

Assignment -4

CS 470 Spring 2018

Note: Only typed submissions are accepted.

Q1. (8 points)

Consider a datagram network using 32-bit host addresses. Suppose a router has four links, numbered 0 through 3, and packets are to be forwarded to the link interfaces as follows:

Destination Address Range	Link Interface
11100000 00000000 00000000 00000000 Through 11100000 00111111 11111111 11111111	0
11100000 01000000 00000000 00000000 through 11100000 01000000 11111111 11111111	1
11100000 01000001 00000000 00000000 through 11100001 01111111 11111111 11111111	2
otherwise	3

a. Provide a forwarding table that has five entries, uses longest prefix matching, and forwards packets to the correct link interfaces.

b. Describe how your forwarding table determines the appropriate link interface for datagrams with destination addresses:

11001000 10010001 01010001 01010101

11100001 01000000 11000011 00111100

11100001 10000000 00010001 01110111

Q2. (7 points)

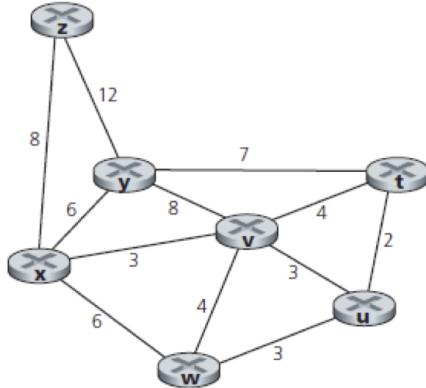
a. Consider sending a 2400-byte datagram into a link that has an MTU of 700 bytes. Suppose the original datagram is stamped with the identification number 422. How many fragments

are generated? What are the values in the various fields in the IP datagram(s) generated related to fragmentation?

b. Suppose datagrams are limited to 1,500 bytes (including header) between source Host A and destination Host B. Assuming a 20-byte IP header, how many datagrams would be required to send an MP3 consisting of 5 million bytes? Explain how you computed your answer.

Q3. (10 points)

Consider the following network. With the indicated link costs, use Dijkstra's shortest-path algorithm to compute the shortest path from x to all network nodes. Show how the algorithm works by computing a table similar to your textbook.



Q4. Use this link: https://gaia.cs.umass.edu/wireshark-labs/Wireshark_IP_v7.0.pdf to find the Wireshark lab for IP. Read the document carefully and answer the questions from the document. In addition attach the print screen of your screen capture with each answer (or set of answers). (15 points)

Q5. Use this link: https://gaia.cs.umass.edu/wireshark-labs/Wireshark_NAT_v7.0.pdf to find the Wireshark lab for NAT. Read the document carefully and answer the questions from the document. In addition attach the print screen of your screen capture with each answer (or set of answers). (10 points) (Extra credit: 3 points, see at the end of the pdf)

Q6. Use this link: https://gaia.cs.umass.edu/wireshark-labs/Wireshark_ICMP_v7.0.pdf to find the Wireshark lab for ICMP. Read the document carefully and answer the questions

Solutions Only

Question 1.

- A. Datagram forwarding table that has five entries, uses longest prefix matching, and forwards packets to the correct link interfaces:

Longest Prefix Match	Link Interface
11100000 00	0
11100000 01000000	1
1110000 or 1110001 0	2
11100001 1	3
otherwise	3

- B. The link interface following datagrams are:

- 11001000 10010001 01010001 01010101: The given address doesn't match to any of the destination address range for link interface 0,1,2. So, it goes to the otherwise prefix match which is link interface 3.
- 11100001 01000000 11000011 00111100: The first 8 bits matches to link interface 2 but also to the link interface 3. But, the next 8 bits after it falls in the address range of 2. So, this address has the link interface 2.
- 11100001 10000000 00010001 01110111: It solely falls in the otherwise address range of link interface 3.

Question 2.

- A. The link has an MTU of 700 bytes and the total size of the datagram being sent is of 2400 bytes excluding the IP header it is: 2380 bytes. But, the maximum size of the data field in the segment excluding the IP header is : 700 bytes - 20 = 680 bytes

$$2380 / 680 \sim 4. \text{ Therefore, we need } \underline{4 \text{ fragments.}}$$

Given, the original datagram is stamped with the identification number 422. The first segment will be of: 700 bytes, with flag set to 1 and offset set to 0. Similarly, the second and third segment will be of: 700 bytes with flag set to 1 and offset set to 85, 170. But the final

segment will be only of: 300 bytes with flag set to 0 and offset set to 255 which indicates that there are no more fragments left to be received.

B. Given,

MTU = 1500 bytes

IP header size = 20 bytes

Size of MP3 = $5 * 10^7$ bytes

Total bytes in data field = $1500 - 20$ bytes = 1480 bytes

But, if the data is carried out in TCP for reliability, then each TCP segment has 20 bytes of header.

So, total bytes in the data field = $1480 - 20$ = 1460 bytes

Now, the total number of fragments required = $5 * 10^7$ bytes / 1460 bytes
= 3425

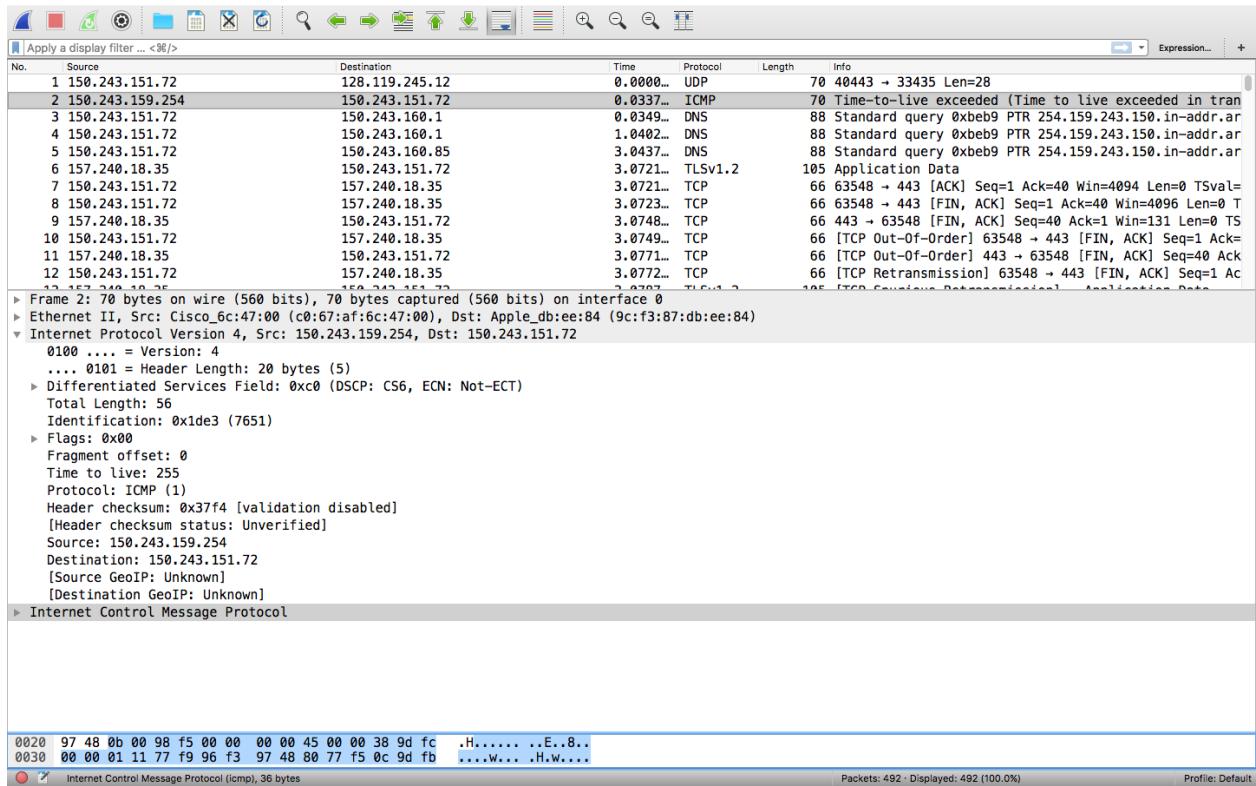
Each 3424 will be of 1500 bytes and the last fragment 3425 will be of, $(5 * 10^7 - 1460 * 3424) + 40 = 960 + 40$ bytes = 1000 bytes.

