Tcpdump - Capture your first packet

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.

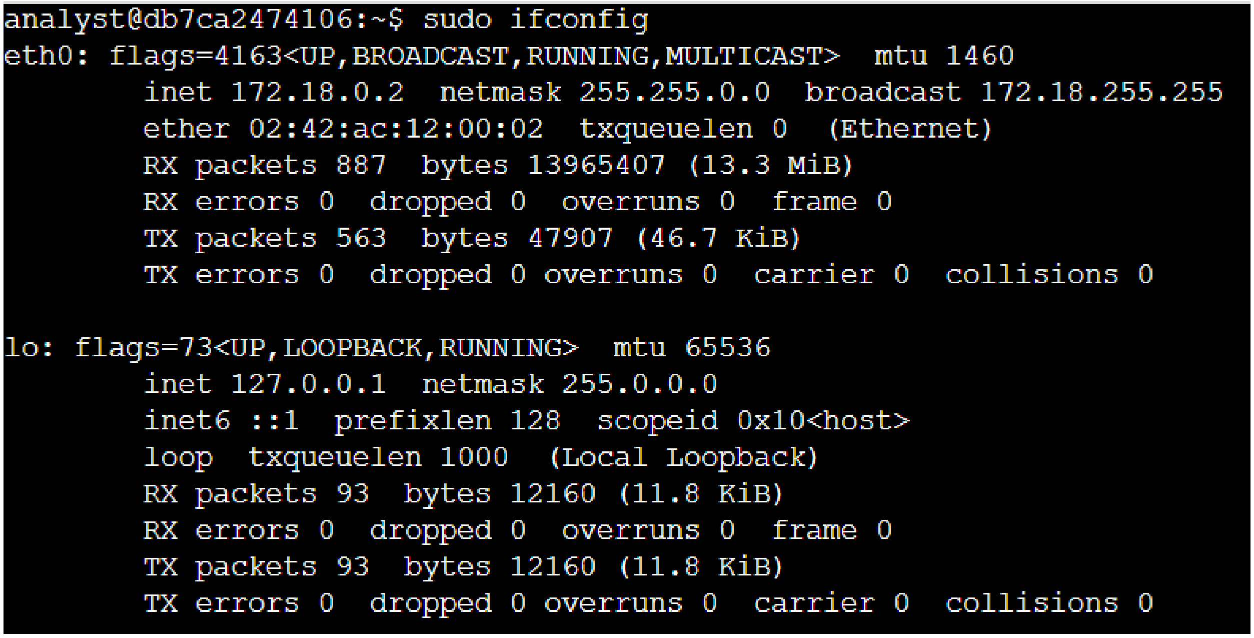
Here’s how you’ll do this: First, you’ll identify network interfaces to capture network packet data. Second, you’ll use tcpdump to filter live network traffic. Third, you’ll capture network traffic using tcpdump. Finally, you’ll filter the captured packet data.

Task 1. Identify network interfaces

In this task, you must identify the network interfaces that can be used to capture network packet data.

Use ifconfig to identify the interfaces that are available:

sudo ifconfig

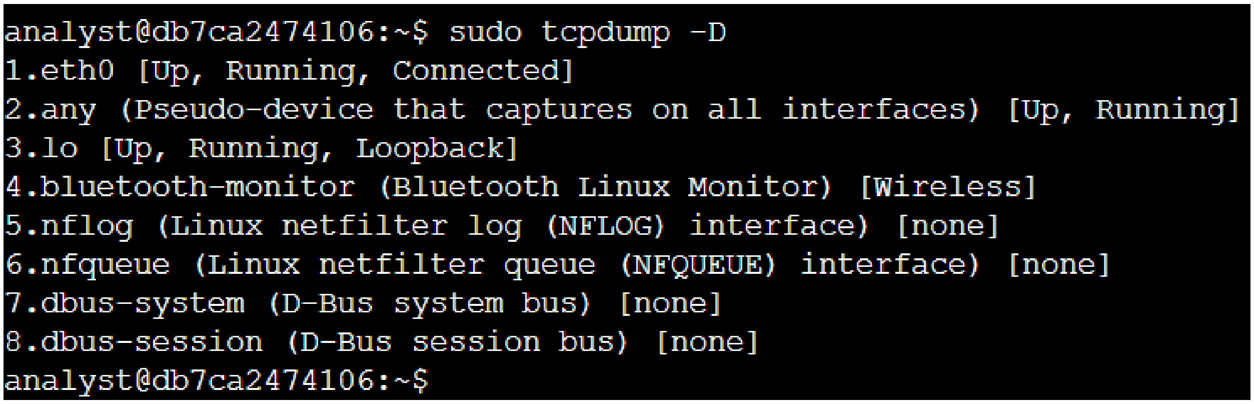


```
analyst@db7ca2474106:~$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1460
        inet 172.18.0.2  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:ac:12:00:02  txqueuelen 0  (Ethernet)
        RX packets 887  bytes 13965407 (13.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 563  bytes 47907 (46.7 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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 93  bytes 12160 (11.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 93  bytes 12160 (11.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

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

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

sudo tcpdump -D



