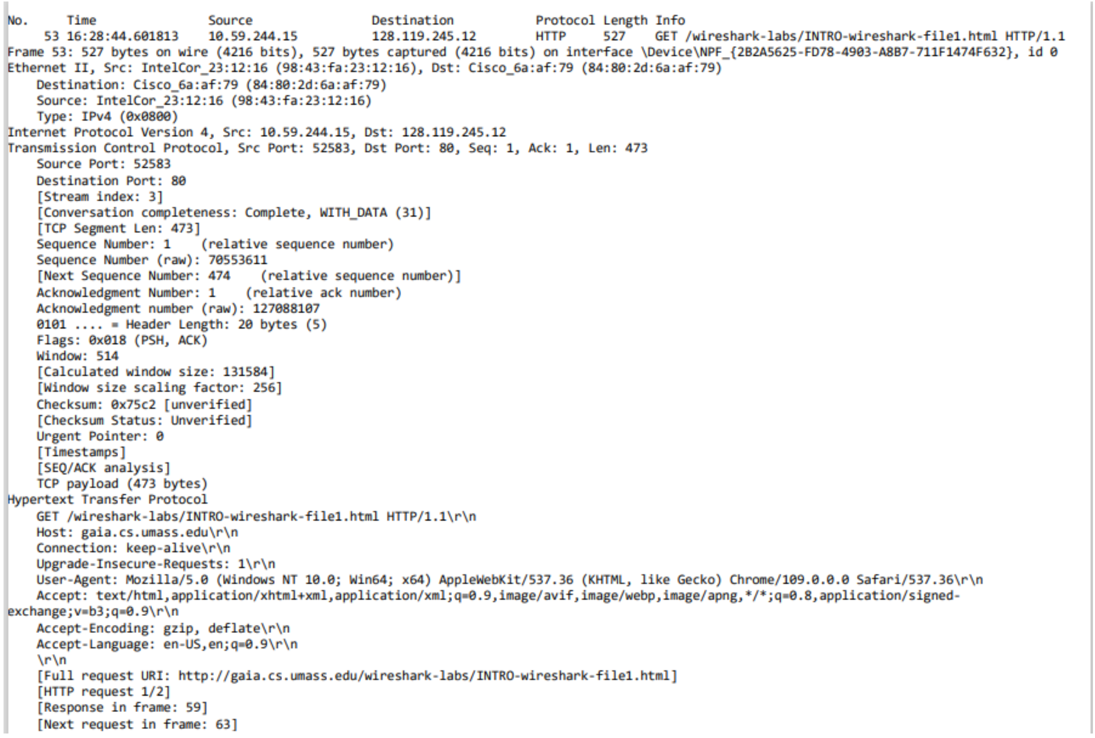
Internet address of my computer: 10.59.244.15



