Linux Network Packet Capture

Project description

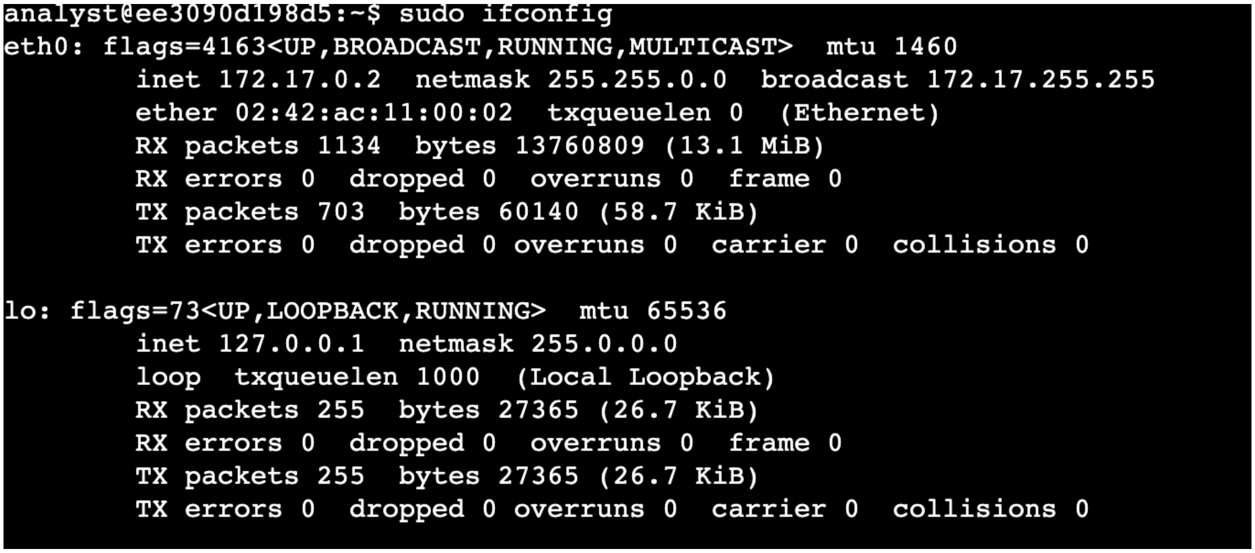
This project is dedicated to cultivating the fundamentals in capturing and analyzing network traffic in a Linux environment through the application of the tcpdump tool. The project explores the intricacies of utilizing tcpdump, a network packet analyzer, to effectively capture, filter, and analyze real-time data from network traffic.

Identify Network Interfaces

-Used ifconfig to identify available network interfaces.

-Utilize tcpdump to list available network interfaces, particularly useful on systems without ifconfig.

-The Ethernet network interface is identified by the entry with the eth prefix.



