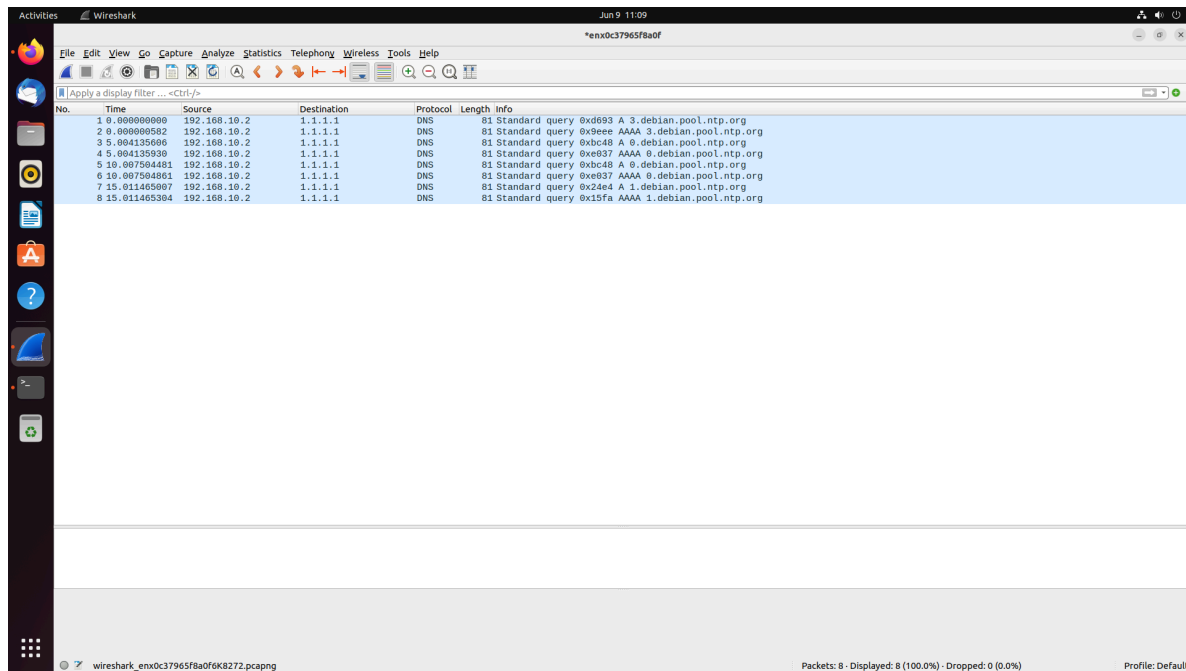


Capture on ethernet interface



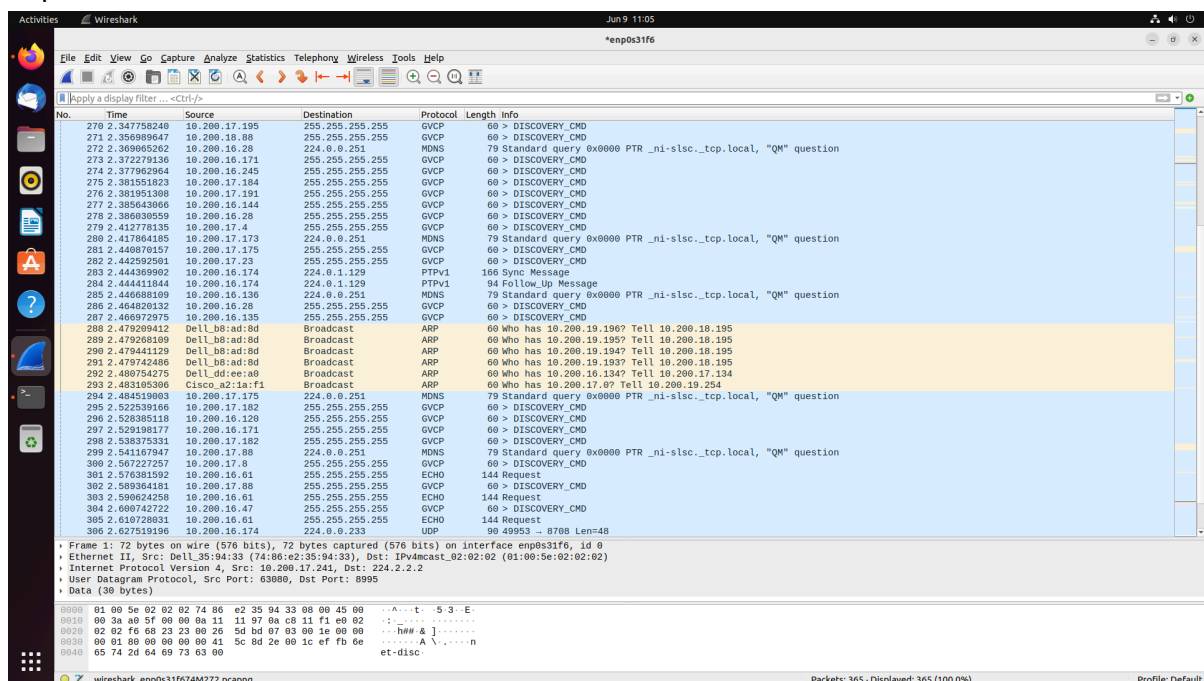
The screenshot shows a Wireshark capture on the ethernet interface 'enx0c37965f8a0f'. The packet list displays 8 packets, all of which are DNS Standard queries to 1.1.1.1. The packet details pane shows the structure of a DNS query, including the question section with 'Standard query query 0xd693 A 3.debian.pool.ntp.org'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xd693 A 3.debian.pool.ntp.org
2	0.000000582	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x9eee AAAA 3.debian.pool.ntp.org
3	5.004135000	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xbcd4 A 0.debian.pool.ntp.org
4	5.004135000	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xe037 AAAA 0.debian.pool.ntp.org
5	10.007504481	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xbcd4 A 0.debian.pool.ntp.org
6	10.007504481	192.168.10.2	1.1.1.1	DNS	81	Standard query 0xe037 AAAA 0.debian.pool.ntp.org
7	15.011465007	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x24ee A 1.debian.pool.ntp.org
8	15.011465304	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x15fa AAAA 1.debian.pool.ntp.org