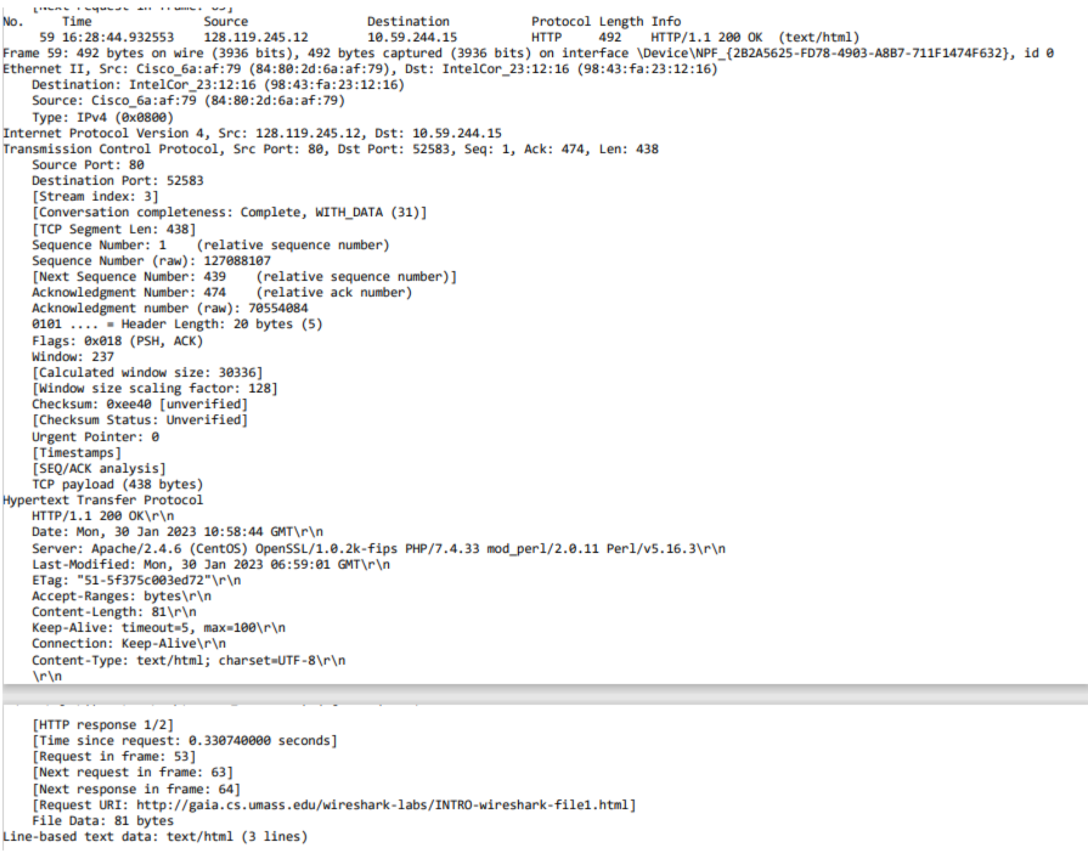
No.	Time	Source	Destination	Protocol	Length	Info
53	16:28:44.601813	10.59.244.15	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
59	16:28:44.932553	128.119.245.12	10.59.244.15	HTTP	492	HTTP/1.1 200 OK (text/html)
63	16:28:45.002183	10.59.244.15	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
64	16:28:45.341082	128.119.245.12	10.59.244.15	HTTP	538	HTTP/1.1 404 Not Found (text/html)

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the "*Selected Packet Only*" and *"Print as displayed"* radial buttons, and then click OK.

Ans:



```
No.     Time               Source                Destination           Protocol Length Info
     53 16:28:44.601813    10.59.244.15          128.119.245.12        HTTP     527    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 53: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF_{2B2A5625-FD78-4903-A8B7-711F1474F632}, id 0
Ethernet II, Src: IntelCor_23:12:16 (98:43:fa:23:12:16), Dst: Cisco_6a:af:79 (84:80:2d:6a:af:79)
    Destination: Cisco_6a:af:79 (84:80:2d:6a:af:79)
    Source: IntelCor_23:12:16 (98:43:fa:23:12:16)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.59.244.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52583, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
    Source Port: 52583
    Destination Port: 80
    [Stream index: 3]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 473]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 70553611
    [Next Sequence Number: 474    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 127088107
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 514
    [Calculated window size: 131584]
    [Window size scaling factor: 256]
    Checksum: 0x75c2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (473 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 59]
    [Next request in frame: 63]
```