Question 3

Step	N'	D(t),p(t)	D(u),p(u)	D(v),p(v)	D(w),p(w)	D(y),p(y)	D(z),p(z)
0	x	∞	∞	3, x	6,x	6, x	8, x
1	xv	7, v	6, v	3, x	6, x	6, x	8, x
2	xvu	7, v	6, v	3, x	6, x	6, x	8, x
3	xvuw	7,v	6, v	3, x	6, x	6, x	8,x
4	xvuw	7, v	6, v	3, x	6, x	6, x	8,x
5	xvuwyt	7, v	6, v	3, x	6, x	6,x	8, x
6	xvuwytz	7, v	6, v	3, x	6, x	6, x	8, x

Question 4

Capturing packets from an execution of traceroute



1. The IP address of my computer is: 150.243.151.72
2. The value in the upper layer protocol field is: ICMP (1)
3. IP header bytes: 20 bytes , payload of the datagram: $56 - 20 = 36$ bytes

```

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
▼ Differentiated Services Field: 0xc0 (DSCP: C
  1100 00.. = Differentiated Services Codepoint: C
  .... ..00 = Explicit Congestion Notification: 0
Total Length: 56

```

4. The IP datagram has not been fragmented. Since, the more fragments = 0.

Flags: 0x00

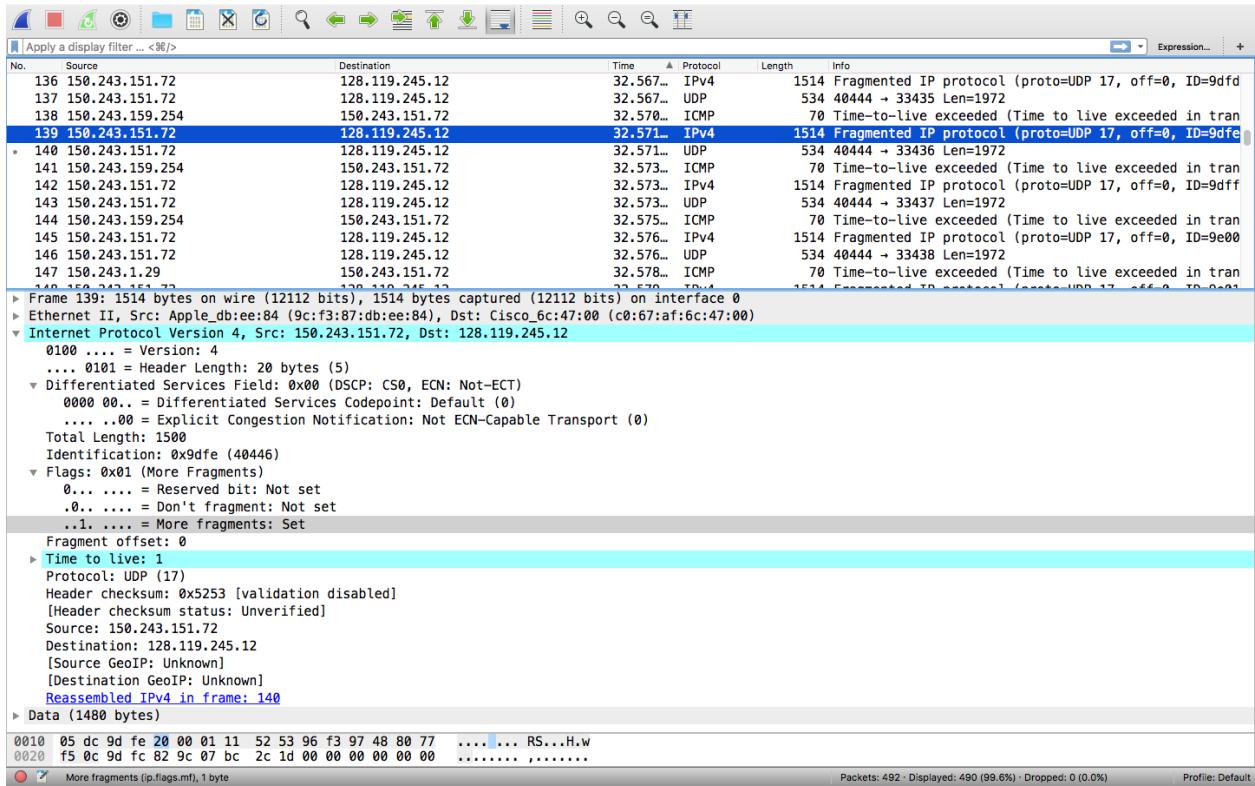
- 0... = Reserved bit: Not set
- .0... = Don't fragment: Not set
- ..0. = More fragments: Not set

5. Identification, time to live, header checksum, (source IP and destination IP) always change.
6. Flags, version, fragment offset, protocol, differentiated services and header length always stays constant. These field should always remain constant as well because we are using the same source and destination, same version IPv4, same ICMP packets and they use the same type of ICMP services. And, the identification, ttl, header checksum should change because each packets have different identifications and since the header changes, so does the checksum.
7. With each ICMP requests, the identification field of the IP datagram increases.
8. The value in the Identification field and the TTL field are: 7651 and 255.
9. The identification of each packets are unique so it always changes. When more than 1 packets has the same identification then they are the fragments from the same packet.

Fragmentation

10. Couldn't find ICMP echo request as I used the MAC instead of the pingplotter. But, the more fragments is equal to 1.
11. The flag is set to more fragment bit. The fragment offset is set to 0 this means this is the first fragment. This datagram has the total length of 1500 including the header.

12. The fragment offset is not 0. It is not the last fragment because the fragment flag is set to more fragments.



13. Total length, flags, fragment offset and checksum.

14. There were 3 fragments created from the original datagram.

```
▼ [3 IPv4 Fragments (3480 bytes): #471(1480), #472(1480), #473(520)]
  [Frame: 471, payload: 0-1479 (1480 bytes)]
  [Frame: 472, payload: 1480-2959 (1480 bytes)]
  [Frame: 473, payload: 2960-3479 (520 bytes)]
  [Fragment count: 3]
```

15. Fragment and offset.

Question 5.

