TCPdump: Packet Capture

Scenario:

You’re a network analyst who needs to use tcpdump to capture and analyze live network traffic from a Linux virtual machine.

The lab starts with your user account, called analyst, already logged in to a Linux terminal.

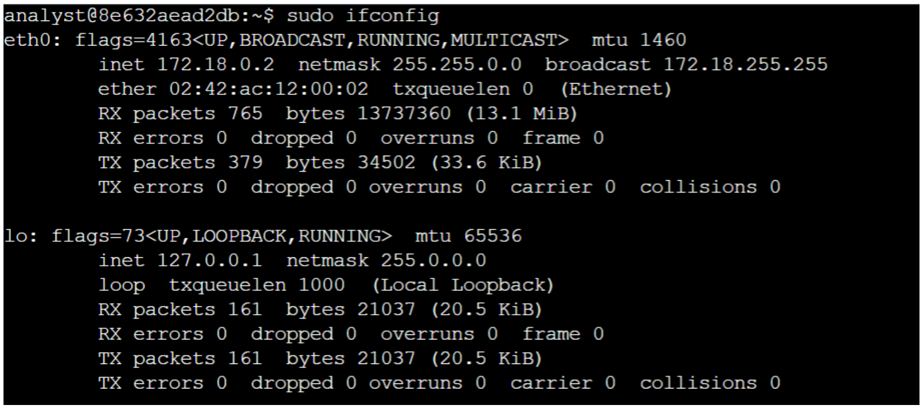
Your Linux user's home directory contains a sample packet capture file that you will use at the end of the lab to answer a few questions about the network traffic that it contains.

Here’s how you’ll do this: First, you’ll identify network interfaces to capture network packet data. Second, you’ll use tcpdump to filter live network traffic. Third, you’ll capture network traffic using tcpdump. Finally, you’ll filter the captured packet data.

Solutions:

1. **Use ifconfig to identify the interfaces that are available:**

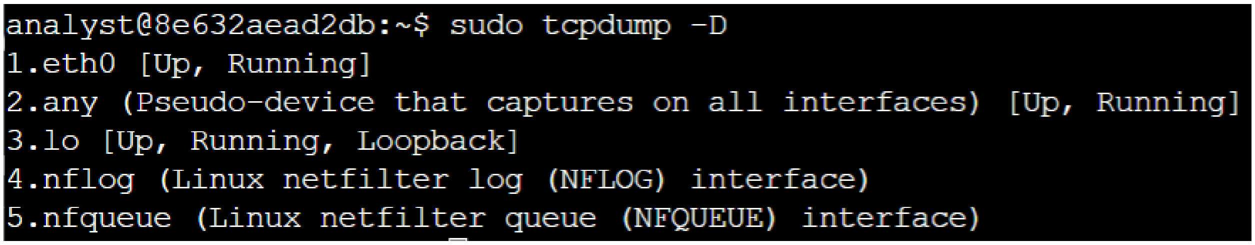
sudo ifconfig



```
analyst@8e632aead2db:~$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1460
        inet 172.18.0.2  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:ac:12:00:02  txqueuelen 0  (Ethernet)
        RX packets 765  bytes 13737360 (13.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 379  bytes 34502 (33.6 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 161  bytes 21037 (20.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 161  bytes 21037 (20.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. **Use tcpdump to identify the interface options available for packet capture:**

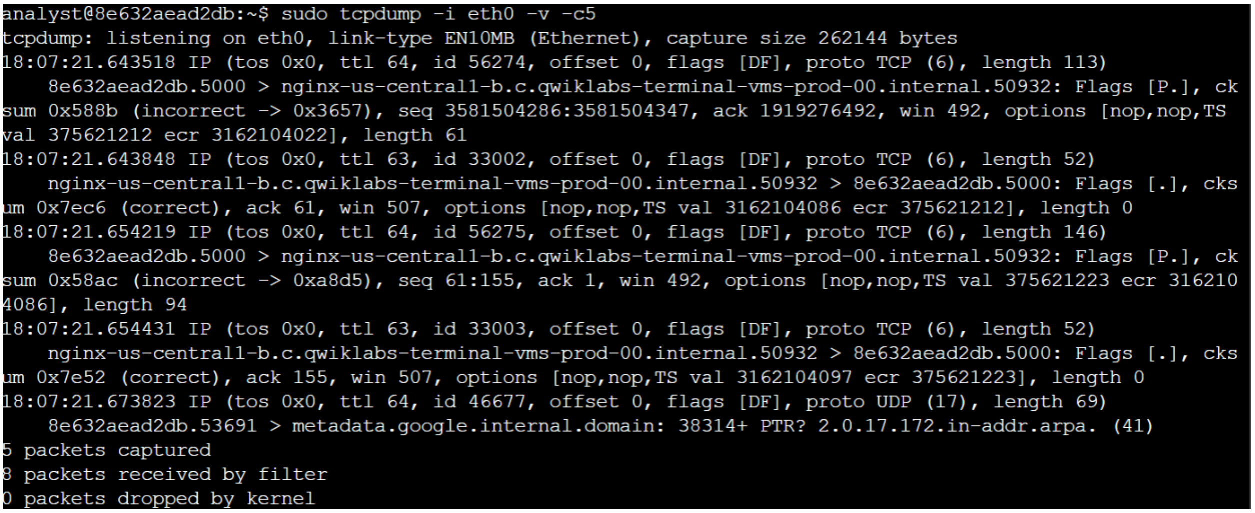
sudo tcpdump -D