Every 5s, two standard queries are made from Pi onto a destination described as 1.1.1.1. This is a DNS (Domain Name System) protocol. We will see later when we apply the UDP (User Datagram Protocol) filter onto the Pi that the DNS still appears. This makes me think DNS is a type of UDP.

From my understanding, a quick Google search reveals DNS requests are just a way of querying the “names” of the destination computers.

Capture on network interface, no filter



The screenshot shows a Wireshark capture on the network interface 'enp0s31f6'. The packet list displays a large number of packets (365) with various protocols including ICMP, ARP, and DNS. The packet details pane shows the structure of a DNS query, including the question section with 'Standard query query 0x0000 PTR _ni-sls-._tcp.local, "QM" question'.

No.	Time	Source	Destination	Protocol	Length	Info
270	2.347758240	10.200.17.195	255.255.255.255	ICMP	60	> DISCOVERY_CMD
271	2.356989647	10.200.18.88	255.255.255.255	ICMP	60	> DISCOVERY_CMD
272	2.369005262	10.200.16.28	224.0.0.251	MDNS	79	Standard query 0x0000 PTR _ni-sls-._tcp.local, "QM" question
273	2.372779136	10.200.16.171	255.255.255.255	ICMP	60	> DISCOVERY_CMD
274	2.377962964	10.200.16.245	255.255.255.255	ICMP	60	> DISCOVERY_CMD
275	2.381551023	10.200.17.184	255.255.255.255	ICMP	60	> DISCOVERY_CMD
276	2.381951306	10.200.17.191	255.255.255.255	ICMP	60	> DISCOVERY_CMD
277	2.385643066	10.200.16.144	255.255.255.255	ICMP	60	> DISCOVERY_CMD
278	2.386030959	10.200.16.28	255.255.255.255	ICMP	60	> DISCOVERY_CMD
279	2.412778135	10.200.17.4	255.255.255.255	ICMP	60	> DISCOVERY_CMD
280	2.417064185	10.200.17.173	224.0.0.251	MDNS	79	Standard query 0x0000 PTR _ni-sls-._tcp.local, "QM" question
281	2.440870157	10.200.17.175	255.255.255.255	ICMP	60	> DISCOVERY_CMD
282	2.442592501	10.200.17.23	255.255.255.255	ICMP	60	> DISCOVERY_CMD
283	2.444369002	10.200.16.174	224.0.1.129	PTPv1	106	Syn Message
284	2.444411844	10.200.16.174	224.0.1.129	PTPv1	94	Follow Up Message
285	2.446088109	10.200.16.130	224.0.0.251	MDNS	79	Standard query 0x0000 PTR _ni-sls-._tcp.local, "QM" question
286	2.464820132	10.200.16.28	255.255.255.255	ICMP	60	> DISCOVERY_CMD
287	2.466972975	10.200.16.135	255.255.255.255	ICMP	60	> DISCOVERY_CMD
288	2.479209412	Dell_B8:ad:8d	Broadcast	ARP	60	Who has 10.200.19.190? Tell 10.200.18.195
289	2.479268109	Dell_B8:ad:8d	Broadcast	ARP	60	Who has 10.200.19.195? Tell 10.200.18.195
290	2.479441129	Dell_B8:ad:8d	Broadcast	ARP	60	Who has 10.200.19.194? Tell 10.200.18.195
291	2.479742486	Dell_B8:ad:8d	Broadcast	ARP	60	Who has 10.200.19.193? Tell 10.200.18.195
292	2.489754275	Dell_d0:ee:a9	Broadcast	ARP	60	Who has 10.200.16.134? Tell 10.200.17.134
293	2.493165306	Cisco_a2:1a:f1	Broadcast	ARP	60	Who has 10.200.17.0? Tell 10.200.19.254
294	2.484519003	10.200.17.175	224.0.0.251	MDNS	79	Standard query 0x0000 PTR _ni-sls-._tcp.local, "QM" question
295	2.522539166	10.200.17.182	255.255.255.255	ICMP	60	> DISCOVERY_CMD
296	2.520385110	10.200.16.120	255.255.255.255	ICMP	60	> DISCOVERY_CMD
297	2.529198177	10.200.16.171	255.255.255.255	ICMP	60	> DISCOVERY_CMD
298	2.538370331	10.200.17.182	255.255.255.255	ICMP	60	> DISCOVERY_CMD
299	2.541107947	10.200.17.88	224.0.0.251	MDNS	79	Standard query 0x0000 PTR _ni-sls-._tcp.local, "QM" question
300	2.567227257	10.200.17.9	255.255.255.255	ICMP	60	> DISCOVERY_CMD
301	2.576381592	10.200.16.61	255.255.255.255	ECHO	144	Request
302	2.589364181	10.200.17.88	255.255.255.255	ICMP	60	> DISCOVERY_CMD
303	2.590624258	10.200.16.61	255.255.255.255	ECHO	144	Request
304	2.600742722	10.200.16.47	255.255.255.255	ICMP	60	> DISCOVERY_CMD
305	2.610728031	10.200.16.61	255.255.255.255	ECHO	144	Request
306	2.627515916	10.200.16.174	224.0.0.233	UDP	90	49553 - 8788 Len=48

A lot of traffic happening on the departmental network. We can see various types of protocols (GVCP, MDNS, PTPv1, ECHO). It is interesting to see that the MDNS ones are also talking about standard queries so this makes me think this is related to regular DNS. A Google search reveals MDNS is like DNS but for smaller networks. ECHO (request) is used regularly to check that the device is still connected to the network. Also interesting that for the most part, packets of the same protocol have the same lengths. Can also see ARP broadcasts for when some computers (Dell) don't have some IP addresses in their ARP table.