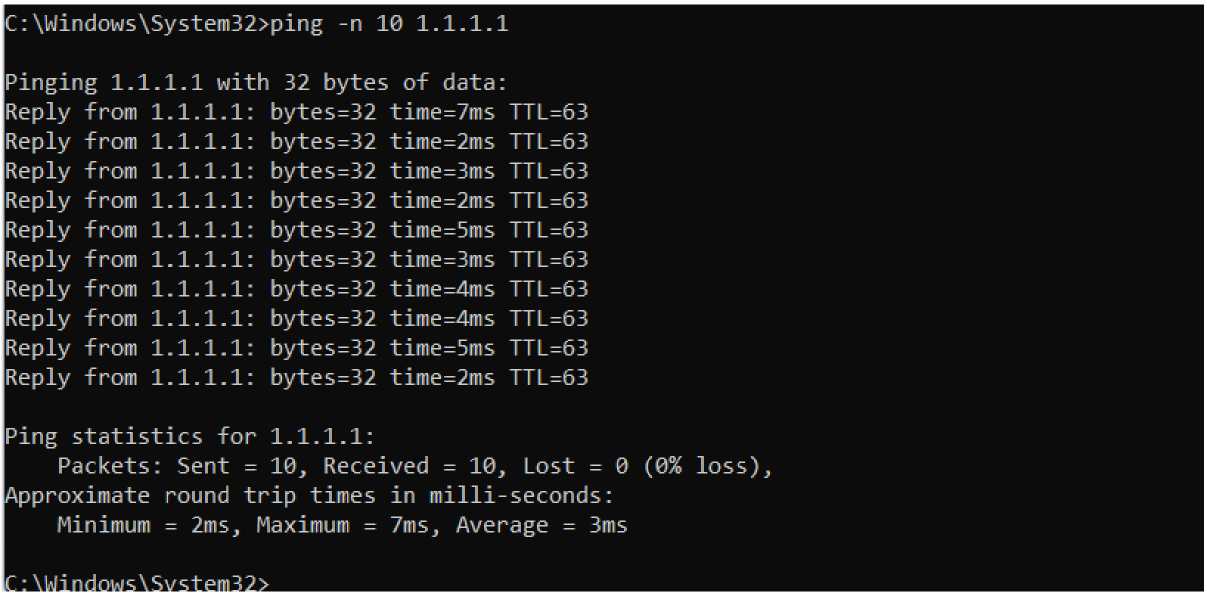


```
No.     Time               Source                Destination           Protocol Length Info
     59 16:28:44.932553    128.119.245.12        10.59.244.15          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 59: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{2B2A5625-FD78-4903-A8B7-711F1474F632}, id 0
Ethernet II, Src: Cisco_6a:af:79 (84:80:2d:6a:af:79), Dst: IntelCor_23:12:16 (98:43:fa:23:12:16)
    Destination: IntelCor_23:12:16 (98:43:fa:23:12:16)
    Source: Cisco_6a:af:79 (84:80:2d:6a:af:79)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.59.244.15
Transmission Control Protocol, Src Port: 80, Dst Port: 52583, Seq: 1, Ack: 474, Len: 438
    Source Port: 80
    Destination Port: 52583
    [Stream index: 3]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 127088107
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 474    (relative ack number)
    Acknowledgment number (raw): 70554084
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xee40 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 30 Jan 2023 10:58:44 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 30 Jan 2023 06:59:01 GMT\r\n
    ETag: "51-5f375c003ed72"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n

    [HTTP response 1/2]
    [Time since request: 0.330740000 seconds]
    [Request in frame: 53]
    [Next request in frame: 63]
    [Next response in frame: 64]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

2. Wireshark_ICMP_v7.0 lab sheet

---

www.ust.hk gave "Request timed out" multiple times. So used ping command on 1.1.1.1

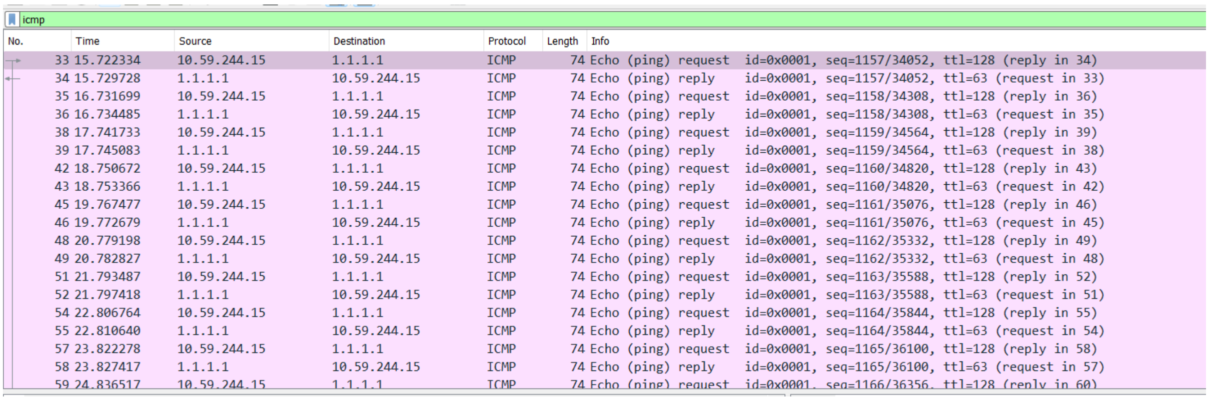


```
C:\Windows\System32>ping -n 10 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=7ms TTL=63
Reply from 1.1.1.1: bytes=32 time=2ms TTL=63
Reply from 1.1.1.1: bytes=32 time=3ms TTL=63
Reply from 1.1.1.1: bytes=32 time=2ms TTL=63
Reply from 1.1.1.1: bytes=32 time=5ms TTL=63
Reply from 1.1.1.1: bytes=32 time=3ms TTL=63
Reply from 1.1.1.1: bytes=32 time=4ms TTL=63
Reply from 1.1.1.1: bytes=32 time=4ms TTL=63
Reply from 1.1.1.1: bytes=32 time=5ms TTL=63
Reply from 1.1.1.1: bytes=32 time=2ms TTL=63