```
analyst@8e632aead2db:~$ sudo tcpdump -D
1.eth0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
```

3. **Inspect the network traffic of a network interface with tcpdump.**
   Filter live network packet data from the eth0 interface with tcpdump:

sudo tcpdump -i eth0 -v -c5



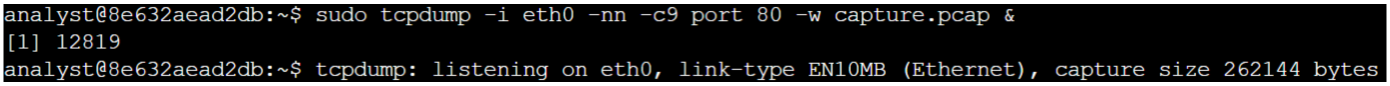
```
analyst@8e632aead2db:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:07:21.643518 IP (tos 0x0, ttl 64, id 56274, offset 0, flags [DF], proto TCP (6), length 113)
    8e632aead2db.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.50932: Flags [P.], ck
sum 0x588b (incorrect -> 0x3657), seq 3581504286:3581504347, ack 1919276492, win 492, options [nop,nop,TS
val 375621212 ecr 3162104022], length 61
18:07:21.643848 IP (tos 0x0, ttl 63, id 33002, offset 0, flags [DF], proto TCP (6), length 52)
    nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.50932 > 8e632aead2db.5000: Flags [.], cks
um 0x7ec6 (correct), ack 61, win 507, options [nop,nop,TS val 3162104086 ecr 375621212], length 0
18:07:21.654219 IP (tos 0x0, ttl 64, id 56275, offset 0, flags [DF], proto TCP (6), length 146)
    8e632aead2db.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.50932: Flags [P.], ck
sum 0x58ac (incorrect -> 0xa8d5), seq 61:155, ack 1, win 492, options [nop,nop,TS val 375621223 ecr 316210
4086], length 94
18:07:21.654431 IP (tos 0x0, ttl 63, id 33003, offset 0, flags [DF], proto TCP (6), length 52)
    nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.50932 > 8e632aead2db.5000: Flags [.], cks
um 0x7e52 (correct), ack 155, win 507, options [nop,nop,TS val 3162104097 ecr 375621223], length 0
18:07:21.673823 IP (tos 0x0, ttl 64, id 46677, offset 0, flags [DF], proto UDP (17), length 69)
    8e632aead2db.53691 > metadata.google.internal.domain: 38314+ PTR? 2.0.17.172.in-addr.arpa. (41)
5 packets captured
8 packets received by filter
0 packets dropped by kernel
```

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

4. **Capture Network Traffic**
   Capture packet data into a file called capture.pcap:

sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &

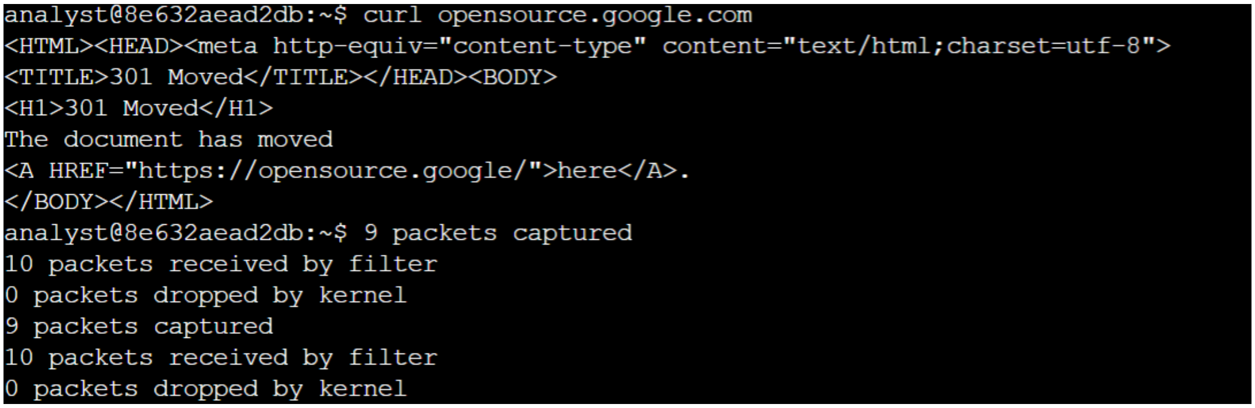
- **-i eth0: Capture data from the eth0 interface.**
- **-nn: Do not attempt to resolve IP addresses or ports to names.This is best practice from a security perspective, as the lookup data may not be valid. It also prevents malicious actors from being alerted to an investigation.**
- **-c9: Capture 9 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.**



