

Exercise 1

Traffic Capture: Task 1

*enx0c37965f8a24							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
Apply a display filter ... <Ctrl-/>							
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

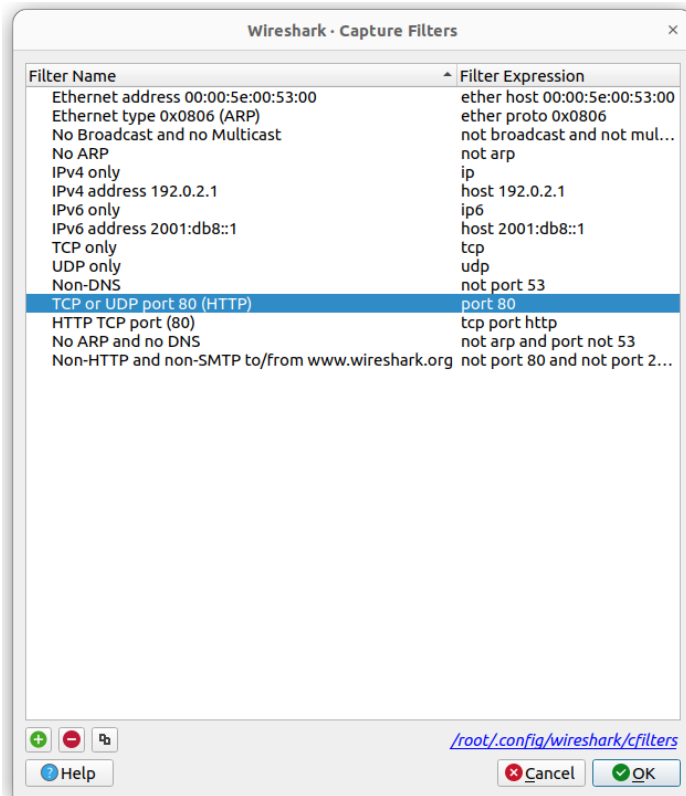
*enx0c37965f8a24							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
Apply a display filter ... <Ctrl-/>							
No.	Time	Source	Destination	Protocol	Length	Info	
13	25.109920972	Raspberr_84:ad:1a	BizlinkT_5f:8a:24	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2	
14	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.

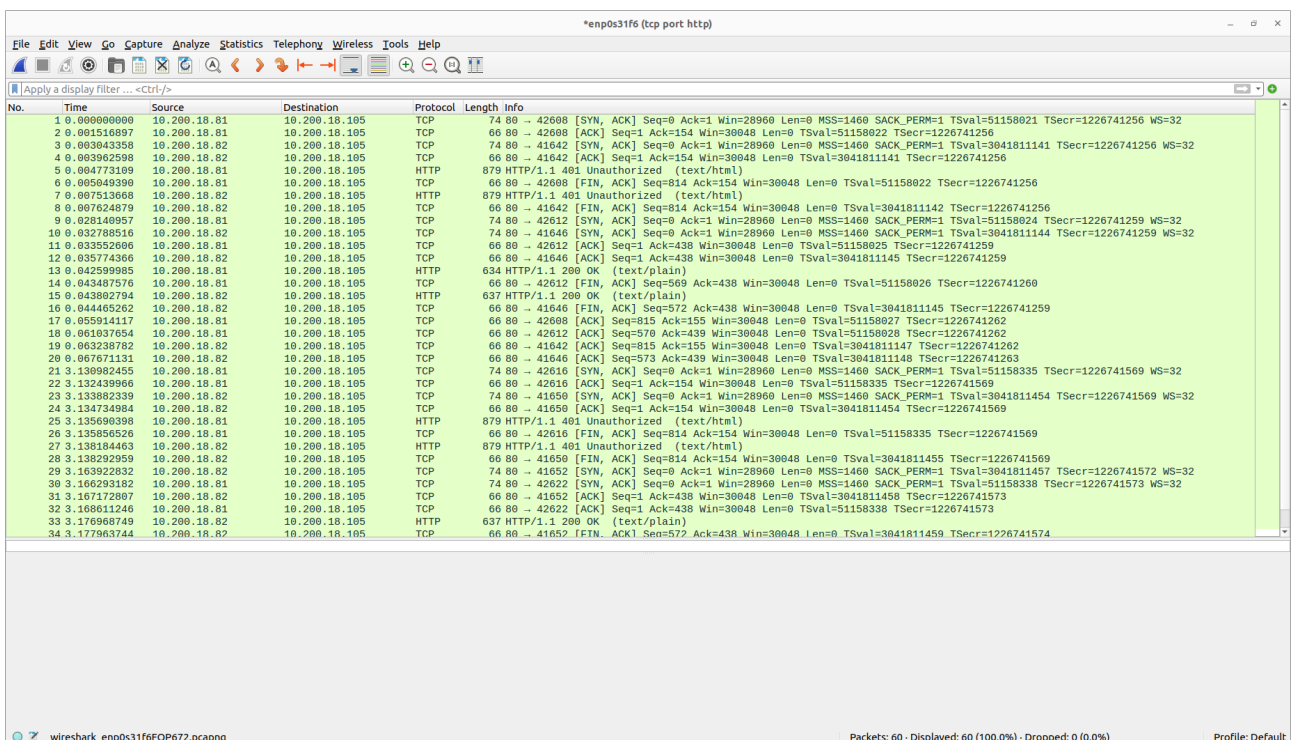
The Address Resolution Protocol packets have different destinations. The ARP protocol tries to find the IP addresses of neighbouring devices when a device connects to the network.