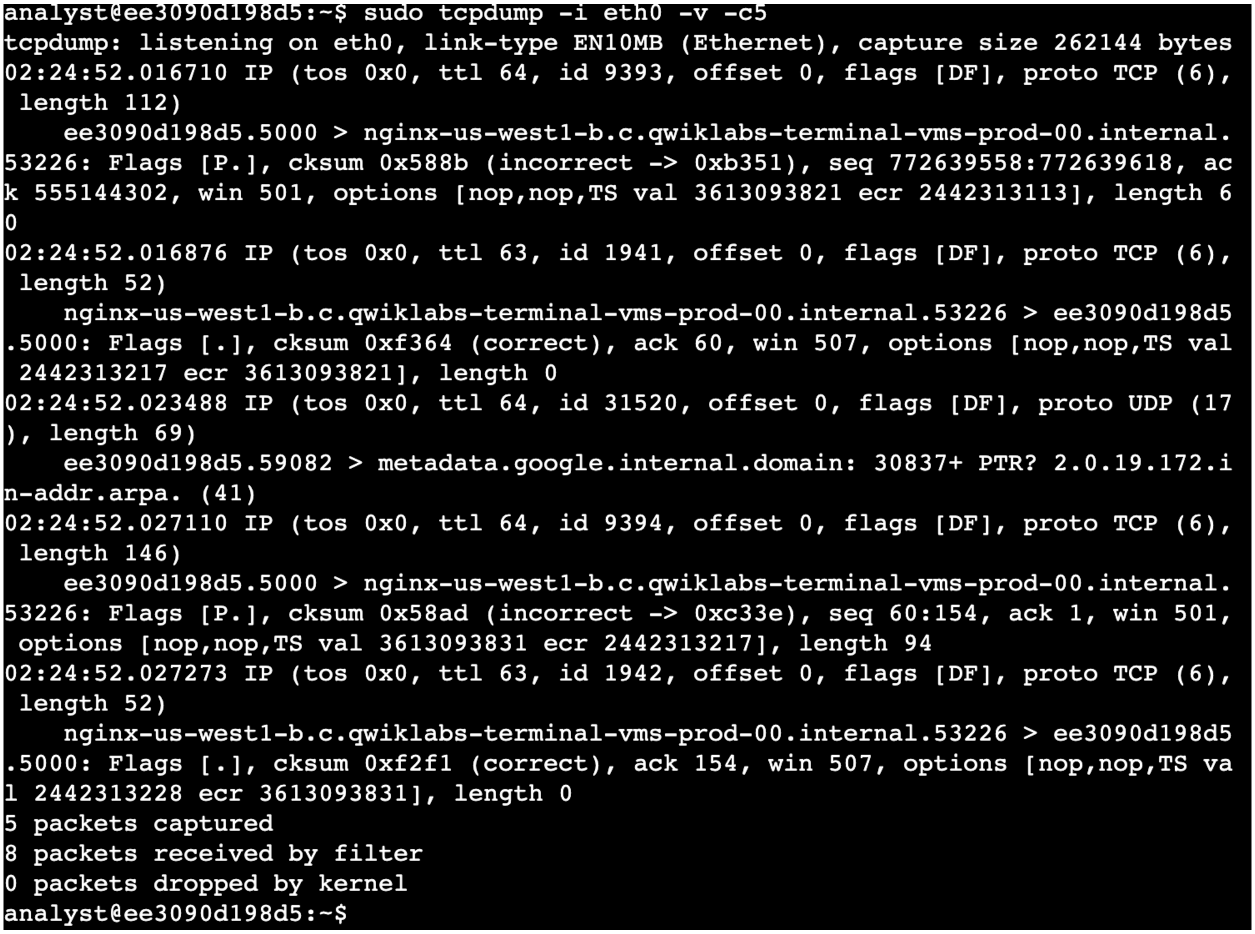
```
analyst@ee3090d198d5:~$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1460
        inet 172.17.0.2  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ac:11:00:02  txqueuelen 0  (Ethernet)
        RX packets 1134  bytes 13760809 (13.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 703  bytes 60140 (58.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 255  bytes 27365 (26.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 255  bytes 27365 (26.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Inspect the network traffic of a network interface with tcpdump

This command will run tcpdump with the following options:

- i eth0: Capture data specifically from the eth0 interface.
- v: Display detailed packet data.
- c5: Capture 5 packets of data.

tcpdump reported that it was listening on the eth0 interface, and it provided information on the link type and the capture size in bytes. On the next line, the first field is the packet's timestamp, followed by the protocol type: IP.The verbose option, -v, has provided more details about the IP packet fields, such as TOS, TTL, offset, flags, internal protocol type (in this case, TCP (6)), and the length of the outer IP packet in bytes

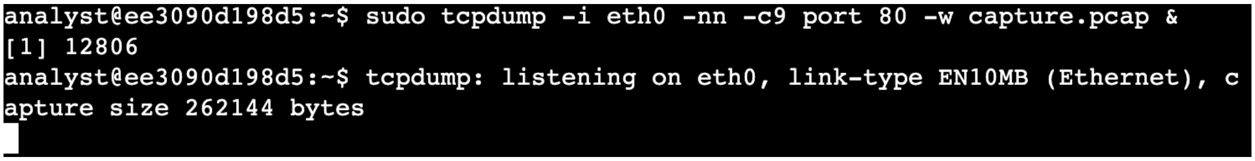