Capture on network interface, HTTP traffic

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.200.17.167	142.250.200.3	TCP	74	37542 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=450428050 TSecr=0 WS=128
2	0.003974368	142.250.200.3	10.200.17.167	TCP	74	80 → 37542 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=1779689265 TSecr=450428050 WS=256
3	0.003986571	10.200.17.167	142.250.200.3	TCP	66	37542 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=450428054 TSecr=1779689265
4	0.004062760	10.200.17.167	142.250.200.3	OCSP	486	Request
5	0.008025544	142.250.200.3	10.200.17.167	TCP	66	80 → 37542 [ACK] Seq=1 Ack=421 Win=268544 Len=0 TSval=1779689269 TSecr=450428054
6	0.049067960	142.250.200.3	10.200.17.167	OCSP	1168	Response
7	0.050018717	10.200.17.167	142.250.200.3	TCP	66	37542 → 80 [ACK] Seq=421 Ack=1103 Win=64128 Len=0 TSval=450428100 TSecr=1779689311
8	0.050018717	10.200.17.167	142.250.200.3	TCP	66	[TCP Keep-Alive] 37542 → 80 [ACK] Seq=420 Ack=1103 Win=64128 Len=0 TSval=450438270 TSecr=1779689311
9	0.1224061125	142.250.200.3	10.200.17.167	TCP	66	[TCP Keep-Alive ACK] 37542 → 80 [ACK] Seq=1103 Ack=421 Win=268800 Len=0 TSval=1779699484 TSecr=450428100
10	0.499403070	10.200.17.167	142.250.200.3	TCP	66	[TCP Keep-Alive] 37542 → 80 [ACK] Seq=420 Ack=1103 Win=64128 Len=0 TSval=450448510 TSecr=1779699484
11	0.463193068	142.250.200.3	10.200.17.167	TCP	66	[TCP Keep-Alive ACK] 80 → 37542 [ACK] Seq=1103 Ack=421 Win=268800 Len=0 TSval=1779709724 TSecr=450428100
12	0.699421138	10.200.17.167	142.250.200.3	TCP	66	[TCP Keep-Alive] 37542 → 80 [ACK] Seq=420 Ack=1103 Win=64128 Len=0 TSval=450458750 TSecr=1779709724
13	0.703415998	142.250.200.3	10.200.17.167	TCP	66	[TCP Keep-Alive ACK] 80 → 37542 [ACK] Seq=1103 Ack=421 Win=268800 Len=0 TSval=1779719964 TSecr=450428100
14	0.508060512	10.200.17.167	185.125.190.97	TCP	74	52488 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=389028699 TSecr=0 WS=128
15	0.591689932	185.125.190.97	10.200.17.167	TCP	74	80 → 52488 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=4118906516 TSecr=389028699 WS=16384
16	0.591751895	10.200.17.167	185.125.190.97	TCP	66	52488 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=389028693 TSecr=4118906516
17	0.591937075	10.200.17.167	185.125.190.97	HTTP	153	GET / HTTP/1.1
