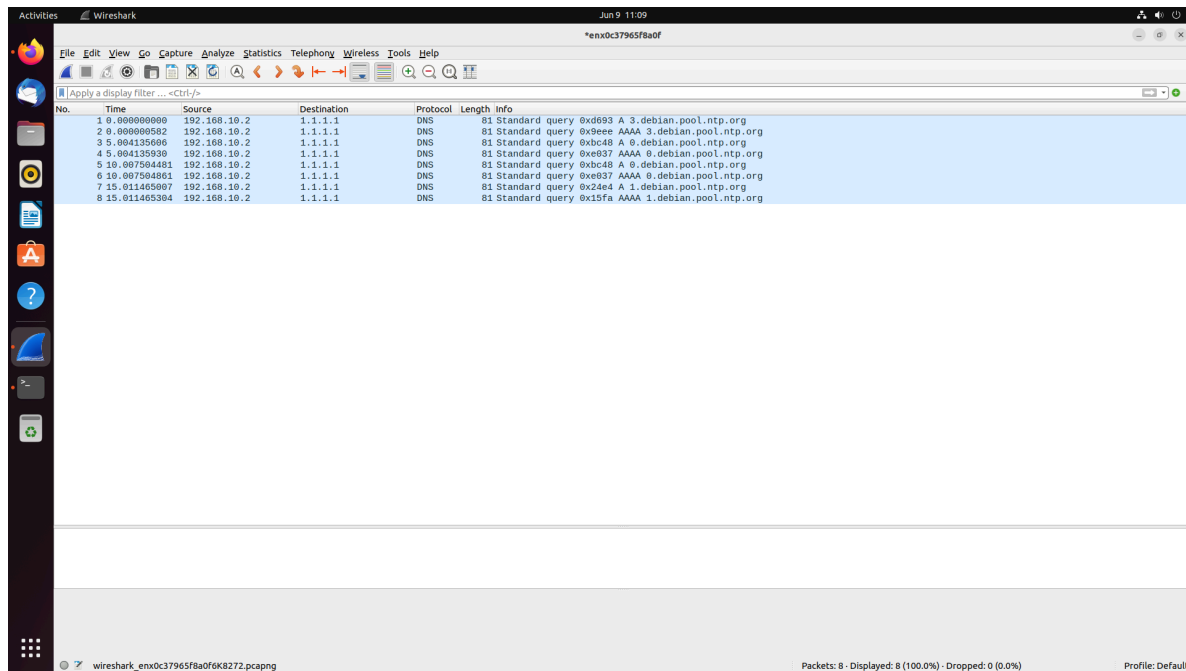


Capture on ethernet interface



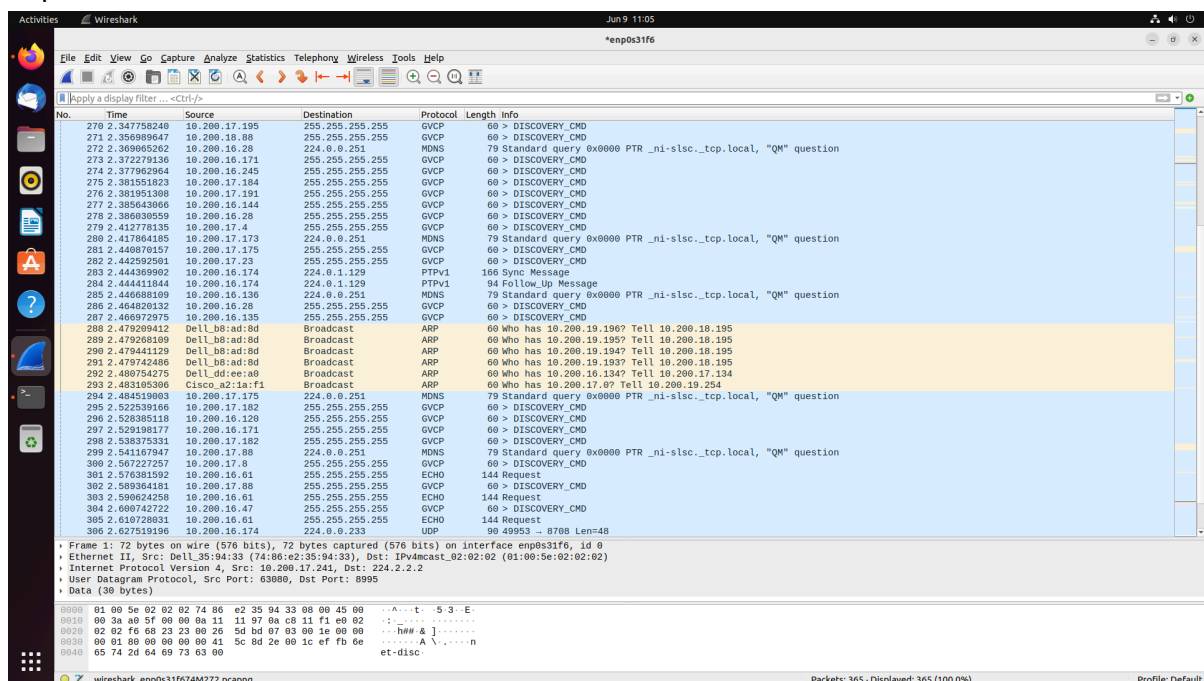
The screenshot shows a Wireshark capture on the ethernet interface 'enx0c37965f8a0f'. The packet list displays eight DNS standard queries from source 192.168.10.2 to destination 1.1.1.1. The queries are for various domain names including 3.debian.pool.ntp.org, 0.debian.pool.ntp.org, 0.debian.pool.ntp.org, 0.debian.pool.ntp.org, 0.debian.pool.ntp.org, 0.debian.pool.ntp.org, 0.debian.pool.ntp.org, and 1.debian.pool.ntp.org. The packet details pane shows the structure of a DNS Standard Query, including the Question section with the query name and type.

| 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

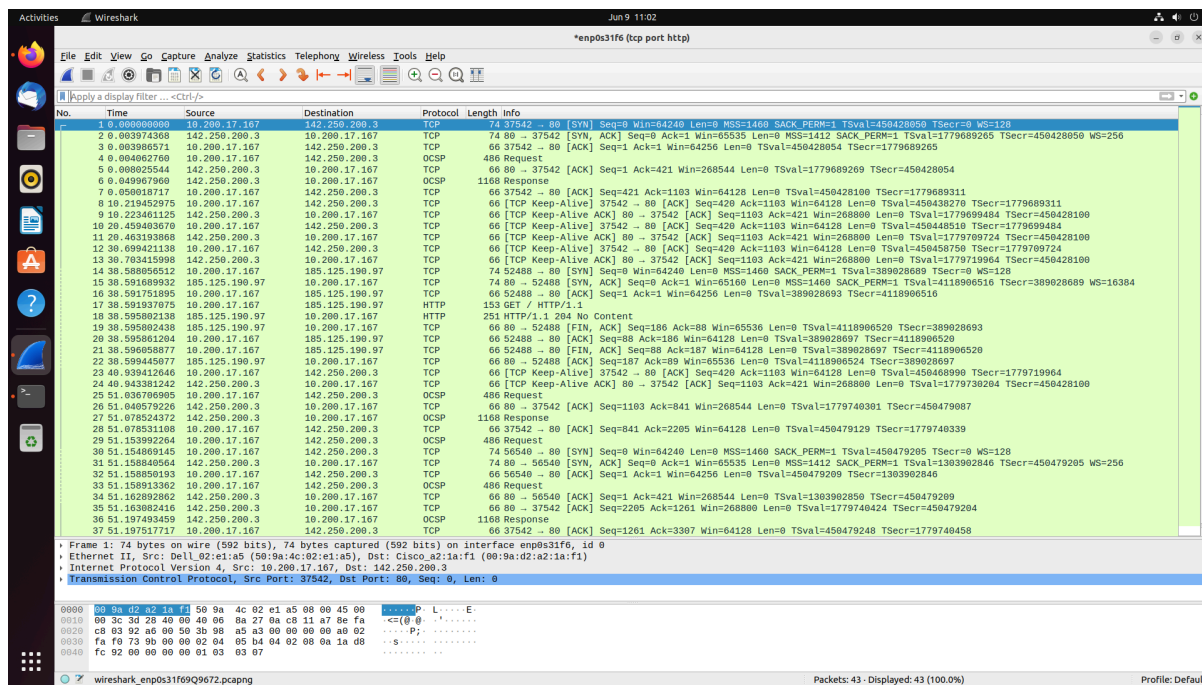


The screenshot shows a Wireshark capture on the network interface 'enp0s31f6'. The packet list displays a large number of packets, including DNS queries, ARP requests, and ICMP Echo requests. The packet details pane shows the structure of a DNS Standard Query, including the Question section with the query name and type. The packet bytes pane shows the raw data of the selected packet, including the DNS query and the response.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|-----------------|----------|--------|---|
| 270 | 2.347758240 | 10.200.17.195 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 271 | 2.356989647 | 10.200.18.88 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 272 | 2.369060526 | 10.200.16.28 | 224.0.0.251 | MDNS | 79 | Standard query 0x0000 PTR _ni._slsc._tcp.local, "QM" question |
| 273 | 2.372779136 | 10.200.16.171 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 274 | 2.377962964 | 10.200.16.245 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 275 | 2.381551023 | 10.200.17.184 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 276 | 2.381951306 | 10.200.17.191 