Ping statistics for 1.1.1.1:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 7ms, Average = 3ms

C:\Windows\System32>
```

1. What is the IP address of your host? What is the IP address of the destination host?

Ans: IP address of my host: 10.59.244.15

IP address of the destination host: 1.1.1.1



```
icmp
No.   Time       Source         Destination    Protocol  Length Info
   33 15.722334  10.59.244.15   1.1.1.1        ICMP        74 Echo (ping) request  id=0x0001, seq=1157/34052, ttl=128 (reply in 34)
   34 15.729728  1.1.1.1        10.59.244.15   ICMP        74 Echo (ping) reply    id=0x0001, seq=1157/34052, ttl=63 (request in 33)
   35 16.731699  10.59.244.15   1.1.1.1        ICMP        74 Echo (ping) request  id=0x0001, seq=1158/34308, ttl=128 (reply in 36)
   36 16.734485  1.1.1.1        10.59.244.15   ICMP        74 Echo (ping) reply    id=0x0001, seq=1158/34308, ttl=63 (request in 35)
   38 17.741733  10.59.244.15   1.1.1.1        ICMP        74 Echo (ping) request  id=0x0001, seq=1159/34564, ttl=128 (reply in 39)
   39 17.745083  1.1.1.1        10.59.244.15   ICMP        74 Echo (ping) reply    id=0x0001, seq=1159/34564, ttl=63 (request in 38)
   42 18.750672  10.59.244.15   1.1.1.1        ICMP        74 Echo (ping) request  id=0x0001, seq=1160/34820, ttl=128 (reply in 43)
   43 18.753366  1.1.1.1        10.59.244.15   ICMP        74 Echo (ping) reply    id=0x0001, seq=1160/34820, ttl=63 (request in 42)
   45 19.767477  10.59.244.15   1.1.1.1        ICMP        74 Echo (ping) request  id=0x0001, seq=1161/35076, ttl=128 (reply in 46)
   46 19.772679  1.1.1.1        10.59.244.15   ICMP        74 Echo (ping) reply    id=0x0001, seq=1161/35076, ttl=63 (request in 45)
   48 20.779198  10.59.244.15   1.1.1.1        ICMP        74 Echo (ping) request  id=0x0001, seq=1162/35332, ttl=128 (reply in 49)
   49 20.782827  1.1.1.1        10.59.244.15   ICMP        74 Echo (ping) reply    id=0x0001, seq=1162/35332, ttl=63 (request in 48)
   51 21.793487  10.59.244.15   1.1.1.1        ICMP        74 Echo (ping) request  id=0x0001, seq=1163/35588, ttl=128 (reply in 52)
   52 21.797418  1.1.1.1        10.59.244.15   ICMP        74 Echo (ping) reply    id=0x0001, seq=1163/35588, ttl=63 (request in 51)
   54 22.806764  10.59.244.15   1.1.1.1        ICMP        74 Echo (ping) request  id=0x0001, seq=1164/35844, ttl=128 (reply in 55)
   55 22.810640  1.1.1.1        10.59.244.15   ICMP        74 Echo (ping) reply    id=0x0001, seq=1164/35844, ttl=63 (request in 54)
   57 23.822278  10.59.244.15   1.1.1.1        ICMP        74 Echo (ping) request  id=0x0001, seq=1165/36100, ttl=128 (reply in 58)
   58 23.827417  1.1.1.1        10.59.244.15   ICMP        74 Echo (ping) reply    id=0x0001, seq=1165/36100, ttl=63 (request in 57)
   59 24.836517  10.59.244.15   1.1.1.1        ICMP        74 Echo (ping) request  id=0x0001, seq=1166/36356, ttl=128 (reply in 60)
```

2. Why is it that an ICMP packet does not have source and destination port numbers?

Ans: The ICMP packet is designed to communicate network-layer information between the hosts and the routers but not between the application layer processes. Because of this, the ICMP packet does not have source and destination port numbers. Each ICMP packet has “Type” and “Code” values. These values identify the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are required to direct the ICMP messages to an application layer process.

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

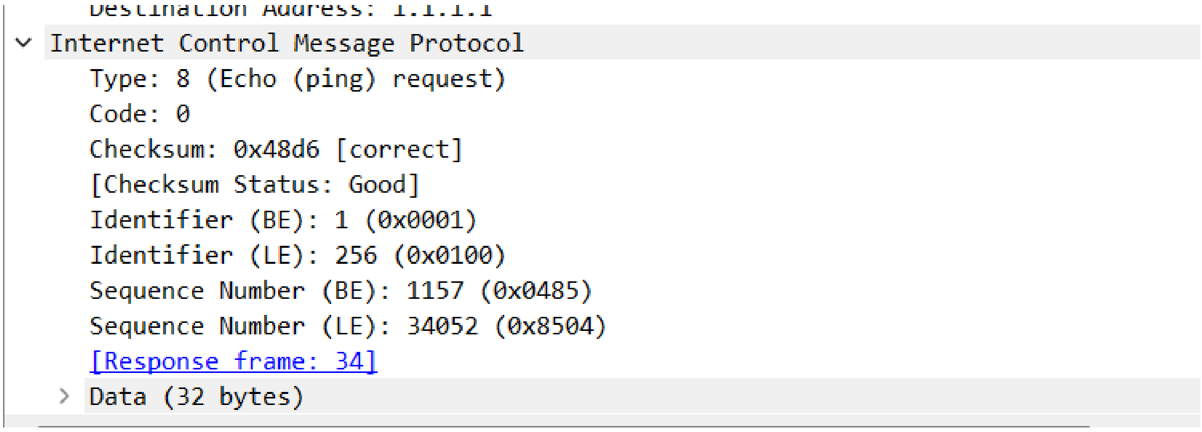
Ans: For a ping request packet:

ICMP Type: 8

ICMP Code: 0

The ICMP packet has Checksum, Identifier, Sequence Number, Data fields.

The checksum, sequence number, identifier fields are **two bytes**.