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.



*enp0s31f6 (tcp port http)

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

captured.pcap

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:

The image shows a Wireshark packet capture window titled "*enx0c37965f8a24 (udp)". The main pane displays a list of 100 packets. The first 99 packets are UDP packets from 192.168.10.1 to 192.168.10.2, each 64 bytes long. The last two packets (307 and 308) are DNS standard queries from 192.168.10.2 to 1.1.1.1, each 81 bytes long.

No.	Time	Source	Destination	Protocol	Length	Info
277	510.791339327	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
278	510.875361272	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
279	510.935450855	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
280	510.987804993	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
281	511.043156391	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
282	511.114178307	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
283	511.167378222	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
284	511.223183441	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
285	511.275216168	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
286	511.335437511	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
287	511.403106213	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
288	511.451383680	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
289	511.523753518	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
290	511.586639522	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
291	511.647161062	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
292	511.703059210	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
293	511.751320222	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
294	511.807216327	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
295	511.859223768	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
296	511.906963093	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
297	511.959113892	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
298	512.035775674	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
299	512.098758792	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
300	512.166492677	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
301	512.215180803	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
302	512.287186391	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
303	512.343261392	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
304	512.403032120	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
305	512.463233396	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
306	512.519168956	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=
307	515.475880204	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x
308	515.475880513	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x

Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface enx0c37965f8a24, id
Ethernet II, Src: Raspberr_84:ad:1a (e4:5f:01:84:ad:1a), Dst: BizlinkT_5f:8a:24 (0c:37:96:5f:8a:24)
Internet Protocol Version 4, Src: 192.168.10.2, Dst: 1.1.1.1
User Datagram Protocol, Src Port: 46898, Dst Port: 53
Domain Name System (query)

0000 0c 37 96 5f 8a 24 e4 5f 01 84 ad 1a 08 00 45 00 ·7·_·\$·_·...·E·

wireshark_enx0c37965f8a249JF072.pcapng Packets: 308 · Displayed: 308 (100.0%) Profile: Default

100 packets from Raspberry PI to lab machine:

*enx0c37965f8a24 (udp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
81	13.735226824	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
82	13.787228112	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
83	13.843222628	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
84	13.899072397	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
85	13.951099709	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
86	13.999235421	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
87	14.047172915	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
88	14.099234908	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
89	14.156762378	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
90	14.215036067	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
91	14.263118377	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
92	14.315060704	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
93	14.363196588	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
94	14.407081569	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
95	14.459142268	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
96	14.519176905	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
97	14.571218947	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
98	14.627531055	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
99	14.679235672	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
100	14.731020466	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
101	14.783086498	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
102	14.831073789	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
103	14.879077853	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
104	14.927241003	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
105	14.987216869	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
106	15.013909724	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x
107	15.013909983	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x
108	15.039242650	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=
109	20.018394170	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x
110	20.018394452	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x
111	25.023259097	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x
112	25.023259404	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x