```
analyst@8e632aead2db:~$ sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &
[1] 12819
analyst@8e632aead2db:~$ tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

5. **Use curl to generate some HTTP (port 80) traffic:**

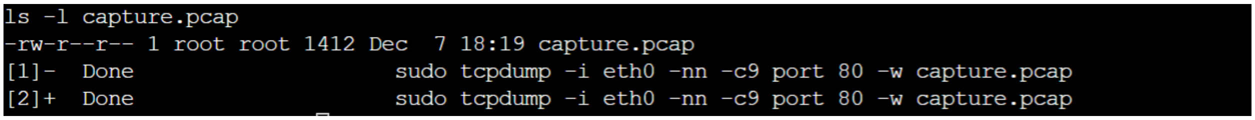
curl opensource.google.com



```
analyst@8e632aead2db:~$ 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@8e632aead2db:~$ 9 packets captured
10 packets received by filter
0 packets dropped by kernel
9 packets captured
10 packets received by filter
0 packets dropped by kernel
```

6. **Verify that packet data has been captured:**

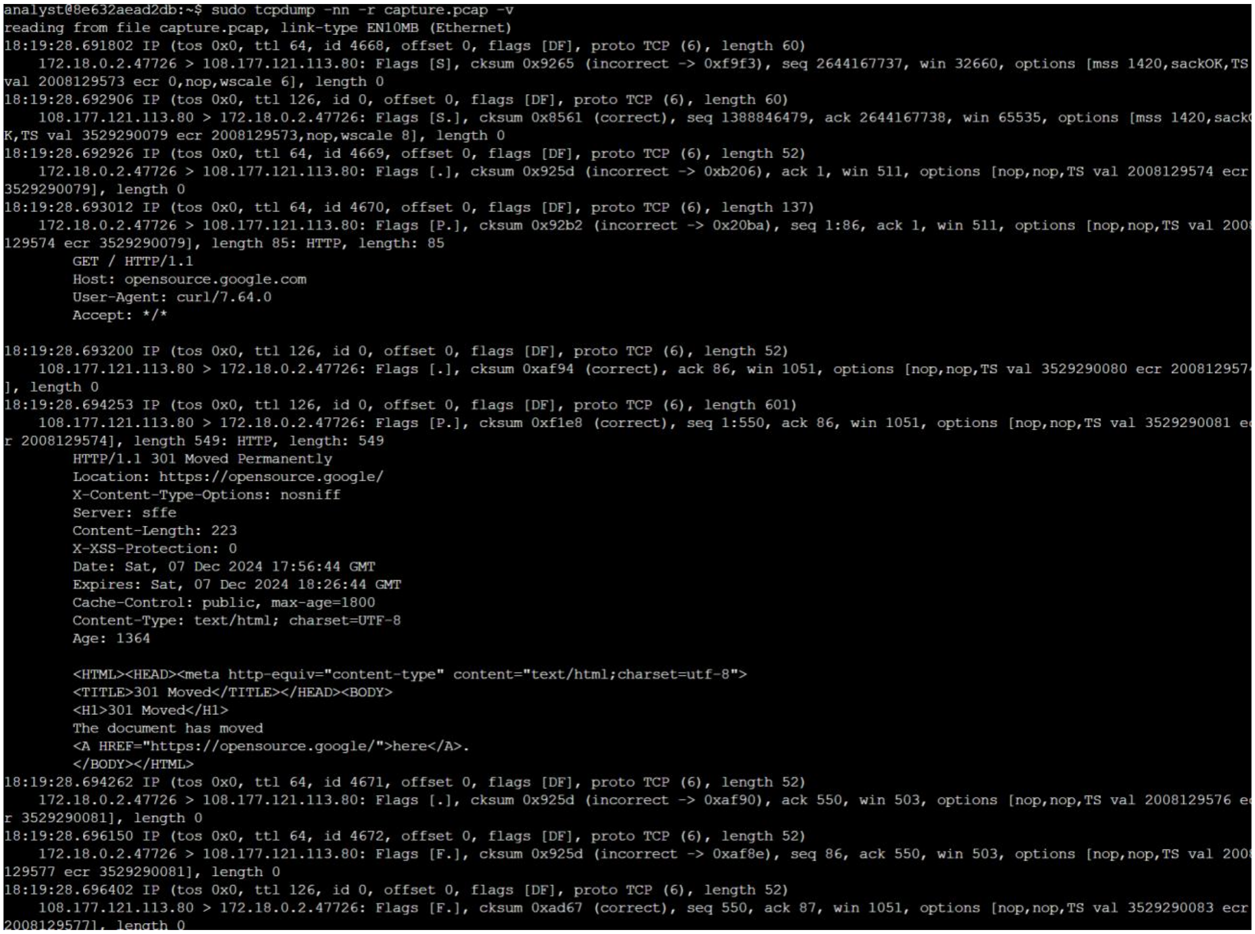
ls -l capture.pcap



```
ls -l capture.pcap
-rw-r--r-- 1 root root 1412 Dec  7 18:19 capture.pcap
[1]-  Done                    sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap
[2]+  Done                    sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap
```