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 277 | 2.385643066 | 10.200.16.144 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 278 | 2.386030959 | 10.200.16.28 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 279 | 2.412778135 | 10.200.17.4 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 280 | 2.417864185 | 10.200.17.173 | 224.0.0.251 | MDNS | 79 | Standard query 0x0000 PTR _ni._slsc._tcp.local, "QM" question |
| 281 | 2.440870157 | 10.200.17.175 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 282 | 2.442592501 | 10.200.17.23 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 283 | 2.444360902 | 10.200.16.174 | 224.0.1.129 | PTPv1 | 166 | 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._slsc._tcp.local, "QM" question |
| 286 | 2.464820132 | 10.200.16.28 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 287 | 2.466972975 | 10.200.16.135 | 255.255.255.255 | GVCP | 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._slsc._tcp.local, "QM" question |
| 295 | 2.522539166 | 10.200.17.182 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 296 | 2.520385110 | 10.200.16.120 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 297 | 2.529198177 | 10.200.16.171 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 298 | 2.538370331 | 10.200.17.182 | 255.255.255.255 | GVCP | 60 | > DISCOVERY_CMD |
| 299 | 2.541817947 | 10.200.17.88 | 224.0.0.251 | MDNS | 79 | Standard query 0x0000 PTR _ni._slsc._tcp.local, "QM" question |
| 300 | 2.567227257 | 10.200.17.9 | 255.255.255.255 | GVCP | 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 | GVCP | 60 | > DISCOVERY_CMD |
| 303 | 2.598024258 | 10.200.16.61 | 255.255.255.255 | ECHO | 144 | Request |
| 304 | 2.608742722 | 10.200.16.47 | 255.255.255.255 | GVCP | 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



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.

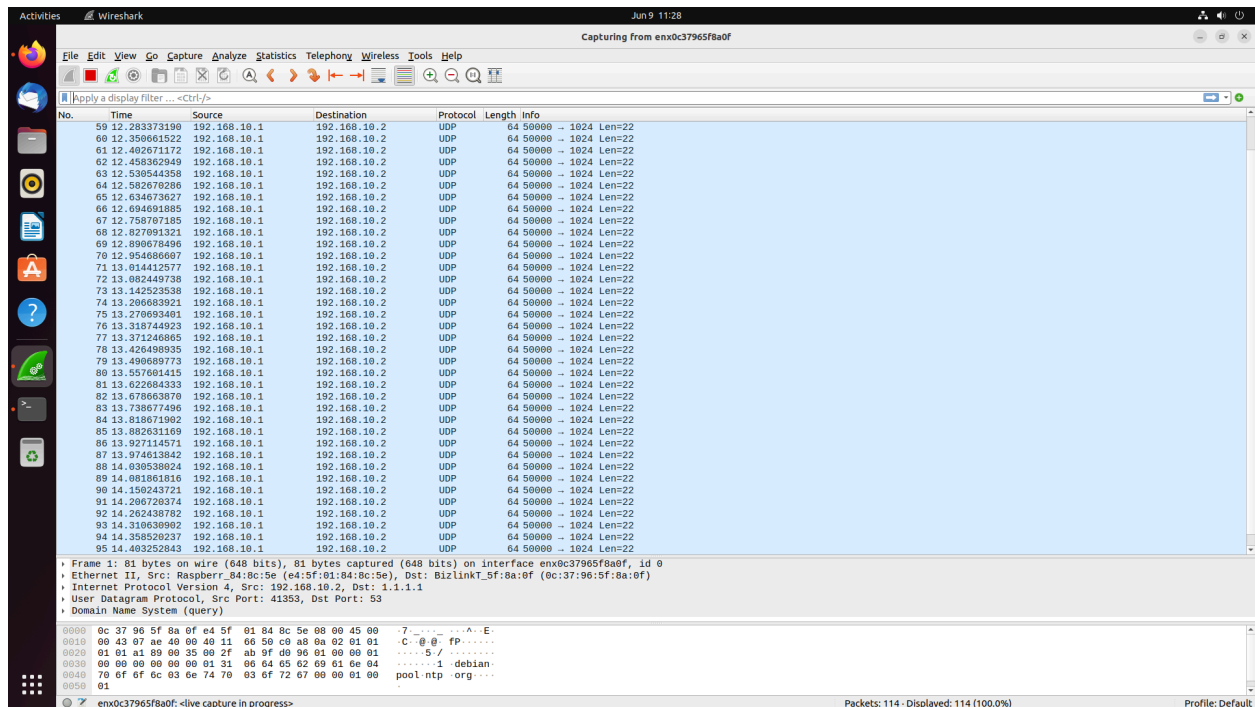