Wireshark Lab: NAT v7.0

Apply a display filter... <%> / Expression... +

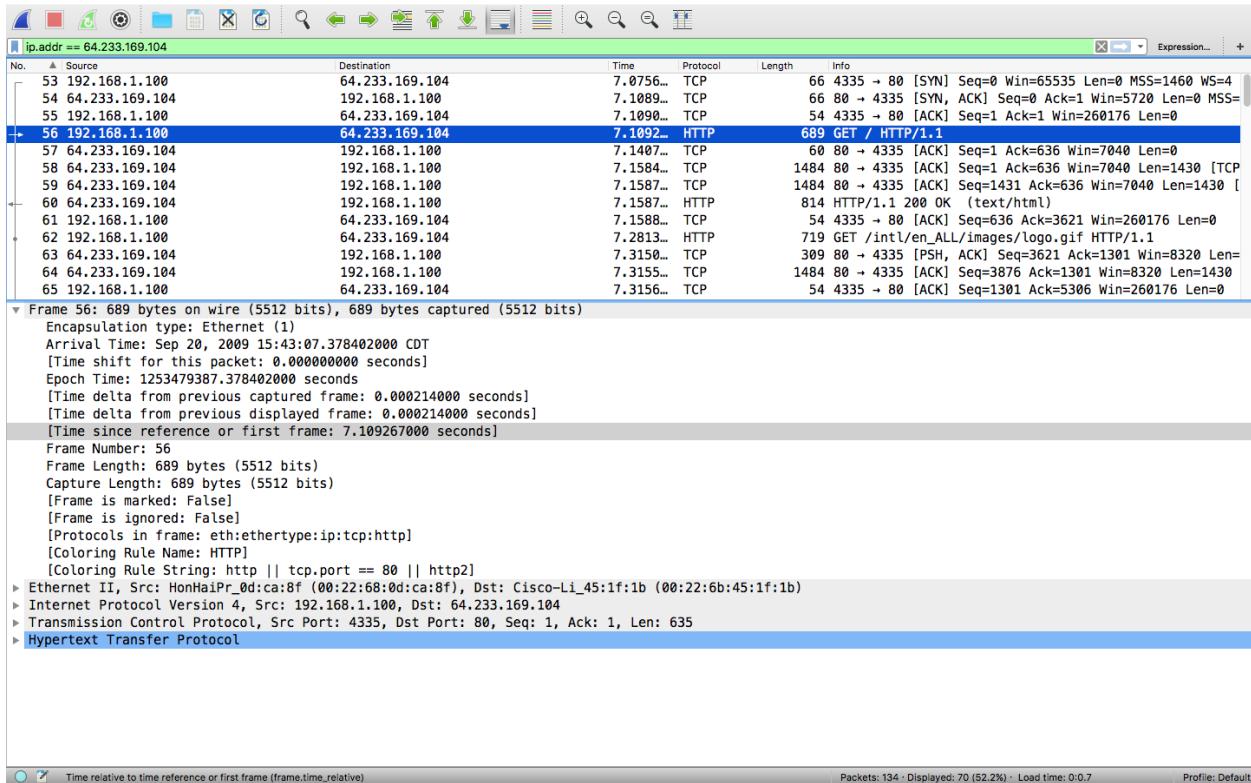
No.	Source	Destination	Time	Protocol	Length	Info
1	192.168.1.100	10.119.240.64	0.0000...	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.
2	192.168.1.100	68.87.71.230	1.1248...	DNS	91	Standard query 0xa9a9 A safebrowsing.clients.google.com
3	68.87.71.230	192.168.1.100	1.1382...	DNS	211	Standard query response 0xa9a9 A safebrowsing.client
4	192.168.1.100	74.125.91.113	1.1403...	TCP	66	4330 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4
5	74.125.91.113	192.168.1.100	1.2078...	TCP	66	80 → 4330 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
6	192.168.1.100	74.125.91.113	1.2078...	TCP	54	4330 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
7	192.168.1.100	74.125.91.113	1.2080...	HTTP	1035	POST /safebrowsing/downloads?client=navclient-auto-f
8	Cisco-Li_45:1f:1b	HonHaiPr_0d:ca:8f	1.2593...	ARP	60	Who has 192.168.1.100 Tell 192.168.1.1
9	HonHaiPr_0d:ca:8f	Cisco-Li_45:1f:1b	1.2593...	ARP	42	192.168.1.100 is at 00:22:68:0d:ca:8f
10	74.125.91.113	192.168.1.100	1.2696...	TCP	60	80 → 4330 [ACK] Seq=1 Ack=982 Win=7744 Len=0
11	74.125.91.113	192.168.1.100	1.2740...	HTTP	853	HTTP/1.1 200 OK [application/vnd.google.safebrowsing]
12	192.168.1.100	74.125.91.113	1.4745...	TCP	54	4330 → 80 [ACK] Seq=982 Ack=800 Win=259376 Len=0
13	74.125.91.113	192.168.1.100	1.5286...	HTTP	853	[TCP Spurious Retransmission] HTTP/1.1 200 OK [appl]

▶ Frame 1: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
 ▶ Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
 ▶ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 10.119.240.64
 ▶ User Datagram Protocol, Src Port: 1028, Dst Port: 161
 ▶ Simple Network Management Protocol

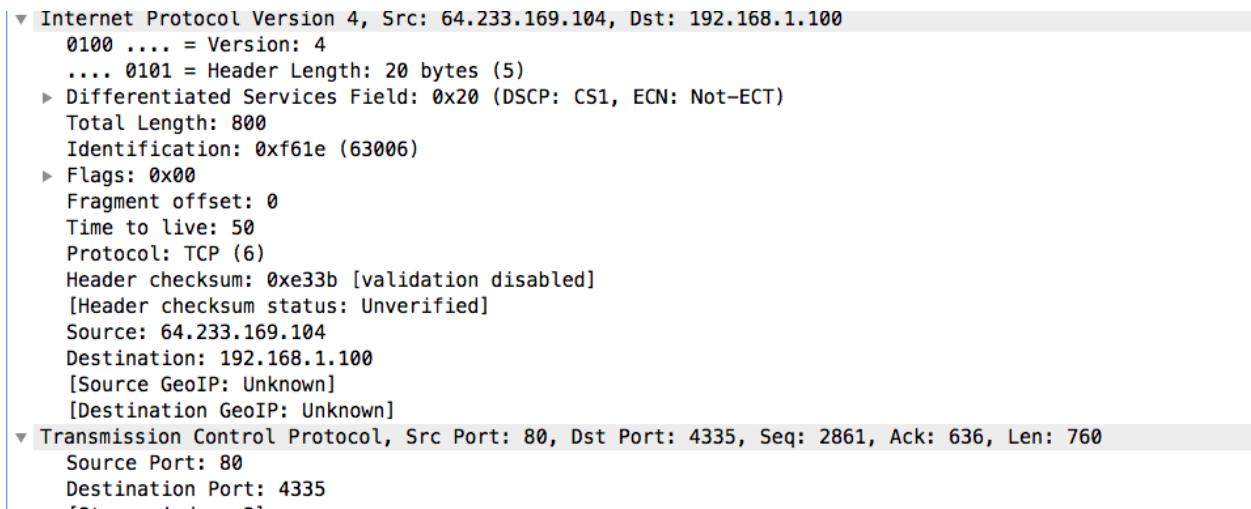
1. The IP address of the client is 192.168.1.100.

2.