7. **In this task, use tcpdump to filter data from the packet capture file you saved previously.**
   Use the tcpdump command to filter the packet header data from the capture.pcap capture file:

sudo tcpdump -nn -r capture.pcap -v



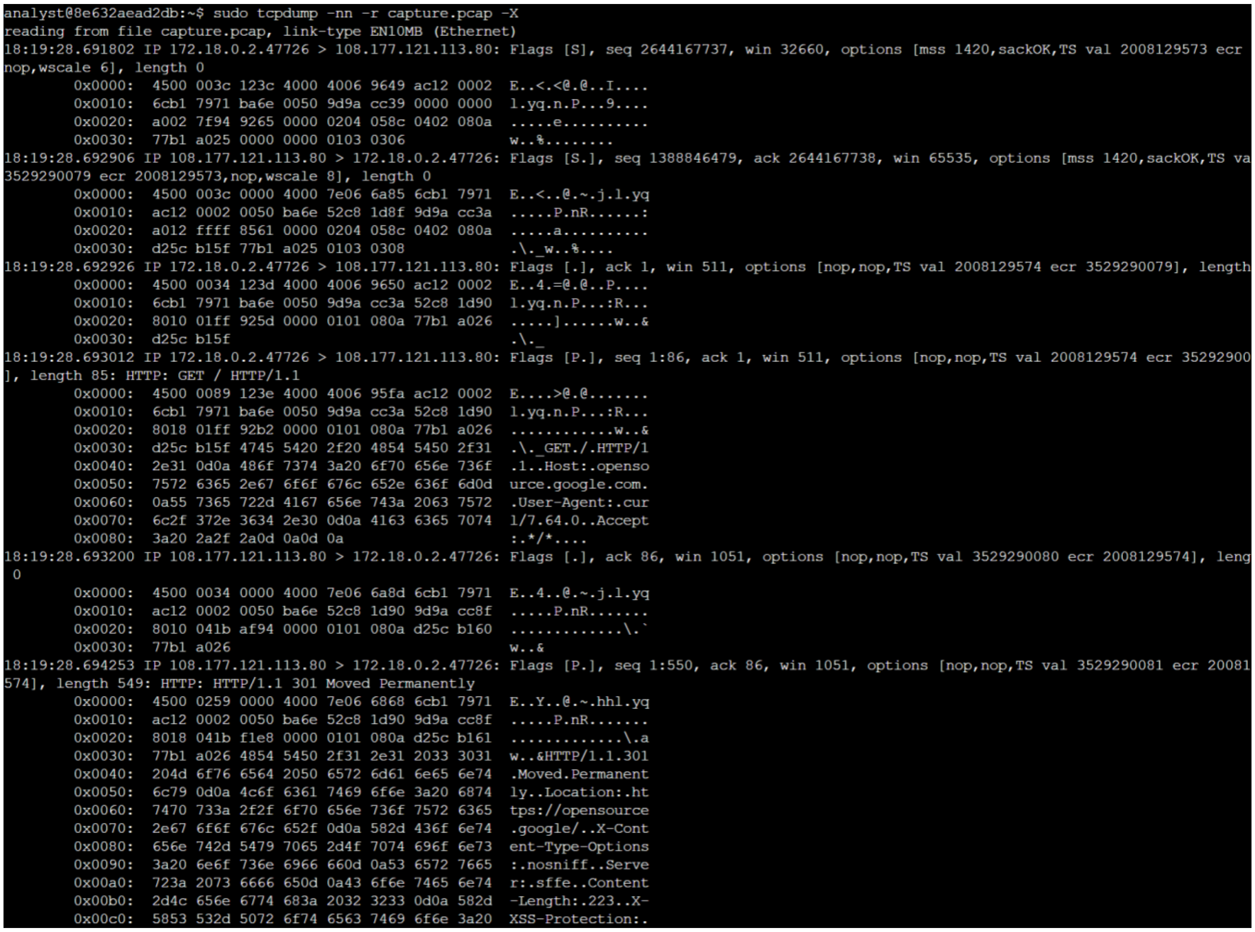
```
analyst@8e632aead2db:~$ sudo tcpdump -nn -r capture.pcap -v
reading from file capture.pcap, link-type EN10MB (Ethernet)
18:19:28.691802 IP (tos 0x0, ttl 64, id 4668, offset 0, flags [DF], proto TCP (6), length 60)
    172.18.0.2.47726 > 108.177.121.113.80: Flags [S], cksum 0x9265 (incorrect -> 0xf9f3), seq 2644167737, win 32660, options [mss 1420,sackOK,TS
val 2008129573 ecr 0,nop,wscale 6], length 0
18:19:28.692906 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    108.177.121.113.80 > 172.18.0.2.47726: Flags [S.], cksum 0x8561 (correct), seq 1388846479, ack 2644167738, win 65535, options [mss 1420,sackO
K,TS val 3529290079 ecr 2008129573,nop,wscale 8], length 0
18:19:28.692926 IP (tos 0x0, ttl 64, id 4669, offset 0, flags [DF], proto TCP (6), length 52)
    172.18.0.2.47726 > 108.177.121.113.80: Flags [.], cksum 0x925d (incorrect -> 0xb206), ack 1, win 511, options [nop,nop,TS val 2008129574 ecr
3529290079], length 0
18:19:28.693012 IP (tos 0x0, ttl 64, id 4670, offset 0, flags [DF], proto TCP (6), length 137)
    172.18.0.2.47726 > 108.177.121.113.80: Flags [P.], cksum 0x92b2 (incorrect -> 0x20ba), seq 1:86, ack 1, win 511, options [nop,nop,TS val 2008
129574 ecr 3529290079], length 85: HTTP, length: 85
        GET / HTTP/1.1
        Host: opensource.google.com
        User-Agent: curl/7.64.0
        Accept: */*

