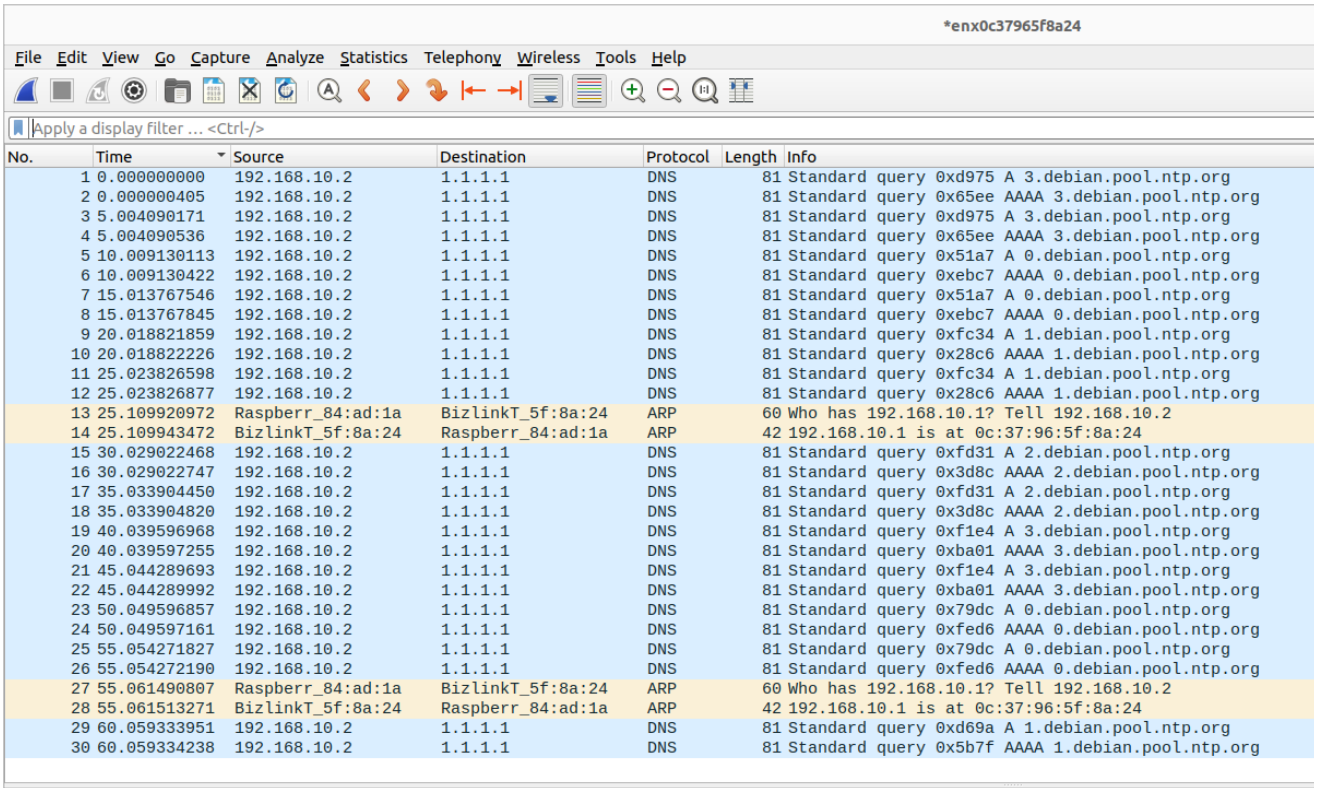
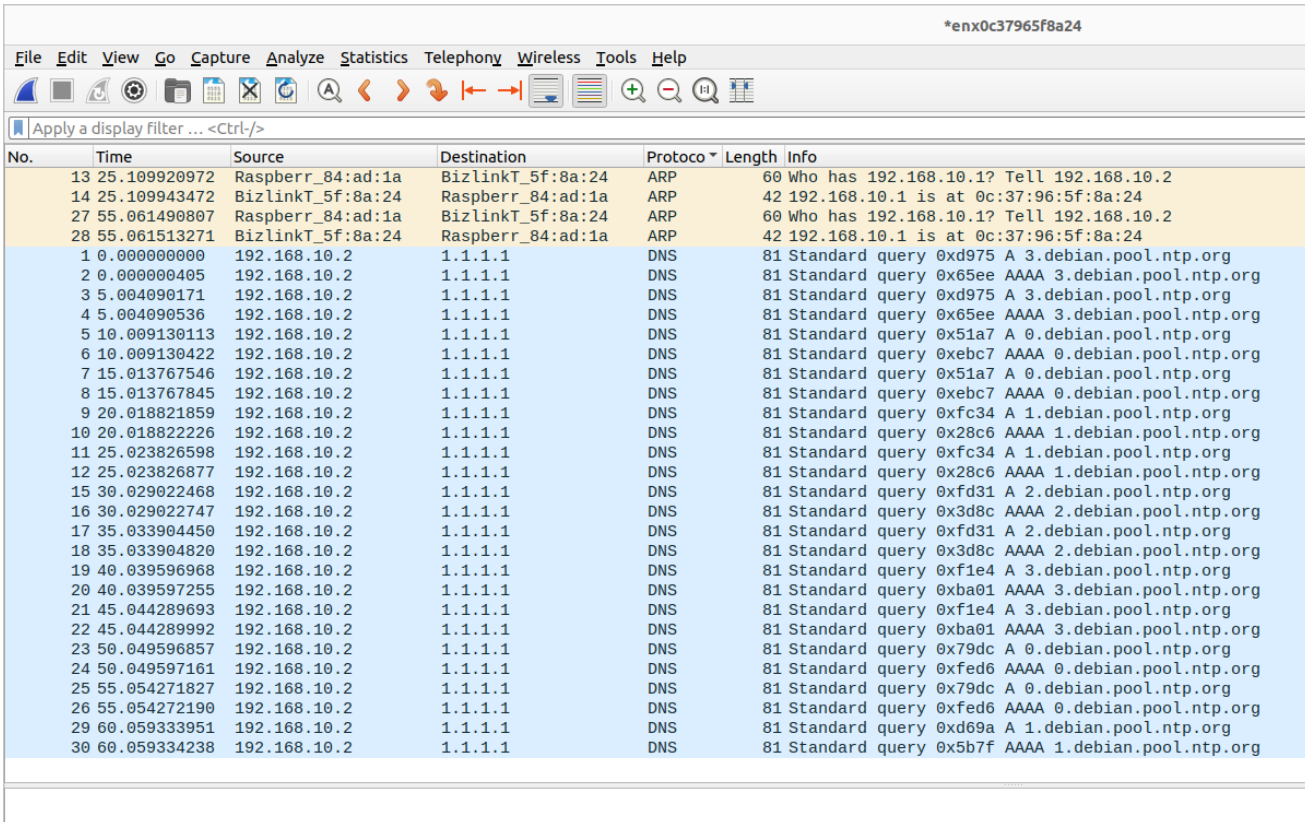
Exercise 1