3. The source and destination IP addresses are: 192.168.1.100 at port 4335, Dst: 64.233.169.104 at port 80.



4. The corresponding 200 OK HTTP message was received at 7.158797. The source IP address is: 64.233.169.104 and port number 80, Dst IP address is : 192.168.1.100 and port number : 4335.



5. The client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267 was at 7.075657 seconds.

The source IP address at TCP SYN segment is: 192.168.1.100 at port 4335 and Destination IP address is: 64.233.169.104 at port 80.

No.	Source	Destination	Time	Protocol	Length	Info
53	192.168.1.100	64.233.169.104	7.0756...	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4
54	64.233.169.104	192.168.1.100	7.1089...	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1460 WS=4
55	192.168.1.100	64.233.169.104	7.1090...	TCP	54	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
56	192.168.1.100	64.233.169.104	7.1092...	HTTP	689	GET / HTTP/1.1
57	64.233.169.104	192.168.1.100	7.1407...	TCP	68	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
58	64.233.169.104	192.168.1.100	7.1584...	TCP	1484	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP]
59	64.233.169.104	192.168.1.100	7.1587...	TCP	1484	80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP]
60	64.233.169.104	192.168.1.100	7.1587...	HTTP	814	HTTP/1.1 200 OK (text/html)
61	192.168.1.100	64.233.169.104	7.1588...	TCP	54	4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
62	192.168.1.100	64.233.169.104	7.2813...	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
63	64.233.169.104	192.168.1.100	7.3150...	TCP	309	80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=0
64	64.233.169.104	192.168.1.100	7.3155...	TCP	1484	80 → 4335 [ACK] Seq=3876 Ack=1301 Win=8320 Len=1430 [TCP]
65	192.168.1.100	64.233.169.104	7.3156...	TCP	54	4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0

▶ Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 ▶ Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
 ▶ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
 ▶ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0

Internet Protocol Version 4 (ip), 20 bytes
 Packets: 134 - Displayed: 70 (52.2%) · Load time: 0:0:7
 Profile: Default

And the source IP address of the ACK segment is: 64.233.169.104 at port 80 and the destination IP address is: 192.168.1.100 at port 4335. The client received the ACK at 7.108986 seconds.

6.

No.	Source	Destination	Time	Protocol	Length	Info
74	Cisco_bf:6c:01	Broadcast	4.9986...	ARP	68	Who has 71.192.37.118? Tell 71.192.32.1
75	Cisco_bf:6c:01	Broadcast	5.1630...	ARP	68	Who has 71.192.32.157? Tell 71.192.32.1
76	Cisco_bf:6c:01	Broadcast	5.3617...	ARP	68	Who has 71.192.35.29? Tell 71.192.32.1
77	169.254.247.145	169.254.255.255	5.3977...	NBNS	92	Name query NB HPAB904C<0>
78	Cisco_bf:6c:01	Broadcast	5.5639...	ARP	68	Who Has 71.192.32.97? Tell 71.192.32.1
79	Dell_58:98:2a	Broadcast	5.6628...	ARP	42	Who has 192.168.1.101? Tell 169.254.247.145
80	71.192.34.104	68.87.71.230	6.0200...	DNS	74	Standard query 0xed6a A www.google.com
81	68.87.71.230	71.192.34.104	6.0327...	DNS	158	Standard query response 0xed6a A www.google.com CNAM
82	71.192.34.104	64.233.169.104	6.0354...	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4
83	64.233.169.104	71.192.34.104	6.0677...	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1460 WS=4
84	71.192.34.104	64.233.169.104	6.0687...	TCP	68	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	71.192.34.104	64.233.169.104	6.0691...	HTTP	689	GET / HTTP/1.1
86	Cisco_bf:6c:01	Broadcast	6.0927...	ARP	68	Who has 71.192.35.144? Tell 71.192.32.1

▶ Frame 82: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 Encapsulation type: Ethernet (1)
 Arrival Time: Sep 20, 2009 15:43:07.766539000 CDT
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1253479387.766539000 seconds
 [Time delta from previous captured frame: 0.002737000 seconds]
 [Time delta from previous displayed frame: 0.002737000 seconds]
 [Time since reference or first frame: 6.035475000 seconds]
 Frame Number: 82
 Frame Length: 66 bytes (528 bits)
 Capture Length: 66 bytes (528 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ether-type:ip:tcp]
 [Coloring Rule Name: HTTP]
 [Coloring Rule String: http || tcp.port == 80 || http2]
 ▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:e6:d6:bf:6c:01)
 ▶ Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
 ▶ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0

Internet Protocol Version 4 (ip), 20 bytes
 Packets: 210 - Displayed: 210 (100.0%) · Load time: 0:0:35
 Profile: Default

It was received at time: 6.067775 seconds

Source IP: 71.192.34.104 AT PORT 4335, Destination IP: 64.233.169.104 AT PORT 80

The source IP, destination IP and their port numbers are different from Q. 3.

7. No. The checksum and flags are changed.

No.	Source	Destination	Time	Protocol	Length	Info
81	68.87.71.230	71.192.34.104	6.0327...	DNS	158	Standard query response 0xed6a A www.google.com CNAM
82	71.192.34.104	64.233.169.104	6.0354...	TCP	66	4335 -> 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4
83	64.233.169.104	71.192.34.104	6.0677...	TCP	66	80 -> 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
84	71.192.34.104	64.233.169.104	6.0687...	TCP	60	4335 -> 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	71.192.34.104	64.233.169.104	6.0691...	HTTP	689	GET / HTTP/1.1
86	Cisco_bf:6c:01	Broadcast	6.0927...	ARP	60	Who has 71.192.35.144? Tell 71.192.32.1
87	64.233.169.104	71.192.34.104	6.0996...	TCP	60	80 -> 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
88	64.233.169.104	71.192.34.104	6.1170...	TCP	1484	80 -> 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP]
89	64.233.169.104	71.192.34.104	6.1174...	TCP	1484	80 -> 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP]
90	64.233.169.104	71.192.34.104	6.1175...	HTTP	814	HTTP/1.1 200 OK (text/html)
91	71.192.34.104	64.233.169.104	6.1185...	TCP	60	4335 -> 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
92	169.254.247.145	169.254.255.255	6.1620...	NBNS	92	Name query NB HPAB9D4C<>0>
93	71.192.34.104	64.233.169.104	6.2413...	HTTP	719	GET /int!/en_ALL/images/logo.gif HTTP/1.1

8. Identification (p.id), 2 bytes

The first message was received at 6.117078 seconds

HTTP 200 OK message source IP: 64.233.169.104, Port: 80

HTTP 200 OK message Destination IP: 71.192.34.104, Port: 4335

Version and flag did not change while ttl, header checksum changed.

9. For SYN:

Time: 6.035475000 seconds

Source IP Address: 71.192.34.104

Destination IP Address: 64.233.169.104

Ttl changed.

