

Juan Miguel C. Manalo
2014-40093
CS 145 THWMXY-HONOR

CS145 Lab Exercise 3: Wireshark Lab - Internet Protocol and Traceroute Operation

1. 9 routers, not including the server hosting the Philippine Daily Inquirer.

```
Terminal
traceroute to www.inquirer.net (104.20.30.186), 30 hops max, 60 byte packets
 1 10.40.80.1 (10.40.80.1) 0.622 ms 0.782 ms 0.939 ms
 2 10.255.0.149 (10.255.0.149) 0.505 ms 0.789 ms 1.006 ms
 3 nat.upd.edu.ph (10.16.1.2) 0.278 ms 0.275 ms 0.266 ms
 4 border-gateway.upd.edu.ph (202.92.128.254) 1.010 ms 1.052 ms 0.964 ms
 5 111.125.73.1 (111.125.73.1) 2.134 ms 2.119 ms 2.139 ms
 6 202.69.178.97 (202.69.178.97) 1.852 ms 1.896 ms 1.847 ms
 7 202.69.174.26 (202.69.174.26) 12.997 ms 12.566 ms 12.573 ms
 8 202.69.178.42 (202.69.178.42) 1.868 ms 1.858 ms 1.850 ms
 9 117.58.222.128 (117.58.222.128) 21.825 ms 21.776 ms 21.804 ms
10 104.20.30.186 (104.20.30.186) 21.582 ms 22.848 ms 22.839 ms
CS145THWMXYHONOR@t3-25 ~$ traceroute www.inquirer.net
 1 10.40.80.1 (10.40.80.1) 0.511 ms 0.941 ms 1.115 ms
 2 10.255.0.149 (10.255.0.149) 0.518 ms 0.782 ms 0.964 ms
 3 nat.upd.edu.ph (10.16.1.2) 0.240 ms 0.252 ms 0.242 ms
 4 border-gateway.upd.edu.ph (202.92.128.254) 1.093 ms 1.084 ms 1.056 ms
 5 111.125.73.1 (111.125.73.1) 2.324 ms 2.173 ms 2.309 ms
 6 202.69.178.97 (202.69.178.97) 1.867 ms 1.717 ms 1.661 ms
 7 202.69.174.26 (202.69.174.26) 1.675 ms 1.756 ms 1.741 ms
 8 202.69.178.42 (202.69.178.42) 1.621 ms 1.652 ms 1.599 ms
 9 117.58.222.128 (117.58.222.128) 21.608 ms 21.600 ms 21.683 ms
10 104.20.31.186 (104.20.31.186) 21.425 ms 21.523 ms 21.605 ms
CS145THWMXYHONOR@t3-25 ~$
```

2. Packet #7

Filter: udp

No.	Time	Source	Destination	Protocol	Length	Info
3	3.719652000	10.40.80.35	10.32.1.7	DNS	76	Standard query 0x4068
4	3.719713000	10.40.80.35	10.32.1.7	DNS	76	Standard query 0x4068
5	3.720345000	10.32.1.7	10.40.80.35	DNS	250	Standard query response 0x4068
6	3.720345000	10.32.1.7	10.40.80.35	DNS	274	Standard query response 0x4068
7	3.743855000	10.40.80.35	104.20.30.186	UDP	74	Source port: 43222
8	3.743891000	10.40.80.35	104.20.30.186	UDP	74	Source port: 46673
9	3.743926000	10.40.80.35	104.20.30.186	UDP	74	Source port: 57327
10	3.743951000	10.40.80.35	104.20.30.186	UDP	74	Source port: 33886
11	3.743981000	10.40.80.35	104.20.30.186	UDP	74	Source port: 37535
12	3.744003000	10.40.80.35	104.20.30.186	UDP	74	Source port: 57261
13	3.744022000	10.40.80.35	104.20.30.186	UDP	74	Source port: 54893
14	3.744040000	10.40.80.35	104.20.30.186	UDP	74	Source port: 46060

Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: WistronI_c6:55:e6 (f8:0f:41:c6:55:e6), Dst: Cisco_f6:ec:48 (c0:62:6b:f6:ec:48)

Internet Protocol Version 4, Src: 10.40.80.35 (10.40.80.35), Dst: 104.20.30.186 (104.20.30.186)

Version: 4

Header Length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

Total Length: 60

Identification: 0x8327 (33575)

Flags: 0x00

Fragment offset: 0

Time to live: 1

Protocol: UDP (17)

Header checksum: 0x5571 [validation disabled]

Source: 10.40.80.35 (10.40.80.35)