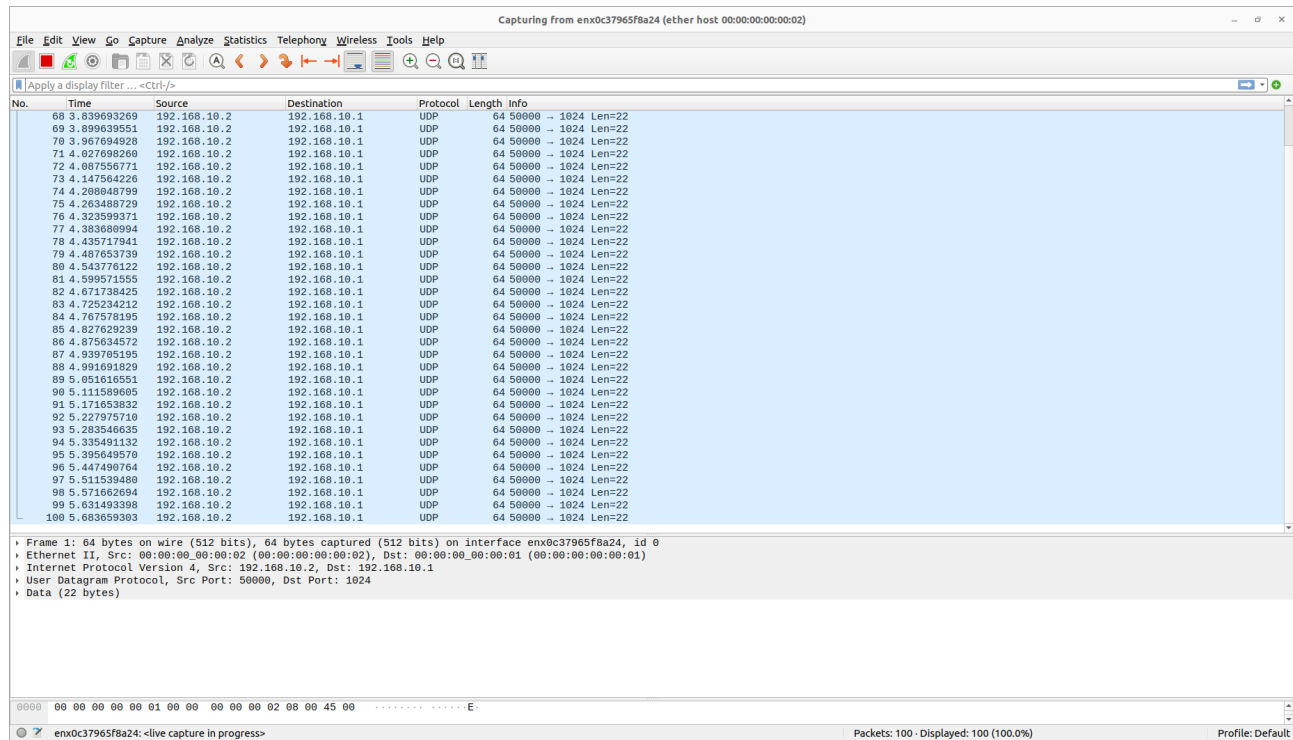
Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface enx0c37965f8a24, id
▶ Ethernet II, Src: Raspberr_84:ad:1a (e4:5f:01:84:ad:1a), Dst: BizlinkT_5f:8a:24 (0c:37:96:5f:8a:24)
▶ Internet Protocol Version 4, Src: 192.168.10.2, Dst: 1.1.1.1
▶ User Datagram Protocol, Src Port: 37553, Dst Port: 53
▶ Domain Name System (query)

