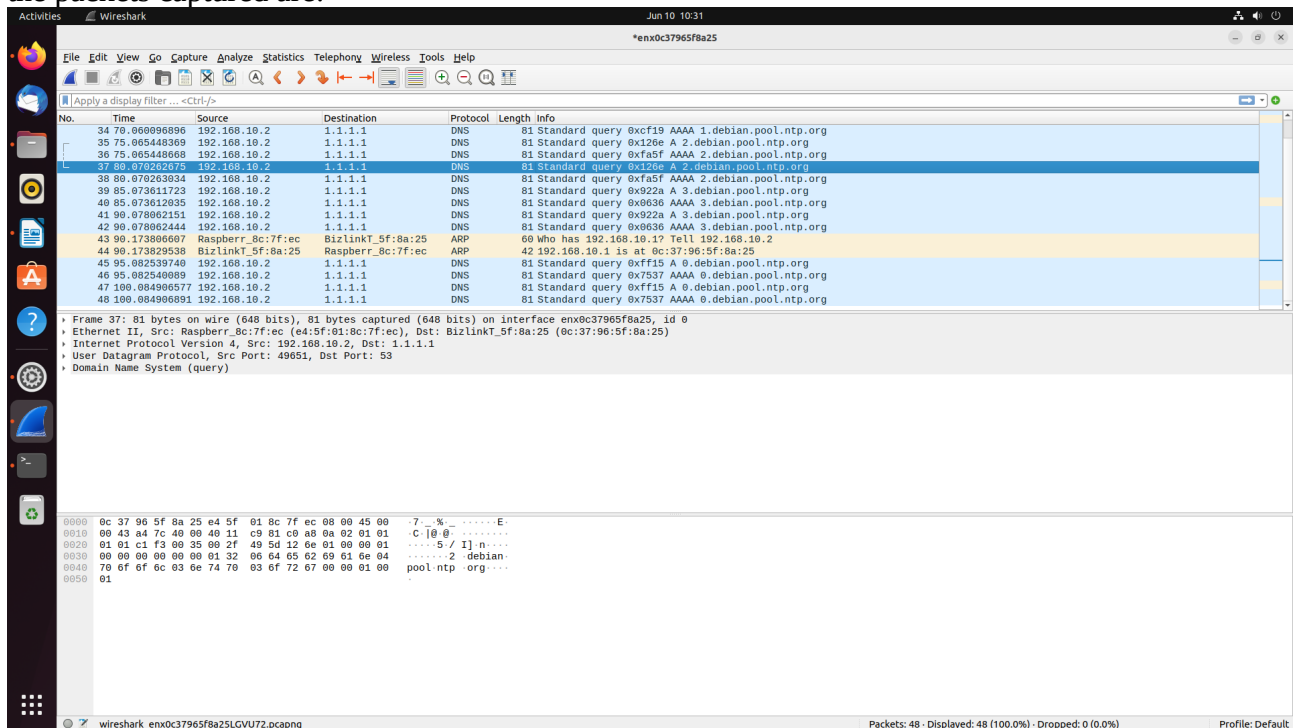
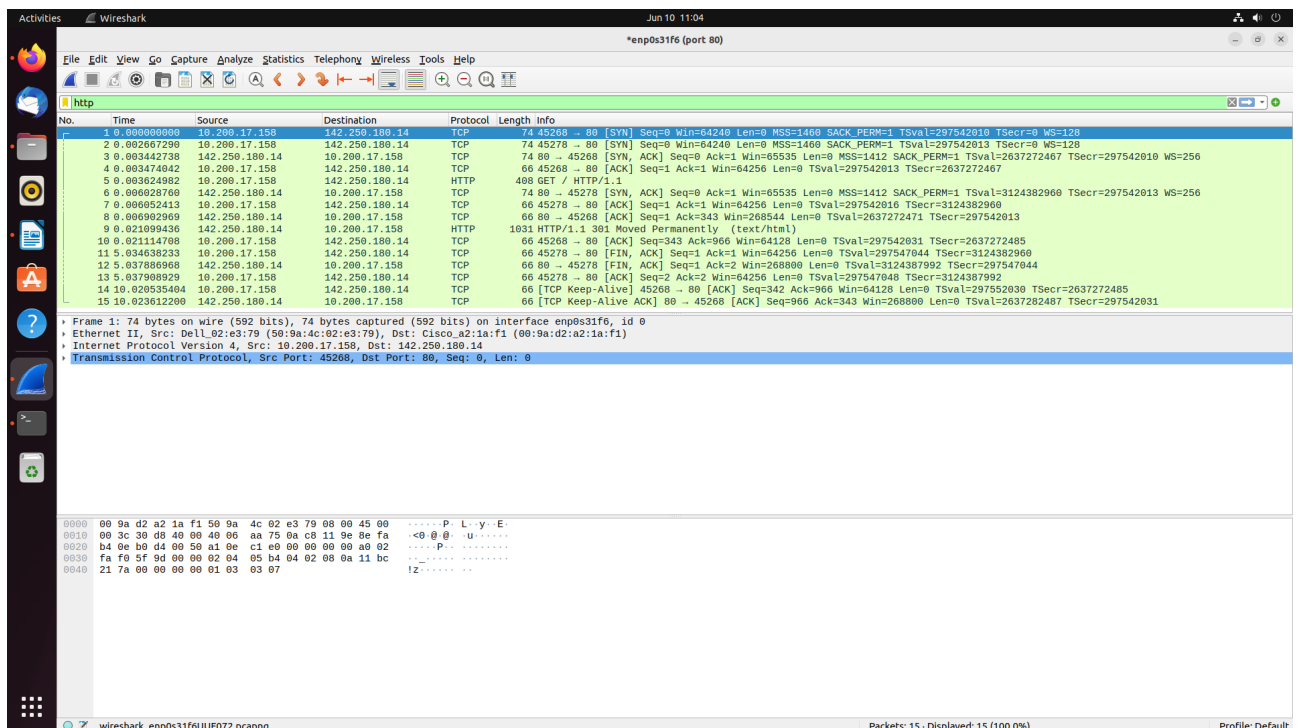


