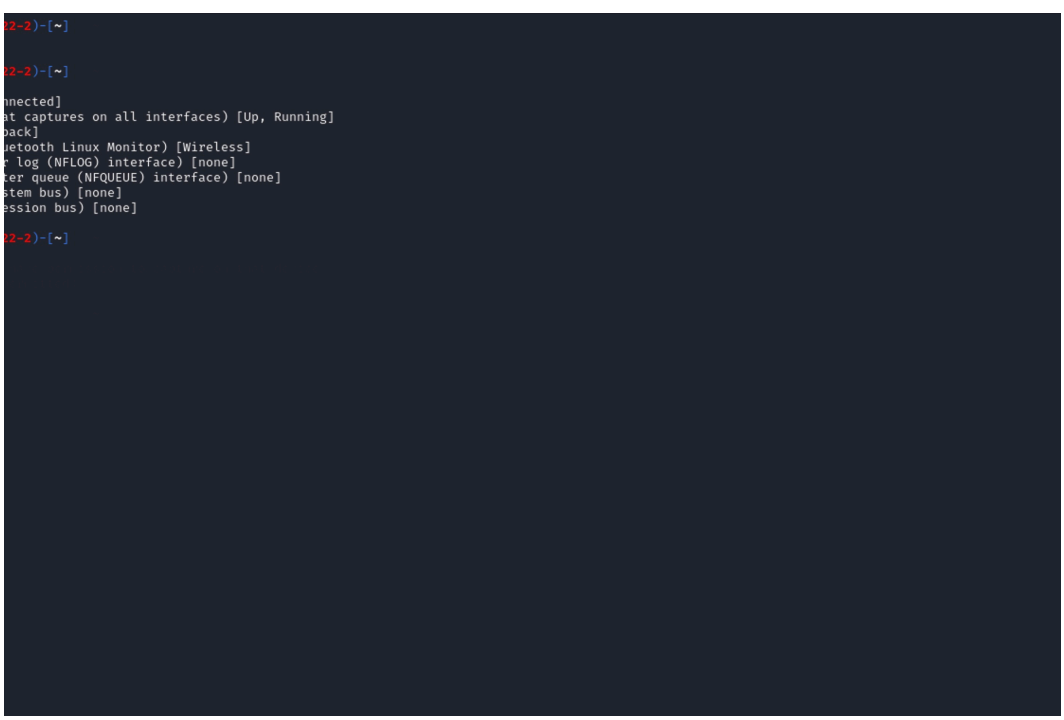
tcpdump lab

1. Enter the **man tcpdump** command to view manual help page for tcpdump:

Help page for tcpdump

2. Enter **tcpdump -D** to view available interfaces on your system:



3. Enter **tcpdump -I any** to listen for any traffic on your interface:
4. Start Firefox and enter a url to see packets displayed in the terminal.

```
root@kali-linux-2022-2: ~
Actions  Edit  View  Help
s-system (D-Bus system bus) [none]
s-session (D-Bus session bus) [none]

root@kali-linux-2022-2)-[~]
cpdump -i any
mp: data link type LINUX_SLL2
mp: verbose output suppressed, use -v[v]... for full protocol decode
ning on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
:30.842245 eth0  M   IP 10.211.55.2.mdns > mdns.mcast.net.mdns: 0 [3q] PTR (QM)? _afpovertcp._tcp.local. PTR (QM)? _rfb._tcp.local. PTR (QM)? _adisk._tcp.local. (64)
:30.842249 eth0  M   IP6 fe80::bcd0:74ff:fe41:f964.mdns > ff02::fb.mdns: 0 [3q] PTR (QM)? _afpovertcp._tcp.local. PTR (QM)? _rfb._tcp.local. PTR (QM)? _adisk._tcp.local. (64)
:30.913026 eth0  Out IP 10.211.55.4.59820 > 10.211.55.1.domain: 25551+ PTR? 2.55.211.10.in-addr.arpa. (42)
:30.944528 eth0  In  IP 10.211.55.1.domain > 10.211.55.4.59820: 25551 NXDomain* 0/1/0 (92)
:30.945215 eth0  Out IP 10.211.55.4.57542 > 10.211.55.1.domain: 578+ PTR? 251.0.0.224.in-addr.arpa. (42)
:30.957149 eth0  In  IP 10.211.55.1.domain > 10.211.55.4.57542: 578 1/0/0 PTR mdns.mcast.net. (70)
:30.958117 eth0  Out IP 10.211.55.4.51909 > 10.211.55.1.domain: 15966+ PTR? 4.6.9.f.1.4.e.f.f.f.4.7.0.d.c.b.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
:30.990829 eth0  In  IP 10.211.55.1.domain > 10.211.55.4.51909: 15966 NXDomain* 0/1/0 (139)
:30.991882 eth0  Out IP 10.211.55.4.53391 > 10.211.55.1.domain: 24259+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
:31.002411 eth0  In  IP 10.211.55.1.domain > 10.211.55.4.53391: 24259 NXDomain 0/1/0 (154)
:31.013713 eth0  Out IP 10.211.55.4.55685 > 10.211.55.1.domain: 47795+ PTR? 4.55.211.10.in-addr.arpa. (42)