No.	Source	Destination	Time	Protocol	Length	Info
77	169.254.247.145	169.254.255.255	5.3977...	NBNS	92	Name query NB HPAB9D4C<>0>
78	Cisco_bf:6c:01	Broadcast	5.5639...	ARP	60	Who has 71.192.32.97? Tell 71.192.32.1
79	Dell_58:98:2a	Broadcast	5.6628...	ARP	42	Who has 192.168.1.16? Tell 169.254.247.145
80	71.192.34.104	68.87.71.230	6.0208...	DNS	74	Standard query 0xed6a A www.google.com
81	68.87.71.230	71.192.34.104	6.0327...	DNS	158	Standard query response 0xed6a A www.google.com CNAM
82	71.192.34.104	64.233.169.104	6.0354...	TCP	66	4335 -> 80 [SYN] Seq=0 Win=65535 Len=1460 WS=4
83	64.233.169.104	71.192.34.104	6.0677...	TCP	66	80 -> 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
84	71.192.34.104	64.233.169.104	6.0687...	TCP	60	4335 -> 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	71.192.34.104	64.233.169.104	6.0691...	HTTP	689	GET / HTTP/1.1
86	Cisco_bf:6c:01	Broadcast	6.0927...	ARP	60	Who has 71.192.35.144? Tell 71.192.32.1
87	64.233.169.104	71.192.34.104	6.0996...	TCP	60	80 -> 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
88	64.233.169.104	71.192.34.104	6.1170...	TCP	1484	80 -> 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP]
89	64.233.169.104	71.192.34.104	6.1174...	HTTP	1484	80 -> 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP]

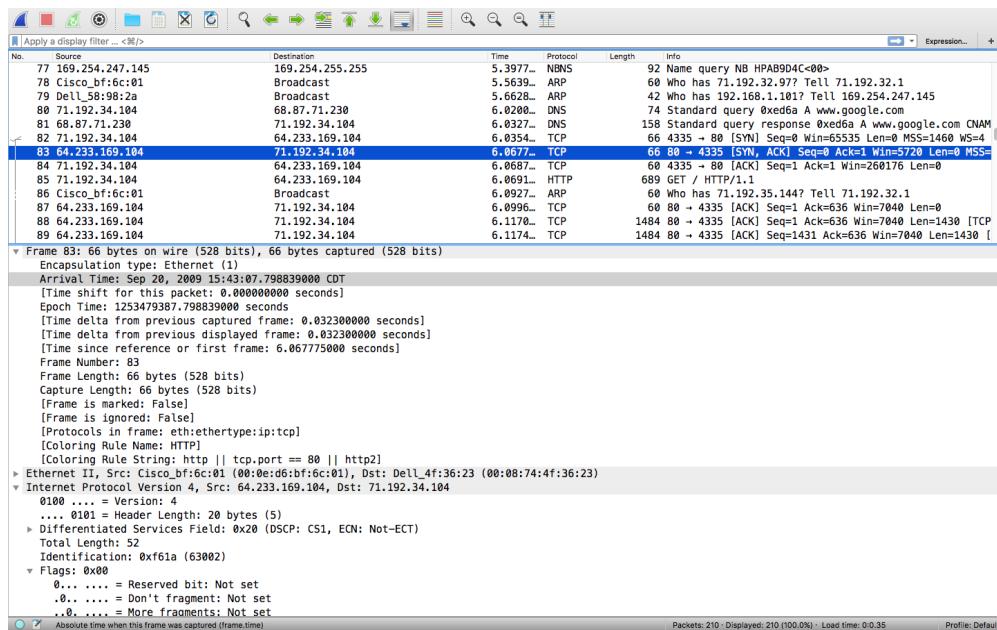
For ACK:

Time: 6.035475000 seconds

Source IP Address: 71.192.34.104

Destination IP Address: 64.233.169.104

Time to live changed



10.

NAT translation table in the NAT router	
WAN SIDE	LAN SIDE
71.192.34.104 Port: 4335	192.168.1.100 port: 4335

EXTRA CREDIT

The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200 OK request/response studied above. For example, in the NAT_home_side trace file, consider the client-to-server GET at time 1.572315, and the GET at time 7.573305.

ANSWER:

HTTP request messages are used when we directly want to invoke our functions via HTTP. To allow for specific segmentation the HTTP takes arguments: request and response. They represent the HTTP request sent to the server and the response that will be returned to the client. The GET at time 1.572315, and the GET at time 7.573305 in the NAT_homw_side trace file represent that the site is not malicious and safe to visit. It represents the safe browsing check that Google implemented. The first URL directs the client to safebrowsing and after making sure that the website is safe, the second URL directs the client to the targeted website. Also, the destination IP address changed in different frames which means that there must be DNS queries in different segments.

Question 6.

ICMP and PING

Url used:

www.ntc.net.np

```
[dikshyas-air:~ dikshya96$ ping -c 10 www.ntc.net.np
PING www.ntc.net.np (202.70.64.2): 56 data bytes
64 bytes from 202.70.64.2: icmp_seq=0 ttl=48 time=750.413 ms
64 bytes from 202.70.64.2: icmp_seq=1 ttl=48 time=305.834 ms
Request timeout for icmp_seq 2
64 bytes from 202.70.64.2: icmp_seq=2 ttl=48 time=1001.550 ms
64 bytes from 202.70.64.2: icmp_seq=3 ttl=48 time=1011.629 ms
64 bytes from 202.70.64.2: icmp_seq=4 ttl=48 time=1006.666 ms
64 bytes from 202.70.64.2: icmp_seq=5 ttl=48 time=454.685 ms
64 bytes from 202.70.64.2: icmp_seq=6 ttl=48 time=319.680 ms
64 bytes from 202.70.64.2: icmp_seq=7 ttl=48 time=1006.877 ms
64 bytes from 202.70.64.2: icmp_seq=8 ttl=48 time=358.350 ms
64 bytes from 202.70.64.2: icmp_seq=9 ttl=48 time=1406.426 ms

--- www.ntc.net.np ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 305.834/762.211/1406.426/362.775 ms
dikshyas-air:~ dikshya96$ ]
```

- The IP address of the host and destination are: 150.243.152.75 and 202.70.64.2

Wireshark Network Traffic Analysis

No.	Source	Destination	Time	Protocol	Length	Info
94	150.243.152.75	202.70.64.2	1.1202...	TCP	587	[TCP Retransmission] 54948 → 443 [PSH, ACK] Seq=54948 Ack=443 Win=14480 Len=587
95	202.70.64.2	150.243.152.75	1.1219...	TCP	74	443 → 54949 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=74
96	202.70.64.2	150.243.152.75	1.1219...	TCP	66	443 → 54948 [ACK] Seq=1 Ack=522 Win=15616 Len=0
97	202.70.64.2	150.243.152.75	1.1219...	TLSv1.2	203	Server Hello, Change Cipher Spec, Encrypted Handshake Message
98	150.243.152.75	202.70.64.2	1.1220...	TCP	66	54949 → 443 [ACK] Seq=1 Ack=1 Win=131744 Len=0
99	150.243.152.75	202.70.64.2	1.1220...	TCP	66	54948 → 443 [ACK] Seq=522 Ack=138 Win=131616 Len=0
100	150.243.152.75	202.70.64.2	1.1223...	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
101	150.243.152.75	202.70.64.2	1.1239...	TLSv1.2	1215	Application Data
102	150.243.152.75	209.85.147.188	1.1376...	TCP	54	64343 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
103	150.243.152.75	150.243.160.1	1.1587...	DNS	74	Standard query 0x1eed A www.ntc.net.np
104	150.243.160.1	150.243.152.75	1.1602...	DNS	98	Standard query response 0x1eed A www.ntc.net.np
→ 105	150.243.152.75	202.70.64.2	1.1611...	ICMP	98	Echo (ping) request id=0x26a1, seq=0/0, ttl=64
106	209.85.147.188	150.243.152.75	1.1634...	TCP	66	[TCP ACKED unseen segment] 443 → 64343 [ACK] Seq=1 Ack=1 Win=4096 Len=0