18	0.595802138	185.125.190.97	10.200.17.167	HTTP	251	HTTP/1.1 204 No Content
19	0.595802438	185.125.190.97	10.200.17.167	TCP	66	80 → 52488 [FIN, ACK] Seq=186 Ack=88 Win=65536 Len=0 TSval=4118906520 TSecr=389028693
20	0.595861294	10.200.17.167	185.125.190.97	TCP	66	52488 → 80 [ACK] Seq=88 Ack=106 Win=64128 Len=0 TSval=389028697 TSecr=4118906520
21	0.596058877	10.200.17.167	185.125.190.97	TCP	66	52488 → 80 [FIN, ACK] Seq=88 Ack=187 Win=64128 Len=0 TSval=389028697 TSecr=4118906520
22	0.599445077	185.125.190.97	10.200.17.167	TCP	66	80 → 52488 [ACK] Seq=187 Ack=89 Win=65536 Len=0 TSval=4118906524 TSecr=389028697
23	0.939412640	10.200.17.167	142.250.200.3	TCP	66	[TCP Keep-Alive] 37542 → 80 [ACK] Seq=420 Ack=1103 Win=64128 Len=0 TSval=450460990 TSecr=1779719964
24	0.943381242	142.250.200.3	10.200.17.167	TCP	66	[TCP Keep-Alive ACK] 80 → 37542 [ACK] Seq=1103 Ack=421 Win=268800 Len=0 TSval=1779730204 TSecr=450428100
25	0.937060905	10.200.17.167	142.250.200.3	OCSP	486	Request
26	0.040579226	142.250.200.3	10.200.17.167	TCP	66	80 → 37542 [ACK] Seq=1103 Ack=2205 Win=64128 Len=0 TSval=1779740301 TSecr=450479087
27	0.078524372	142.250.200.3	10.200.17.167	OCSP	1168	Response
28	0.078531108	10.200.17.167	142.250.200.3	TCP	66	37542 → 80 [ACK] Seq=841 Ack=2205 Win=64128 Len=0 TSval=450479129 TSecr=1779740339
29	0.153992264	10.200.17.167	142.250.200.3	OCSP	486	Request
30	0.154869145	10.200.17.167	142.250.200.3	TCP	74	56548 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=450479205 TSecr=0 WS=128
31	0.155846064	142.250.200.3	10.200.17.167	TCP	74	80 → 56548 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=1303902846 TSecr=450479205 WS=256
32	0.158859193	10.200.17.167	142.250.200.3	TCP	66	56548 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=450479209 TSecr=1303902846
33	0.158913362	10.200.17.167	142.250.200.3	OCSP	486	Request
34	0.162892862	142.250.200.3	10.200.17.167	TCP	66	80 → 56548 [ACK] Seq=1 Ack=421 Win=268544 Len=0 TSval=1303902859 TSecr=450479209
35	0.163882416	142.250.200.3	10.200.17.167	TCP	66	80 → 37542 [ACK] Seq=2205 Ack=1261 Win=268800 Len=0 TSval=1779740424 TSecr=450479204
36	0.197493459	142.250.200.3	10.200.17.167	OCSP	1168	Response
37	0.197517717	10.200.17.167	142.250.200.3	TCP	66	37542 → 80 [ACK] Seq=1261 Ack=3307 Win=64128 Len=0 TSval=450479248 TSecr=1779740458