```
    Destination Address: 1.1.1.1
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x48d6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1157 (0x0485)
    Sequence Number (LE): 34052 (0x8504)
    [Response frame: 34]
  > Data (32 bytes)
```

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

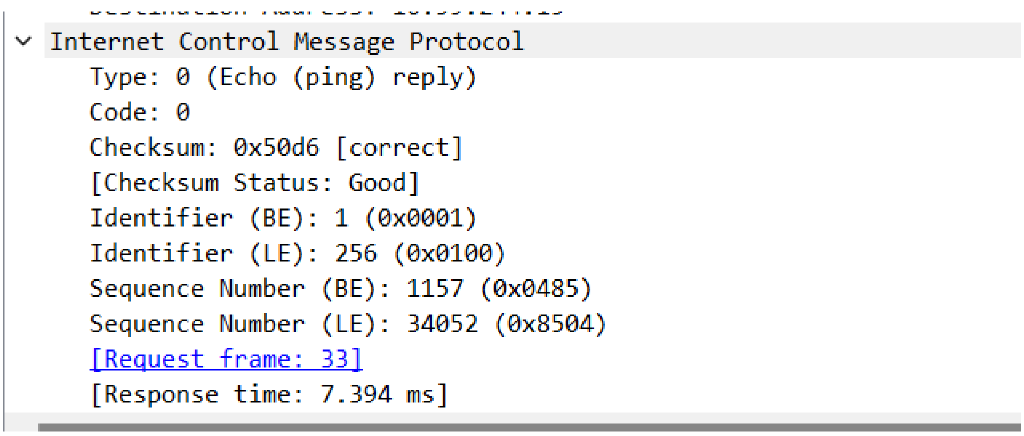
Ans: For a ping reply packet:

ICMP Type: 0

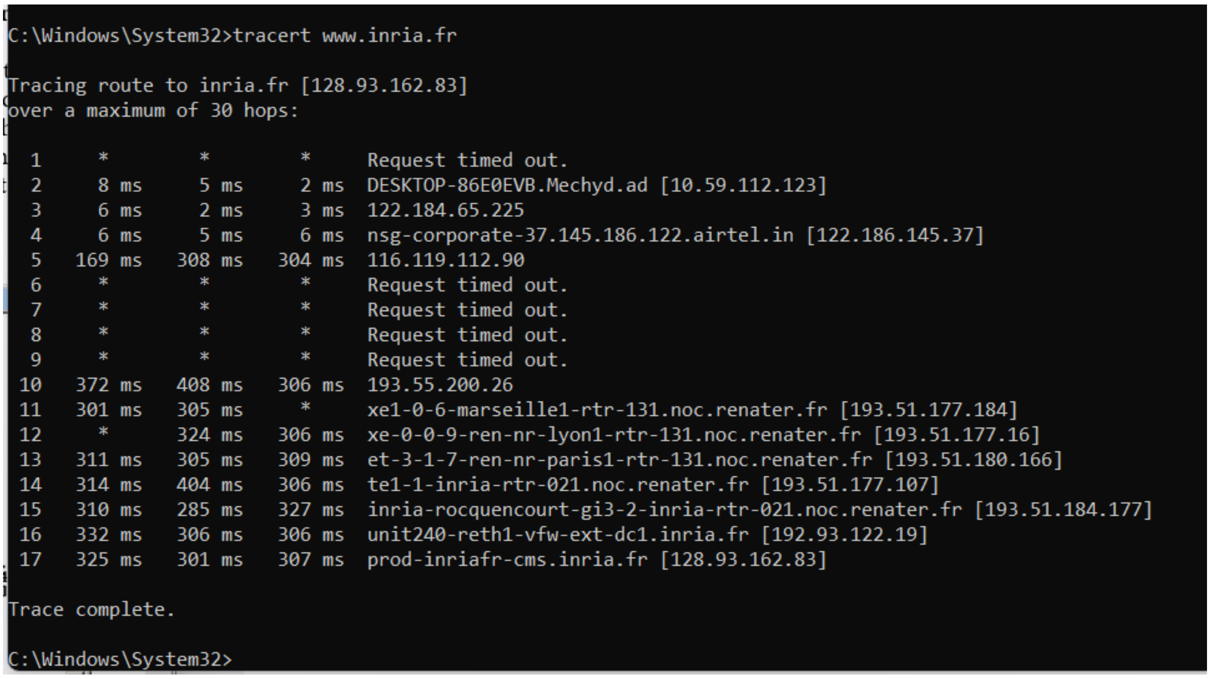
ICMP Code: 0

The ICMP packet has Checksum, Identifier, Sequence Number, Data fields.

The checksum, sequence number, identifier fields are **two bytes**.