Capture on Pi using tcpdump (manual termination)

```
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 808021836:808022024, 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: 108068 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 192.168.10.2.59081 > 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: 108068 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 192.168.10.2.59081 > 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 188:408, 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 417111068 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 417111068], 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)

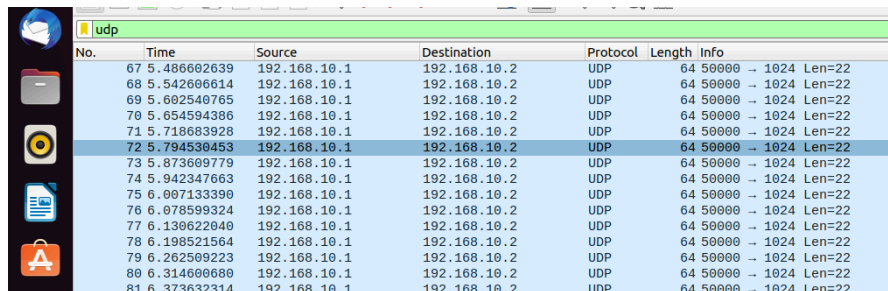
```
pi@p4pi: ~$ tcpdump -r captured.pcap
reading from file captured.pcap, link-type EN10MB (Ethernet), snapshot length 262144
16:53:52.636794 IP 192.168.10.2.ssh > 192.168.10.1.48360: Flags [P.], seq 800913572:800913696, ack 1017298720, win 501, options [nop,nop,TS val 417218282 ecr 1666375104], length 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: AAAAA? 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: AAAAA? 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: AAAAA? 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: AAAAA? 3.debian.pool.ntp.org. (39)
pi@p4pi: ~$
```

Send 100 packets from Pi to 192.168.10.2

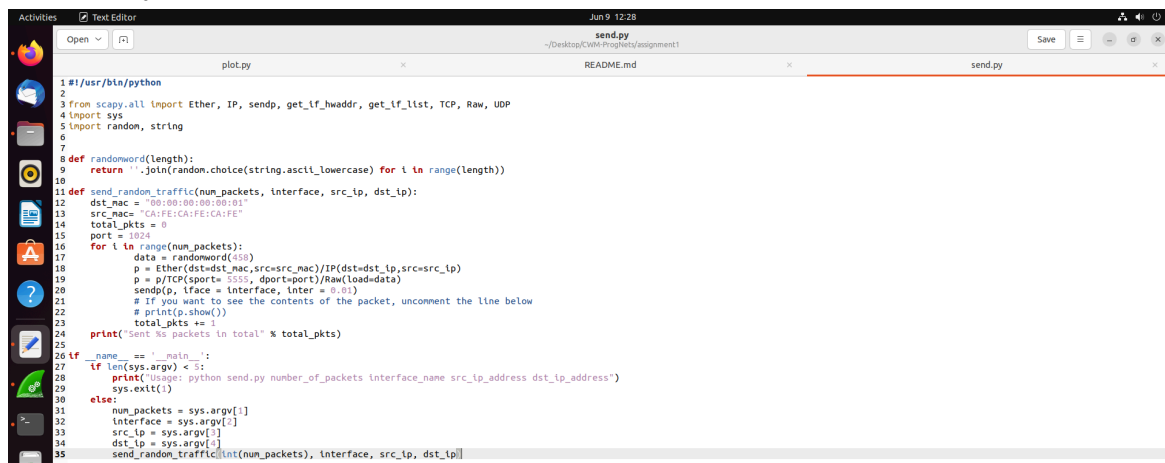


Transport protocol used is UDP. The payload is 22 bytes, but the total length is 81 bytes. For reference for the next section, source port is 50000

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. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top indicates 'Capturing from enxc37965f8a0f (tcp)' and the date 'Jun 9 12:28'. The main packet list pane shows a series of TCP retransmissions from source 192.168.10.1 to destination 192.168.10.2. The first packet (No. 365) is a SYN packet with Seq=0, Win=8192, Len=458. Subsequent packets (No. 