```
analyst@db7ca2474106:~$ sudo tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
analyst@db7ca2474106:~$
```

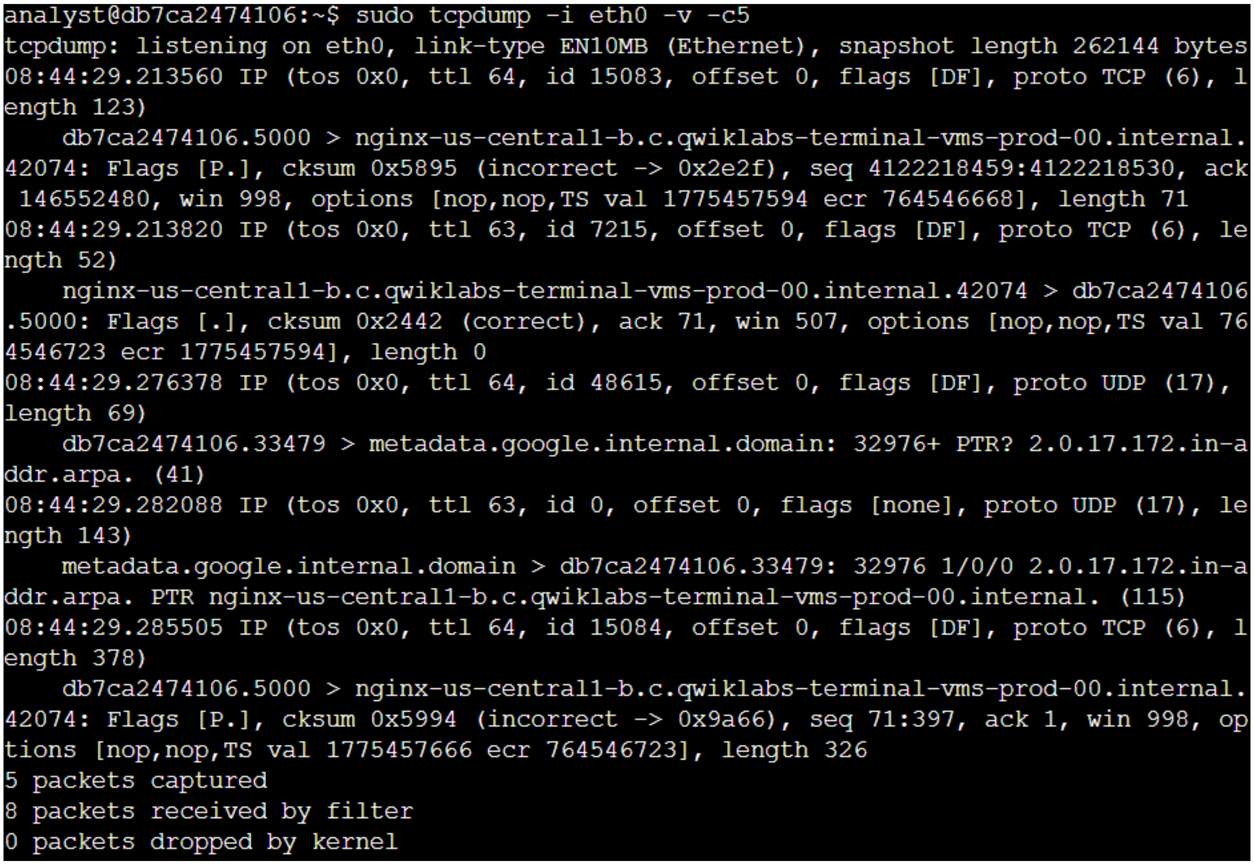
This command will also allow you to identify which network interfaces are available. This may be useful on systems that do not include the ifconfig command.

Task 2. Inspect the network traffic of a network interface with tcpdump

In this task, you must use tcpdump to filter live network packet traffic on an interface.

Filter live network packet data from the eth0 interface with tcpdump:

sudo tcpdump -i eth0 -v -c5



```
analyst@db7ca2474106:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:44:29.213560 IP (tos 0x0, ttl 64, id 15083, offset 0, flags [DF], proto TCP (6), l
ength 123)
    db7ca2474106.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.
42074: Flags [P.], cksum 0x5895 (incorrect -> 0x2e2f), seq 4122218459:4122218530, ack
 146552480, win 998, options [nop,nop,TS val 1775457594 ecr 764546668], length 71
08:44:29.213820 IP (tos 0x0, ttl 63, id 7215, offset 0, flags [DF], proto TCP (6), le
ngth 52)
    nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.42074 > db7ca2474106
.5000: Flags [.], cksum 0x2442 (correct), ack 71, win 507, options [nop,nop,TS val 76
4546723 ecr 1775457594], length 0
08:44:29.276378 IP (tos 0x0, ttl 64, id 48615, offset 0, flags [DF], proto UDP (17),
length 69)
    db7ca2474106.33479 > metadata.google.internal.domain: 32976+ PTR? 2.0.17.172.in-a
ddr.arpa. (41)
08:44:29.282088 IP (tos 0x0, ttl 63, id 0, offset 0, flags [none], proto UDP (17), le
ngth 143)
    metadata.google.internal.domain > db7ca2474106.33479: 32976 1/0/0 2.0.17.172.in-a
ddr.arpa. PTR nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal. (115)
08:44:29.285505 IP (tos 0x0, ttl 64, id 15084, offset 0, flags [DF], proto TCP (6), l
ength 378)
    db7ca2474106.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.
42074: Flags [P.], cksum 0x5994 (incorrect -> 0x9a66), seq 71:397, ack 1, win 998, op
tions [nop,nop,TS val 1775457666 ecr 764546723], length 326
5 packets captured
8 packets received by filter
0 packets dropped by kernel
```

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.

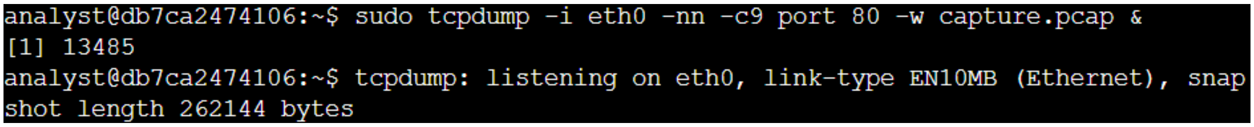
Task 3. Capture network traffic with tcpdump

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:

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

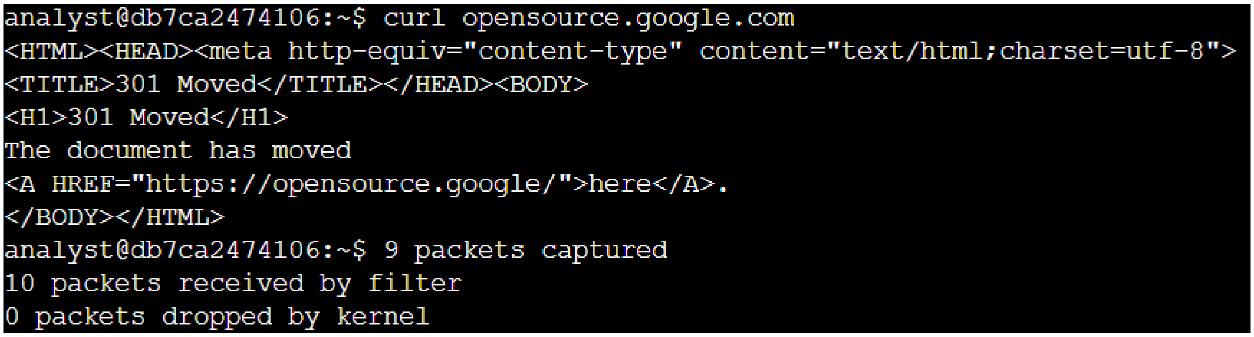
- -i eth0: Capture data from the eth0 interface.
- -nn: Do not attempt to resolve IP addresses or ports to names.This is best practice from a security perspective, as the lookup data may not be valid. It also prevents malicious actors from being alerted to an investigation.
- -c9: Capture 9 packets of 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@db7ca2474106:~$ sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &
[1] 13485
analyst@db7ca2474106:~$ tcpdump: listening on eth0, link-type EN10MB (Ethernet), snap
shot length 262144 bytes
```