```
analyst@ee3090d198d5:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
02:24:52.016710 IP (tos 0x0, ttl 64, id 9393, offset 0, flags [DF], proto TCP (6),
 length 112)
    ee3090d198d5.5000 > nginx-us-west1-b.c.qwiklabs-terminal-vms-prod-00.internal.
53226: Flags [P.], cksum 0x588b (incorrect -> 0xb351), seq 772639558:772639618, ac
k 555144302, win 501, options [nop,nop,TS val 3613093821 ecr 2442313113], length 6
0
02:24:52.016876 IP (tos 0x0, ttl 63, id 1941, offset 0, flags [DF], proto TCP (6),
 length 52)
    nginx-us-west1-b.c.qwiklabs-terminal-vms-prod-00.internal.53226 > ee3090d198d5
.5000: Flags [.], cksum 0xf364 (correct), ack 60, win 507, options [nop,nop,TS val
 2442313217 ecr 3613093821], length 0
02:24:52.023488 IP (tos 0x0, ttl 64, id 31520, offset 0, flags [DF], proto UDP (17
), length 69)
    ee3090d198d5.59082 > metadata.google.internal.domain: 30837+ PTR? 2.0.19.172.i
n-addr.arpa. (41)
02:24:52.027110 IP (tos 0x0, ttl 64, id 9394, offset 0, flags [DF], proto TCP (6),
 length 146)
    ee3090d198d5.5000 > nginx-us-west1-b.c.qwiklabs-terminal-vms-prod-00.internal.
53226: Flags [P.], cksum 0x58ad (incorrect -> 0xc33e), seq 60:154, ack 1, win 501,
 options [nop,nop,TS val 3613093831 ecr 2442313217], length 94
02:24:52.027273 IP (tos 0x0, ttl 63, id 1942, offset 0, flags [DF], proto TCP (6),
 length 52)
    nginx-us-west1-b.c.qwiklabs-terminal-vms-prod-00.internal.53226 > ee3090d198d5
.5000: Flags [.], cksum 0xf2f1 (correct), ack 154, win 507, options [nop,nop,TS va
l 2442313228 ecr 3613093831], length 0
5 packets captured
8 packets received by filter
0 packets dropped by kernel
analyst@ee3090d198d5:~$
```

Capture network traffic with tcpdump

Use a filter and other tcpdump configuration options to save a small sample that contains only web (TCP port 80) network packet data.

Capture packet data into a file called capture.pcap:

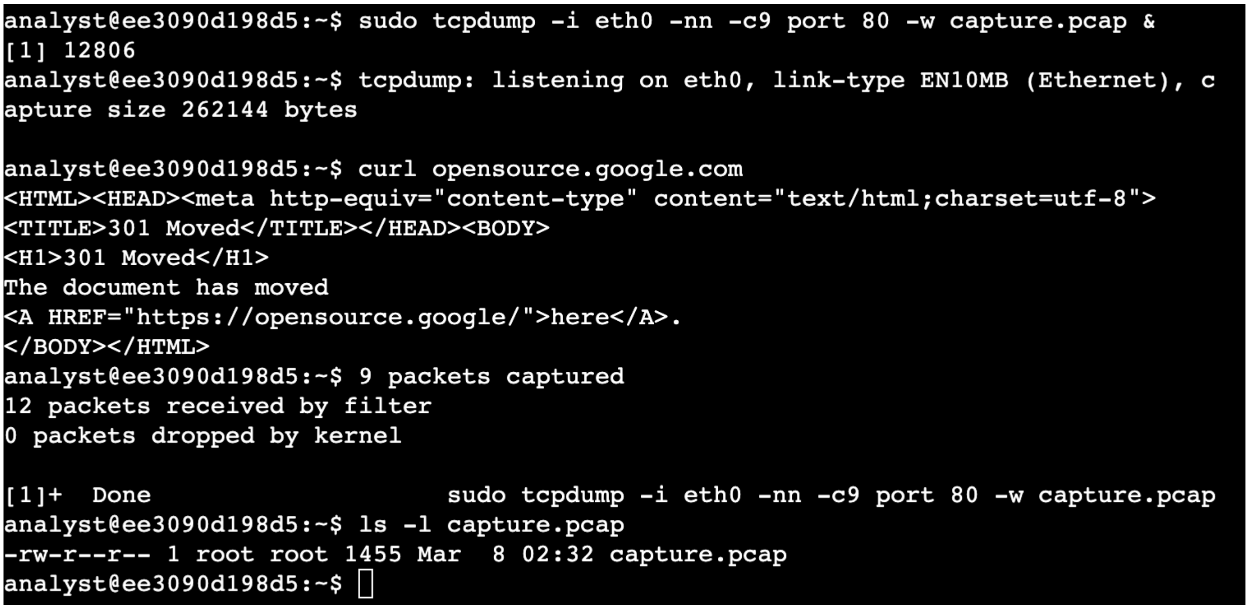