:31.049556 eth0  In  IP 10.211.55.1.domain > 10.211.55.4.55685: 47795 NXDomain* 0/1/0 (98)
:31.050381 eth0  Out IP 10.211.55.4.47548 > 10.211.55.1.domain: 57233+ PTR? 1.55.211.10.in-addr.arpa. (42)
:31.084830 eth0  In  IP 10.211.55.1.domain > 10.211.55.4.47548: 57233 NXDomain* 0/1/0 (92)
:36.021387 eth0  Out ARP, Request who-has 10.211.55.1 tell 10.211.55.4, length 28
:36.022015 eth0  In  ARP, Reply 10.211.55.1 is-at 00:1c:42:00:00:18 (oui Unknown), length 28
:42.461379 eth0  Out IP 10.211.55.4.43458 > 10.211.55.1.domain: 27242+ A? espn.com. (26)
:42.461410 eth0  Out IP 10.211.55.4.43458 > 10.211.55.1.domain: 46959+ AAAA? espn.com. (26)
:42.494240 eth0  In  IP 10.211.55.1.domain > 10.211.55.4.43458: 46959 8/0/0 AAAA 2600:9000:252f:2c00:d:ac18:e2c0:93a1, AAAA 2600:9000:252f:5200:d:ac18:e2c0:93a1, AAAA 2600:9000:
00:d:ac18:e2c0:93a1, AAAA 2600:9000:252f:0:d:ac18:e2c0:93a1, AAAA 2600:9000:252f:9600:d:ac18:e2c0:93a1, AAAA 2600:9000:252f:e400:d:ac18:e2c0:93a1, AAAA 2600:9000:252f:2e00:d:ac
93a1, AAAA 2600:9000:252f:c600:d:ac18:e2c0:93a1 (250)
:47.464332 eth0  Out IP 10.211.55.4.43458 > 10.211.55.1.domain: 27242+ A? espn.com. (26)
:47.493163 eth0  In  IP 10.211.55.1.domain > 10.211.55.4.43458: 27242 4/0/0 A 18.160.78.20, A 18.160.78.9, A 18.160.78.29, A 18.160.78.128 (90)
:47.493332 eth0  Out IP 10.211.55.4.43458 > 10.211.55.1.domain: 46959+ AAAA? espn.com. (26)
:47.505568 eth0  In  IP 10.211.55.1.domain > 10.211.55.4.43458: 46959 8/0/0 AAAA 2600:9000:252f:6a00:d:ac18:e2c0:93a1, AAAA 2600:9000:252f:fe00:d:ac18:e2c0:93a1, AAAA 2600:9000:
00:d:ac18:e2c0:93a1, AAAA 2600:9000:252f:200:d:ac18:e2c0:93a1, AAAA 2600:9000:252f:9600:d:ac18:e2c0:93a1, AAAA 2600:9000:252f:8e00:d:ac18:e2c0:93a1, AAAA 2600:9000:252f:7a00:d:a