Traffic Capture:
Task 1



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xd975 A 3.debian.pool.ntp.org
2	0.000000405	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x65ee AAAA 3.debian.pool.ntp.org
3	5.004090171	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xd975 A 3.debian.pool.ntp.org
4	5.004090536	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x65ee AAAA 3.debian.pool.ntp.org
5	10.009130113	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x51a7 A 0.debian.pool.ntp.org
6	10.009130422	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xebc7 AAAA 0.debian.pool.ntp.org
7	15.013767546	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x51a7 A 0.debian.pool.ntp.org
8	15.013767845	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xebc7 AAAA 0.debian.pool.ntp.org
9	20.018821859	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfc34 A 1.debian.pool.ntp.org
10	20.018822226	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x28c6 AAAA 1.debian.pool.ntp.org
11	25.023826598	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfc34 A 1.debian.pool.ntp.org
12	25.023826877	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x28c6 AAAA 1.debian.pool.ntp.org
13	25.109920972	Raspberr_84:ad:1a	BizlinkT_5f:8a:24	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
14	25.109943472	BizlinkT_5f:8a:24	Raspberr_84:ad:1a	ARP	42	192.168.10.1 is at 0c:37:96:5f:8a:24
15	30.029022468	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfd31 A 2.debian.pool.ntp.org
16	30.029022747	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x3d8c AAAA 2.debian.pool.ntp.org
17	35.033904450	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfd31 A 2.debian.pool.ntp.org
18	35.033904820	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x3d8c AAAA 2.debian.pool.ntp.org
19	40.039596968	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xf1e4 A 3.debian.pool.ntp.org
20	40.039597255	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xba01 AAAA 3.debian.pool.ntp.org
21	45.044289693	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xf1e4 A 3.debian.pool.ntp.org
22	45.044289992	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xba01 AAAA 3.debian.pool.ntp.org
23	50.049596857	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x79dc A 0.debian.pool.ntp.org
24	50.049597161	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfed6 AAAA 0.debian.pool.ntp.org
25	55.054271827	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x79dc A 0.debian.pool.ntp.org
26	55.054272190	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfed6 AAAA 0.debian.pool.ntp.org
27	55.061490807	Raspberr_84:ad:1a	BizlinkT_5f:8a:24	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
28	55.061513271	BizlinkT_5f:8a:24	Raspberr_84:ad:1a	ARP	42	192.168.10.1 is at 0c:37:96:5f:8a:24
29	60.059333951	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xd69a A 1.debian.pool.ntp.org
30	60.059334238	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x5b7f AAAA 1.debian.pool.ntp.org