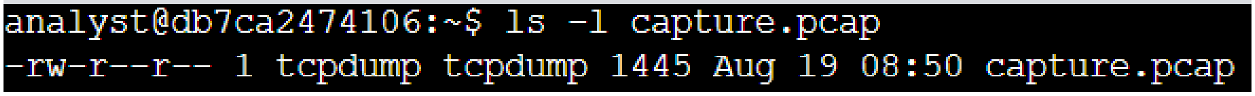
Use curl to generate some HTTP (port 80) traffic:

curl opensource.google.com



```
analyst@db7ca2474106:~$ 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@db7ca2474106:~$ 9 packets captured
10 packets received by filter
0 packets dropped by kernel
```

Verify the packet data has been captured: ls -l capture.pcap.

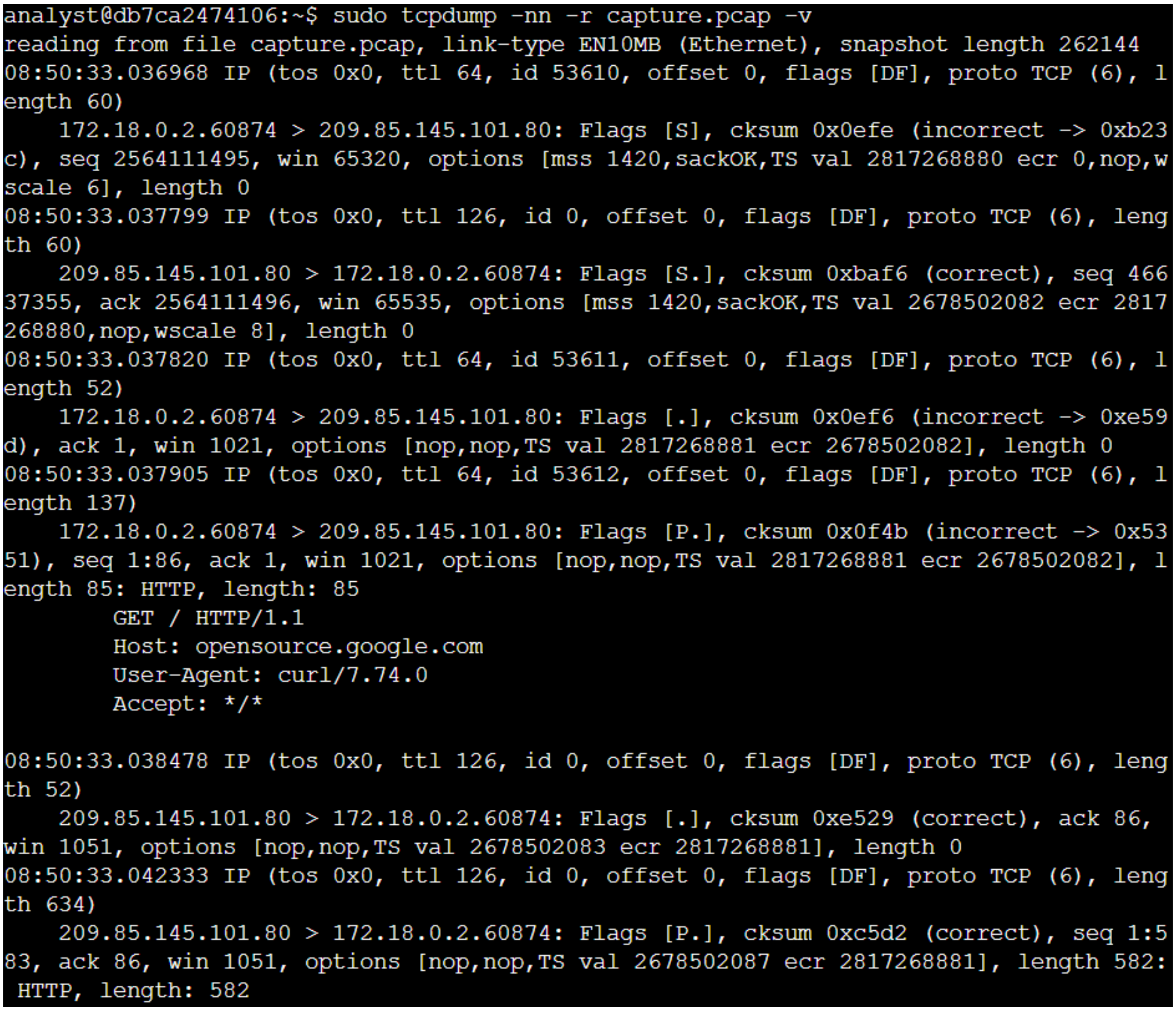


```
analyst@db7ca2474106:~$ ls -l capture.pcap
-rw-r--r-- 1 tcpdump tcpdump 1445 Aug 19 08:50 capture.pcap
```