0:93a1, AAAA 2600:9000:252f:a200:d:ac18:e2c0:93a1 (250)
:47.507163 eth0  Out IP 10.211.55.4.59854 > server-18-160-78-20.atl59.r.cloudfront.net.http: Flags [S], seq 2257940259, win 64240, options [mss 1460,sackOK,TS val 3684620726 ecr
wscale 7], length 0
:47.507396 eth0  Out IP 10.211.55.4.59870 > server-18-160-78-20.atl59.r.cloudfront.net.http: Flags [S], seq 3291129707, win 64240, options [mss 1460,sackOK,TS val 3684620727 ecr
wscale 7], length 0
:47.517387 eth0  In  IP server-18-160-78-20.atl59.r.cloudfront.net.http > 10.211.55.4.59870: Flags [S.], seq 128561555, ack 3291129708, win 32768, options [mss 1460,wscale 1,nop
th 0
:47.517387 eth0  In  IP server-18-160-78-20.atl59.r.cloudfront.net.http > 10.211.55.4.59854: Flags [S.], seq 2141600876, ack 2257940260, win 32768, options [mss 1460,wscale 1,no
gth 0
:47.517517 eth0  Out IP 10.211.55.4.59870 > server-18-160-78-20.atl59.r.cloudfront.net.http: Flags [.], ack 1, win 502, length 0
:47.517565 eth0  Out IP 10.211.55.4.59854 > server-18-160-78-20.atl59.r.cloudfront.net.http: Flags [.], ack 1, win 502, length 0
:47.518036 eth0  Out IP 10.211.55.4.59870 > server-18-160-78-20.atl59.r.cloudfront.net.http: Flags [P.], seq 1:321, ack 1, win 502, length 320: HTTP: GET / HTTP/1.1
:47.520691 eth0  In  IP server-18-160-78-20.atl59.r.cloudfront.net.http > 10.211.55.4.59870: Flags [.], ack 321, win 16384, length 0
:47.542923 eth0  In  IP server-18-160-78-20.atl59.r.cloudfront.net.http > 10.211.55.4.59870: Flags [P.], seq 1:726, ack 321, win 16384, length 725: HTTP: HTTP/1.1 301 Moved Perm

:47.542979 eth0  Out IP 10.211.55.4.59870 > server-18-160-78-20.atl59.r.cloudfront.net.http: Flags [.], ack 726, win 501, length 0
:47.549282 eth0  Out IP 10.211.55.4.48902 > 10.211.55.1.domain: 21521+ A? www.espn.com. (30)