Frame 105: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 ▶ Ethernet II, Src: Apple_db:e8:84 (9cf3:87:db:ee:84), Dst: Cisco_6c:47:00 (c0:67:af:6c:47:00)
 ▶ Internet Protocol Version 4, Src: 150.243.152.75, Dst: 202.70.64.2
 ▶ Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x2ee8 [correct]
 [Checksum Status: Good]
 Identifier (BE): 9889 (0x26a1)
 Identifier (LE): 41254 (0xa126)
 Sequence number (BE): 0 (0x0000)
 Sequence number (LE): 0 (0x0000)
 [Response frame: 127]
 Timestamp from icmp data: May 2, 2018 14:42:00.870388000 CDT
 [Timestamp from icmp data (relative): 0.000180000 seconds]
 ▶ Data (48 bytes)

- An ICMP packet does not have source and destination port numbers because ICMP only communicates between the host and the routers, not between the application layer processes. The network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

```
▶ Internet Protocol Version 4, Src: 150.243.152.75, Dst: 202.70.64.2
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x2ee8 [correct]
  [Checksum Status: Good]
  Identifier (BE): 9889 (0x26a1)
  Identifier (LE): 41254 (0xa126)
  Sequence number (BE): 0 (0x0000)
  Sequence number (LE): 0 (0x0000)
  [Response frame: 127]
  Timestamp from icmp data: May 2, 2018 14:42:00.870388000 CDT
  [Timestamp from icmp data (relative): 0.000180000 seconds]
  ▶ Data (48 bytes)
```

3. The Ping request packet:

The ICMP type and code numbers are: 8 and 0. The ICMP packets have other fields like checksum, identifier, sequence numbers and timestamp. The checksum, identifier and sequence number each has 2 bytes.

Screenshot of Wireshark showing network traffic. The packet list shows several DNS queries and responses, and a single ICMP Echo (ping) request from source IP 150.243.152.75 to destination IP 202.70.64.2. The details pane shows the ICMP header fields: Type: 8 (Echo (ping) request), Code: 0, Checksum: 0x2ee8 [correct], Identifier (BE): 9889 (0x26a1), Identifier (LE): 41254 (0xa126), Sequence number (BE): 0 (0x0000), Sequence number (LE): 0 (0x0000). The timestamp from icmp data is May 2, 2018 14:42:00.870388000 CDT.

```

No. Source Destination Time Protocol Length Info
103 150.243.152.75 150.243.160.1 1.1587... DNS 74 Standard query 0x1eed A www.ntc.net.np
104 150.243.160.1 150.243.152.75 1.1602... DNS 90 Standard query response 0x1eed A www.ntc.net.np
→ 105 150.243.152.75 202.70.64.2 1.1611... ICMP 98 Echo (ping) request id=0x26a1, seq=0/0, ttl=64
106 209.85.147.188 150.243.152.75 1.1634... TCP 66 [TCP ACKed unseen segment] 443 → 64343 [ACK] Seq=1266 Ack=1266
107 150.243.223.249 224.0.0.1 1.3576... IGMPv2 42 Membership Query, general
108 fe80::12f3:11ff:fe99:63af ff02::1 1.3576... IGMPv6 86 Multicast Listener Query
109 150.243.152.75 202.70.64.2 1.9031... TCP 1266 [TCP Retransmission] 54948 → 443 [PSH, ACK] Seq=1266 Ack=1266
110 202.70.64.2 150.243.152.75 1.9067... TCP 78 [TCP Dup ACK 96#1] 443 → 54948 [ACK] Seq=138 Ack=138
111 202.70.64.2 150.243.152.75 1.9074... TCP 1514 [TCP Previous segment not captured] 443 → 54948
112 202.70.64.2 150.243.152.75 1.9074... TCP 1408 [TCP Previous segment not captured] 443 → 54948
113 202.70.64.2 150.243.152.75 1.9075... TCP 66 [TCP Previous segment not captured] 443 → 54948
114 150.243.152.75 202.70.64.2 1.9076... TCP 78 [TCP Dup ACK 99#1] 54948 → 443 [ACK] Seq=1722 Ack=1722
115 150.243.152.75 202.70.64.2 1.9076... TCP 86 [TCP Dup ACK 99#2] 54948 → 443 [ACK] Seq=1722 Ack=1722

▶ Frame 105: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Apple_db:ee:84 (9c:f3:87:db:ee:84), Dst: Cisco_6c:47:00 (c0:67:af:6c:47:00)
▶ Internet Protocol Version 4, Src: 150.243.152.75, Dst: 202.70.64.2
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x2ee8 [correct]
  [Checksum Status: Good]
  Identifier (BE): 9889 (0x26a1)
  Identifier (LE): 41254 (0xa126)
  Sequence number (BE): 0 (0x0000)
  Sequence number (LE): 0 (0x0000)
  [Response frame: 127]
  Timestamp from icmp data: May 2, 2018 14:42:00.870388000 CDT
  [Timestamp from icmp data (relative): 0.000180000 seconds]
▶ Data (48 bytes)

Internet Protocol Version 4 (ip), 20 bytes
  Profile: Default
  Packets: 233 · Displayed: 233 (100.0%)
  ▶ Internet Protocol Version 4, Src: 150.243.152.75, Dst: 202.70.64.2
  ▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2ee8 [correct]
    [Checksum Status: Good]
    Identifier (BE): 9889 (0x26a1)
    Identifier (LE): 41254 (0xa126)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Response frame: 127]
    Timestamp from icmp data: May 2, 2018 14:42:00.870388000 CDT
    [Timestamp from icmp data (relative): 0.000180000 seconds]
  ▶ Data (48 bytes)

```

4. The corresponding Ping reply Packet:

▼ Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x36e8 [correct]
[Checksum Status: Good]
Identifier (BE): 9889 (0x26a1)
Identifier (LE): 41254 (0xa126)
Sequence number (BE): 0 (0x0000)
Sequence number (LE): 0 (0x0000)
[Request frame: 105]
[Response time: 750.120 ms]
Timestamp from icmp data: May 2, 2018 14:42:00.870388000 CDT
[Timestamp from icmp data (relative): 0.750300000 seconds]
[Reliable (48 bytes)]

NetworkMiner Screenshot showing network traffic analysis.