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s31f6, id 0
Ethernet II, Src: Dell_02:e1:a5 (50:9a:4c:02:e1:a5), Dst: Cisco_a2:1a:f1 (00:0a:d2:a2:1a:f1)
Internet Protocol Version 4, Src: 10.200.17.167, Dst: 142.250.200.3
Transmission Control Protocol, Src Port: 37542, Dst Port: 80, Seq: 0, Len: 0

Packets: 43 - Displayed: 43 (100.0%) Profile: Default

In order to capture HTTP traffic, I needed to access the web in some way (e.g. doing a Google search). We can see even a 1-minute browser search requires a lot of packets to be sent.

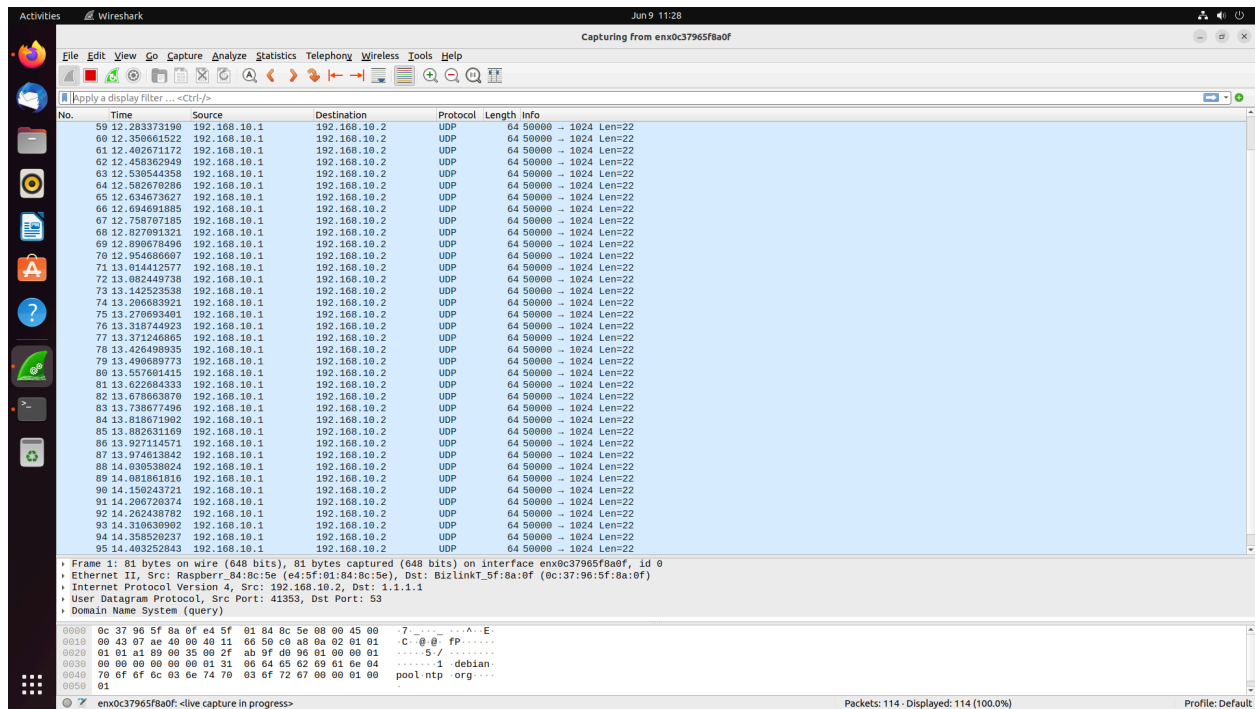
Capture on Pi using tcpdump (manual termination)

```
Activities Terminal Jun 9 11:14
pi@p4pi: ~
Last login: Thu May 16 15:55:47 2024
pi@p4pi: ~$ ls
pi@p4pi: ~$ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:51:34.576884 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 808821836:808822024, ack 1017294804, win 501, options [nop,nop,TS val 417080223 ecr 1666237015], length 188
16:51:34.577430 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 188, win 524, options [nop,nop,TS val 1666237096 ecr 417080223], length 0
16:51:34.654759 IP 192.168.10.2.46366 > 1.1.1.1.domain: 10868+ PTR? 2.10.168.192.in-addr.arpa. (43)
16:51:35.891281 IP 192.168.10.2.45792 > 1.1.1.1.domain: 21013+ A? 0.debian.pool.ntp.org. (39)
16:51:35.891380 IP 192.168.10.2.59901 > 1.1.1.1.domain: 59129+ AAAA? 0.debian.pool.ntp.org. (39)
16:51:39.658052 IP 192.168.10.2.46366 > 1.1.1.1.domain: 10868+ PTR? 2.10.168.192.in-addr.arpa. (43)
16:51:40.894930 IP 192.168.10.2.45792 > 1.1.1.1.domain: 21013+ A? 0.debian.pool.ntp.org. (39)
16:51:40.894996 IP 192.168.10.2.59901 > 1.1.1.1.domain: 59129+ AAAA? 0.debian.pool.ntp.org. (39)
16:51:44.663565 IP 192.168.10.2.34441 > 1.1.1.1.domain: 4423+ PTR? 1.10.168.192.in-addr.arpa. (43)
16:51:45.898904 IP 192.168.10.2.58257 > 1.1.1.1.domain: 54287+ A? 1.debian.pool.ntp.org. (39)
16:51:45.899608 IP 192.168.10.2.35202 > 1.1.1.1.domain: 21929+ AAAA? 1.debian.pool.ntp.org. (39)
16:51:49.668063 IP 192.168.10.2.34441 > 1.1.1.1.domain: 4423+ PTR? 1.10.168.192.in-addr.arpa. (43)
16:51:54.673848 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 488:408, ack 1, win 501, options [nop,nop,TS val 417100319 ecr 1666237096], length 220
16:51:54.673926 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 408:596, ack 1, win 501, options [nop,nop,TS val 417100320 ecr 1666237096], length 188
16:51:54.674119 IP 192.168.10.2.53086 > 1.1.1.1.domain: 52284+ PTR? 1.1.1.1.in-addr.arpa. (38)
16:51:54.674484 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 408, win 546, options [nop,nop,TS val 1666257193 ecr 417100319], length 0
16:51:54.674484 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 596, win 509, options [nop,nop,TS val 1666257193 ecr 417100320], length 0
16:52:04.687743 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 596:736, ack 1, win 501, options [nop,nop,TS val 417110333 ecr 1666257193], length 140
16:52:04.687847 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 736:964, ack 1, win 501, options [nop,nop,TS val 417110334 ecr 1666257193], length 228
16:52:04.688061 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 964:1488, ack 1, win 501, options [nop,nop,TS val 417110334 ecr 1666257193], length 524
16:52:04.688118 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 1488:2436, ack 1, win 501, options [nop,nop,TS val 417110334 ecr 1666257193], length 948
16:52:04.688246 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 736, win 592, options [nop,nop,TS val 1666267207 ecr 417110333], length 0