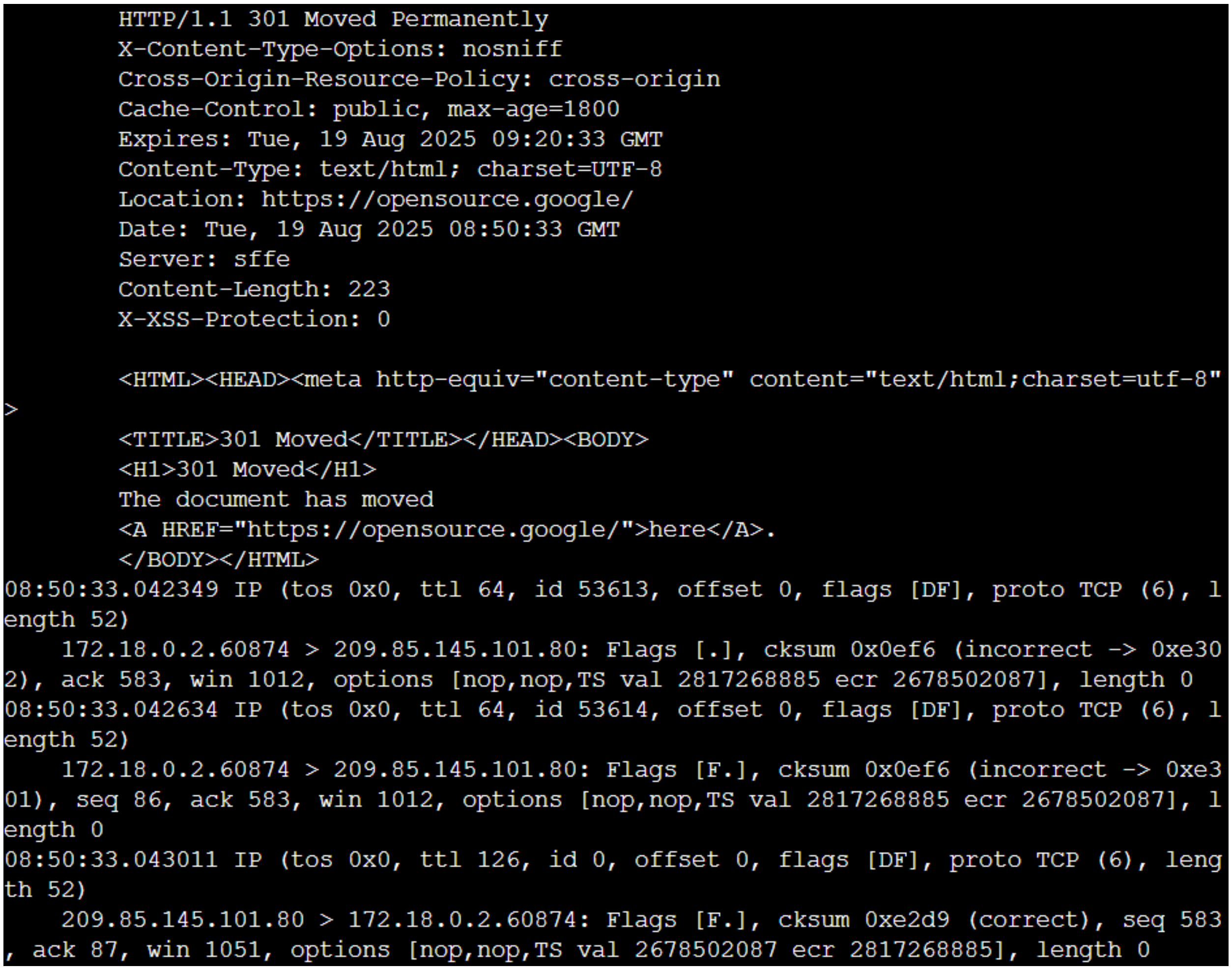
Task 4. Filter the captured packet data

Use the tcpdump command to filter the packet header data from the capture.pcap capture file:

sudo tcpdump -nn -r capture.pcap -v



```
analyst@db7ca2474106:~$ sudo tcpdump -nn -r capture.pcap -v
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
08:50:33.036968 IP (tos 0x0, ttl 64, id 53610, offset 0, flags [DF], proto TCP (6), l
ength 60)
    172.18.0.2.60874 > 209.85.145.101.80: Flags [S], cksum 0x0efe (incorrect -> 0xb23
c), seq 2564111495, win 65320, options [mss 1420,sackOK,TS val 2817268880 ecr 0,nop,w
scale 6], length 0
08:50:33.037799 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), leng
th 60)
    209.85.145.101.80 > 172.18.0.2.60874: Flags [S.], cksum 0xbaf6 (correct), seq 466
37355, ack 2564111496, win 65535, options [mss 1420,sackOK,TS val 2678502082 ecr 2817
268880,nop,wscale 8], length 0
08:50:33.037820 IP (tos 0x0, ttl 64, id 53611, offset 0, flags [DF], proto TCP (6), l
ength 52)
    172.18.0.2.60874 > 209.85.145.101.80: Flags [.], cksum 0x0ef6 (incorrect -> 0xe59
d), ack 1, win 1021, options [nop,nop,TS val 2817268881 ecr 2678502082], length 0
08:50:33.037905 IP (tos 0x0, ttl 64, id 53612, offset 0, flags [DF], proto TCP (6), l
ength 137)
    172.18.0.2.60874 > 209.85.145.101.80: Flags [P.], cksum 0x0f4b (incorrect -> 0x53
51), seq 1:86, ack 1, win 1021, options [nop,nop,TS val 2817268881 ecr 2678502082], l
ength 85: HTTP, length: 85
        GET / HTTP/1.1
        Host: opensource.google.com
        User-Agent: curl/7.74.0
        Accept: */*

08:50:33.038478 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), leng
th 52)
    209.85.145.101.80 > 172.18.0.2.60874: Flags [.], cksum 0xe529 (correct), ack 86,
win 1051, options [nop,nop,TS val 2678502083 ecr 2817268881], length 0
08:50:33.042333 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), leng
th 634)
    209.85.145.101.80 > 172.18.0.2.60874: Flags [P.], cksum 0xc5d2 (correct), seq 1:5
83, ack 86, win 1051, options [nop,nop,TS val 2678502087 ecr 2817268881], length 582:
 HTTP, length: 582
```