Exercise 1

For interface enx0c37965f8a25, address 192.168.10.1, the packets captured are:



The packets captured are DNS.



For interface enp0s31f6, address 10.200.17.158/22, to capture the http traffic, the filter port “TCP or UDP port 80 (HTTP): port 80” can be used. The packets captured when going to google.com are shown above.

On the Raspberry Pi,

```
Activities Terminal Jun 10 11:10
pi@p4pi: ~
valid_lft forever preferred_lft forever
ubuntu@ubuntu:~/CWM-ProgNets$ ssh pi@192.168.10.2
The authenticity of host '192.168.10.2 (192.168.10.2)' can't be established.
ED25519 key fingerprint is SHA256:ppE8WGaRo3i2vNP15d5x15oUk+q8Oym+Dt5QXhwg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.2' (ED25519) to the list of known hosts.
pi@192.168.10.2's password:
Linux p4pi 5.15.84-v8-p4pi #1 SMP PREEMPT Sat Feb 10 15:22:14 UTC 2024 aarch64

Last login: Thu May 16 22:21:12 2024
pi@p4pi: ~$ scp -r /home/pi/CWM-ProgNets pi@192.168.10.2:ubuntu/CWM-ProgNets
pi@192.168.10.2's password:
scp: ubuntu/CWM-ProgNets: No such file or directory
pi@p4pi: ~$ scp -r /home/pi/CWM-ProgNets pi@192.168.10.2:home/CWM-ProgNets
pi@192.168.10.2's password:
scp: home/CWM-ProgNets: No such file or directory
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
^C23:13:10.949336 IP 192.168.10.2.ssh > 192.168.10.1.47094: Flags [P.], seq 1235888996:1235889112, ack 2864289494, win 501, options [nop,nop,TS val 724486200 ecr 2840429043], length 116

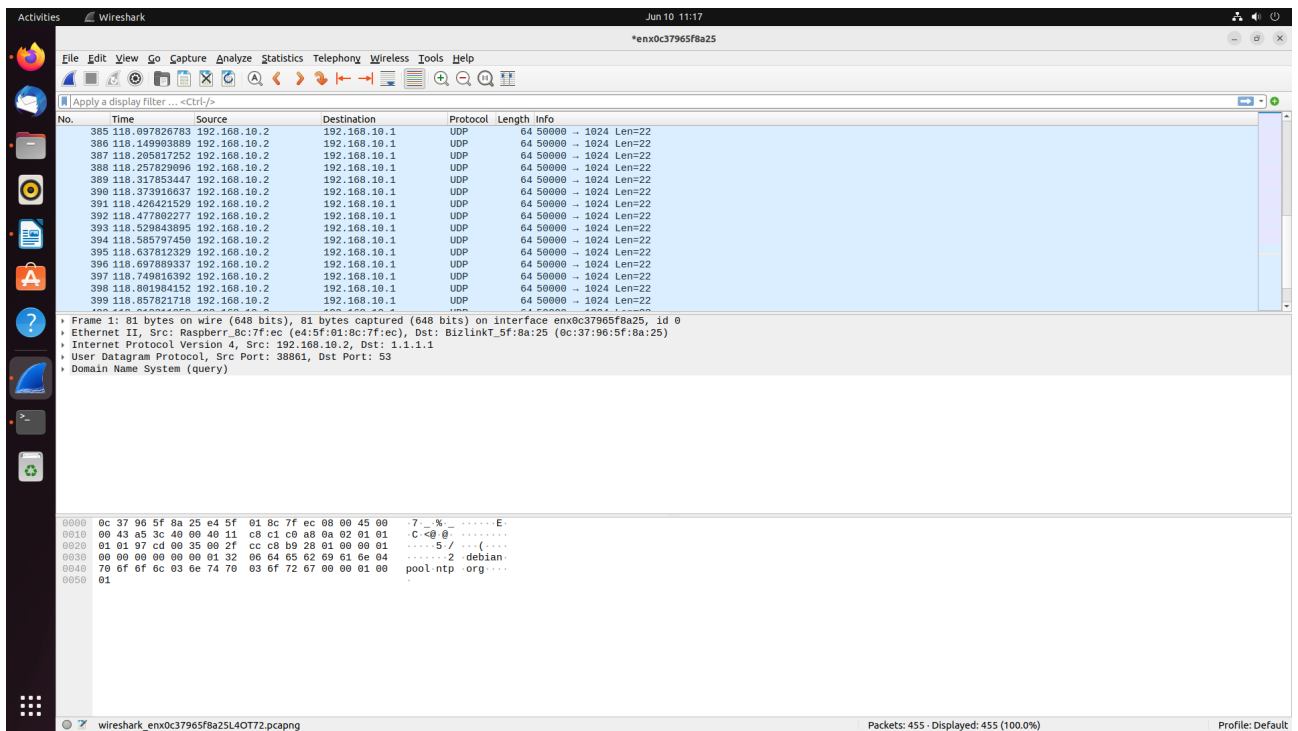
1 packet captured
23 packets received by filter
3 packets dropped by kernel
pi@p4pi: ~$ sudo tcpdump -i eth0 -c 10 -w captured.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
pi@p4pi: ~$
```