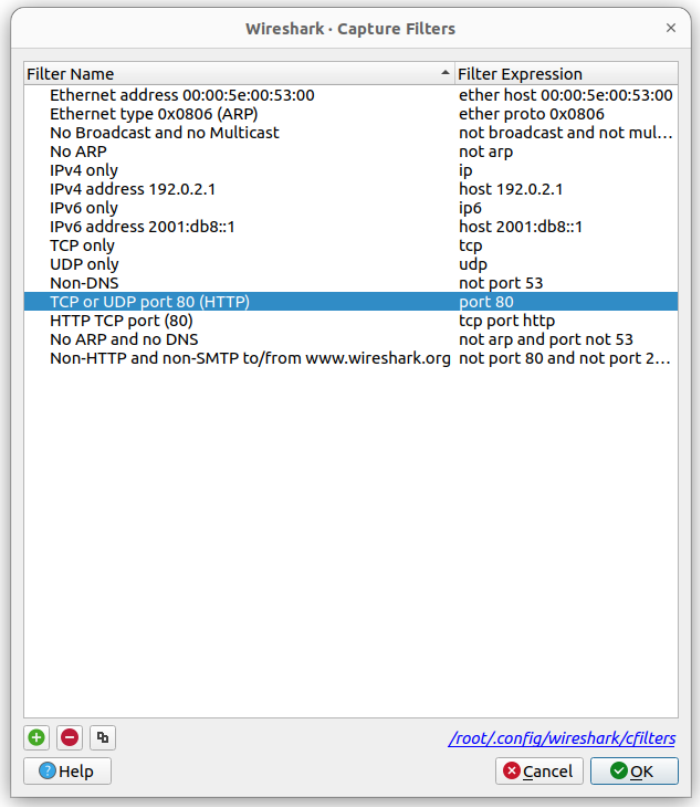


No.	Time	Source	Destination	Protocol	Length	Info
13	25.109920972	Raspberr_84:ad:1a	BizlinkT_5f:8a:24	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
14	25.109943472	BizlinkT_5f:8a:24	Raspberr_84:ad:1a	ARP	42	192.168.10.1 is at 0c:37:96:5f:8a:24
27	55.061490807	Raspberr_84:ad:1a	BizlinkT_5f:8a:24	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
28	55.061513271	BizlinkT_5f:8a:24	Raspberr_84:ad:1a	ARP	42	192.168.10.1 is at 0c:37:96:5f:8a:24
1	0.000000000	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xd975 A 3.debian.pool.ntp.org
2	0.000000405	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x65ee AAAA 3.debian.pool.ntp.org
3	5.004090171	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xd975 A 3.debian.pool.ntp.org
4	5.004090536	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x65ee AAAA 3.debian.pool.ntp.org
5	10.009130113	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x51a7 A 0.debian.pool.ntp.org
6	10.009130422	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xebc7 AAAA 0.debian.pool.ntp.org
7	15.013767546	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x51a7 A 0.debian.pool.ntp.org
8	15.013767845	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xebc7 AAAA 0.debian.pool.ntp.org
9	20.018821859	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfc34 A 1.debian.pool.ntp.org
10	20.018822226	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x28c6 AAAA 1.debian.pool.ntp.org
11	25.023826598	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfc34 A 1.debian.pool.ntp.org
12	25.023826877	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x28c6 AAAA 1.debian.pool.ntp.org
15	30.029022468	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfd31 A 2.debian.pool.ntp.org
16	30.029022747	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x3d8c AAAA 2.debian.pool.ntp.org
17	35.033904450	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfd31 A 2.debian.pool.ntp.org
18	35.033904820	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x3d8c AAAA 2.debian.pool.ntp.org
19	40.039596968	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xf1e4 A 3.debian.pool.ntp.org
20	40.039597255	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xba01 AAAA 3.debian.pool.ntp.org
21	45.044289693	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xf1e4 A 3.debian.pool.ntp.org
22	45.044289992	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xba01 AAAA 3.debian.pool.ntp.org
23	50.049596857	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x79dc A 0.debian.pool.ntp.org
24	50.049597161	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfed6 AAAA 0.debian.pool.ntp.org
25	55.054271827	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x79dc A 0.debian.pool.ntp.org
26	55.054272190	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xfed6 AAAA 0.debian.pool.ntp.org
29	60.059333951	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xd69a A 1.debian.pool.ntp.org
30	60.059334238	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x5b7f AAAA 1.debian.pool.ntp.org