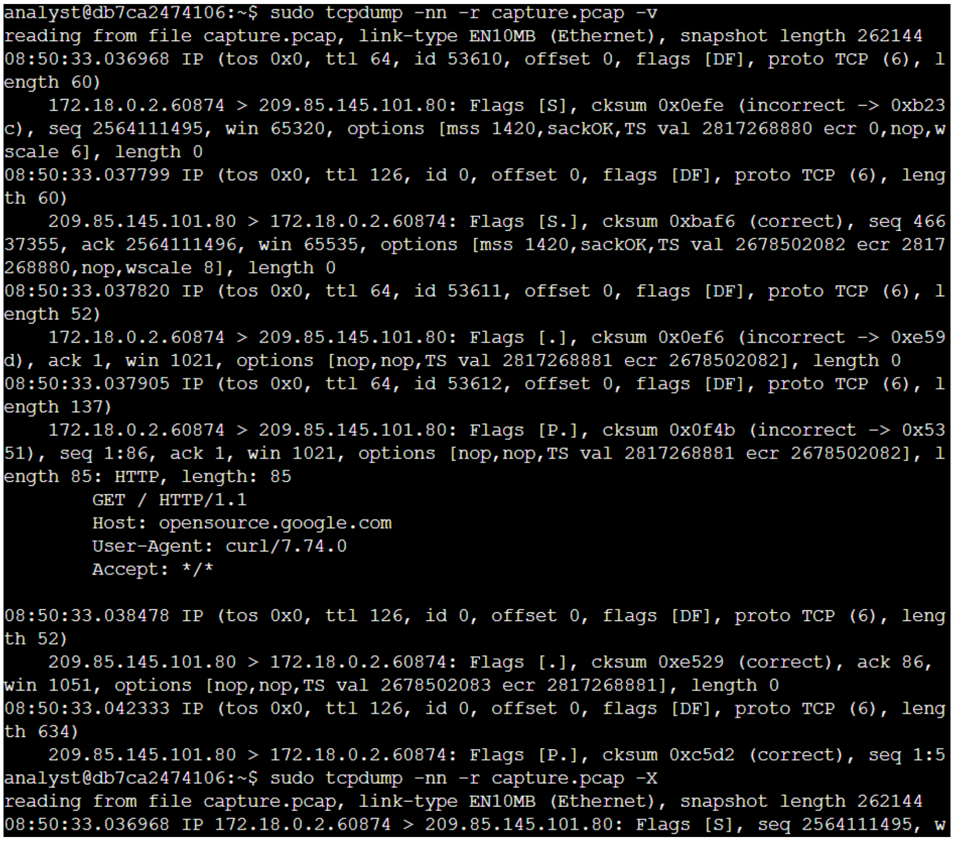
```
        HTTP/1.1 301 Moved Permanently
        X-Content-Type-Options: nosniff
        Cross-Origin-Resource-Policy: cross-origin
        Cache-Control: public, max-age=1800
        Expires: Tue, 19 Aug 2025 09:20:33 GMT
        Content-Type: text/html; charset=UTF-8
        Location: https://opensource.google/
        Date: Tue, 19 Aug 2025 08:50:33 GMT
        Server: sffe
        Content-Length: 223
        X-XSS-Protection: 0

        <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>
08:50:33.042349 IP (tos 0x0, ttl 64, id 53613, offset 0, flags [DF], proto TCP (6), l
ength 52)
    172.18.0.2.60874 > 209.85.145.101.80: Flags [.], cksum 0x0ef6 (incorrect -> 0xe30
2), ack 583, win 1012, options [nop,nop,TS val 2817268885 ecr 2678502087], length 0
08:50:33.042634 IP (tos 0x0, ttl 64, id 53614, offset 0, flags [DF], proto TCP (6), l
ength 52)
    172.18.0.2.60874 > 209.85.145.101.80: Flags [F.], cksum 0x0ef6 (incorrect -> 0xe3
01), seq 86, ack 583, win 1012, options [nop,nop,TS val 2817268885 ecr 2678502087], l
ength 0
08:50:33.043011 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), leng
th 52)
    209.85.145.101.80 > 172.18.0.2.60874: Flags [F.], cksum 0xe2d9 (correct), seq 583
, ack 87, win 1051, options [nop,nop,TS val 2678502087 ecr 2817268885], length 0
```

This command will run tcpdump with the following options:

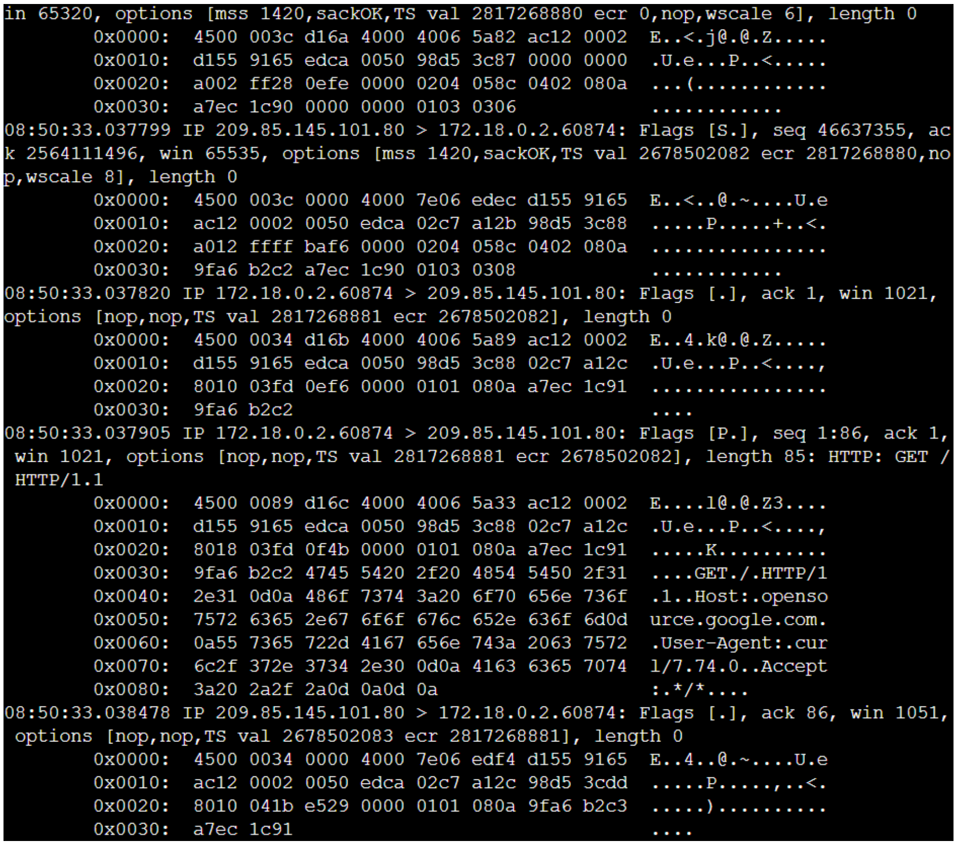
- -nn: Disable port and protocol name lookup.
- -r: Read capture data from the named file.
- -v: Display detailed packet data.