```
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x50d6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1157 (0x0485)
    Sequence Number (LE): 34052 (0x8504)
    [Request frame: 33]
    [Response time: 7.394 ms]
```

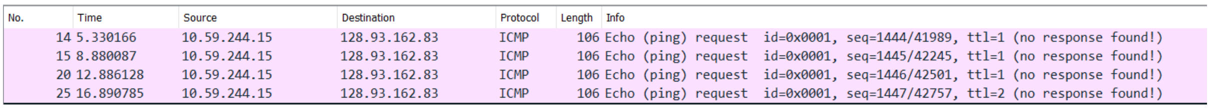


```
C:\Windows\System32>tracert www.inria.fr

Tracing route to inria.fr [128.93.162.83]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     8 ms     5 ms     2 ms  DESKTOP-86E0EVB.Mechyd.ad [10.59.112.123]
  3     6 ms     2 ms     3 ms  122.184.65.225
  4     6 ms     5 ms     6 ms  nsg-corporate-37.145.186.122.airtel.in [122.186.145.37]
  5   169 ms   308 ms   304 ms  116.119.112.90
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10   372 ms   408 ms   306 ms  193.55.200.26
 11   301 ms   305 ms     *     xe1-0-6-marseille1-rtr-131.noc.renater.fr [193.51.177.184]
 12     *      324 ms   306 ms  xe-0-0-9-ren-nr-lyon1-rtr-131.noc.renater.fr [193.51.177.16]
 13   311 ms   305 ms   309 ms  et-3-1-7-ren-nr-paris1-rtr-131.noc.renater.fr [193.51.180.166]
 14   314 ms   404 ms   306 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 15   310 ms   285 ms   327 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 16   332 ms   306 ms   306 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 17   325 ms   301 ms   307 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.