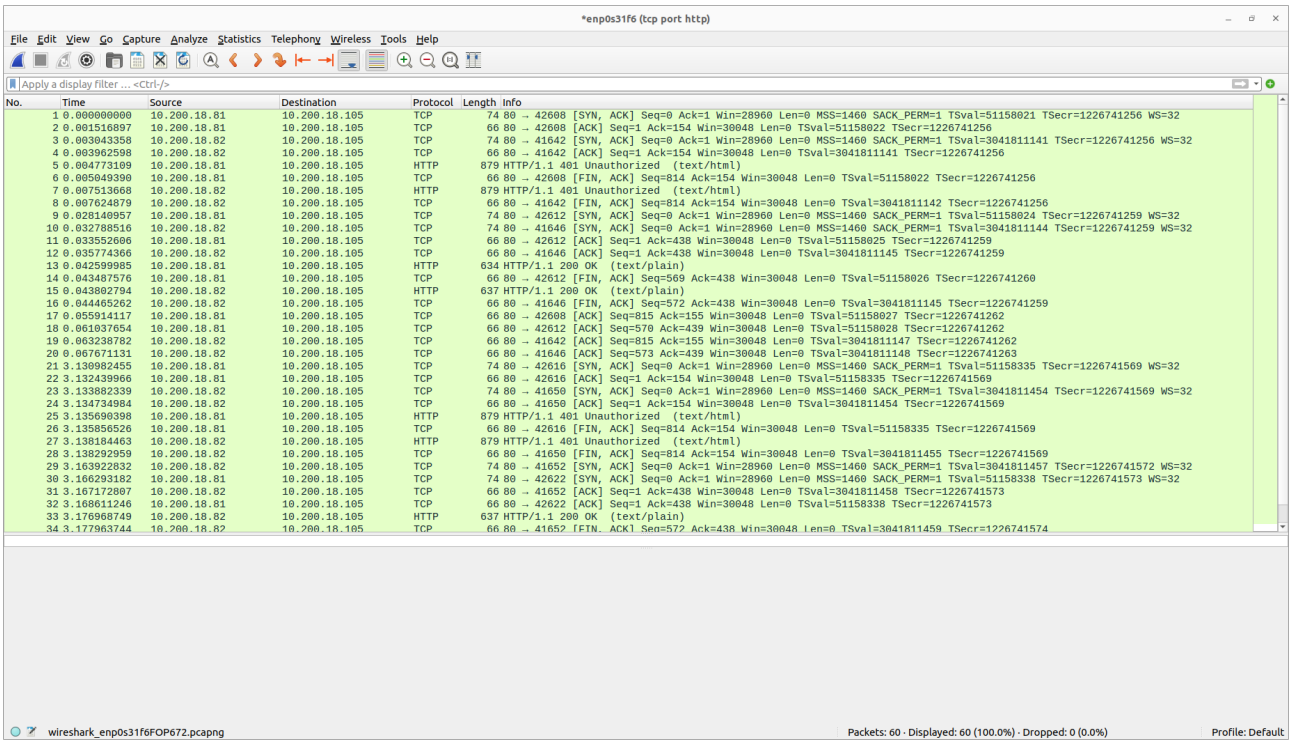
There are 2 different types of packets that are captured. Packets with an ARP protocol and packets with a DNS protocol.
The Address Resolution Protocol packets have different destinations. The ARP protocol tries to find the IP addresses of neighbouring devices when a device connects the the network.

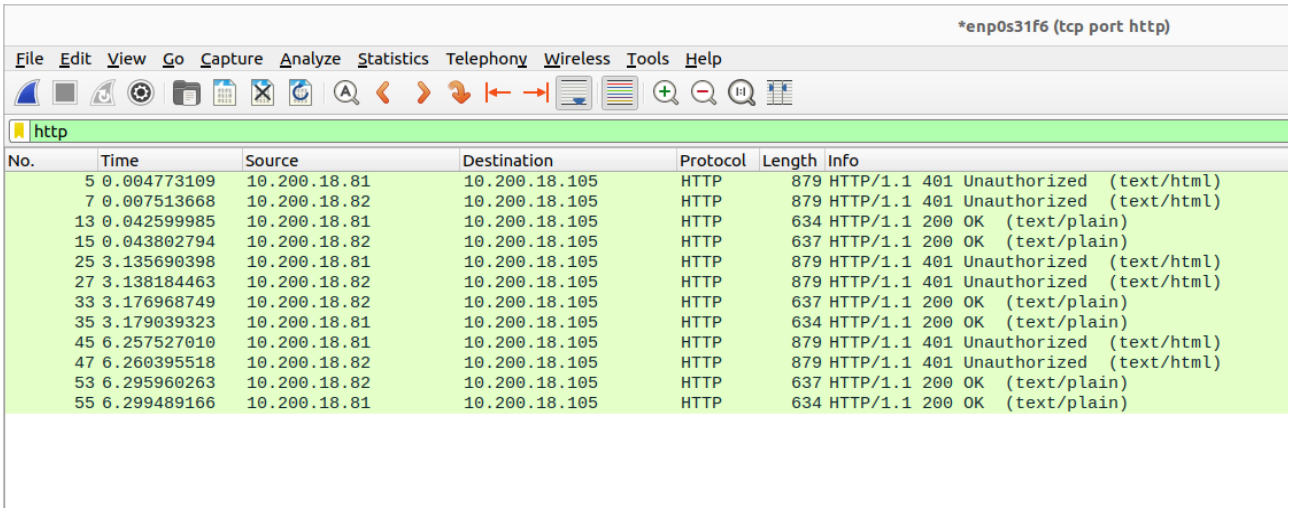
The Domain Name System packets have the destination 1.1.1.1. The DNS protocol links IP addresses with domain names that are written with english characters rather than needing to remember the actual IP address

Task 2



First I used the TCP or UDP port 80 capture filter so I was only left with HTTP and TCP packets.