```
analyst@ee3090d198d5:~$ sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &
[1] 12806
analyst@ee3090d198d5:~$ tcpdump: listening on eth0, link-type EN10MB (Ethernet), c
apture size 262144 bytes
```

This command will run tcpdump in the background with the following options:

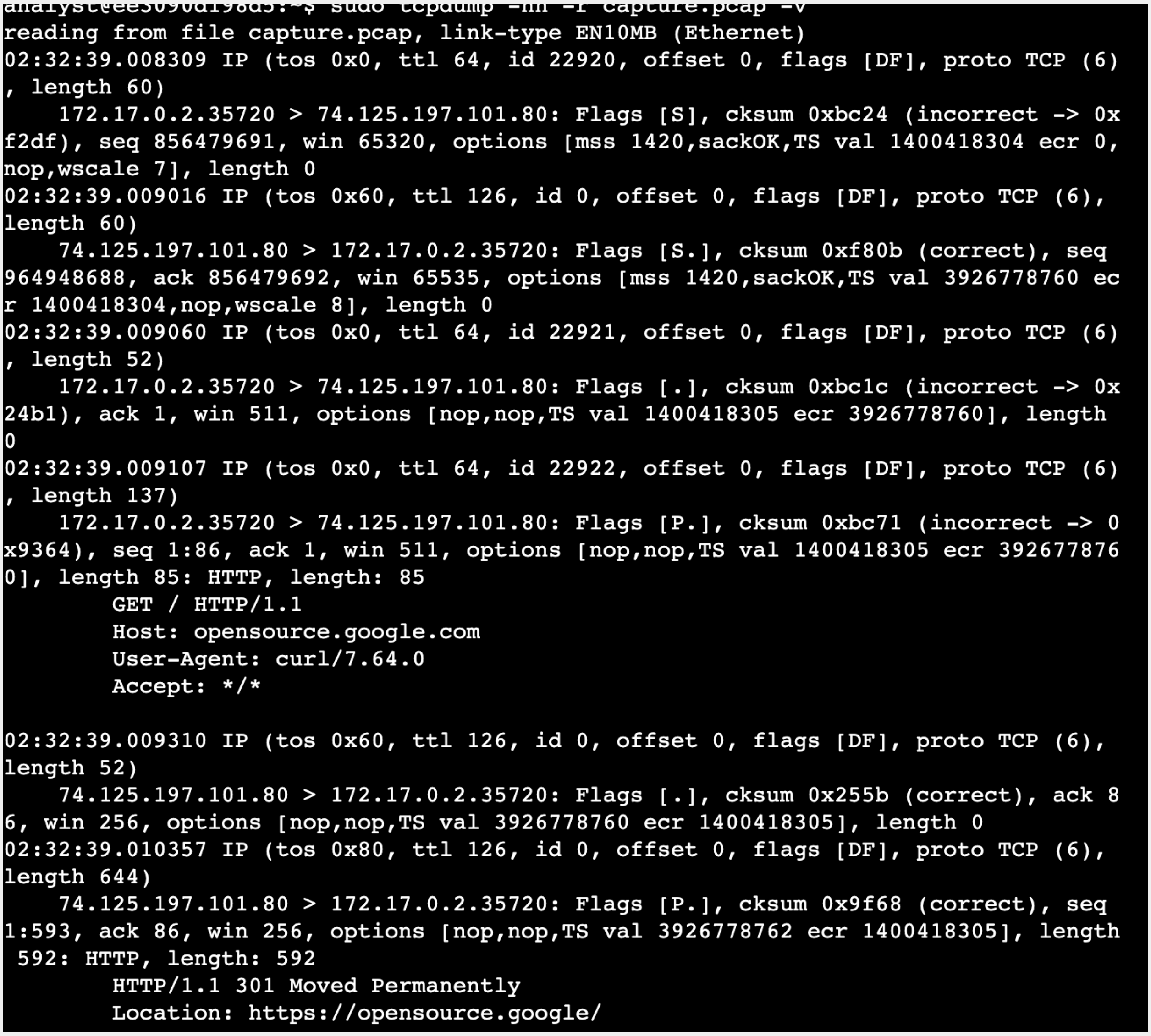
- i eth0: Capture data from the eth0 interface.
- nn: Do not attempt to resolve IP addresses or ports to names.This is best practice from a security perspective, as the lookup data may not be valid. It also prevents malicious actors from being alerted to an investigation.
- c9: Capture 9 packets of data and then exit.
- port 80: Filter only port 80 traffic. This is the default HTTP port.
- w capture.pcap: Save the captured data to the named file.
- &: This is an instruction to the Bash shell to run the command in the background.

When the curl command is used like this to open a website, it generates some HTTP (TCP port 80) traffic that can be captured.