C:\Windows\System32>
```

5. What is the IP address of your host? What is the IP address of the target destination host?

Ans: IP address of my host: 10.59.244.15

IP address of the target destination host: 128.93.62.83



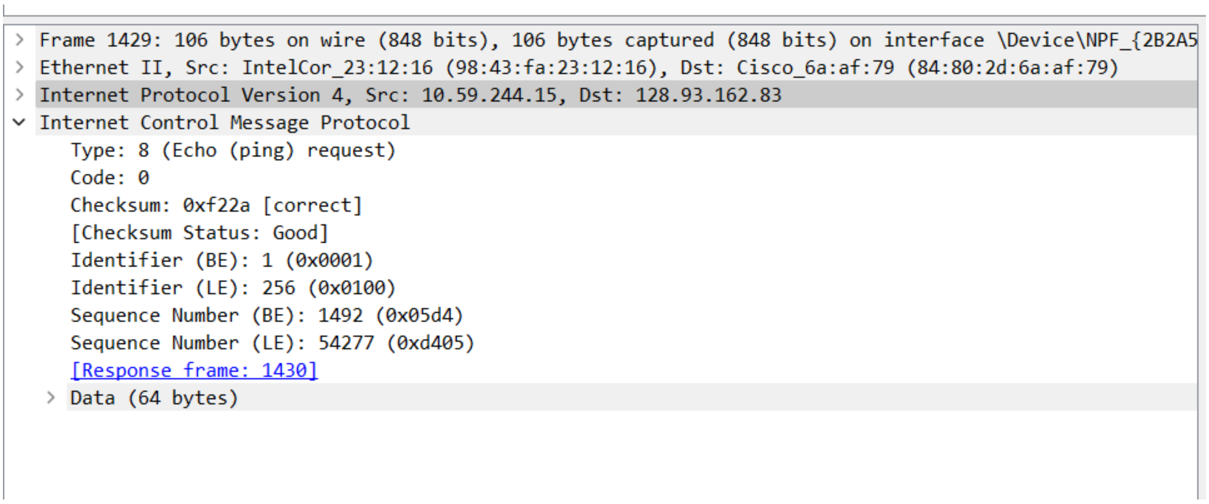
No.	Time	Source	Destination	Protocol	Length	Info
14	5.330166	10.59.244.15	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1444/41989, ttl=1 (no response found!)
15	8.880087	10.59.244.15	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1445/42245, ttl=1 (no response found!)
20	12.886128	10.59.244.15	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1446/42501, ttl=1 (no response found!)
25	16.890785	10.59.244.15	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1447/42757, ttl=2 (no response found!)

6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

Ans: **No**, if ICMP sent UDP packets instead, then IP protocol number will be **0x11**.

7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

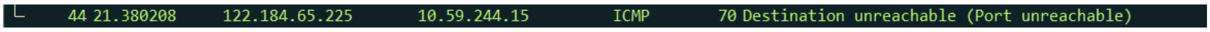
Ans: The ICMP echo packet has the same fields similar to ICMP ping query packets (data visible in question 3 of this lab).



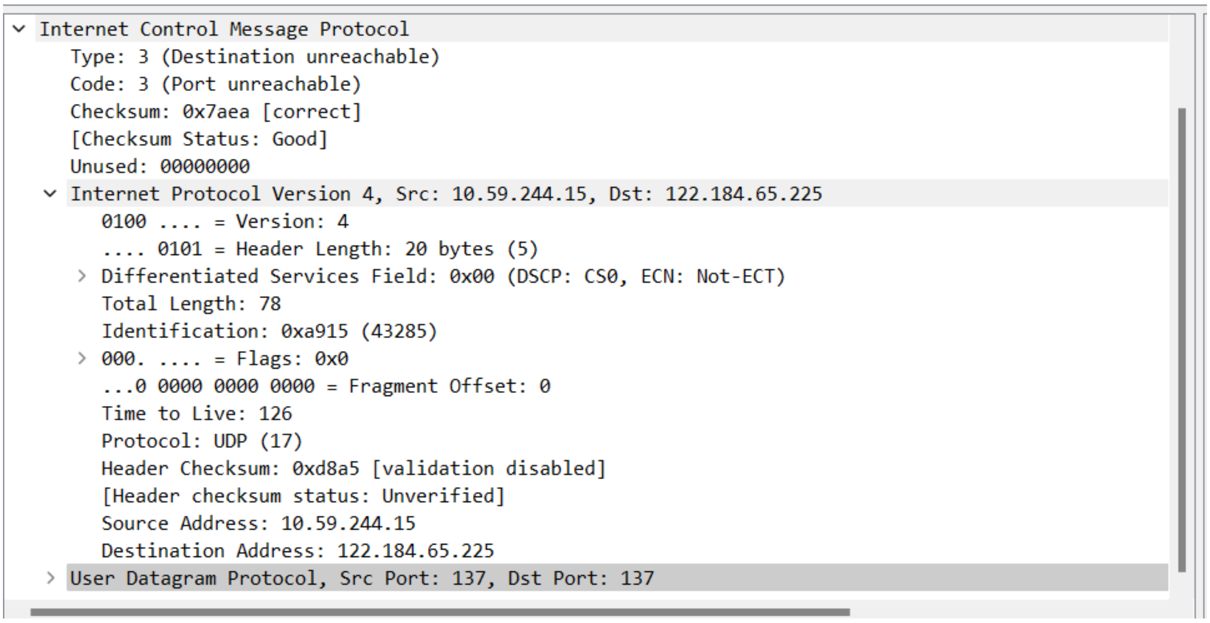
```
> Frame 1429: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{2B2A5
> Ethernet II, Src: IntelCor_23:12:16 (98:43:fa:23:12:16), Dst: Cisco_6a:af:79 (84:80:2d:6a:af:79)
> Internet Protocol Version 4, Src: 10.59.244.15, Dst: 128.93.162.83
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf22a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1492 (0x05d4)
    Sequence Number (LE): 54277 (0xd405)
    [Response frame: 1430]
  > Data (64 bytes)
```

8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

Ans: The fields include the **header of the failed IP pack**et and **first 64 bits of the failed IP packet.**