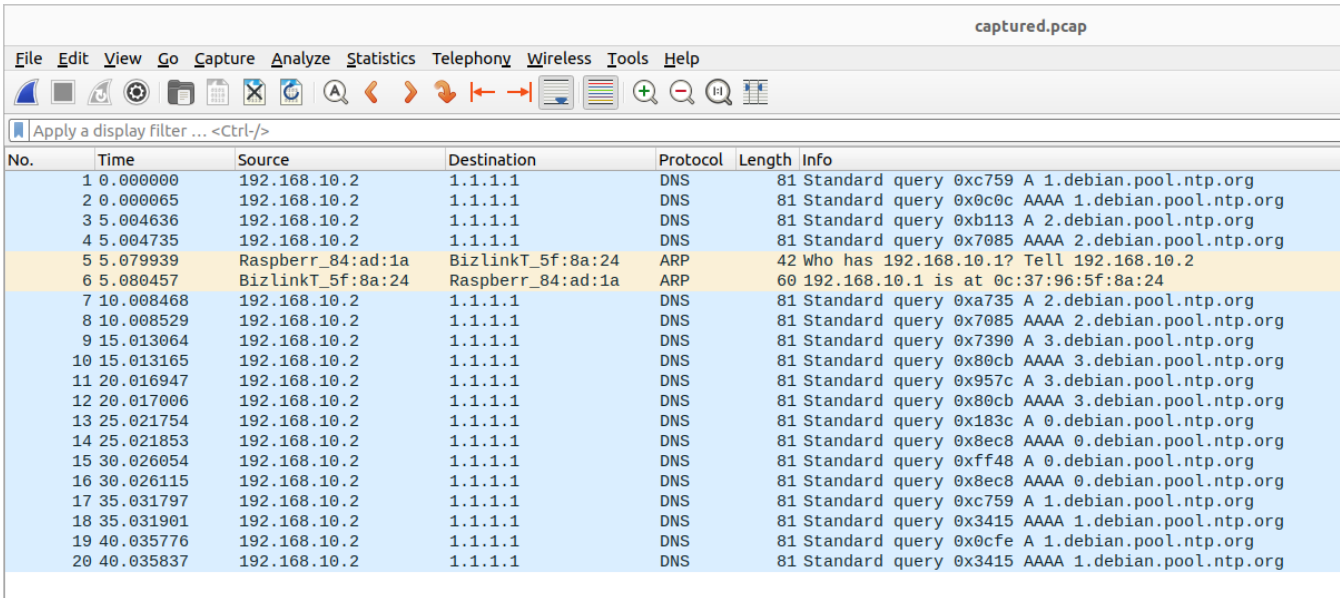




No.	Time	Source	Destination	Protocol	Length	Info
5	0.004773109	10.200.18.81	10.200.18.105	HTTP	879	HTTP/1.1 401 Unauthorized (text/html)
7	0.007513668	10.200.18.82	10.200.18.105	HTTP	879	HTTP/1.1 401 Unauthorized (text/html)
13	0.042599985	10.200.18.81	10.200.18.105	HTTP	634	HTTP/1.1 200 OK (text/plain)
15	0.043802794	10.200.18.82	10.200.18.105	HTTP	637	HTTP/1.1 200 OK (text/plain)
25	3.135690398	10.200.18.81	10.200.18.105	HTTP	879	HTTP/1.1 401 Unauthorized (text/html)
27	3.138184463	10.200.18.82	10.200.18.105	HTTP	879	HTTP/1.1 401 Unauthorized (text/html)
33	3.176968749	10.200.18.82	10.200.18.105	HTTP	637	HTTP/1.1 200 OK (text/plain)
35	3.179039323	10.200.18.81	10.200.18.105	HTTP	634	HTTP/1.1 200 OK (text/plain)
45	6.257527010	10.200.18.81	10.200.18.105	HTTP	879	HTTP/1.1 401 Unauthorized (text/html)
47	6.260395518	10.200.18.82	10.200.18.105	HTTP	879	HTTP/1.1 401 Unauthorized (text/html)
53	6.295960263	10.200.18.82	10.200.18.105	HTTP	637	HTTP/1.1 200 OK (text/plain)
55	6.299489166	10.200.18.81	10.200.18.105	HTTP	634	HTTP/1.1 200 OK (text/plain)