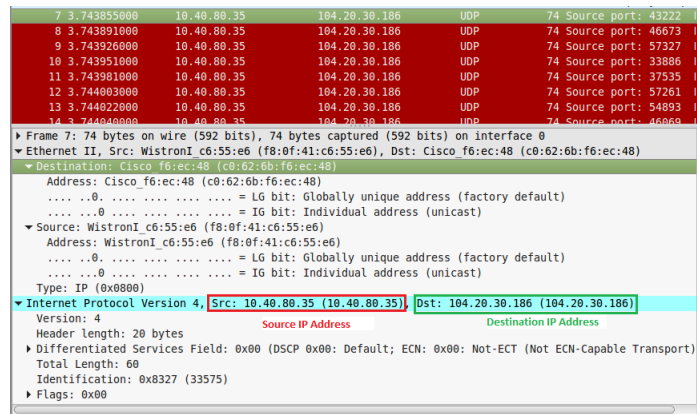
Destination: 104.20.30.186 (104.20.30.186)

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

User Datagram Protocol, Src Port: 43222 (43222), Dst Port: traceroute (33434)

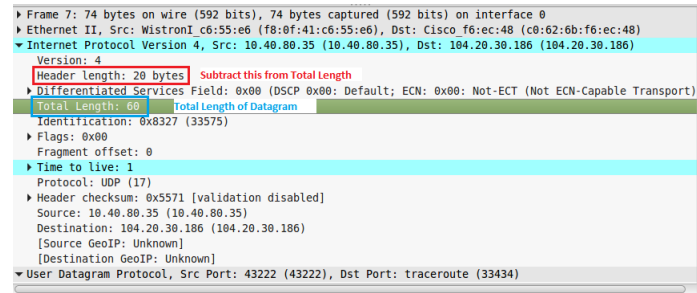
3. IP Address (Computer): 10.40.80.35
IP Address (Website): 104.20.30.186



4. IP Header: **20 bytes**

IP Datagram Payload: **40 bytes**

As annotated, the total length of the IP Datagram is 60 bytes. To get the payload, subtract the IP Header bytes from the total length of the datagram. Hence, $60 - 20 = 40$ bytes.



5. The Identification and the Checksum. They are as follows:

- Packet #7: 0x8327 (Identification), 0x5571 (Checksum)
- Packet #8: 0x8328 (Identification), 0x5570 (Checksum)
- Packet #9: 0x8329 (Identification), 0x556f (Checksum)

6. The Internet Protocol Version, Header Length, Differentiated Services Field, Flags, TTL, Protocol, Source, and Destination.

7. The values in the Identification field increase by 1 each succeeding packet.

8. Traceroute does not assume that the ICMP messages will arrive in order. It depends on the delay time of each UDP packet. An ICMP message is associated to its corresponding UDP packet through the Source and Destination Ports in the UDP header.

No.	Time	Source	Destination	Protocol	Length	Info
12	3.744003	10.40.80.35	104.20.30.186	UDP	74	57261 → 33439 Len=32
13	3.744022	10.40.80.35	104.20.30.186	UDP	74	54893 → 33440 Len=32
14	3.744040	10.40.80.35	104.20.30.186	UDP	74	46069 → 33441 Len=32
15	3.744063	10.40.80.35	104.20.30.186	UDP	74	33848 → 33442 Len=32
16	3.744088	10.40.80.35	104.20.30.186	UDP	74	38814 → 33443 Len=32
17	3.744110	10.40.80.35	104.20.30.186	UDP	74	38999 → 33444 Len=32
18	3.744127	10.40.80.35	104.20.30.186	UDP	74	58659 → 33445 Len=32
19	3.744160	10.40.80.35	104.20.30.186	UDP	74	39737 → 33446 Len=32
20	3.744182	10.40.80.35	104.20.30.186	UDP	74	33465 → 33447 Len=32
21	3.744204	10.40.80.35	104.20.30.186	UDP	74	39933 → 33448 Len=32
22	3.744214	10.16.1.2	10.40.80.35	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
23	3.744226	10.40.80.35	104.20.30.186	UDP	74	44931 → 33449 Len=32
24	3.744238	10.16.1.2	10.40.80.35	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
25	3.744245	10.16.1.2	10.40.80.35	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
26	3.744279	10.40.80.35	104.20.30.186	UDP	74	56907 → 33450 Len=32
27	3.744323	10.40.80.35	104.20.30.186	UDP	74	48215 → 33451 Len=32

▶ Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 ▶ Ethernet II, Src: WistronI_c6:55:e6 (f8:0f:41:c6:55:e6), Dst: Cisco_f6:ec:48 (c0:62:6b:f6:ec:48)
 ▶ Internet Protocol Version 4, Src: 10.40.80.35, Dst: 104.20.30.186
 ▶ User Datagram Protocol, Src Port: 54893, Dst Port: 33440
 ▶ Data (32 bytes)

The Source and Destination Ports are the same as its corresponding ICMP message.