```
└    44 21.380208     122.184.65.225      10.59.244.15       ICMP      70 Destination unreachable (Port unreachable)
```

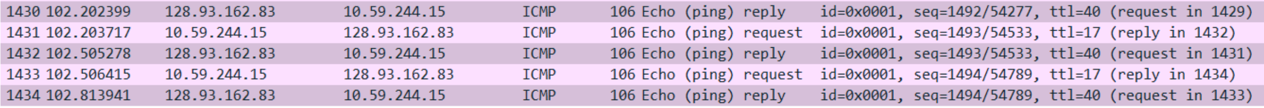


```
v Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x7aea [correct]
    [Checksum Status: Good]
    Unused: 00000000
  v Internet Protocol Version 4, Src: 10.59.244.15, Dst: 122.184.65.225
        0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
      > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 78
        Identification: 0xa915 (43285)
      > 000. .... = Flags: 0x0
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 126
        Protocol: UDP (17)
        Header Checksum: 0xd8a5 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 10.59.244.15
        Destination Address: 122.184.65.225
  > User Datagram Protocol, Src Port: 137, Dst Port: 137
```

9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

Ans: The last three ICMP packets received by the source host are marked in grey shade.

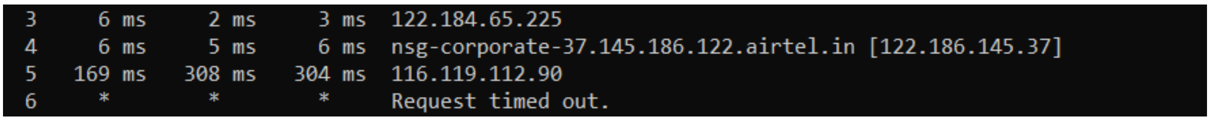
These packets are ICMP are of message **Type: 0** which are **echo reply packets**.



```
1430 102.202399   128.93.162.83    10.59.244.15     ICMP   106 Echo (ping) reply    id=0x0001, seq=1492/54277, ttl=40 (request in 1429)
1431 102.203717   10.59.244.15     128.93.162.83    ICMP   106 Echo (ping) request  id=0x0001, seq=1493/54533, ttl=17 (reply in 1432)
1432 102.505278   128.93.162.83    10.59.244.15     ICMP   106 Echo (ping) reply    id=0x0001, seq=1493/54533, ttl=40 (request in 1431)
1433 102.506415   10.59.244.15     128.93.162.83    ICMP   106 Echo (ping) request  id=0x0001, seq=1494/54789, ttl=17 (reply in 1434)
1434 102.813941   128.93.162.83    10.59.244.15     ICMP   106 Echo (ping) reply    id=0x0001, seq=1494/54789, ttl=40 (request in 1433)
```

10. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

Ans: There is a significant delay from **step 4 to step 5** which is longer than others. This can be due to the hop between two countries.



```
 3     6 ms     2 ms     3 ms  122.184.65.225
 4     6 ms     5 ms     6 ms  nsg-corporate-37.145.186.122.airtel.in [122.186.145.37]
 5   169 ms   308 ms   304 ms  116.119.112.90
 6     *        *        *     Request timed out.
```