:47.561121 eth0  Out IP 10.211.55.4.51230 > 10.211.55.1.domain: 63861+ PTR? 20.78.160.18.in-addr.arpa. (43)
```

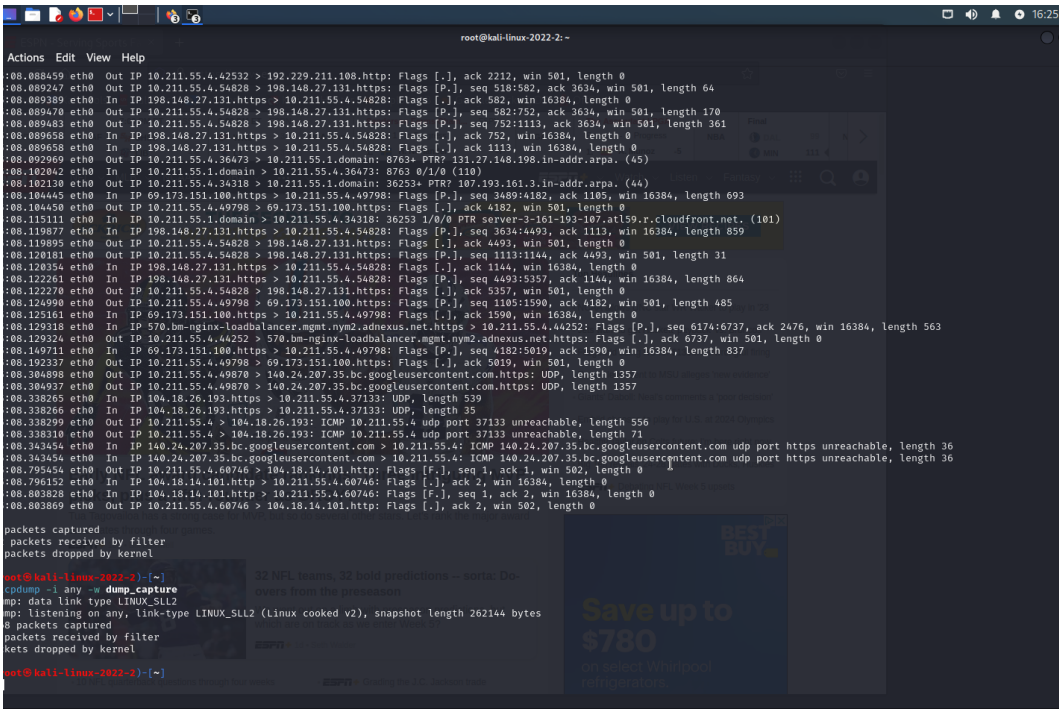
Packets from www.ESPN.com

```
h0  Out IP 10.211.55.4.49798 > 69.173.151.100.https: Flags [.], ack 3489, win 501, length 0
h0  Out IP 10.211.55.4.49798 > 69.173.151.100.https: Flags [P.], seq 668:1105, ack 3489, win 501, length 437
h0  In  IP 69.173.151.100.https > 10.211.55.4.49798: Flags [.], ack 1105, win 16384, length 0
h0  In  IP server-3-161-193-107.atl59.r.cloudfront.net.https > 10.211.55.4.54617: UDP, length 1452
h0  In  IP server-3-161-193-107.atl59.r.cloudfront.net.https > 10.211.55.4.54617: UDP, length 111
h0  In  IP server-3-161-193-107.atl59.r.cloudfront.net.https > 10.211.55.4.54617: UDP, length 116
h0  Out IP 10.211.55.4.54617 > server-3-161-193-107.atl59.r.cloudfront.net.https: UDP, length 95
h0  In  IP 192.229.211.108.http > 10.211.55.4.42532: Flags [P.], seq 1475:2212, ack 1246, win 16384, length 737: HTTP: HTTP/1.1 200 OK
h0  Out IP 10.211.55.4.42532 > 192.229.211.108.http: Flags [.], ack 2212, win 501, length 0
h0  Out IP 10.211.55.4.54828 > 198.148.27.131.https: Flags [P.], seq 518:582, ack 3634, win 501, length 64
h0  In  IP 198.148.27.131.https > 10.211.55.4.54828: Flags [.], ack 582, win 16384, length 0
h0  Out IP 10.211.55.4.54828 > 198.148.27.131.https: Flags [P.], seq 582:752, ack 3634, win 501, length 170
h0  Out IP 10.211.55.4.54828 > 198.148.27.131.https: Flags [P.], seq 752:1113, ack 3634, win 501, length 361
h0  In  IP 198.148.27.131.https > 10.211.55.4.54828: Flags [.], ack 752, win 16384, length 0
h0  In  IP 198.148.27.131.https > 10.211.55.4.54828: Flags [.], ack 1113, win 16384, length 0