16:52:04.688246 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 964, win 614, options [nop,nop,TS val 1666267207 ecr 417110334], length 0
16:52:04.688393 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 1488, win 637, options [nop,nop,TS val 1666267207 ecr 417110334], length 0
16:52:04.688394 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 2436, win 660, options [nop,nop,TS val 1666267207 ecr 417110334], length 0
16:52:04.790193 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 2436:3720, ack 1, win 501, options [nop,nop,TS val 417110436 ecr 1666267207], length 1284
16:52:04.790772 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 3720, win 682, options [nop,nop,TS val 1666267210 ecr 417110436], length 0
16:52:04.893988 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 3720:4068, ack 1, win 501, options [nop,nop,TS val 417110540 ecr 1666267310], length 348
16:52:04.894515 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 4068, win 705, options [nop,nop,TS val 1666267413 ecr 417110540], length 0
16:52:04.997986 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 4068:4416, ack 1, win 501, options [nop,nop,TS val 417110644 ecr 1666267413], length 348
16:52:04.998548 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 4416, win 727, options [nop,nop,TS val 1666267517 ecr 417110644], length 0
16:52:05.101966 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 4416:4764, ack 1, win 501, options [nop,nop,TS val 417110748 ecr 1666267517], length 348
16:52:05.102473 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 4764, win 750, options [nop,nop,TS val 1666267621 ecr 417110748], length 0
16:52:05.205989 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 4764:5112, ack 1, win 501, options [nop,nop,TS val 417110852 ecr 1666267621], length 348
16:52:05.206557 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 5112, win 773, options [nop,nop,TS val 1666267725 ecr 417110852], length 0
16:52:05.310083 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 5112:5460, ack 1, win 501, options [nop,nop,TS val 417110956 ecr 1666267725], length 348
16:52:05.310566 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 5460, win 795, options [nop,nop,TS val 1666267829 ecr 417110956], length 0
16:52:05.413392 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 5460:5808, ack 1, win 501, options [nop,nop,TS val 417111060 ecr 1666267829], length 348
16:52:05.414562 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 5808, win 818, options [nop,nop,TS val 1666267933 ecr 417111060], length 0
16:52:05.521988 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 5808:6156, ack 1, win 501, options [nop,nop,TS val 417111168 ecr 1666267933], length 348
16:52:05.522500 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 6156, win 841, options [nop,nop,TS val 1666268041 ecr 417111168], length 0
16:52:05.625965 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 6156:6504, ack 1, win 501, options [nop,nop,TS val 417111272 ecr 1666268041], length 348
16:52:05.626524 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 6504, win 863, options [nop,nop,TS val 1666268145 ecr 417111272], length 0
16:52:05.730616 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 6504:6852, ack 1, win 501, options [nop,nop,TS val 417111376 ecr 1666268145], length 348
16:52:05.730493 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 6852, win 886, options [nop,nop,TS val 1666268249 ecr 417111376], length 0
16:52:05.833591 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 6852:7200, ack 2, win 501, options [nop,nop,TS val 417111408 ecr 1666268249], length 348
```