```
analyst@ee3090d198d5:~$ sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &
[1] 12806
analyst@ee3090d198d5:~$ tcpdump: listening on eth0, link-type EN10MB (Ethernet), c
apture size 262144 bytes

analyst@ee3090d198d5:~$ curl opensource.google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://opensource.google/">here</A>.
</BODY></HTML>
analyst@ee3090d198d5:~$ 9 packets captured
12 packets received by filter
0 packets dropped by kernel

[1]+  Done                    sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap
analyst@ee3090d198d5:~$ ls -l capture.pcap
-rw-r--r-- 1 root root 1455 Mar  8 02:32 capture.pcap
analyst@ee3090d198d5:~$
```

Verify that packet data has been captured

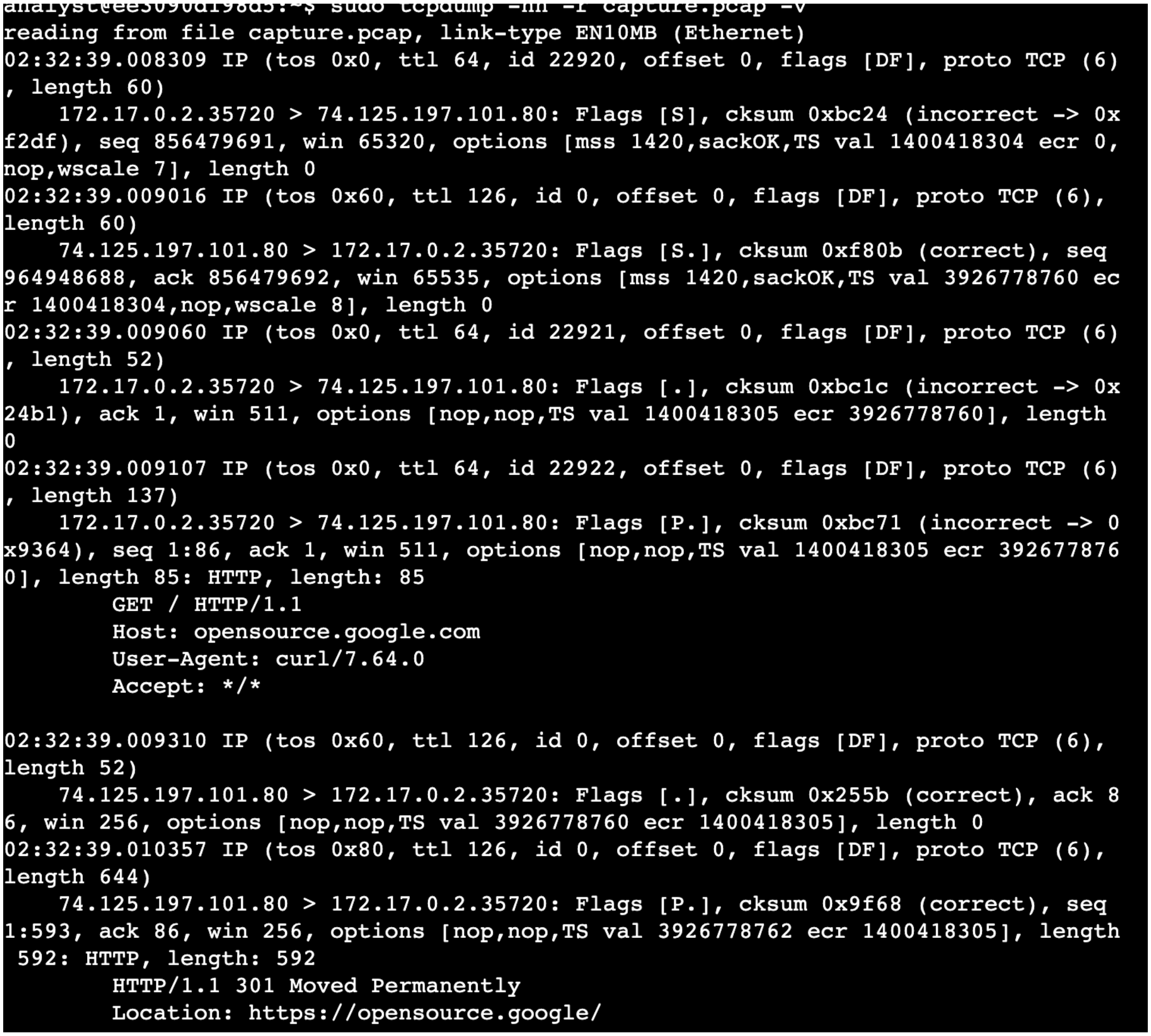


