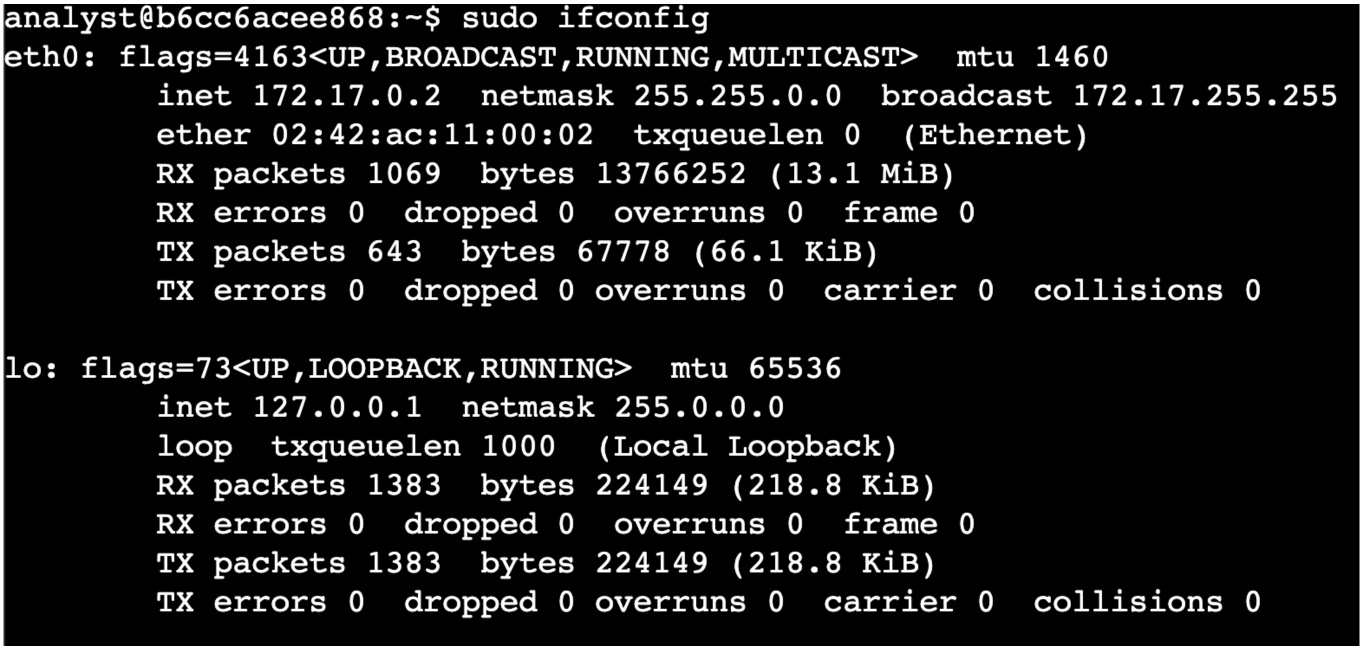
tcpdump-ex1

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

Use `ifconfig` to identify the interfaces that are available:

`sudo ifconfig`

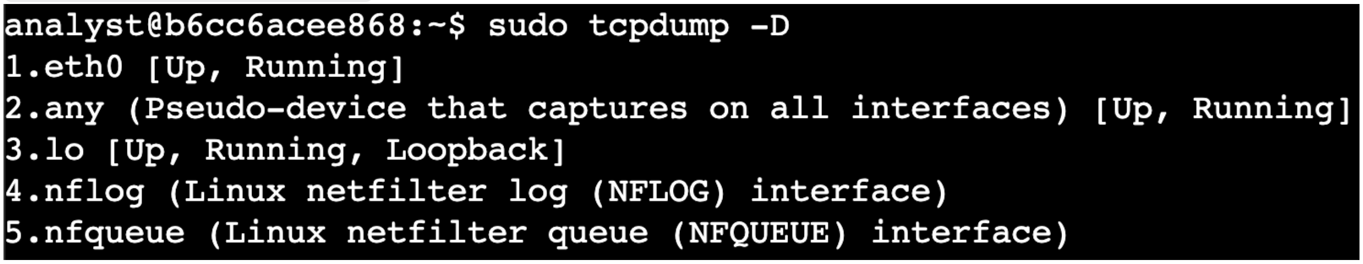


```
analyst@b6cc6acee868:~$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1460
        inet 172.17.0.2  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ac:11:00:02  txqueuelen 0  (Ethernet)
        RX packets 1069  bytes 13766252 (13.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 643  bytes 67778 (66.1 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 1383  bytes 224149 (218.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1383  bytes 224149 (218.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

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

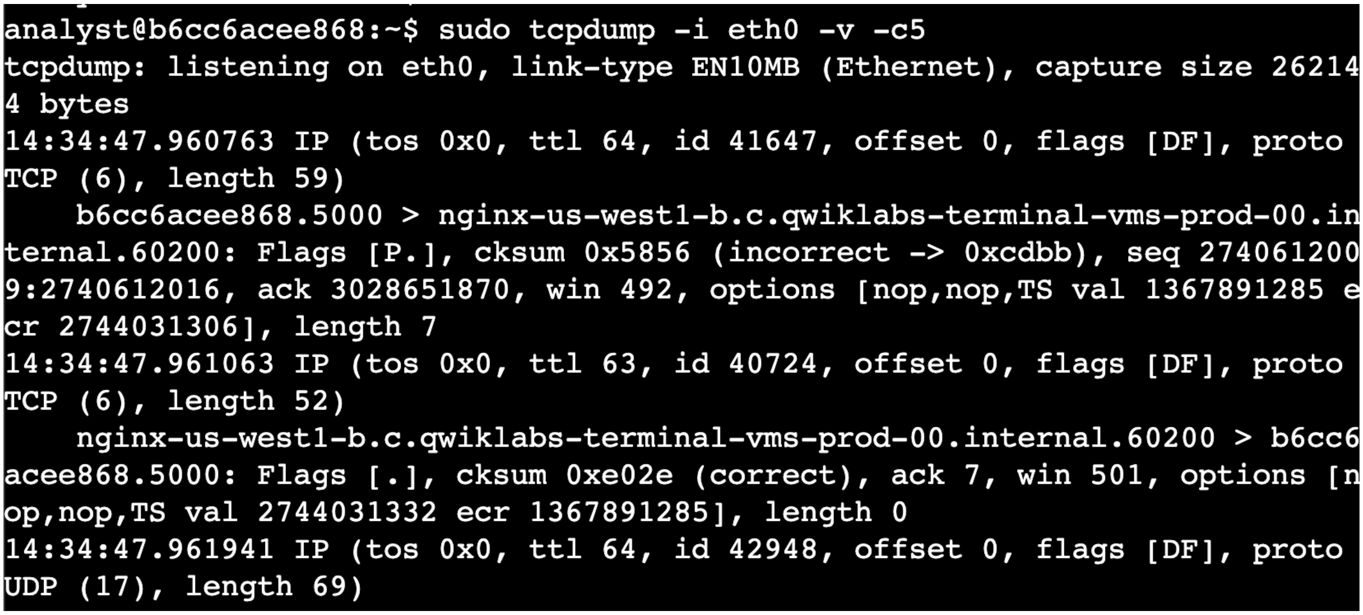
`sudo tcpdump -D`



```
analyst@b6cc6acee868:~$ 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)
```

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