Captured on Pi using tcpdump (limit to 10 packets)

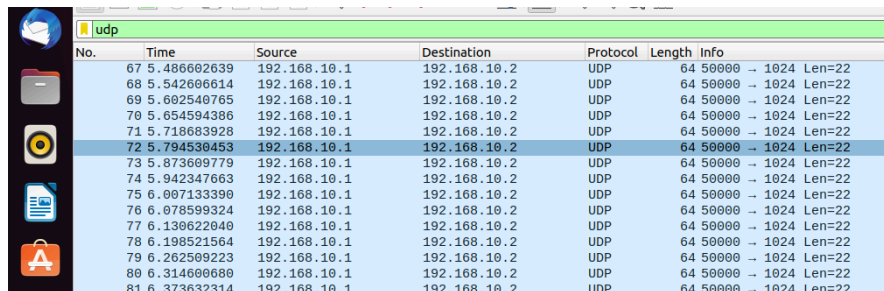
```
pi@p4pi: ~$ tcpdump -r captured.pcap
reading from file captured.pcap, link-type EN10MB (Ethernet), snapshot length 262144
16:53:52.636794 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 800913572:800913696, ack 1017298720, win 501, options [nop,nop,TS val 417218282 ecr 1666375104], length 124
16:53:52.637174 IP 192.168.10.1.48360 > 192.168.10.2.ssh: Flags [.], ack 124, win 3259, options [nop,nop,TS val 1666375155 ecr 417218282], length 0
16:53:55.995981 IP 192.168.10.2.40137 > 1.1.1.1.domain: 15016+ A? 2.debian.pool.ntp.org. (39)
16:53:55.996088 IP 192.168.10.2.49870 > 1.1.1.1.domain: 41997+ AAAA? 2.debian.pool.ntp.org. (39)
16:54:00.999430 IP 192.168.10.2.51303 > 1.1.1.1.domain: 32694+ A? 2.debian.pool.ntp.org. (39)
16:54:00.999493 IP 192.168.10.2.49870 > 1.1.1.1.domain: 41997+ AAAA? 2.debian.pool.ntp.org. (39)
16:54:06.003235 IP 192.168.10.2.50639 > 1.1.1.1.domain: 53784+ A? 3.debian.pool.ntp.org. (39)
16:54:06.003341 IP 192.168.10.2.43570 > 1.1.1.1.domain: 37415+ AAAA? 3.debian.pool.ntp.org. (39)
16:54:11.007003 IP 192.168.10.2.49407 > 1.1.1.1.domain: 52190+ A? 3.debian.pool.ntp.org. (39)
16:54:11.007068 IP 192.168.10.2.43570 > 1.1.1.1.domain: 37415+ AAAA? 3.debian.pool.ntp.org. (39)
pi@p4pi: ~$
```