```
analyst@ee5090d198d5:~$ sudo tcpdump -nn -r capture.pcap -v
reading from file capture.pcap, link-type EN10MB (Ethernet)
02:32:39.008309 IP (tos 0x0, ttl 64, id 22920, offset 0, flags [DF], proto TCP (6)
, length 60)
    172.17.0.2.35720 > 74.125.197.101.80: Flags [S], cksum 0xbc24 (incorrect -> 0x
f2df), seq 856479691, win 65320, options [mss 1420,sackOK,TS val 1400418304 ecr 0,
nop,wscale 7], length 0
02:32:39.009016 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], proto TCP (6),
length 60)
    74.125.197.101.80 > 172.17.0.2.35720: Flags [S.], cksum 0xf80b (correct), seq
964948688, ack 856479692, win 65535, options [mss 1420,sackOK,TS val 3926778760 ec
r 1400418304,nop,wscale 8], length 0
02:32:39.009060 IP (tos 0x0, ttl 64, id 22921, offset 0, flags [DF], proto TCP (6)
, length 52)
    172.17.0.2.35720 > 74.125.197.101.80: Flags [.], cksum 0xbc1c (incorrect -> 0x
24b1), ack 1, win 511, options [nop,nop,TS val 1400418305 ecr 3926778760], length
0
02:32:39.009107 IP (tos 0x0, ttl 64, id 22922, offset 0, flags [DF], proto TCP (6)
, length 137)
    172.17.0.2.35720 > 74.125.197.101.80: Flags [P.], cksum 0xbc71 (incorrect -> 0
x9364), seq 1:86, ack 1, win 511, options [nop,nop,TS val 1400418305 ecr 392677876
0], length 85: HTTP, length: 85
        GET / HTTP/1.1
        Host: opensource.google.com
        User-Agent: curl/7.64.0
        Accept: */*

02:32:39.009310 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], proto TCP (6),
length 52)
    74.125.197.101.80 > 172.17.0.2.35720: Flags [.], cksum 0x255b (correct), ack 8
6, win 256, options [nop,nop,TS val 3926778760 ecr 1400418305], length 0
02:32:39.010357 IP (tos 0x80, ttl 126, id 0, offset 0, flags [DF], proto TCP (6),
length 644)
    74.125.197.101.80 > 172.17.0.2.35720: Flags [P.], cksum 0x9f68 (correct), seq
1:593, ack 86, win 256, options [nop,nop,TS val 3926778762 ecr 1400418305], length
 592: HTTP, length: 592
        HTTP/1.1 301 Moved Permanently
        Location: https://opensource.google/
```

Filter the captured packet data

This command will run tcpdump with the following options:
-nn: Disable port and protocol name lookup.
-r: Read capture data from the named file.
-v: Display detailed packet data.
You must specify the -nn switch again here, as you want to make sure tcpdump does not perform name lookups of either IP addresses or ports, since this can alert threat actors.

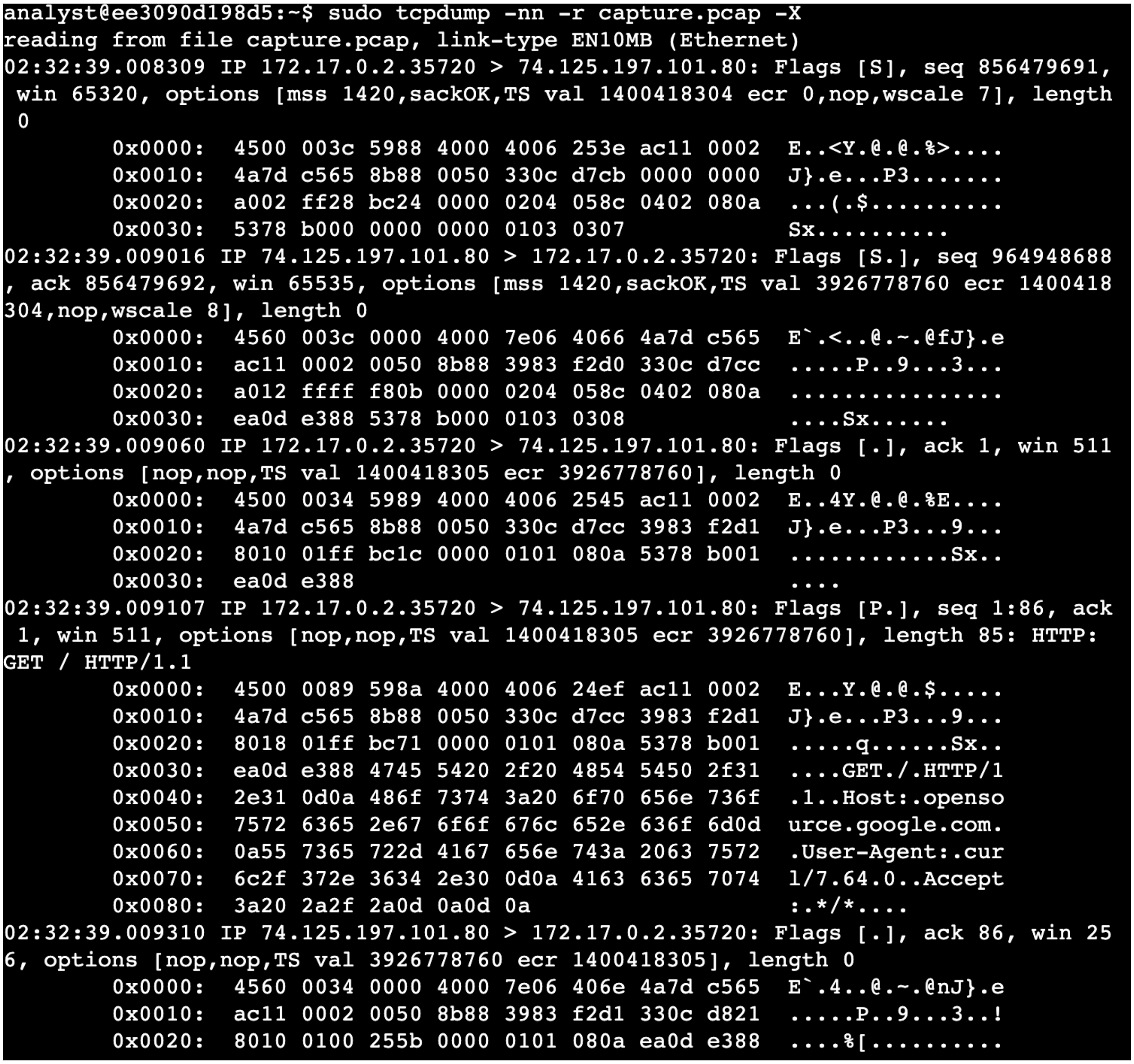
This returns output data similar to the following:



```
analyst@ee3090d198d5:~$ sudo tcpdump -nn -r capture.pcap -v
reading from file capture.pcap, link-type EN10MB (Ethernet)
02:32:39.008309 IP (tos 0x0, ttl 64, id 22920, offset 0, flags [DF], proto TCP (6)
, length 60)
    172.17.0.2.35720 > 74.125.197.101.80: Flags [S], cksum 0xbc24 (incorrect -> 0x
f2df), seq 856479691, win 65320, options [mss 1420,sackOK,TS val 1400418304 ecr 0,
nop,wscale 7], length 0
02:32:39.009016 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], proto TCP (6),
length 60)
    74.125.197.101.80 > 172.17.0.2.35720: Flags [S.], cksum 0xf80b (correct), seq
964948688, ack 856479692, win 65535, options [mss 1420,sackOK,TS val 3926778760 ec
r 1400418304,nop,wscale 8], length 0
02:32:39.009060 IP (tos 0x0, ttl 64, id 22921, offset 0, flags [DF], proto TCP (6)
, length 52)
    172.17.0.2.35720 > 74.125.197.101.80: Flags [.], cksum 0xbc1c (incorrect -> 0x
24b1), ack 1, win 511, options [nop,nop,TS val 1400418305 ecr 3926778760], length
0
02:32:39.009107 IP (tos 0x0, ttl 64, id 22922, offset 0, flags [DF], proto TCP (6)
, length 137)
    172.17.0.2.35720 > 74.125.197.101.80: Flags [P.], cksum 0xbc71 (incorrect -> 0
x9364), seq 1:86, ack 1, win 511, options [nop,nop,TS val 1400418305 ecr 392677876
0], length 85: HTTP, length: 85
        GET / HTTP/1.1
        Host: opensource.google.com
        User-Agent: curl/7.64.0
        Accept: */*

02:32:39.009310 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], proto TCP (6),
length 52)
    74.125.197.101.80 > 172.17.0.2.35720: Flags [.], cksum 0x255b (correct), ack 8
6, win 256, options [nop,nop,TS val 3926778760 ecr 1400418305], length 0
02:32:39.010357 IP (tos 0x80, ttl 126, id 0, offset 0, flags [DF], proto TCP (6),
length 644)
    74.125.197.101.80 > 172.17.0.2.35720: Flags [P.], cksum 0x9f68 (correct), seq
1:593, ack 86, win 256, options [nop,nop,TS val 3926778762 ecr 1400418305], length
 592: HTTP, length: 592
        HTTP/1.1 301 Moved Permanently
        Location: https://opensource.google/
```

The -nn switch again here, as you want to make sure tcpdump does not perform name lookups of either IP addresses or ports, since this can alert threat actors.

This command will run tcpdump with the following options:
-nn: Disable port and protocol name lookup.
-r: Read capture data from the named file.
-X: Display the hexadecimal and ASCII output format packet data. Security analysts can analyze hexadecimal and ASCII output to detect patterns or anomalies during malware analysis or forensic analysis.