Filter the extended packet data from the capture.pcap capture file:

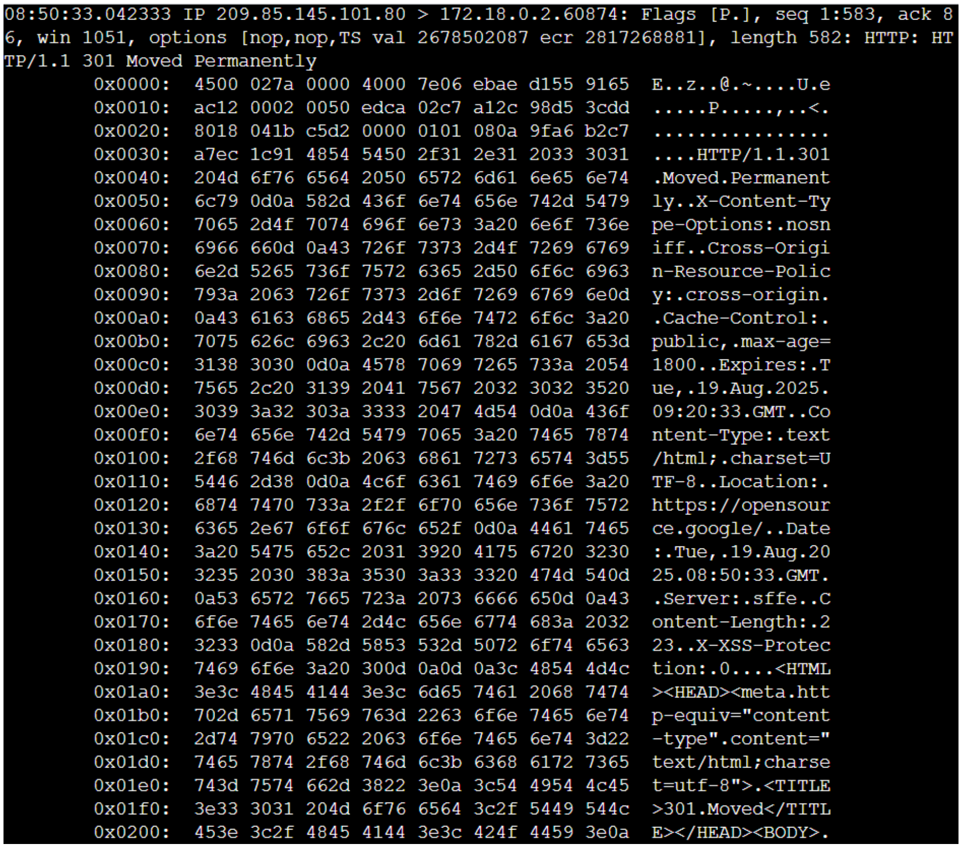
sudo tcpdump -nn -r capture.pcap -X



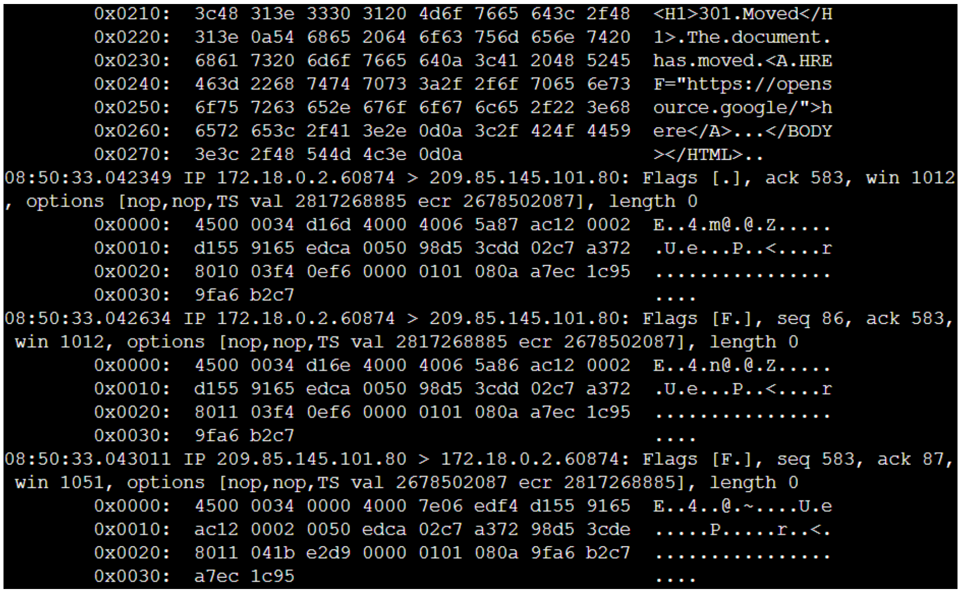
```
analyst@db7ca2474106:~$ sudo tcpdump -nn -r capture.pcap -v
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
08:50:33.036968 IP (tos 0x0, ttl 64, id 53610, offset 0, flags [DF], proto TCP (6), l
ength 60)
    172.18.0.2.60874 > 209.85.145.101.80: Flags [S], cksum 0x0efe (incorrect -> 0xb23
c), seq 2564111495, win 65320, options [mss 1420,sackOK,TS val 2817268880 ecr 0,nop,w
scale 6], length 0
08:50:33.037799 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), leng
th 60)
    209.85.145.101.80 > 172.18.0.2.60874: Flags [S.], cksum 0xbaf6 (correct), seq 466
37355, ack 2564111496, win 65535, options [mss 1420,sackOK,TS val 2678502082 ecr 2817
268880,nop,wscale 8], length 0
08:50:33.037820 IP (tos 0x0, ttl 64, id 53611, offset 0, flags [DF], proto TCP (6), l
ength 52)
    172.18.0.2.60874 > 209.85.145.101.80: Flags [.], cksum 0x0ef6 (incorrect -> 0xe59
d), ack 1, win 1021, options [nop,nop,TS val 2817268881 ecr 2678502082], length 0
08:50:33.037905 IP (tos 0x0, ttl 64, id 53612, offset 0, flags [DF], proto TCP (6), l
ength 137)
    172.18.0.2.60874 > 209.85.145.101.80: Flags [P.], cksum 0x0f4b (incorrect -> 0x53
51), seq 1:86, ack 1, win 1021, options [nop,nop,TS val 2817268881 ecr 2678502082], l
ength 85: HTTP, length: 85
        GET / HTTP/1.1
        Host: opensource.google.com
        User-Agent: curl/7.74.0
        Accept: */*

08:50:33.038478 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), leng
th 52)
    209.85.145.101.80 > 172.18.0.2.60874: Flags [.], cksum 0xe529 (correct), ack 86,
win 1051, options [nop,nop,TS val 2678502083 ecr 2817268881], length 0
08:50:33.042333 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), leng
th 634)
    209.85.145.101.80 > 172.18.0.2.60874: Flags [P.], cksum 0xc5d2 (correct), seq 1:5
analyst@db7ca2474106:~$ sudo tcpdump -nn -r capture.pcap -X
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
08:50:33.036968 IP 172.18.0.2.60874 > 209.85.145.101.80: Flags [S], seq 2564111495, w
```



```
in 65320, options [mss 1420,sackOK,TS val 2817268880 ecr 0,nop,wscale 6], length 0
        0x0000:  4500 003c d16a 4000 4006 5a82 ac12 0002  E..<.j@.@.Z.....
        0x0010:  d155 9165 edca 0050 98d5 3c87 0000 0000  .U.e...P..<.....
        0x0020:  a002 ff28 0efe 0000 0204 058c 0402 080a  ...(............
        0x0030:  a7ec 1c90 0000 0000 0103 0306            ............
08:50:33.037799 IP 209.85.145.101.80 > 172.18.0.2.60874: Flags [S.], seq 46637355, ac
k 2564111496, win 65535, options [mss 1420,sackOK,TS val 2678502082 ecr 2817268880,no
p,wscale 8], length 0
        0x0000:  4500 003c 0000 4000 7e06 edec d155 9165  E..<..@.~....U.e
        0x0010:  ac12 0002 0050 edca 02c7 a12b 98d5 3c88  .....P.....+..<.
        0x0020:  a012 ffff baf6 0000 0204 058c 0402 080a  ................
        0x0030:  9fa6 b2c2 a7ec 1c90 0103 0308            ............
08:50:33.037820 IP 172.18.0.2.60874 > 209.85.145.101.80: Flags [.], ack 1, win 1021,