I then used the display filter to filter out the HTTP packets

Task 3

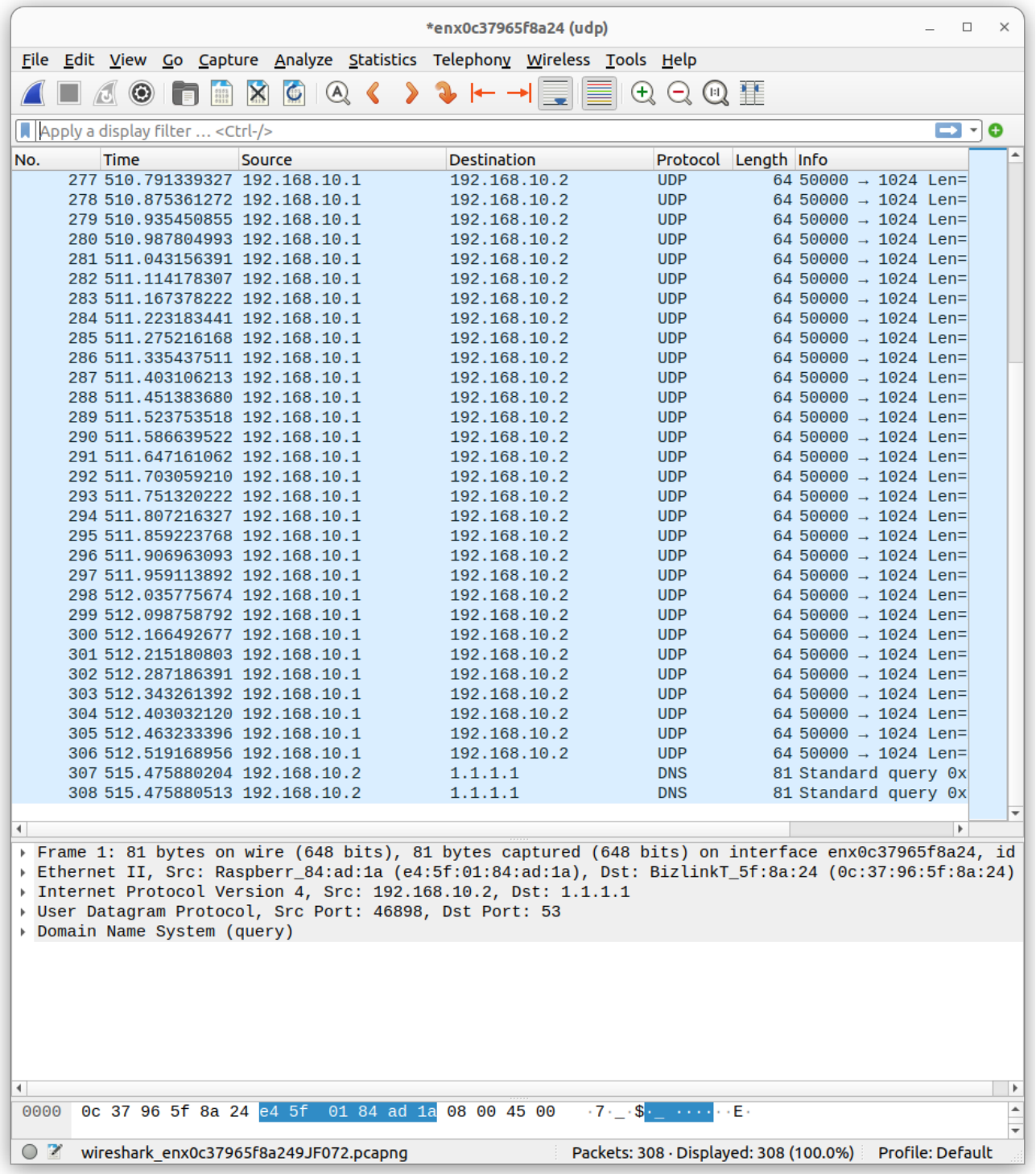


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xc759 A 1.debian.pool.ntp.org
2	0.000065	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x0c0c AAAA 1.debian.pool.ntp.org
3	5.004636	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xb113 A 2.debian.pool.ntp.org
4	5.004735	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x7085 AAAA 2.debian.pool.ntp.org
5	5.079939	Raspberr_84:ad:1a	BizlinkT_5f:8a:24	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
6	5.080457	BizlinkT_5f:8a:24	Raspberr_84:ad:1a	ARP	60	192.168.10.1 is at 0c:37:96:5f:8a:24
7	10.008468	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xa735 A 2.debian.pool.ntp.org
8	10.008529	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x7085 AAAA 2.debian.pool.ntp.org
9	15.013064	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x7390 A 3.debian.pool.ntp.org
10	15.013165	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x80cb AAAA 3.debian.pool.ntp.org
11	20.016947	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x957c A 3.debian.pool.ntp.org
12	20.017006	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x80cb AAAA 3.debian.pool.ntp.org
13	25.021754	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x183c A 0.debian.pool.ntp.org
14	25.021853	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x8ec8 AAAA 0.debian.pool.ntp.org
15	30.026054	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xff48 A 0.debian.pool.ntp.org
16	30.026115	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x8ec8 AAAA 0.debian.pool.ntp.org
17	35.031797	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xc759 A 1.debian.pool.ntp.org
18	35.031901	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x3415 AAAA 1.debian.pool.ntp.org
19	40.035776	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x0cfe A 1.debian.pool.ntp.org
20	40.035837	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x3415 AAAA 1.debian.pool.ntp.org

