

Student Information

Full Name: İsmail Şahin
ID Number: 2264653

Answer 1

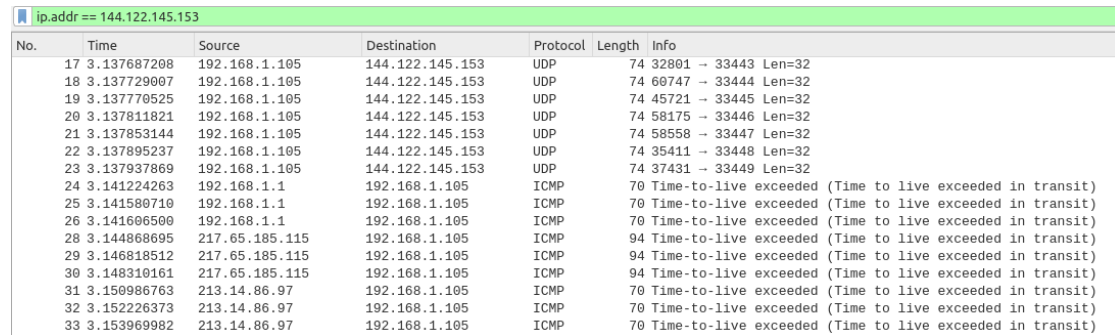
As you see from output above (Figure ??), I have not been able to see the whole path to the metu.edu.tr. Because, In the fourth and all outputs after fifth one I got ‘***’ as output. This means that the hop does not respond. I have send my UDP packet but, I did not get any ICMP response in a time such as 5sec(timeout interval). It can be because of firewalls or some other network problems. Some hops does not response to udp message.

```
ismail@ismail-laptop:~$ traceroute metu.edu.tr
traceroute to metu.edu.tr (144.122.145.153), 30 hops max, 60 byte packets
 1 _gateway (192.168.1.1)  4.058 ms  4.278 ms  4.233 ms
 2 217.65.185.115 (217.65.185.115)  7.448 ms  9.355 ms  10.803 ms
 3 host-213-14-86-97.reverse.supersonic.net (213.14.86.97)  13.437 ms  14.634 ms  16.334 ms
 4 * * *
 5 144.122.1.18 (144.122.1.18)  56.804 ms  56.810 ms  56.782 ms
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
ismail@ismail-laptop:~$
```

Figure 1: A caption that is output of the traceroute

Answer 2

We can understand from wireshark capture above (Figure ??) that, as a default method, traceroute sends UDP probe packets with ttl and listens for an ICMP (time exceed) reply from a gateway. It starts with a ttl of one and increases ttl one by one until it get a ICMP (port unreachable) reply or hit max. This is generally 30 hops as default.



No.	Time	Source	Destination	Protocol	Length	Info
17	3.137687208	192.168.1.105	144.122.145.153	UDP	74	32801 → 33443 Len=32
18	3.137729007	192.168.1.105	144.122.145.153	UDP	74	60747 → 33444 Len=32
19	3.137770525	192.168.1.105	144.122.145.153	UDP	74	45721 → 33445 Len=32
20	3.137811821	192.168.1.105	144.122.145.153	UDP	74	58175 → 33446 Len=32
21	3.137853144	192.168.1.105	144.122.145.153	UDP	74	58558 → 33447 Len=32
22	3.137895237	192.168.1.105	144.122.145.153	UDP	74	35411 → 33448 Len=32
23	3.137937869	192.168.1.105	144.122.145.153	UDP	74	37431 → 33449 Len=32
24	3.141224263	192.168.1.1	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
25	3.141580710	192.168.1.1	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
26	3.141606500	192.168.1.1	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
28	3.144868695	217.65.185.115	192.168.1.105	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
29	3.146818512	217.65.185.115	192.168.1.105	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
30	3.148310161	217.65.185.115	192.168.1.105	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
31	3.150986763	213.14.86.97	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
32	3.152226373	213.14.86.97	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
33	3.153969982	213.14.86.97	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Figure 2: A caption that is output of the wireshark