18:19:28.693200 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    108.177.121.113.80 > 172.18.0.2.47726: Flags [.], cksum 0xaf94 (correct), ack 86, win 1051, options [nop,nop,TS val 3529290080 ecr 2008129574
], length 0
18:19:28.694253 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), length 601)
    108.177.121.113.80 > 172.18.0.2.47726: Flags [P.], cksum 0xf1e8 (correct), seq 1:550, ack 86, win 1051, options [nop,nop,TS val 3529290081 ec
r 2008129574], length 549: HTTP, length: 549
        HTTP/1.1 301 Moved Permanently
        Location: https://opensource.google/
        X-Content-Type-Options: nosniff
        Server: sffe
        Content-Length: 223
        X-XSS-Protection: 0
        Date: Sat, 07 Dec 2024 17:56:44 GMT
        Expires: Sat, 07 Dec 2024 18:26:44 GMT
        Cache-Control: public, max-age=1800
        Content-Type: text/html; charset=UTF-8
        Age: 1364

        <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>
18:19:28.694262 IP (tos 0x0, ttl 64, id 4671, offset 0, flags [DF], proto TCP (6), length 52)
    172.18.0.2.47726 > 108.177.121.113.80: Flags [.], cksum 0x925d (incorrect -> 0xaf90), ack 550, win 503, options [nop,nop,TS val 2008129576 ec
r 3529290081], length 0
18:19:28.696150 IP (tos 0x0, ttl 64, id 4672, offset 0, flags [DF], proto TCP (6), length 52)
    172.18.0.2.47726 > 108.177.121.113.80: Flags [F.], cksum 0x925d (incorrect -> 0xaf8e), seq 86, ack 550, win 503, options [nop,nop,TS val 2008
129577 ecr 3529290081], length 0
18:19:28.696402 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    108.177.121.113.80 > 172.18.0.2.47726: Flags [F.], cksum 0xad67 (correct), seq 550, ack 87, win 1051, options [nop,nop,TS val 3529290083 ecr
2008129577], length 0
```