options [nop,nop,TS val 2817268881 ecr 2678502082], length 0
        0x0000:  4500 0034 d16b 4000 4006 5a89 ac12 0002  E..4.k@.@.Z.....
        0x0010:  d155 9165 edca 0050 98d5 3c88 02c7 a12c  .U.e...P..<....,
        0x0020:  8010 03fd 0ef6 0000 0101 080a a7ec 1c91  ................
        0x0030:  9fa6 b2c2                                ....
08:50:33.037905 IP 172.18.0.2.60874 > 209.85.145.101.80: Flags [P.], seq 1:86, ack 1,
 win 1021, options [nop,nop,TS val 2817268881 ecr 2678502082], length 85: HTTP: GET /
 HTTP/1.1
        0x0000:  4500 0089 d16c 4000 4006 5a33 ac12 0002  E....l@.@.Z3....
        0x0010:  d155 9165 edca 0050 98d5 3c88 02c7 a12c  .U.e...P..<....,
        0x0020:  8018 03fd 0f4b 0000 0101 080a a7ec 1c91  .....K..........
        0x0030:  9fa6 b2c2 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 3734 2e30 0d0a 4163 6365 7074  l/7.74.0..Accept
        0x0080:  3a20 2a2f 2a0d 0a0d 0a                   :.*/*....
08:50:33.038478 IP 209.85.145.101.80 > 172.18.0.2.60874: Flags [.], ack 86, win 1051,
 options [nop,nop,TS val 2678502083 ecr 2817268881], length 0
        0x0000:  4500 0034 0000 4000 7e06 edf4 d155 9165  E..4..@.~....U.e
        0x0010:  ac12 0002 0050 edca 02c7 a12c 98d5 3cdd  .....P.....,..<.
        0x0020:  8010 041b e529 0000 0101 080a 9fa6 b2c3  .....)..........
        0x0030:  a7ec 1c91                                ....
```



```
08:50:33.042333 IP 209.85.145.101.80 > 172.18.0.2.60874: Flags [P.], seq 1:583, ack 8
6, win 1051, options [nop,nop,TS val 2678502087 ecr 2817268881], length 582: HTTP: HT
TP/1.1 301 Moved Permanently
        0x0000:  4500 027a 0000 4000 7e06 ebae d155 9165  E..z..@.~....U.e
        0x0010:  ac12 0002 0050 edca 02c7 a12c 98d5 3cdd  .....P.....,..<.
        0x0020:  8018 041b c5d2 0000 0101 080a 9fa6 b2c7  ................
        0x0030:  a7ec 1c91 4854 5450 2f31 2e31 2033 3031  ....HTTP/1.1.301
        0x0040:  204d 6f76 6564 2050 6572 6d61 6e65 6e74  .Moved.Permanent
        0x0050:  6c79 0d0a 582d 436f 6e74 656e 742d 5479  ly..X-Content-Ty
        0x0060:  7065 2d4f 7074 696f 6e73 3a20 6e6f 736e  pe-Options:.nosn
        0x0070:  6966 660d 0a43 726f 7373 2d4f 7269 6769  iff..Cross-Origi
        0x0080:  6e2d 5265 736f 7572 6365 2d50 6f6c 6963  n-Resource-Polic
        0x0090:  793a 2063 726f 7373 2d6f 7269 6769 6e0d  y:.cross-origin.
        0x00a0:  0a43 6163 6865 2d43 6f6e 7472 6f6c 3a20  .Cache-Control:.
        0x00b0:  7075 626c 6963 2c20 6d61 782d 6167 653d  public,.max-age=
        0x00c0:  3138 3030 0d0a 4578 7069 7265 733a 2054  1800..Expires:.T
        0x00d0:  7565 2c20 3139 2041 7567 2032 3032 3520  ue,.19.Aug.2025.
        0x00e0:  3039 3a32 303a 3333 2047 4d54 0d0a 436f  09:20:33.GMT..Co
        0x00f0:  6e74 656e 742d 5479 7065 3a20 7465 7874  ntent-Type:.text
        0x0100:  2f68 746d 6c3b 2063 6861 7273 6574 3d55  /html;.charset=U
        0x0110:  5446 2d38 0d0a 4c6f 6361 7469 6f6e 3a20  TF-8..Location:.
        0x0120:  6874 7470 733a 2f2f 6f70 656e 736f 7572  https://opensour
        0x0130:  6365 2e67 6f6f 676c 652f 0d0a 4461 7465  ce.google/..Date
        0x0140:  3a20 5475 652c 2031 3920 4175 6720 3230  :.Tue,.19.Aug.20