Answer 3

When we used -I flag, We used ICMP ECHO for probes. This means that we sent ICMP probe packets not UDP packets. We changed protocol that we used to send packets. I got different Wireshark capture because, Protocol is changed and every protocol can have some different rules. From wireshark capture, we can see that there is no UDP packet send. I got different route trace because, some routers or gateways can act on type of packet (UDP,ICMP etc.) My traceroute and wireshark outputs are above (Figure ??, Figure ??).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.1	224.0.0.1	IGMPv2	60	Membership Query, general
2	0.000407135	192.168.1.1	224.0.0.12	IGMPv2	60	Membership Report group 224.0.0.12
3	0.204799177	192.168.1.107	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
4	1.573390236	192.168.1.105	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
5	2.381075549	192.168.1.105	192.168.1.1	DNS	82	Standard query 0xf177 AAAA metu.edu.tr OPT
6	2.424854058	192.168.1.1	192.168.1.105	DNS	133	Standard query response 0xf177 AAAA metu.edu.tr SOA ns1.metu...
7	2.425464233	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=1/256, ttl=1 (no response...
8	2.425513499	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=2/512, ttl=1 (no response...
9	2.425535799	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=3/768, ttl=1 (no response...
10	2.425559028	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=4/1024, ttl=2 (no respons...
11	2.425576308	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=5/1280, ttl=2 (no respons...
12	2.425596283	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=6/1536, ttl=2 (no respons...
13	2.425616474	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=7/1792, ttl=3 (no respons...
14	2.425634856	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=8/2048, ttl=3 (no respons...
15	2.425647285	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=9/2304, ttl=3 (no respons...
16	2.425660540	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=10/2560, ttl=4 (no respon...
17	2.425672531	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=11/2816, ttl=4 (no respon...
18	2.425684712	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=12/3072, ttl=4 (no respon...
19	2.425698307	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=13/3328, ttl=5 (no respon...
20	2.425709650	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=14/3584, ttl=5 (no respon...
21	2.425720691	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=15/3840, ttl=5 (no respon...
22	2.425734187	192.168.1.105	144.122.145.153	ICMP	74	Echo (ping) request id=0x0008, seq=16/4096, ttl=6 (no respon...
23	2.428998669	192.168.1.1	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
24	2.429247215	192.168.1.1	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Figure 3: A caption that is output of the wireshark

```
ismail@ismail-laptop:~$ traceroute metu.edu.tr -I
traceroute to metu.edu.tr (144.122.145.153), 30 hops max, 60 byte packets
 1  gateway (192.168.1.1)  3.567 ms  3.746 ms  3.761 ms
 2  217.65.185.115 (217.65.185.115)  8.483 ms  8.864 ms  10.838 ms
 3  host-213-14-86-97.reverse.superonline.net (213.14.86.97)  13.026 ms  14.710 ms  15.946 ms
 4  144.122.1.18 (144.122.1.18)  31.803 ms  31.834 ms  33.774 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
ismail@ismail-laptop:~$
```

Figure 4: A caption that is output of the traceroute

Answer 4

- www.unaj.edu.ar - 170.210.44.19 (Argentina)
- upm.edu.my - 211.25.98.234 (Malaysia)

(Bonus) Firstly I tried to reach to website of National University Guillermo Brown (www.unab.edu.ar) but I couldn't. I reached to 170.210.0.33(closest one) ip adress. After that I used -I option (that uses ICMP to send requests) but, I got same result. After that I tried with -T option that uses TCP protocol to send request and being secure of TCP, generally requests are not firewalled and not lost. With -T option I have reached to website.

Answer 5

Value is ICMP (1).

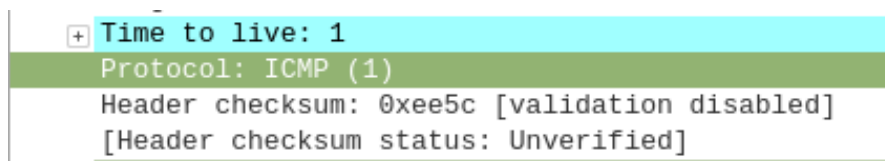


Figure 5: A caption that is IPv4 protocol value.

Answer 6

20 bytes are in IP header. Total length is 92 bytes. If we subtract IP header from total length, we find bytes in the payload of the IP datagram so, there is 72 bytes in the payload of the IP datagram.

Answer 7

Identification field : 0x9987 (39303)

TTL field : 246

These values changes among other TTL exceeded packets. Identification field is unique value, it changes in all messages. TTL field is not unique, it can be same in some messages but it can change message to message.

Answer 8

If more fragments bit become 1 (set), we can tell that the datagram has been fragmented but, as we see from the figure, More fragments bit is 1, so the datagram has been fragmented.

```
[-] Flags: 0x2000, More fragments
    0... .. = Reserved bit: Not set
    .0... .. = Don't fragment: Not set
    ..1. .... = More fragments: Set
```

Figure 6: A caption that is IPv4 value.

Answer 9

When I look at the first datagram of ip header, I cannot tell how many fragments have been created by the fragmentation. I can only know that if there is fragment after that with more fragments bit.

However, If I look at wireshark capture, I see that the frame is number 3 and it is first one (from offset) and it say that it is reassembled in frame 5. This means that three (3,4,5) fragment has been created by fragmentation.

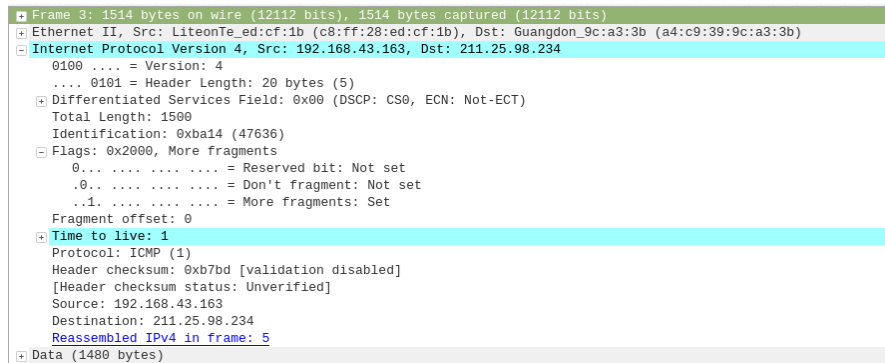


Figure 7: A caption that is IPv4 value.

Answer 10

- Total length
- Flags
- Fragment offset
- Checksum