- **-nn: Disable port and protocol name lookup.**
- **-r: Read capture data from the named file.**
- **-v: Display detailed packet data.**

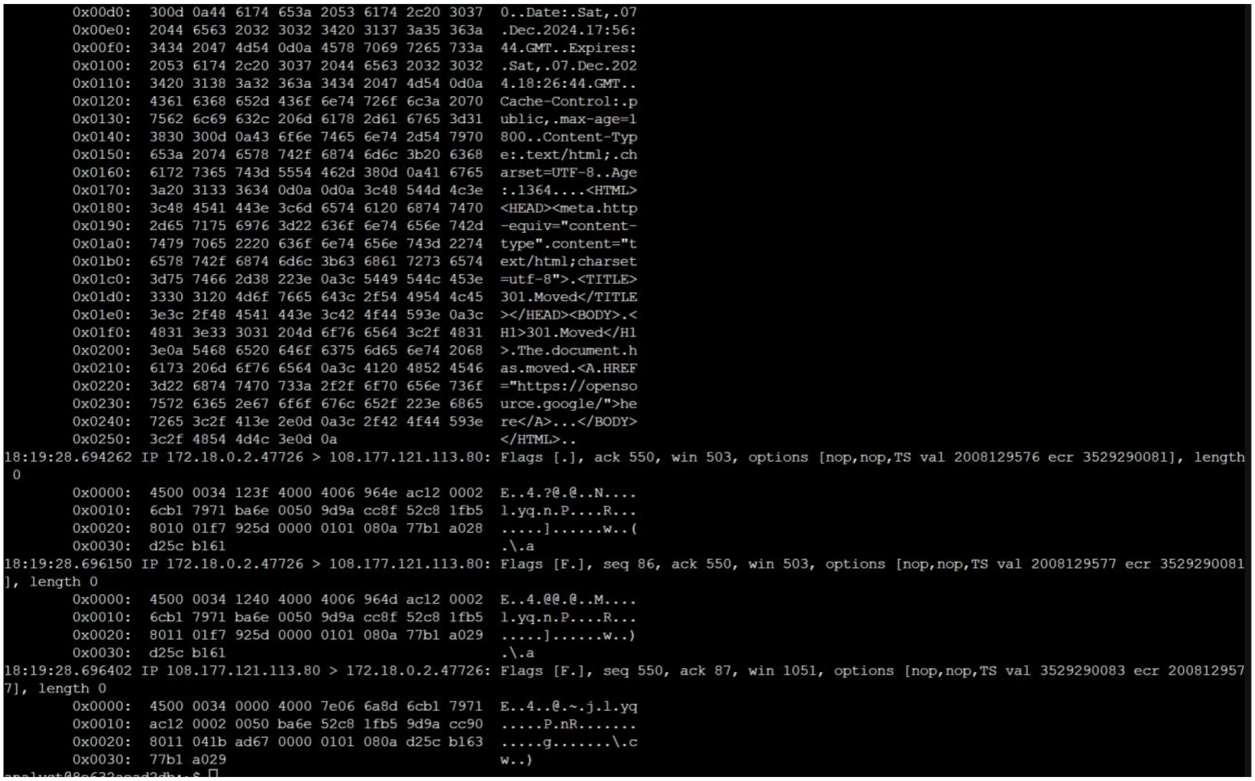
8. **Use the tcpdump command to filter the extended packet data from the capture.pcap capture file:**