The packets captured are:

```
Activities Terminal Jun 10 11:12
pi@p4pi: ~
Last login: Thu May 16 22:21:12 2024
pi@p4pi: ~$ scp -r /home/pi/CWM-ProgNets pi@192.168.10.2:ubuntu/CWM-ProgNets
pi@192.168.10.2's password:
scp: ubuntu/CWM-ProgNets: No such file or directory
pi@p4pi: ~$ scp -r /home/pi/CWM-ProgNets pi@192.168.10.2:home/CWM-ProgNets
pi@192.168.10.2's password:
scp: home/CWM-ProgNets: No such file or directory
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
^C23:13:10.949336 IP 192.168.10.2.ssh > 192.168.10.1.47094: Flags [P.], seq 1235888996:1235889112, ack 2864289494, win 501, options [nop,nop,TS val 724486200 ecr 2840429043], length 116

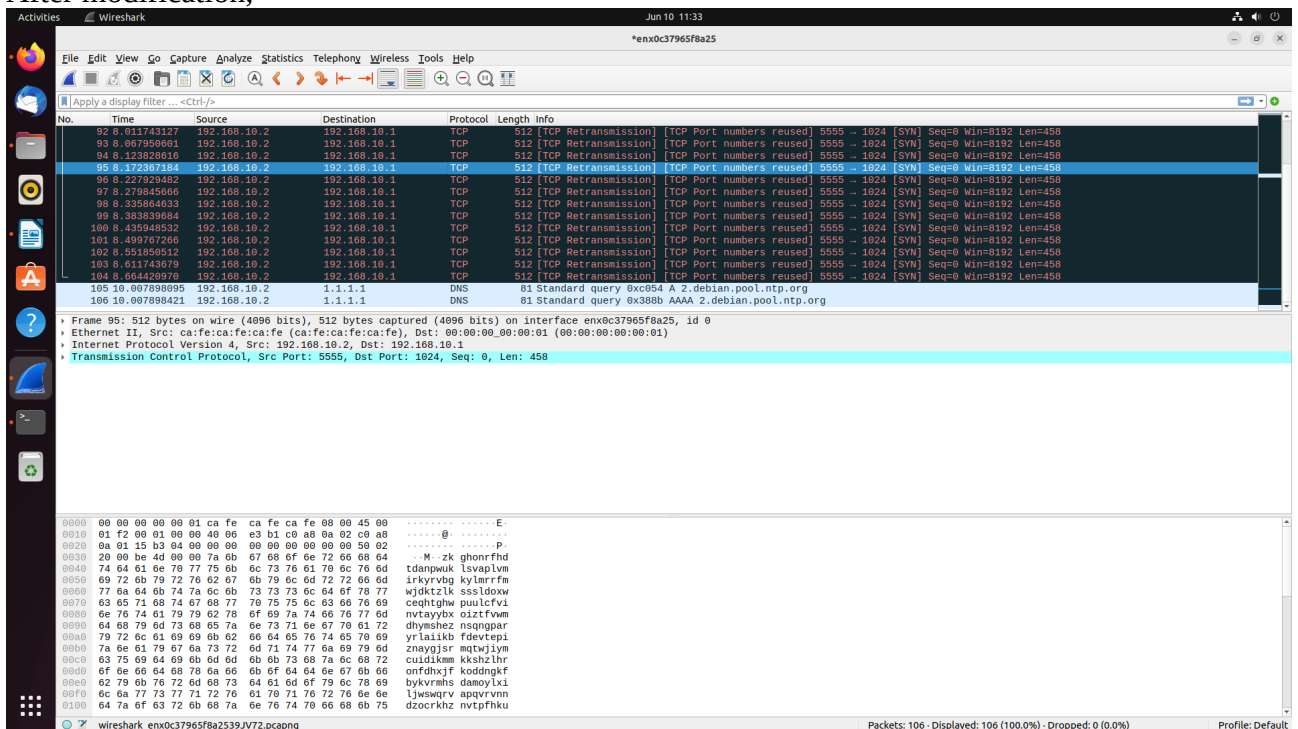
1 packet captured
23 packets received by filter
3 packets dropped by kernel
pi@p4pi: ~$ sudo tcpdump -i eth0 -c 10 -w captured.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
reading from file captured.pcap, link-type EN10MB (Ethernet), snapshot length 262144
23:14:11.421161 IP 192.168.10.2.ssh > 192.168.10.1.47094: Flags [P.], seq 1235891496:1235891540, ack 2864291258, win 501, options [nop,nop,TS val 724546671 ecr 2840489534], length 44
23:14:11.421276 IP 192.168.10.2.ssh > 192.168.10.1.47094: Flags [P.], seq 44:96, ack 1, win 501, options [nop,nop,TS val 724546672 ecr 2840489534], length 52