h0  Out IP 10.211.55.4.36473 > 10.211.55.1.domain: 8763+ PTR? 131.27.148.198.in-addr.arpa. (45)
h0  In  IP 10.211.55.1.domain > 10.211.55.4.36473: 8763 0/1/0 (110)
h0  Out IP 10.211.55.4.34318 > 10.211.55.1.domain: 36253+ PTR? 107.193.161.3.in-addr.arpa. (44)
h0  In  IP 69.173.151.100.https > 10.211.55.4.49798: Flags [P.], seq 3489:4182, ack 1105, win 16384, length 693
h0  Out IP 10.211.55.4.49798 > 69.173.151.100.https: Flags [.], ack 4182, win 501, length 0
h0  In  IP 10.211.55.1.domain > 10.211.55.4.34318: 36253 1/0/0 PTR server-3-161-193-107.atl59.r.cloudfront.net. (101)
h0  In  IP 198.148.27.131.https > 10.211.55.4.54828: Flags [P.], seq 3634:4493, ack 1113, win 16384, length 859
h0  Out IP 10.211.55.4.54828 > 198.148.27.131.https: Flags [.], ack 4493, win 501, length 0
h0  Out IP 10.211.55.4.54828 > 198.148.27.131.https: Flags [P.], seq 1113:1144, ack 4493, win 501, length 31
h0  In  IP 198.148.27.131.https > 10.211.55.4.54828: Flags [.], ack 1144, win 16384, length 0
h0  In  IP 198.148.27.131.https > 10.211.55.4.54828: Flags [P.], seq 4493:5357, ack 1144, win 16384, length 864
h0  Out IP 10.211.55.4.54828 > 198.148.27.131.https: Flags [.], ack 5357, win 501, length 0
h0  Out IP 10.211.55.4.49798 > 69.173.151.100.https: Flags [P.], seq 1105:1590, ack 4182, win 501, length 485
h0  In  IP 69.173.151.100.https > 10.211.55.4.49798: Flags [.], ack 1590, win 16384, length 0
h0  In  IP 570.bm-nginx-loadbalancer.mgmt.nym2.adnexus.net.https > 10.211.55.4.44252: Flags [P.], seq 6174:6737, ack 2476, win 16384, length 563
h0  Out IP 10.211.55.4.44252 > 570.bm-nginx-loadbalancer.mgmt.nym2.adnexus.net.https: Flags [.], ack 6737, win 501, length 0
h0  In  IP 69.173.151.100.https > 10.211.55.4.49798: Flags [P.], seq 4182:5019, ack 1590, win 16384, length 837