sudo tcpdump -nn -r capture.pcap -X

- **-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@8e632aead2db:~$ sudo tcpdump -nn -r capture.pcap -X
reading from file capture.pcap, link-type EN10MB (Ethernet)
18:19:28.691802 IP 172.18.0.2.47726 > 108.177.121.113.80: Flags [S], seq 2644167737, win 32660, options [mss 1420,sackOK,TS val 2008129573 ecr
nop,wscale 6], length 0
        0x0000:  4500 003c 123c 4000 4006 9649 ac12 0002  E..<.<@.@..I....
        0x0010:  6cb1 7971 ba6e 0050 9d9a cc39 0000 0000  l.yq.n.P...9....
        0x0020:  a002 7f94 9265 0000 0204 058c 0402 080a  .....e..........
        0x0030:  77b1 a025 0000 0000 0103 0306            w..%........
18:19:28.692906 IP 108.177.121.113.80 > 172.18.0.2.47726: Flags [S.], seq 1388846479, ack 2644167738, win 65535, options [mss 1420,sackOK,TS va
3529290079 ecr 2008129573,nop,wscale 8], length 0
        0x0000:  4500 003c 0000 4000 7e06 6a85 6cb1 7971  E..<..@.~.j.l.yq
        0x0010:  ac12 0002 0050 ba6e 52c8 1d8f 9d9a cc3a  .....P.nR......:
        0x0020:  a012 ffff 8561 0000 0204 058c 0402 080a  .....a..........
        0x0030:  d25c b15f 77b1 a025 0103 0308            .\._w..%....
18:19:28.692926 IP 172.18.0.2.47726 > 108.177.121.113.80: Flags [.], ack 1, win 511, options [nop,nop,TS val 2008129574 ecr 3529290079], length
        0x0000:  4500 0034 123d 4000 4006 9650 ac12 0002  E..4.=@.@..P....
        0x0010:  6cb1 7971 ba6e 0050 9d9a cc3a 52c8 1d90  l.yq.n.P...:R...
        0x0020:  8010 01ff 925d 0000 0101 080a 77b1 a026  .....]......w..&
        0x0030:  d25c b15f                                .\._
18:19:28.693012 IP 172.18.0.2.47726 > 108.177.121.113.80: Flags [P.], seq 1:86, ack 1, win 511, options [nop,nop,TS val 2008129574 ecr 35292900
], length 85: HTTP: GET / HTTP/1.1
        0x0000:  4500 0089 123e 4000 4006 95fa ac12 0002  E....>@.@.......
        0x0010:  6cb1 7971 ba6e 0050 9d9a cc3a 52c8 1d90  l.yq.n.P...:R...
        0x0020:  8018 01ff 92b2 0000 0101 080a 77b1 a026  ............w..&
        0x0030:  d25c b15f 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                   :.*/*....
18:19:28.693200 IP 108.177.121.113.80 > 172.18.0.2.47726: Flags [.], ack 86, win 1051, options [nop,nop,TS val 3529290080 ecr 2008129574], leng
 0
        0x0000:  4500 0034 0000 4000 7e06 6a8d 6cb1 7971  E..4..@.~.j.l.yq
        0x0010:  ac12 0002 0050 ba6e 52c8 1d90 9d9a cc8f  .....P.nR.......
        0x0020:  8010 041b af94 0000 0101 080a d25c b160  .............\.`
        0x0030:  77b1 a026                                w..&
18:19:28.694253 IP 108.177.121.113.80 > 172.18.0.2.47726: Flags [P.], seq 1:550, ack 86, win 1051, options [nop,nop,TS val 3529290081 ecr 20081
574], length 549: HTTP: HTTP/1.1 301 Moved Permanently
        0x0000:  4500 0259 0000 4000 7e06 6868 6cb1 7971  E..Y..@.~.hhl.yq
        0x0010:  ac12 0002 0050 ba6e 52c8 1d90 9d9a cc8f  .....P.nR.......
        0x0020:  8018 041b f1e8 0000 0101 080a d25c b161  .............\.a
        0x0030:  77b1 a026 4854 5450 2f31 2e31 2033 3031  w..&HTTP/1.1.301
        0x0040:  204d 6f76 6564 2050 6572 6d61 6e65 6e74  .Moved.Permanent
        0x0050:  6c79 0d0a 4c6f 6361 7469 6f6e 3a20 6874  ly..Location:.ht
        0x0060:  7470 733a 2f2f 6f70 656e 736f 7572 6365  tps://opensource
        0x0070:  2e67 6f6f 676c 652f 0d0a 582d 436f 6e74  .google/..X-Cont
        0x0080:  656e 742d 5479 7065 2d4f 7074 696f 6e73  ent-Type-Options
        0x0090:  3a20 6e6f 736e 6966 660d 0a53 6572 7665  :.nosniff..Serve
        0x00a0:  723a 2073 6666 650d 0a43 6f6e 7465 6e74  r:.sffe..Content
        0x00b0:  2d4c 656e 6774 683a 2032 3233 0d0a 582d  -Length:.223..X-
        0x00c0:  5853 532d 5072 6f74 6563 7469 6f6e 3a20  XSS-Protection:.
```