9. Packet #22 (caused by Packet #13)

No.	Time	Source	Destination	Protocol	Length	Info
12	3.744003	10.40.80.35	104.20.30.186	UDP	74	57261 → 33439 Len=32
13	3.744022	10.40.80.35	104.20.30.186	UDP	74	54893 → 33440 Len=32
14	3.744040	10.40.80.35	104.20.30.186	UDP	74	46069 → 33441 Len=32
15	3.744063	10.40.80.35	104.20.30.186	UDP	74	33848 → 33442 Len=32
16	3.744088	10.40.80.35	104.20.30.186	UDP	74	38814 → 33443 Len=32
17	3.744110	10.40.80.35	104.20.30.186	UDP	74	38999 → 33444 Len=32
18	3.744127	10.40.80.35	104.20.30.186	UDP	74	58659 → 33445 Len=32
19	3.744160	10.40.80.35	104.20.30.186	UDP	74	39737 → 33446 Len=32
20	3.744182	10.40.80.35	104.20.30.186	UDP	74	33465 → 33447 Len=32
21	3.744204	10.40.80.35	104.20.30.186	UDP	74	39933 → 33448 Len=32
22	3.744214	10.16.1.2	10.40.80.35	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

▶ Frame 22: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 ▶ Ethernet II, Src: Cisco_f6:ec:48 (c0:62:6b:f6:ec:48), Dst: WistronI_c6:55:e6 (f8:0f:41:c6:55:e6)
 ▶ Internet Protocol Version 4, Src: 10.16.1.2, Dst: 10.40.80.35
 ▶ Internet Control Message Protocol
 Type: 11 (Time-to-live exceeded)
 Code: 0 (Time to live exceeded in transit)
 Checksum: 0xc57 [correct]
 [Checksum Status: Good]
 ▶ Internet Protocol Version 4, Src: 10.40.80.35, Dst: 104.20.30.186
 ▶ User Datagram Protocol, Src Port: 54893, Dst Port: 33440
 Source Port: 54893
 Destination Port: 33440
 Length: 40
 Checksum: 0xd071 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 8]

This is an ICMP Protocol, reading "Time-to-live exceeded".

Notice the IP Address and Ports of the Source and Destination. They are the same as those in Packet #13.

No.	Time	Source	Destination	Protocol	Length	Info
12	3.744003	10.40.80.35	104.20.30.186	UDP	74	57261 → 33439 Len=32
13	3.744022	10.40.80.35	104.20.30.186	UDP	74	54893 → 33440 Len=32
14	3.744040	10.40.80.35	104.20.30.186	UDP	74	46069 → 33441 Len=32
15	3.744063	10.40.80.35	104.20.30.186	UDP	74	33848 → 33442 Len=32
16	3.744088	10.40.80.35	104.20.30.186	UDP	74	38814 → 33443 Len=32
17	3.744110	10.40.80.35	104.20.30.186	UDP	74	38999 → 33444 Len=32
18	3.744127	10.40.80.35	104.20.30.186	UDP	74	58659 → 33445 Len=32
19	3.744160	10.40.80.35	104.20.30.186	UDP	74	39737 → 33446 Len=32
20	3.744182	10.40.80.35	104.20.30.186	UDP	74	33465 → 33447 Len=32
21	3.744204	10.40.80.35	104.20.30.186	UDP	74	39933 → 33448 Len=32
22	3.744214	10.16.1.2	10.40.80.35	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Fragment offset: 0
 Time to live: 3 Packet's TTL=3
 Protocol: UDP (17)
 Header checksum: 0x536b [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.40.80.35
 Destination: 104.20.30.186
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 ▶ User Datagram Protocol, Src Port: 54893, Dst Port: 33440
 Source Port: 54893
 Destination Port: 33440
 Length: 40
 Checksum: 0xe152 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 8]

The Source and Destination IP Addresses are the same as described in the ICMP message.

The Source and Destination Ports are the same as described in the packet's corresponding ICMP message (Packet #22).