23:14:11.421364 IP 192.168.10.2.ssh > 192.168.10.1.47094: Flags [P.], seq 96:164, ack 1, win 501, options [nop,nop,TS val 724546672 ecr 2840489534], length 68
23:14:11.421458 IP 192.168.10.2.ssh > 192.168.10.1.47094: Flags [P.], seq 164:232, ack 1, win 501, options [nop,nop,TS val 724546672 ecr 2840489534], length 68
23:14:11.421765 IP 192.168.10.1.47094 > 192.168.10.2.ssh: Flags [R], ack 44, win 637, options [nop,nop,TS val 2840489586 ecr 724546671], length 0
23:14:11.421766 IP 192.168.10.1.47094 > 192.168.10.2.ssh: Flags [R], ack 96, win 637, options [nop,nop,TS val 2840489586 ecr 724546672], length 0
23:14:11.421766 IP 192.168.10.1.47094 > 192.168.10.2.ssh: Flags [R], ack 164, win 637, options [nop,nop,TS val 2840489586 ecr 724546672], length 0
23:14:11.421818 IP 192.168.10.1.47094 > 192.168.10.2.ssh: Flags [R], ack 232, win 637, options [nop,nop,TS val 2840489586 ecr 724546672], length 0
23:14:15.989899 IP 192.168.10.2.46938 > 1.1.1.1.domain: 60912+ A? 3.debtan.pool.ntp.org. (39)
23:14:15.989899 IP 192.168.10.2.60879 > 1.1.1.1.domain: 25870+ AAAA? 3.debtan.pool.ntp.org. (39)
pi@p4pi: ~$
```

Sending from the Raspberry Pi to the local machine, the packets are:



A filter “UDP” can be used to capture only these packets.
The packets are 64 Bytes.
It uses UDP.

After modification,



Link to repo:
<https://github.com/Y-J-Xue/CWM-ProgNets>