```
sudo tcpdump -i eth0 -v -c5
```



```
analyst@b6cc6acee868:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 26214
4 bytes
14:34:47.960763 IP (tos 0x0, ttl 64, id 41647, offset 0, flags [DF], proto
TCP (6), length 59)
    b6cc6acee868.5000 > nginx-us-west1-b.c.qwiklabs-terminal-vms-prod-00.in
ternal.60200: Flags [P.], cksum 0x5856 (incorrect -> 0xcdbb), seq 274061200
9:2740612016, ack 3028651870, win 492, options [nop,nop,TS val 1367891285 e
cr 2744031306], length 7
14:34:47.961063 IP (tos 0x0, ttl 63, id 40724, offset 0, flags [DF], proto
TCP (6), length 52)
    nginx-us-west1-b.c.qwiklabs-terminal-vms-prod-00.internal.60200 > b6cc6
acee868.5000: Flags [.], cksum 0xe02e (correct), ack 7, win 501, options [n
op,nop,TS val 2744031332 ecr 1367891285], length 0
14:34:47.961941 IP (tos 0x0, ttl 64, id 42948, offset 0, flags [DF], proto
UDP (17), length 69)
```

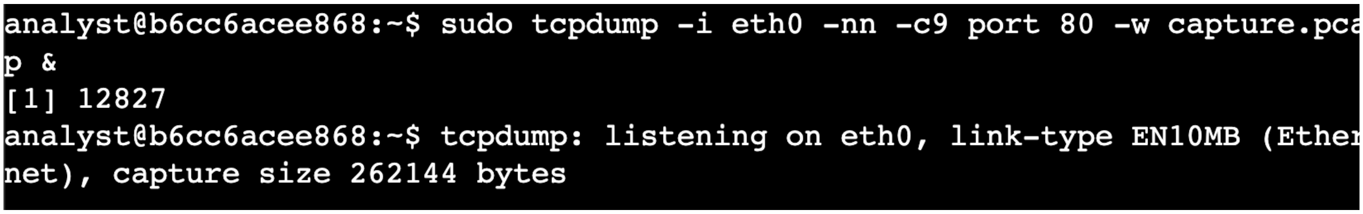
Capture packet data into a file called `capture.pcap`:

```
sudo tcpdump -i etho0 -nn -c9 port 80 -w capture.pcap &
```

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.