10. Timestamp Delays:

- UDP1 = 3.744214 s - 3.744022 s = 192 ms
- UDP2 = 3.744238 s - 3.744040 s = 198 ms
- UDP3 = 3.744245 s - 3.744063 s = 182 ms

Delay based on Traceroute Values:

#	UDP1	UDP2	UDP3
1	0.622 ms	0.782 ms	0.939 ms
2	0.505 ms	0.789 ms	1.006 ms
3	0.278 ms	0.275 ms	0.266 ms
4	1.010 ms	1.052 ms	0.964 ms
5	2.134 ms	2.119 ms	2.139 ms
6	1.852 ms	1.896 ms	1.847 ms
7	12.997 ms	12.566 ms	12.573 ms
8	1.868 ms	1.858 ms	1.850 ms
9	21.825 ms	21.776 ms	21.804 ms
10	21.582 ms	22.848 ms	22.839 ms
Total	64.673 ms	65.961 ms	66.281 ms
X Hops (3)	194.02 ms	197.88 ms	198.84 ms

No.	Time	Source	Destination	Protocol	Length	Info
12	3.744093	10.40.80.35	104.20.30.186	UDP	74	57261 → 33439 Len=32
13	3.744022	10.40.80.35	104.20.30.186	UDP	74	54893 → 33440 Len=32
14	3.744040	10.40.80.35	104.20.30.186	UDP	74	46069 → 33441 Len=32
15	3.744063	10.40.80.35	104.20.30.186	UDP	74	33848 → 33442 Len=32
19	3.744160	10.40.80.35	104.20.30.186	UDP	74	39737 → 33446 Len=32
22	3.744214	10.16.1.2	10.40.80.35	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
23	3.744226	10.40.80.35	104.20.30.186	UDP	74	44931 → 33449 Len=32
24	3.744238	10.16.1.2	10.40.80.35	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
25	3.744245	10.16.1.2	10.40.80.35	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
26	3.744279	10.40.80.35	104.20.30.186	UDP	74	56907 → 33450 Len=32
27	3.744323	10.40.80.35	104.20.30.186	UDP	74	48215 → 33451 Len=32

```
Terminal
traceroute to www.inquirer.net (104.20.30.186), 30 hops max, 60 byte packets
 1 10.40.80.1 (10.40.80.1) 0.622 ms 0.782 ms 0.939 ms
 2 10.255.0.149 (10.255.0.149) 0.505 ms 0.789 ms 1.006 ms
 3 nat.upd.edu.ph (10.16.1.2) 0.278 ms 0.275 ms 0.266 ms
 4 border-gateway.upd.edu.ph (202.92.128.254) 1.010 ms 1.052 ms 0.964 ms
 5 111.125.73.1 (111.125.73.1) 2.134 ms 2.119 ms 2.139 ms
 6 202.69.178.97 (202.69.178.97) 1.852 ms 1.896 ms 1.847 ms
 7 202.69.174.26 (202.69.174.26) 12.997 ms 12.566 ms 12.573 ms
 8 202.69.178.42 (202.69.178.42) 1.868 ms 1.858 ms 1.850 ms
 9 117.58.222.128 (117.58.222.128) 21.825 ms 21.776 ms 21.804 ms
10 104.20.30.186 (104.20.30.186) 21.582 ms 22.848 ms 22.839 ms
CS145THWMMXYHONOR@t13-25 ~ $ traceroute www.inquirer.net
traceroute to www.inquirer.net (104.20.31.186), 30 hops max, 60 byte packets
 1 10.40.80.1 (10.40.80.1) 0.511 ms 0.941 ms 1.115 ms
 2 10.255.0.149 (10.255.0.149) 0.518 ms 0.782 ms 0.964 ms
 3 nat.upd.edu.ph (10.16.1.2) 0.240 ms 0.252 ms 0.242 ms
 4 border-gateway.upd.edu.ph (202.92.128.254) 1.093 ms 1.084 ms 1.056 ms
 5 111.125.73.1 (111.125.73.1) 2.324 ms 2.173 ms 2.309 ms
 6 202.69.178.97 (202.69.178.97) 1.867 ms 1.717 ms 1.661 ms
 7 202.69.174.26 (202.69.174.26) 1.675 ms 1.756 ms 1.741 ms
 8 202.69.178.42 (202.69.178.42) 1.621 ms 1.652 ms 1.599 ms
 9 117.58.222.128 (117.58.222.128) 21.608 ms 21.600 ms 21.683 ms
10 104.20.31.186 (104.20.31.186) 21.425 ms 21.523 ms 21.605 ms
CS145THWMMXYHONOR@t13-25 ~ $
```