```
analyst@ee3090d198d5:~$ sudo tcpdump -nn -r capture.pcap -X
reading from file capture.pcap, link-type EN10MB (Ethernet)
02:32:39.008309 IP 172.17.0.2.35720 > 74.125.197.101.80: Flags [S], seq 856479691,
 win 65320, options [mss 1420,sackOK,TS val 1400418304 ecr 0,nop,wscale 7], length
 0
        0x0000:  4500 003c 5988 4000 4006 253e ac11 0002  E..<Y.@.@.%>....
        0x0010:  4a7d c565 8b88 0050 330c d7cb 0000 0000  J}.e...P3.......
        0x0020:  a002 ff28 bc24 0000 0204 058c 0402 080a  ...(.$..........
        0x0030:  5378 b000 0000 0000 0103 0307            Sx..........
02:32:39.009016 IP 74.125.197.101.80 > 172.17.0.2.35720: Flags [S.], seq 964948688
, ack 856479692, win 65535, options [mss 1420,sackOK,TS val 3926778760 ecr 1400418
304,nop,wscale 8], length 0
        0x0000:  4560 003c 0000 4000 7e06 4066 4a7d c565  E`.<..@.~.@fJ}.e
        0x0010:  ac11 0002 0050 8b88 3983 f2d0 330c d7cc  .....P..9...3...
        0x0020:  a012 ffff f80b 0000 0204 058c 0402 080a  ................
        0x0030:  ea0d e388 5378 b000 0103 0308            ....Sx......
02:32:39.009060 IP 172.17.0.2.35720 > 74.125.197.101.80: Flags [.], ack 1, win 511
, options [nop,nop,TS val 1400418305 ecr 3926778760], length 0
        0x0000:  4500 0034 5989 4000 4006 2545 ac11 0002  E..4Y.@.@.%E....
        0x0010:  4a7d c565 8b88 0050 330c d7cc 3983 f2d1  J}.e...P3...9...
        0x0020:  8010 01ff bc1c 0000 0101 080a 5378 b001  ............Sx..
        0x0030:  ea0d e388                                ....
02:32:39.009107 IP 172.17.0.2.35720 > 74.125.197.101.80: Flags [P.], seq 1:86, ack
 1, win 511, options [nop,nop,TS val 1400418305 ecr 3926778760], length 85: HTTP:
GET / HTTP/1.1
        0x0000:  4500 0089 598a 4000 4006 24ef ac11 0002  E...Y.@.@.$.....
        0x0010:  4a7d c565 8b88 0050 330c d7cc 3983 f2d1  J}.e...P3...9...
        0x0020:  8018 01ff bc71 0000 0101 080a 5378 b001  .....q......Sx..
        0x0030:  ea0d e388 4745 5420 2f20 4854 5450 2f31  ....GET./.HTTP/1
        0x0040:  2e31 0d0a 486f 7374 3a20 6f70 656e 736f  .1..Host:.openso
        0x0050:  7572 6365 2e67 6f6f 676c 652e 636f 6d0d  urce.google.com.
        0x0060:  0a55 7365 722d 4167 656e 743a 2063 7572  .User-Agent:.cur
        0x0070:  6c2f 372e 3634 2e30 0d0a 4163 6365 7074  l/7.64.0..Accept
        0x0080:  3a20 2a2f 2a0d 0a0d 0a                   :.*/*....
02:32:39.009310 IP 74.125.197.101.80 > 172.17.0.2.35720: Flags [.], ack 86, win 25
6, options [nop,nop,TS val 3926778760 ecr 1400418305], length 0
        0x0000:  4560 0034 0000 4000 7e06 406e 4a7d c565  E`.4..@.~.@nJ}.e
        0x0010:  ac11 0002 0050 8b88 3983 f2d1 330c d821  .....P..9...3..!
        0x0020:  8010 0100 255b 0000 0101 080a ea0d e388  ....%[..........
```