```
analyst@b6cc6acee868:~$ sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pca
p &
[1] 12827
analyst@b6cc6acee868:~$ tcpdump: listening on eth0, link-type EN10MB (Ether
net), capture size 262144 bytes
```

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

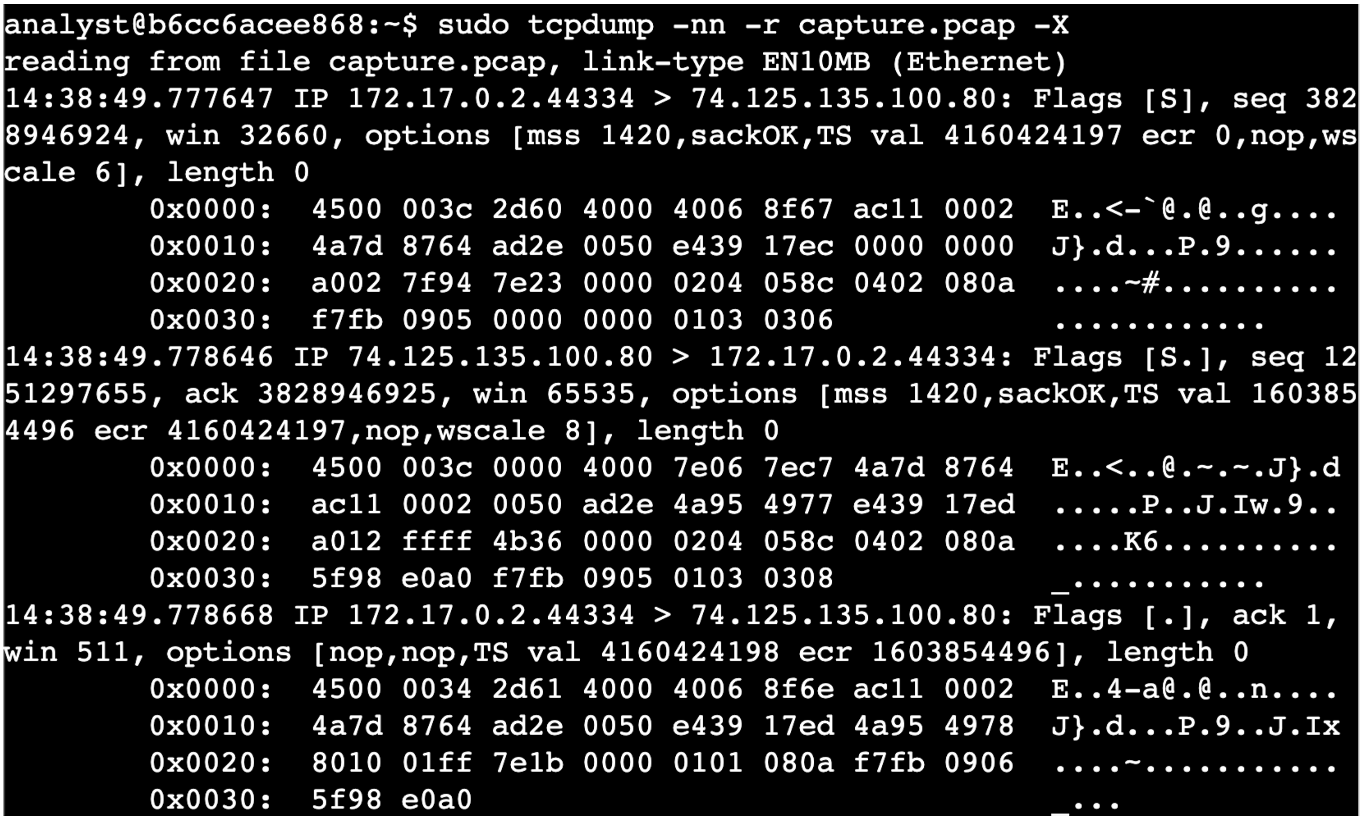
`sudo tcpdump -nn -r capture.pcap -v`

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

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

`sudo tcpdump -nn -r capture.pacap -X`

- `-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@b6cc6acee868:~$ sudo tcpdump -nn -r capture.pcap -X
reading from file capture.pcap, link-type EN10MB (Ethernet)
14:38:49.777647 IP 172.17.0.2.44334 > 74.125.135.100.80: Flags [S], seq 382
8946924, win 32660, options [mss 1420,sackOK,TS val 4160424197 ecr 0,nop,ws
cale 6], length 0
        0x0000:  4500 003c 2d60 4000 4006 8f67 ac11 0002  E..<-`@.@..g....
        0x0010:  4a7d 8764 ad2e 0050 e439 17ec 0000 0000  J}.d...P.9......
        0x0020:  a002 7f94 7e23 0000 0204 058c 0402 080a  ....~#..........
        0x0030:  f7fb 0905 0000 0000 0103 0306            ............
14:38:49.778646 IP 74.125.135.100.80 > 172.17.0.2.44334: Flags [S.], seq 12
51297655, ack 3828946925, win 65535, options [mss 1420,sackOK,TS val 160385
4496 ecr 4160424197,nop,wscale 8], length 0
        0x0000:  4500 003c 0000 4000 7e06 7ec7 4a7d 8764  E..<..@.~.~.J}.d
        0x0010:  ac11 0002 0050 ad2e 4a95 4977 e439 17ed  .....P..J.Iw.9..
        0x0020:  a012 ffff 4b36 0000 0204 058c 0402 080a  ....K6..........
        0x0030:  5f98 e0a0 f7fb 0905 0103 0308            _...........
14:38:49.778668 IP 172.17.0.2.44334 > 74.125.135.100.80: Flags [.], ack 1,
win 511, options [nop,nop,TS val 4160424198 ecr 1603854496], length 0
        0x0000:  4500 0034 2d61 4000 4006 8f6e ac11 0002  E..4-a@.@..n....
        0x0010:  4a7d 8764 ad2e 0050 e439 17ed 4a95 4978  J}.d...P.9..J.Ix
        0x0020:  8010 01ff 7e1b 0000 0101 080a f7fb 0906  ....~...........
        0x0030:  5f98 e0a0                                _...
```