        0x0150:  3235 2030 383a 3530 3a33 3320 474d 540d  25.08:50:33.GMT.
        0x0160:  0a53 6572 7665 723a 2073 6666 650d 0a43  .Server:.sffe..C
        0x0170:  6f6e 7465 6e74 2d4c 656e 6774 683a 2032  ontent-Length:.2
        0x0180:  3233 0d0a 582d 5853 532d 5072 6f74 6563  23..X-XSS-Protec
        0x0190:  7469 6f6e 3a20 300d 0a0d 0a3c 4854 4d4c  tion:.0....<HTML
        0x01a0:  3e3c 4845 4144 3e3c 6d65 7461 2068 7474  ><HEAD><meta.htt
        0x01b0:  702d 6571 7569 763d 2263 6f6e 7465 6e74  p-equiv="content
        0x01c0:  2d74 7970 6522 2063 6f6e 7465 6e74 3d22  -type".content="
        0x01d0:  7465 7874 2f68 746d 6c3b 6368 6172 7365  text/html;charse
        0x01e0:  743d 7574 662d 3822 3e0a 3c54 4954 4c45  t=utf-8">.<TITLE
        0x01f0:  3e33 3031 204d 6f76 6564 3c2f 5449 544c  >301.Moved</TITL
        0x0200:  453e 3c2f 4845 4144 3e3c 424f 4459 3e0a  E></HEAD><BODY>.
```



```
        0x0210:  3c48 313e 3330 3120 4d6f 7665 643c 2f48  <H1>301.Moved</H
        0x0220:  313e 0a54 6865 2064 6f63 756d 656e 7420  1>.The.document.
        0x0230:  6861 7320 6d6f 7665 640a 3c41 2048 5245  has.moved.<A.HRE
        0x0240:  463d 2268 7474 7073 3a2f 2f6f 7065 6e73  F="https://opens
        0x0250:  6f75 7263 652e 676f 6f67 6c65 2f22 3e68  ource.google/">h
        0x0260:  6572 653c 2f41 3e2e 0d0a 3c2f 424f 4459  ere</A>...</BODY
        0x0270:  3e3c 2f48 544d 4c3e 0d0a                 ></HTML>..
08:50:33.042349 IP 172.18.0.2.60874 > 209.85.145.101.80: Flags [.], ack 583, win 1012
, options [nop,nop,TS val 2817268885 ecr 2678502087], length 0
        0x0000:  4500 0034 d16d 4000 4006 5a87 ac12 0002  E..4.m@.@.Z.....
        0x0010:  d155 9165 edca 0050 98d5 3cdd 02c7 a372  .U.e...P..<....r
        0x0020:  8010 03f4 0ef6 0000 0101 080a a7ec 1c95  ................
        0x0030:  9fa6 b2c7                                ....
08:50:33.042634 IP 172.18.0.2.60874 > 209.85.145.101.80: Flags [F.], seq 86, ack 583,
 win 1012, options [nop,nop,TS val 2817268885 ecr 2678502087], length 0
        0x0000:  4500 0034 d16e 4000 4006 5a86 ac12 0002  E..4.n@.@.Z.....
        0x0010:  d155 9165 edca 0050 98d5 3cdd 02c7 a372  .U.e...P..<....r
        0x0020:  8011 03f4 0ef6 0000 0101 080a a7ec 1c95  ................
        0x0030:  9fa6 b2c7                                ....
08:50:33.043011 IP 209.85.145.101.80 > 172.18.0.2.60874: Flags [F.], seq 583, ack 87,
 win 1051, options [nop,nop,TS val 2678502087 ecr 2817268885], length 0
        0x0000:  4500 0034 0000 4000 7e06 edf4 d155 9165  E..4..@.~....U.e
        0x0010:  ac12 0002 0050 edca 02c7 a372 98d5 3cde  .....P.....r..<.
        0x0020:  8011 041b e2d9 0000 0101 080a 9fa6 b2c7  ................
        0x0030:  a7ec 1c95                                ....
```

- -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.

- ***Note:*** *Hexadecimal, also known as hex or base 16, uses 16 symbols to represent values, including the digits 0-9 and letters A, B, C, D, E, and F. American Standard Code for Information Interchange (ASCII) is a character encoding standard that uses a set of characters to represent text in digital form.*