Selected packet details:

No.	Source	Destination	Time	Protocol	Length	Info
123	202.70.64.2	150.243.152.75	1.9106...	TCP	1514	[TCP Out-Of-Order] 443 → 54948 [ACK] Seq=4482 Ac
124	150.243.152.75	202.70.64.2	1.9107...	TCP	86	54948 → 443 [ACK] Seq=1722 Ack=5930 Win=129680 L
125	202.70.64.2	150.243.152.75	1.9113...	TCP	1514	[TCP Out-Of-Order] 443 → 54948 [ACK] Seq=5930 Ac
126	202.70.64.2	150.243.152.75	1.9113...	TCP	97	[TCP Out-Of-Order] 443 → 54948 [PSH, ACK] Seq=87
127	202.70.64.2	150.243.152.75	1.9113...	ICMP	98	Echo (ping) reply id=0x26a1, seq=0/0, ttl=48
128	172.217.9.46	150.243.152.75	1.9113...	TLSv1.2	187	Application Data
129	150.243.152.75	202.70.64.2	1.9114...	TCP	78	54948 → 443 [ACK] Seq=1722 Ack=8720 Win=128256 L
130	202.70.64.2	150.243.152.75	1.9114...	TCP	66	54948 → 443 [ACK] Seq=1722 Ack=8752 Win=128224 L
131	150.243.152.75	172.217.9.46	1.9114...	TCP	66	54989 → 443 [ACK] Seq=1 Ack=122 Win=4092 Len=0 T
132	172.217.9.46	150.243.152.75	1.9115...	TLSv1.2	187	[TCP Spurious Retransmission], Application Data
133	150.243.152.75	172.217.9.46	1.9116...	TCP	78	[TCP Dup ACK 131#1] 54893 → 443 [ACK] Seq=1 Ack=
134	150.243.152.75	202.70.64.2	1.9126...	TCP	66	54948 → 443 [FIN, ACK] Seq=1722 Ack=8752 Win=131
135	150.243.152.75	224.0.0.251	2.0418...	IGMPv2	46	Membership Report group 224.0.0.251

Frame 127: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

Ethernet II, Src: Cisco_6c:47:00 (c0:67:a6:c4:47:00), Dst: Apple_dbe:ee:84 (9c:f3:87:db:ee:84)

Internet Protocol Version 4, Src: 202.70.64.2, Dst: 150.243.152.75

Internet Control Message Protocol

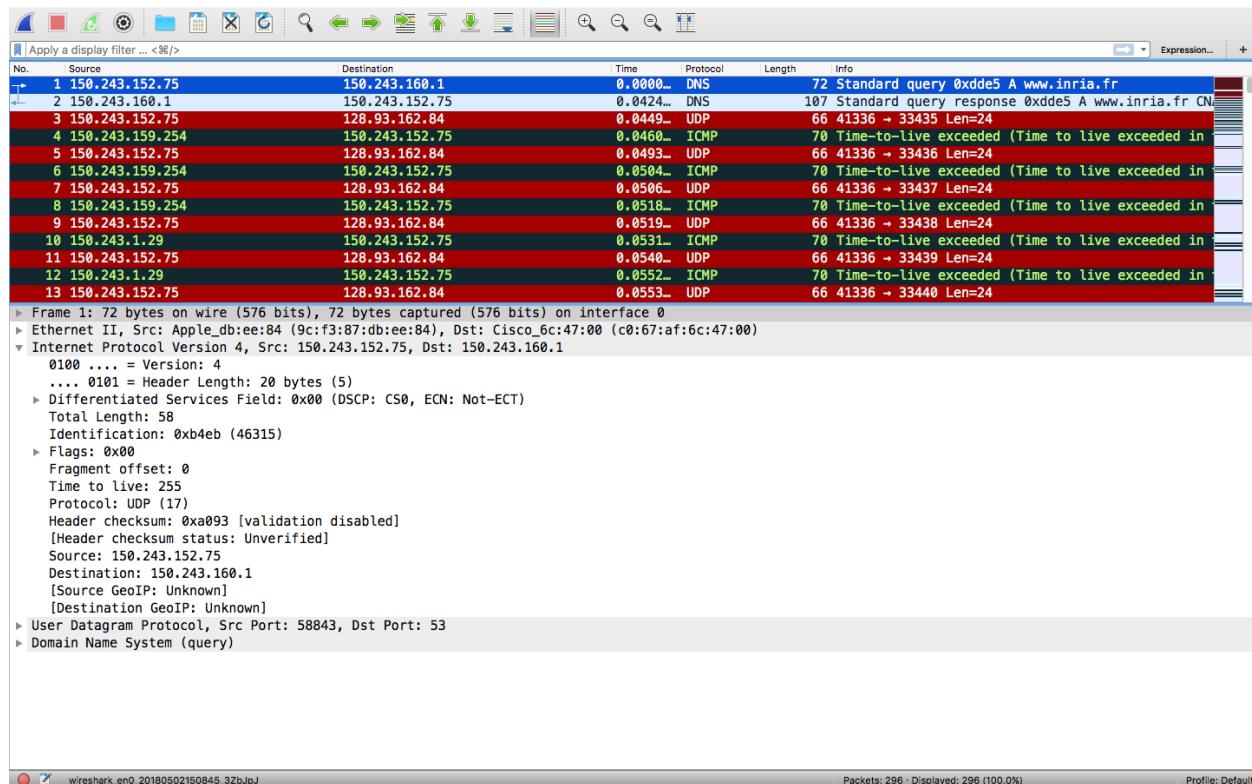
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x36e8 [correct]
[Checksum Status: Good]
Identifier (BE): 9889 (0x26a1)
Identifier (LE): 41254 (0xa126)
Sequence number (BE): 0 (0x0000)
Sequence number (LE): 0 (0x0000)
[\[Request frame: 1051\]](#)
[Response time: 750.120 ms]
Timestamp from icmp data: May 2, 2018 14:42:00.870388000 CDT
[Timestamp from icmp data (relative): 0.750300000 seconds]

Data (48 bytes)

The ICMP type and code are: 0,0. The ICMP packets have other fields like: checksum, identifier, sequence numbers and timestamps. the checksum, sequence number and identifier fields have 2 bytes.

The ICMP and TRACEROUTE

```
dikshya-air:~ dikshya96$ traceroute www.inria.fr
traceroute to ezp3.inria.fr (128.93.162.84), 64 hops max, 52 byte packets
 1  150.243.159.254 (150.243.159.254)  1.756 ms  1.250 ms  1.272 ms
 2  150.243.1.29 (150.243.1.29)  1.292 ms  1.216 ms  1.321 ms
 3  209.152.144.201 (209.152.144.201)  9.389 ms  9.045 ms  11.675 ms
 4  * * bluebird-network.10gigabitethernet5-4.core1.mci3.he.net (216.66.74.38)  16.843 ms
 5  10ge4-4.core1.mci3.he.net (216.66.74.37)  17.772 ms  16.301 ms  24.439 ms
 6  100ge8-1.core2.ch1.he.net (184.105.81.210)  36.219 ms  28.455 ms  29.313 ms
 7  100ge16-1.core1.nyc4.he.net (184.105.223.162)  50.205 ms  44.854 ms  45.221 ms
 8  100ge4-1.core1.par2.he.net (184.105.81.78)  120.110 ms  122.756 ms  129.347 ms
 9  renater.equinix-ix.fr (195.42.145.38)  120.969 ms
renater.par.franceix.net (37.49.236.19)  117.884 ms  117.407 ms
10  193.51.180.44 (193.51.180.44)  123.230 ms
xe0-1-2-paris1-rtr-131.noc.renater.fr (193.51.177.88)  119.226 ms  124.270 ms
11  * * *
12  inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr (193.51.184.177)  131.284 ms  117.066 ms  123.747 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
```



5. The IP address of the host and the target destination host is: 150.243.152.75 and 128.93.162.84

```

▼ Internet Protocol Version 4, Src: 150.243.152.75, Dst: 128.93.162.84
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0xa19b (41371)
▶ Flags: 0x00
  Fragment offset: 0
  Time to live: 12
  Protocol: UDP (17)
  Header checksum: 0xbb2d [validation disabled]
  [Header checksum status: Unverified]
  Source: 150.243.152.75
  Destination: 128.93.162.84
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
▶ User Datagram Protocol, Src Port: 41336, Dst Port: 33469
▶ Data (24 bytes)