0000 0c 37 96 5f 8a 24 e4 5f 01 84 ad 1a 08 00 45 00 ·7·_·\$·_·.....E·

wireshark_enx0c37965f8a24W1O172.pcapng Packets: 112 · Displayed: 112 (100.0%) Profile: Default

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”:



The screenshot shows the Wireshark network protocol analyzer interface. The title bar indicates it is capturing from interface `enxC37965F8a24` (ether host 00:00:00:00:00:02). The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various actions like starting/stopping capture, saving, and zooming. The display filter bar shows `Apply a display filter ... <Ctrl-F>`. The packet list pane displays 100 packets, all of type UDP, with source IP 192.168.10.2 and destination IP 192.168.10.1. The packet details pane for the selected packet (No. 100) shows the following structure:

- Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface `enxC37965F8a24`, id 0
- Ethernet II, Src: 00:00:00:00:00:02 (00:00:00:00:00:02), Dst: 00:00:00:00:00:01 (00:00:00:00:00:01)
- Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.1
- User Datagram Protocol, Src Port: 50000, Dst Port: 1024
- Data (22 bytes)

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
68	3.839693269	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
69	3.899639551	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
70	3.967694928	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
71	4.027698260	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
72	4.087556771	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
73	4.147564226	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
74	4.208048799	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
75	4.263488729	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
76	4.323599371	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
77	4.383680994	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
78	4.435717941	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
79	4.487653739	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
80	4.543776122	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
81	4.599571555	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
82	4.671738425	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
83	4.725234212	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
84	4.767578195	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
85	4.827629239	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
86	4.875634572	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
87	4.939705195	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
88	4.991691829	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
89	5.051616551	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
90	5.111580605	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
91	5.171653832	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
92	5.227975710	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
93	5.283546635	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
94	5.335491132	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
95	5.395649570	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
96	5.447490764	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
97	5.511539480	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
98	5.571662694	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
99	5.631493398	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22
100	5.683659383	192.168.10.2	192.168.10.1	UDP	64	50000 → 1024 Len=22

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:

The image shows a Wireshark packet capture window titled "Capturing from enxc37965f8a24 (ether host CA:FE:CA:FE:CA:FE)". The packet list on the left shows a series of TCP retransmissions (512) from 192.168.10.1 to 192.168.10.2 on port 5555. The packet details pane on the right shows the selected packet (No. 100) as a Transmission Control Protocol (TCP) segment with Seq=0, Win=8192, Len=458, and Data (458 bytes). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
68	4.334061016	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
69	4.336987465	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
70	4.484513958	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
71	4.549236161	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
72	4.604188852	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
73	4.660085001	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
74	4.716598736	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
75	4.769332514	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
76	4.836688864	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
77	4.905229969	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
78	4.969833074	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
79	5.031980528	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
80	5.124907349	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
81	5.176888220	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
82	5.205020841	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
83	5.317591796	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
84	5.377040962	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
85	5.435806674	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
86	5.492645310	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
87	5.563749556	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
88	5.616707455	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
89	5.673160886	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
90	5.728902243	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
91	5.781023699	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
92	5.853561518	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
93	5.921380825	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
94	5.980869964	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
95	6.044405758	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
96	6.100905051	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
97	6.172255463	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
98	6.228803223	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
99	6.296872618	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
100	6.365075594	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=458

Frame 1: 512 bytes on wire (4096 bits), 512 bytes captured (4096 bits) on interface enxc37965f8a24, id 0
Ethernet II, Src: ca:fe:ca:fe:ca:fe (ca:fe:ca:fe:ca:fe), Dst: 00:00:00:00:00:01 (00:00:00:00:00:01)
Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.2
Transmission Control Protocol, Src Port: 5555, Dst Port: 1024, Seq: 0, Len: 458
Data (458 bytes)

0000 00 00 00 00 00 01 ca fe ca fe ca fe 08 00 45 00E

enxc37965f8a24: <live capture in progress> Packets: 100 - Displayed: 100 (100.0%) Profile: Default

Link to repository:

<https://github.com/VKing15/CWM-ProgNets.git>