366-399) are retransmissions of the same SYN packet. The packet details pane shows the selected packet (No. 400) as a TCP Retransmission with Seq=0, Win=8192, Len=458. The packet bytes pane shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|--------------|--------------|----------|--------|---|
| 365 | 0.540688769 | 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 |
| 366 | 0.597066121 | 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 |
| 367 | 0.657115366 | 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 |
| 368 | 0.726944900 | 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 |
| 369 | 0.805936361 | 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 |
| 370 | 0.885062084 | 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 |
| 371 | 0.933636302 | 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 |
| 372 | 0.924866428 | 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 |
| 373 | 0.105140005 | 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 |
| 374 | 0.172793022 | 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 |
| 375 | 0.248695407 | 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 |
| 376 | 0.292708552 | 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 |
| 377 | 0.369131298 | 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 |
| 378 | 0.424363636 | 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 |
| 379 | 0.479972280 | 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 |
| 380 | 0.564906479 | 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 |
| 381 | 0.624950278 | 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 |
| 382 | 0.685979897 | 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 |
| 383 | 0.761119770 | 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 |
| 384 | 0.821229310 | 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 |
| 385 | 0.876978679 | 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 |
| 386 | 0.945126086 | 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 |
| 387 | 0.903955488 | 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 |
| 388 | 0.956108435 | 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 |
| 389 | 0.105494930 | 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 |
| 390 | 0.148941892 | 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 |
| 391 | 0.205108596 | 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 |
| 392 | 0.268985234 | 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 |
| 393 | 0.330366207 | 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 |
| 394 | 0.396968468 | 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 |
| 395 | 0.473732861 | 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 |
| 396 | 0.515718183 | 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 |
| 397 | 0.568095730 | 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 |
| 398 | 0.629408057 | 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 |
| 399 | 0.677066148 | 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 |
| 400 | 0.726944310 | 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 400: 512 bytes on wire (4096 bits), 512 bytes captured (4096 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: 458

0000 00 00 00 00 00 01 ca fe ca fe ca fe 00 00 45 00E
0010 01 f2 00 01 00 00 40 00 e3 b1 c0 a8 0a 01 c0 a8@.....
0020 0a 02 15 b3 04 00 00 00 00 00 00 00 00 50 02P.
0030 29 00 00 00 00 00 77 0a 70 74 0a 0e 7a 05 79 05@..wmptjnzey
0040 7a 78 09 6f 72 78 05 71 70 05 65 6f 70 6a 64 68zLorxqd peevynhd
0050 6e 77 6b 64 72 6d 64 65 7a 70 68 71 7a 70 63 70nkdmdz phzpcp

enxc37965f8a0f: live capture in progress

Packets: 400 · Displayed: 400 (100.0%) Profile: Default

Can see the protocol is TCP, source port changed from 50000 to 5555, payload changed from 22 to 458 bytes, total length changed from 81 to 512 bytes.