Send 100 packets from Pi to 192.168.10.2

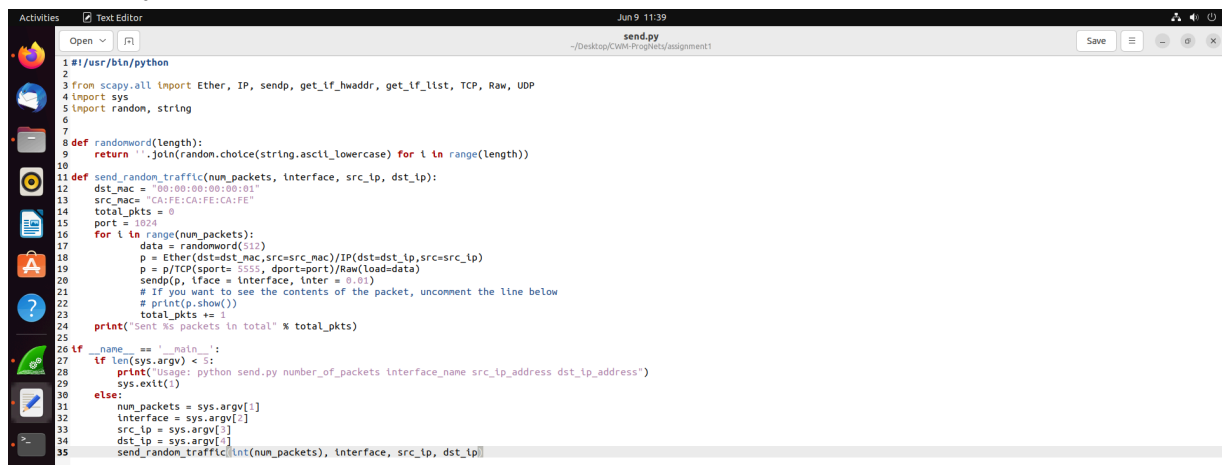


Transport protocol used is UDP. The length is 22 bits. For reference for the next section, source port is 50000

Can apply a UDP filter to only capture the packets we send



Modified Python file:



After changing to TCP, and applying TCP filter:

The image shows a Wireshark packet capture window titled "enxc37965f8a0f (tcp)". The packet list pane displays a series of TCP retransmissions. The first packet (No. 65) is a SYN packet from 192.168.10.1 to 192.168.10.2, port 5555, with a sequence number of 0 and a window size of 8192. Subsequent packets (Nos. 66-100) are retransmissions of this SYN packet, each with a "Retransmission" flag and a "Port numbers reused" message. The packet details pane for packet 100 shows the "Transmission Control Protocol" section with "Src Port: 5555", "Dst Port: 1024", "Seq: 0", and "Len: 512". The packet bytes pane shows the raw data of the SYN packet, including the Ethernet II header, Internet Protocol Version 4 header, and the TCP header with the SYN flag set.

No.	Time	Source	Destination	Protocol	Length	Info
65	3.933087058	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
66	4.001107228	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
67	4.006772189	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
68	4.112938020	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
69	4.177091169	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
70	4.245095377	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
71	4.300513562	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
72	4.372376360	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
73	4.425095377	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
74	4.489102809	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
75	4.553103754	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
76	4.604925099	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
77	4.670772990	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
78	4.725137672	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
79	4.797074702	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
80	4.848659940	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
81	4.912000759	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
82	4.969103789	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
83	5.031033330	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
84	5.085045319	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
85	5.145108392	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
86	5.201119342	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
87	5.256785495	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
88	5.321088882	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
89	5.392839111	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
90	5.453097588	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
91	5.557108940	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
92	5.605107161	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
93	5.665112027	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
94	5.721114053	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
95	5.777109655	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
96	5.840824680	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
97	5.923574012	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
98	5.997622250	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
99	6.105080895	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512
100	6.157080600	192.168.10.1	192.168.10.2	TCP	566	[TCP Retransmission] [TCP Port numbers reused] 5555 --> 1024 [SYN] Seq=0 Win=8192 Len=512

Frame 1: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface enxc37965f8a0f, 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: 512
Data (512 bytes)
0000 00 00 00 00 00 01 ca fe ca fe ca fe 00 00 45 00E
0010 02 28 00 01 00 00 40 00 e3 7b c0 a8 0a 01 c0 a8-...-...
0020 0a 02 15 b3 04 00 00 00 00 00 00 00 00 50 02P..
0030 20 00 55 bc 00 00 77 63 63 71 63 76 65 62 78 61 U..wc.cqcvbxa
0040 6f 6e 6d 65 6e 62 68 67 6b 62 72 66 63 64 6a 79 omnenbng kbrcfody
0050 73 74 6d 78 7a 79 63 69 62 6f 6d 6e 77 6d 67 7a stmxyzci bonnmwmgz

Can see the protocol is TCP, source port changed from 50000 to 5555, len from 22 to 512.