```

6. The IP protocol number will not be 01 for the probe packets instead it will be 17.

```

Flags: 0x00
Fragment offset: 0
Time to live: 12
Protocol: UDP (17)
Header checksum: 0xbb2e [validation disabled]

```

7. Yes, it is different from the ICMP ping query packets in the first half of this lab. It has just the “time-to-live extended” information

No.	Source	Destination	Time	Protocol	Length	Info
4	150.243.159.254	150.243.152.75	0.0460...	ICMP	70	Time-to-live exceeded (Time to live exceeded in)
6	150.243.159.254	150.243.152.75	0.0504...	ICMP	70	Time-to-live exceeded (Time to live exceeded in)
8	150.243.159.254	150.243.152.75	0.0518...	ICMP	70	Time-to-live exceeded (Time to live exceeded in)
10	150.243.1.29	150.243.152.75	0.0531...	ICMP	70	Time-to-live exceeded (Time to live exceeded in)
12	150.243.1.29	150.243.152.75	0.0552...	ICMP	70	Time-to-live exceeded (Time to live exceeded in)
14	150.243.1.29	150.243.152.75	0.0565...	ICMP	70	Time-to-live exceeded (Time to live exceeded in)
16	209.152.144.201	150.243.152.75	0.0659...	ICMP	94	Time-to-live exceeded (Time to live exceeded in)
20	209.152.144.201	150.243.152.75	0.0794...	ICMP	94	Time-to-live exceeded (Time to live exceeded in)
22	209.152.144.201	150.243.152.75	0.0912...	ICMP	94	Time-to-live exceeded (Time to live exceeded in)
27	216.66.74.38	150.243.152.75	10.110...	ICMP	70	Time-to-live exceeded (Time to live exceeded in)
29	216.66.74.37	150.243.152.75	10.129...	ICMP	70	Time-to-live exceeded (Time to live exceeded in)
31	216.66.74.37	150.243.152.75	10.146...	ICMP	70	Time-to-live exceeded (Time to live exceeded in)
33	216.66.74.37	150.243.152.75	10.170...	ICMP	70	Time-to-live exceeded (Time to live exceeded in)

Frame 4: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: Cisco_6c:47:00 (c0:67:af:6c:47:00), Dst: Apple_db:ee:84 (9c:f3:87:db:ee:84)
 Internet Protocol Version 4, Src: 150.243.159.254, Dst: 150.243.152.75
 ▶ Internet Control Message Protocol
 Type: 11 (Time-to-Live exceeded)
 Code: 0 (Time to live exceeded in transit)
 Checksum: 0x4722 (correct)
 [Checksum Status: Good]
 ▶ Internet Protocol Version 4, Src: 150.243.152.75, Dst: 128.93.162.84
 ▶ User Datagram Protocol, Src Port: 41336, Dst Port: 33435
 ▶ Destination Port: 33435
 Length: 32
 Checksum: 0x89a9 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 1]

Internet Protocol Version 4 (ip), 20 bytes
 Packets: 298 - Displayed: 31 (10.5%) - Dropped: 0 (0.0%)
 Profile: Default

8. It includes the packet of the ping and also includes IPv4 and UDP.

▼	Internet Control Message Protocol
	Type: 11 (Time-to-live exceeded)
	Code: 0 (Time to live exceeded in transit)
	Checksum: 0x4722 [correct]
	[Checksum Status: Good]
►	Internet Protocol Version 4, Src: 150.243.152.75, Dst: 128.93.162.84
►	User Datagram Protocol, Src Port: 41336, Dst Port: 33435

9. It is different from the error packets as

- the code =
- type = 11
- TTL = 245
- Header checksum = unverified
- Flags “don’t fragment” is not in the last three ICMP packet.

They are different as all the datagram made it to the host before TTL expired.

No.	Source	Destination	Time	Protocol	Length	Info
103	150.243.152.75	209.85.234.189	23.911...	TCP	66	54779 → 443 [ACK] Seq=501 Ack=421 Win=4094 Len=0
104	150.243.152.75	128.93.162.84	26.525...	UDP	66	41336 → 33468 Len=24
105	193.51.184.177	150.243.152.75	26.656...	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
106	150.243.152.75	128.93.162.84	26.657...	UDP	66	41336 → 33469 Len=24
107	193.51.184.177	150.243.152.75	26.774...	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
108	150.243.152.75	128.93.162.84	26.774...	UDP	66	41336 → 33470 Len=24
109	193.51.184.177	150.243.152.75	26.897...	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
110	150.243.152.75	128.93.162.84	26.898...	UDP	66	41336 → 33471 Len=24
111	150.243.152.75	209.85.147.188	30.257...	TCP	54	64343 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
112	209.85.147.188	150.243.152.75	30.283...	TCP	66	[TCP ACKed unseen segment] 443 → 64343 [ACK] Seq=1 Ack=1 Win=4096 Len=0
113	150.243.152.75	128.93.162.84	31.983...	UDP	66	41336 → 33472 Len=24
114	150.243.152.75	128.93.162.84	36.908...	UDP	66	41336 → 33473 Len=24
115	Cisco_bd:34:90	Broadcast	38.244...	WLCCP	78	U, func=UI; SNAP, OUI 0x004096 (Cisco Wireless LAN Controller)

10. * Figure 4*

```
dikshyas-air:~ dikshya96$ traceroute www.inria.fr
traceroute to ezp3.inria.fr (128.93.162.84), 64 hops max, 52 byte packets
 1  150.243.159.254 (150.243.159.254)  1.756 ms  1.250 ms  1.272 ms
 2  150.243.1.29 (150.243.1.29)  1.292 ms  1.216 ms  1.321 ms
 3  209.152.144.201 (209.152.144.201)  9.389 ms  9.045 ms  11.675 ms
 4  * * bluebird-network.10gigabitethernet5-4.core1.mci3.he.net (216.66.74.38)  16.843 ms
 5  10ge4-4.core1.mci3.he.net (216.66.74.37)  17.772 ms  16.301 ms  24.439 ms
 6  100ge8-1.core2.chi1.he.net (184.105.81.210)  36.219 ms  28.455 ms  29.313 ms
 7  100ge16-1.core1.ny4.he.net (184.105.223.162)  50.205 ms  44.854 ms  45.221 ms
 8  100ge4-1.core1.par2.he.net (184.105.81.78)  120.110 ms  122.756 ms  129.347 ms
 9  renater.equinix-ix.fr (195.42.145.38)  120.969 ms
     renater.par.franceix.net (37.49.236.19)  117.884 ms  117.407 ms
10  193.51.180.44 (193.51.180.44)  123.230 ms
     xe0-1-2-paris1-rtr-131.noc.renater.fr (193.51.177.88)  119.226 ms  124.270 ms
11  * * *
12  inria-roquencourt-te1-4-inria-rtr-021.noc.renater.fr (193.51.184.177)  131.284 ms  117.066 ms  123.747 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
```

In Line 7 and Line 8, we can find a huge time difference. Line 8 has significantly longer delay. The IP address on Line 7; 184.105.223.162 is from New York, USA while the IP address in Line 8; 184.105.81.78 is from Paris, France. This is a transatlantic.