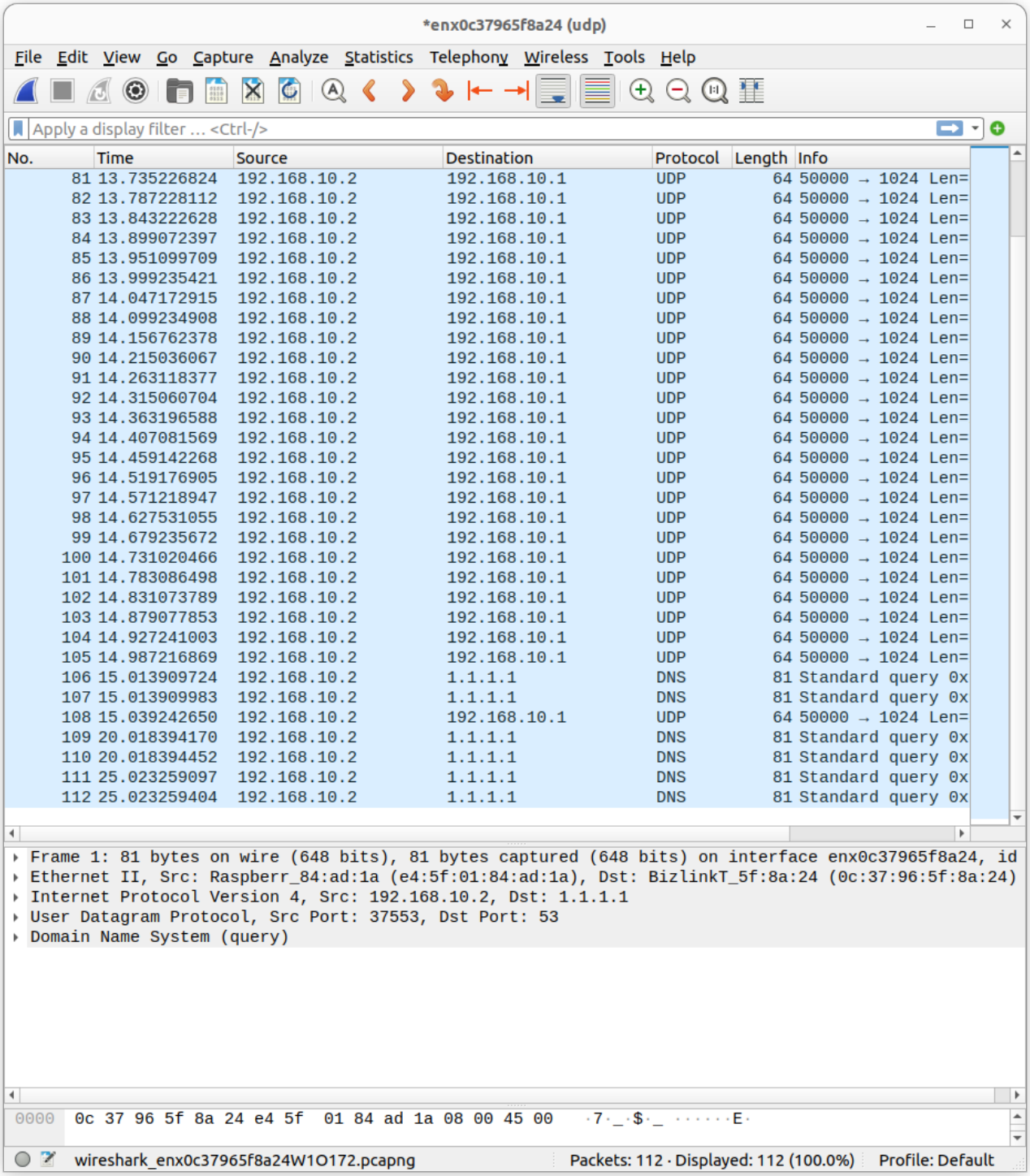
I used the tcpdump command to send 20 packets and then I opened it with wireshark to view them.

Sending traffic
Task 1

100 packets from lab machine to Raspberry PI:

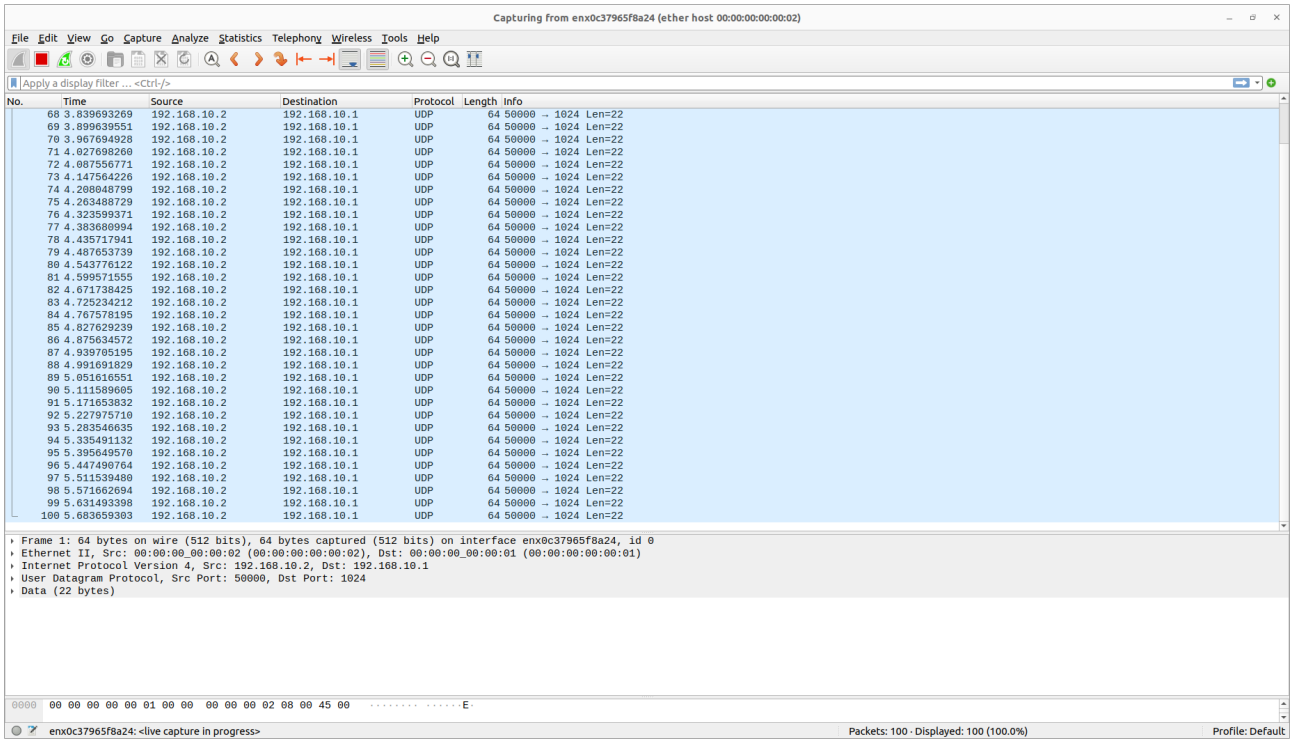


100 packets from Raspberry PI to lab machine:



Task 2.1:

Capturing only the 100 sent packets to the lab machine from the Raspberry PI by using the filter “ether host = 00:00:00:00:00:02”:



Task 2.2:

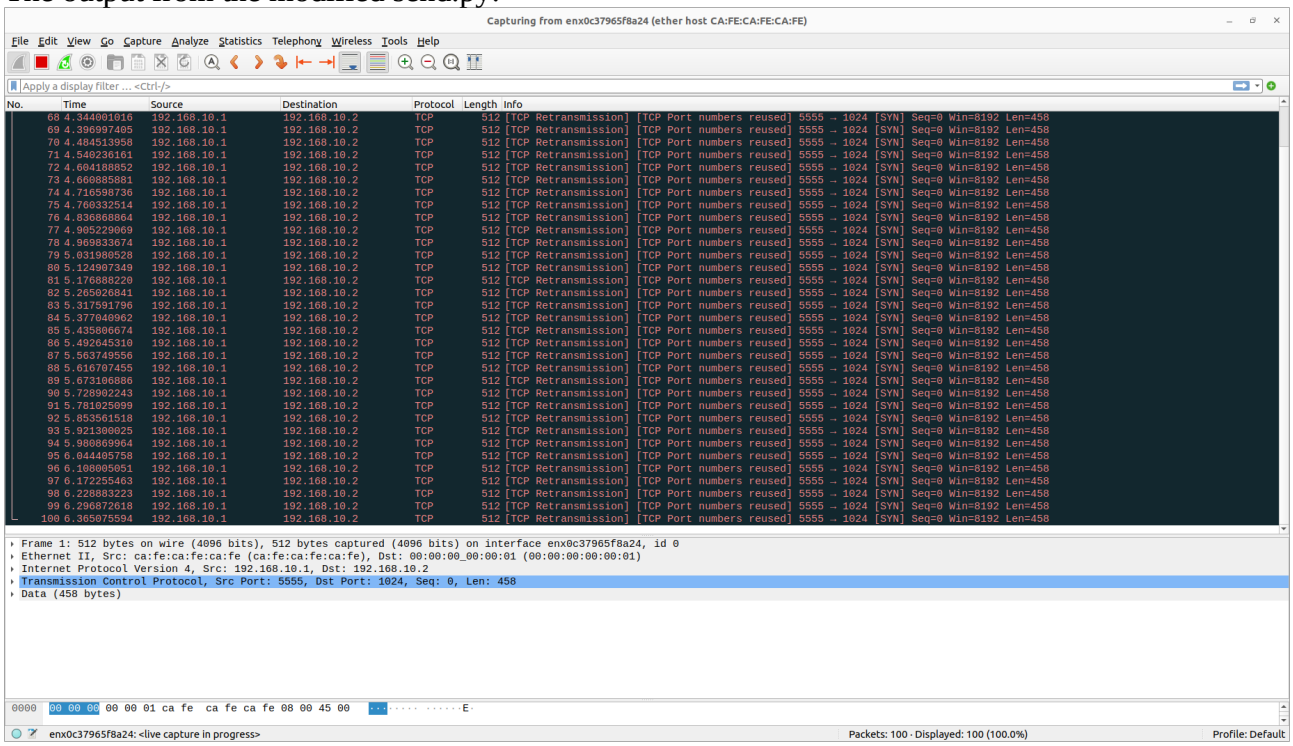
The packet size is 64 bits as seen from the length column or the frame window.

Task 2.3:

The protocol of the packet is UDP as seen from the protocol column.

Task 3:

The output from the modified send.py:



Link to repository:
https://github.com/VKing15/CWM-ProgNets.git