h0  Out IP 10.211.55.4.49798 > 69.173.151.100.https: Flags [.], ack 5019, win 501, length 0
h0  Out IP 10.211.55.4.49870 > 140.24.207.35.bc.googleusercontent.com.https: UDP, length 1357
h0  Out IP 10.211.55.4.49870 > 140.24.207.35.bc.googleusercontent.com.https: UDP, length 1357
h0  In  IP 104.18.26.193.https > 10.211.55.4.37133: UDP, length 539
h0  In  IP 104.18.26.193.https > 10.211.55.4.37133: UDP, length 35
h0  Out IP 10.211.55.4 > 104.18.26.193: ICMP 10.211.55.4 udp port 37133 unreachable, length 556
h0  Out IP 10.211.55.4 > 104.18.26.193: ICMP 10.211.55.4 udp port 37133 unreachable, length 71
h0  In  IP 140.24.207.35.bc.googleusercontent.com > 10.211.55.4: ICMP 140.24.207.35.bc.googleusercontent.com udp port https unreachable, length 36
h0  In  IP 140.24.207.35.bc.googleusercontent.com > 10.211.55.4: ICMP 140.24.207.35.bc.googleusercontent.com udp port https unreachable, length 36
h0  Out IP 10.211.55.4.60746 > 104.18.14.101.http: Flags [F.], seq 1, ack 1, win 502, length 0
h0  In  IP 104.18.14.101.http > 10.211.55.4.60746: Flags [.], ack 2, win 16384, length 0
h0  In  IP 104.18.14.101.http > 10.211.55.4.60746: Flags [F.], seq 1, ack 2, win 16384, length 0
h0  Out IP 10.211.55.4.60746 > 104.18.14.101.http: Flags [.], ack 2, win 502, length 0

red
ived by filter
ed by kernel
```

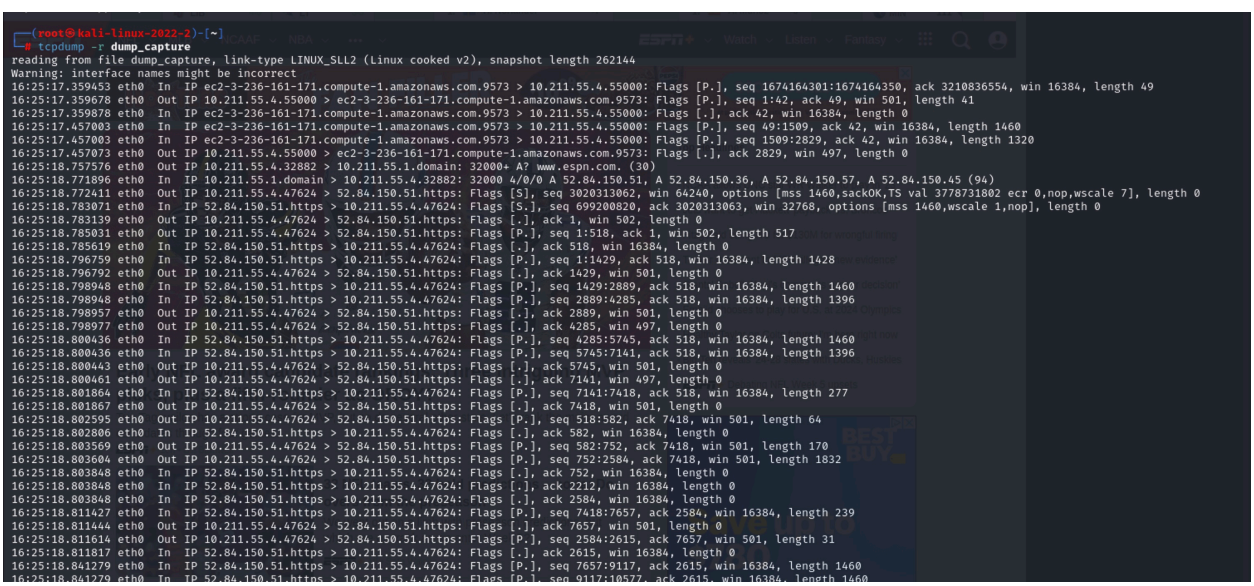
Packets from www.ESPN.com

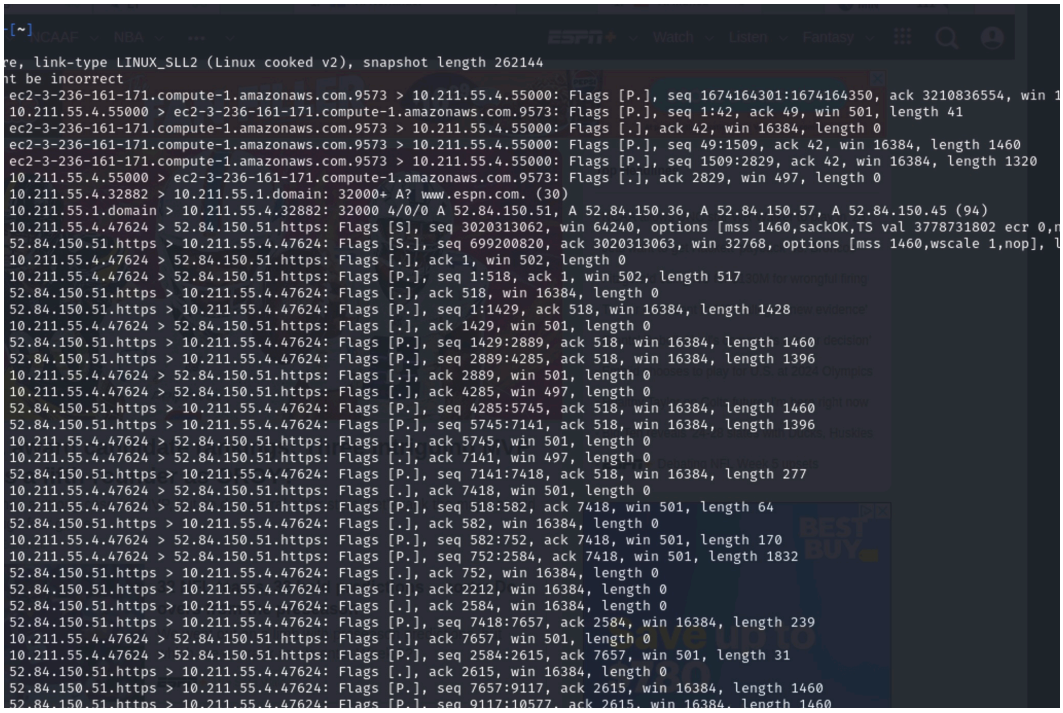
5. Enter **tcpdump -I any -w dump_capture** to redirect the output to a capture file called dump_capture:



Caption

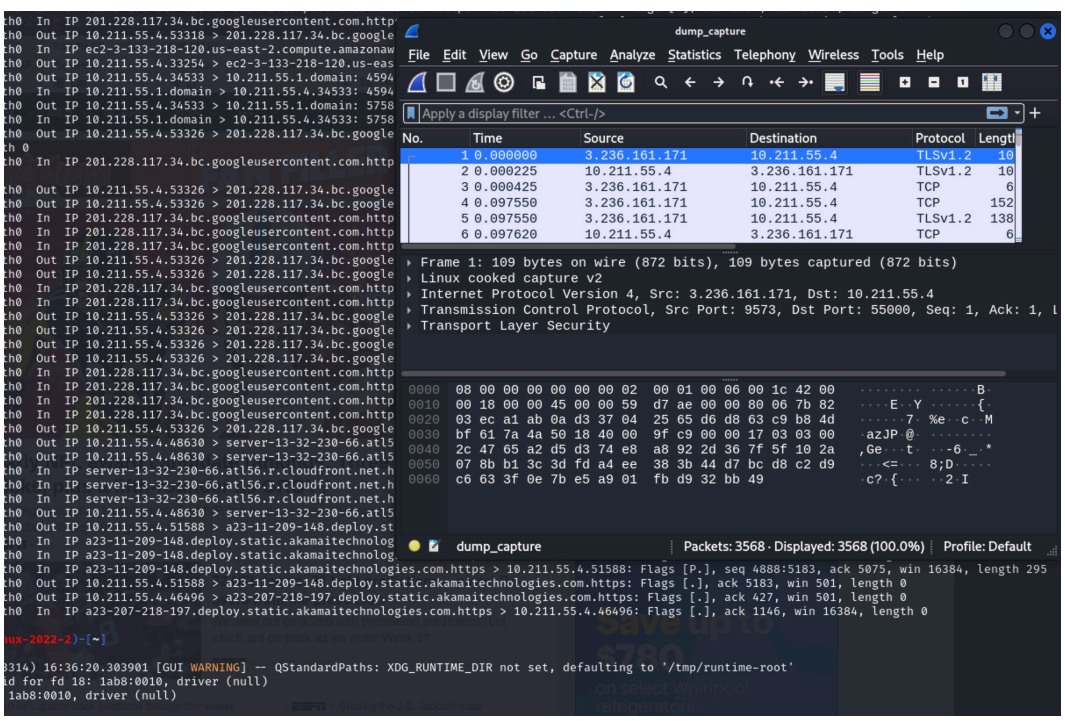
6. Use the command **tcpdump -r dump_capture** to view the dump capture:





Caption

7. Return to the terminal and enter **wireshark** to view the capture in Wireshark:



Caption