```
        0x00d0:  300d 0a44 6174 653a 2053 6174 2c20 3037  0..Date:.Sat,.07
        0x00e0:  2044 6563 2032 3032 3420 3137 3a35 363a  .Dec.2024.17:56:
        0x00f0:  3434 2047 4d54 0d0a 4578 7069 7265 733a  44.GMT..Expires:
        0x0100:  2053 6174 2c20 3037 2044 6563 2032 3032  .Sat,.07.Dec.202
        0x0110:  3420 3138 3a32 363a 3434 2047 4d54 0d0a  4.18:26:44.GMT..
        0x0120:  4361 6368 652d 436f 6e74 726f 6c3a 2070  Cache-Control:.p
        0x0130:  7562 6c69 632c 206d 6178 2d61 6765 3d31  ublic,.max-age=1
        0x0140:  3830 300d 0a43 6f6e 7465 6e74 2d54 7970  800..Content-Typ
        0x0150:  653a 2074 6578 742f 6874 6d6c 3b20 6368  e:.text/html;.ch
        0x0160:  6172 7365 743d 5554 462d 380d 0a41 6765  arset=UTF-8..Age
        0x0170:  3a20 3133 3634 0d0a 0d0a 3c48 544d 4c3e  :.1364....<HTML>
        0x0180:  3c48 4541 443e 3c6d 6574 6120 6874 7470  <HEAD><meta.http
        0x0190:  2d65 7175 6976 3d22 636f 6e74 656e 742d  -equiv="content-
        0x01a0:  7479 7065 2220 636f 6e74 656e 743d 2274  type".content="t
        0x01b0:  6578 742f 6874 6d6c 3b63 6861 7273 6574  ext/html;charset
        0x01c0:  3d75 7466 2d38 223e 0a3c 5449 544c 453e  =utf-8">.<TITLE>
        0x01d0:  3330 3120 4d6f 7665 643c 2f54 4954 4c45  301.Moved</TITLE
        0x01e0:  3e3c 2f48 4541 443e 3c42 4f44 593e 0a3c  ></HEAD><BODY>.<
        0x01f0:  4831 3e33 3031 204d 6f76 6564 3c2f 4831  H1>301.Moved</H1
        0x0200:  3e0a 5468 6520 646f 6375 6d65 6e74 2068  >.The.document.h
        0x0210:  6173 206d 6f76 6564 0a3c 4120 4852 4546  as.moved.<A.HREF
        0x0220:  3d22 6874 7470 733a 2f2f 6f70 656e 736f  ="https://openso
        0x0230:  7572 6365 2e67 6f6f 676c 652f 223e 6865  urce.google/">he
        0x0240:  7265 3c2f 413e 2e0d 0a3c 2f42 4f44 593e  re</A>...</BODY>
        0x0250:  3c2f 4854 4d4c 3e0d 0a                   </HTML>..
18:19:28.694262 IP 172.18.0.2.47726 > 108.177.121.113.80: Flags [.], ack 550, win 503, options [nop,nop,TS val 2008129576 ecr 3529290081], length
 0
        0x0000:  4500 0034 123f 4000 4006 964e ac12 0002  E..4.?@.@..N....
        0x0010:  6cb1 7971 ba6e 0050 9d9a cc8f 52c8 1fb5  l.yq.n.P....R...
        0x0020:  8010 01f7 925d 0000 0101 080a 77b1 a028  .....]......w..(
        0x0030:  d25c b161                                .\.a
18:19:28.696150 IP 172.18.0.2.47726 > 108.177.121.113.80: Flags [F.], seq 86, ack 550, win 503, options [nop,nop,TS val 2008129577 ecr 3529290081
], length 0
        0x0000:  4500 0034 1240 4000 4006 964d ac12 0002  E..4.@@.@..M....
        0x0010:  6cb1 7971 ba6e 0050 9d9a cc8f 52c8 1fb5  l.yq.n.P....R...
        0x0020:  8011 01f7 925d 0000 0101 080a 77b1 a029  .....]......w..)
        0x0030:  d25c b161                                .\.a
18:19:28.696402 IP 108.177.121.113.80 > 172.18.0.2.47726: Flags [F.], seq 550, ack 87, win 1051, options [nop,nop,TS val 3529290083 ecr 200812957
7], length 0
        0x0000:  4500 0034 0000 4000 7e06 6a8d 6cb1 7971  E..4..@.~.j.l.yq
        0x0010:  ac12 0002 0050 ba6e 52c8 1fb5 9d9a cc90  .....P.nR.......
        0x0020:  8011 041b ad67 0000 0101 080a d25c b163  .....g.......\.c
        0x0030:  77b1 a029                                w..)
analyst@8e632aead2db:~$ 
```