Tcpdump packet captures in Linux terminal

First, I want to identify all network interfaces that I'm connected to, I show only 2 (eth0 – Ethernet & lo – loopback):

```
analyst@27f1a1a1be77:~$ 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 969  bytes 14019299 (13.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 604  bytes 56596 (55.2 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 115  bytes 14312 (13.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 115  bytes 14312 (13.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

analyst@27f1a1a1be77:~$
```

With the eth0 interface available, I want to capture data specifically for that interface, capturing at 5 packets of data:

```
analyst@27f1a1a1be77:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
03:45:31.757754 IP (tos 0x0, ttl 64, id 33604, offset 0, flags [DF], proto TCP (6), l
ength 122)
    27f1a1a1be77.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.
38926: Flags [P.], cksum 0x5894 (incorrect -> 0x260c), seq 4043454014:4043454084, ack
 3280841744, win 998, options [nop,nop,TS val 911957602 ecr 1617215126], length 70
03:45:31.757985 IP (tos 0x0, ttl 63, id 46166, offset 0, flags [DF], proto TCP (6), l
ength 52)
    nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.38926 > 27f1a1a1be77
.5000: Flags [.], cksum 0x256f (correct), ack 70, win 507, options [nop,nop,TS val 16
17215309 ecr 911957602], length 0
03:45:31.841873 IP (tos 0x0, ttl 64, id 65154, offset 0, flags [DF], proto UDP (17),
length 69)
    27f1a1a1be77.41275 > metadata.google.internal.domain: 30554+ PTR? 2.0.17.172.in-a
ddr.arpa. (41)
03:45:31.850627 IP (tos 0x0, ttl 64, id 33605, offset 0, flags [DF], proto TCP (6), l
ength 143)
    27f1a1a1be77.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.
38926: Flags [P.], cksum 0x58a9 (incorrect -> 0xcd8c), seq 70:161, ack 1, win 998, op
tions [nop,nop,TS val 911957695 ecr 1617215309], length 91
03:45:31.850769 IP (tos 0x0, ttl 63, id 0, offset 0, flags [none], proto UDP (17), le
ngth 143)
    metadata.google.internal.domain > 27f1a1a1be77.41275: 30554 1/0/0 2.0.17.172.in-a
ddr.arpa. PTR nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal. (115)
5 packets captured
10 packets received by filter
0 packets dropped by kernel
```

I'm able to analyze most of the data in the first 2 returned lines, like eth0 listening channel, timestamp, protocol type, tos, ttl, length of outer IP packet, etc.:

```
analyst@27f1a1a1be77:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
03:45:31.757754 IP (tos 0x0, ttl 64, id 33604, offset 0, flags [DF], proto TCP (6), l
ength 122)
    27f1a1a1be77.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.
38926: Flags [P.], cksum 0x5894 (incorrect -> 0x260c), seq 4043454014:4043454084, ack
 3280841744, win 998, options [nop,nop,TS val 911957602 ecr 1617215126], length 70
03:45:31.757985 IP (tos 0x0, ttl 63, id 46166, offset 0, flags [DF], proto TCP (6), l
ength 52)
    nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.38926 > 27f1a1a1be77
.5000: Flags [.], cksum 0x256f (correct), ack 70, win 507, options [nop,nop,TS val 16
17215309 ecr 911957602], length 0
03:45:31.841873 IP (tos 0x0, ttl 64, id 65154, offset 0, flags [DF], proto UDP (17),
length 69)
    27f1a1a1be77.41275 > metadata.google.internal.domain: 30554+ PTR? 2.0.17.172.in-a
ddr.arpa. (41)
03:45:31.850627 IP (tos 0x0, ttl 64, id 33605, offset 0, flags [DF], proto TCP (6), l
ength 143)
    27f1a1a1be77.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.
38926: Flags [P.], cksum 0x58a9 (incorrect -> 0xcd8c), seq 70:161, ack 1, win 998, op
tions [nop,nop,TS val 911957695 ecr 1617215309], length 91
03:45:31.850769 IP (tos 0x0, ttl 63, id 0, offset 0, flags [none], proto UDP (17), le
ngth 143)
    metadata.google.internal.domain > 27f1a1a1be77.41275: 30554 1/0/0 2.0.17.172.in-a
ddr.arpa. PTR nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal. (115)
5 packets captured
10 packets received by filter
0 packets dropped by kernel
```

The next line shows the 2 systems that are communicating in the direction of the arrow" > "with the [P.] meaning Pushed and acknowledged. This packet is pushing out data:

```
analyst@27f1a1a1be77:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
03:45:31.757754 IP (tos 0x0, ttl 64, id 33604, offset 0, flags [DF], proto TCP (6), l
ength 122)
    27f1a1a1be77.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.
38926: Flags [P.], cksum 0x5894 (incorrect -> 0x260c), seq 4043454014:4043454084, ack
 3280841744, win 998, options [nop,nop,TS val 911957602 ecr 1617215126], length 70
03:45:31.757985 IP (tos 0x0, ttl 63, id 46166, offset 0, flags [DF], proto TCP (6), l
ength 52)
    nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.38926 > 27f1a1a1be77
.5000: Flags [.], cksum 0x256f (correct), ack 70, win 507, options [nop,nop,TS val 16
17215309 ecr 911957602], length 0
03:45:31.841873 IP (tos 0x0, ttl 64, id 65154, offset 0, flags [DF], proto UDP (17),
length 69)
    27f1a1a1be77.41275 > metadata.google.internal.domain: 30554+ PTR? 2.0.17.172.in-a
ddr.arpa. (41)
03:45:31.850627 IP (tos 0x0, ttl 64, id 33605, offset 0, flags [DF], proto TCP (6), l
ength 143)
    27f1a1a1be77.5000 > nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal.
38926: Flags [P.], cksum 0x58a9 (incorrect -> 0xcd8c), seq 70:161, ack 1, win 998, op
tions [nop,nop,TS val 911957695 ecr 1617215309], length 91
03:45:31.850769 IP (tos 0x0, ttl 63, id 0, offset 0, flags [none], proto UDP (17), le
ngth 143)
    metadata.google.internal.domain > 27f1a1a1be77.41275: 30554 1/0/0 2.0.17.172.in-a
ddr.arpa. PTR nginx-us-central1-b.c.qwiklabs-terminal-vms-prod-00.internal. (115)
5 packets captured
10 packets received by filter
0 packets dropped by kernel
```

Now, I want to capture network traffic containing only web (TCP Port 80) network packet data, saving it to a named file (-w capture.pcap), while instructing Bash to run the command in the background (&):

```
analyst@27f1a1a1be77:~$ sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &
[1] 13692
analyst@27f1a1a1be77:~$ tcpdump: listening on eth0, link-type EN10MB (Ethernet), snap
shot length 262144 bytes
```

Now I'll use the ***curl*** command to generate some HTTP data to be captured:

```
analyst@27f1a1a1be77:~$ 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@27f1a1a1be77:~$ 9 packets captured
10 packets received by filter
0 packets dropped by kernel
```

This can now be captured using the ***ls -l*** command + the file name, if captured, DONE will show:

```
ls -l capture.pcap
-rw-r--r-- 1 tcpdump tcpdump 1455 Jul 24 04:17 capture.pcap
[1]+  Done                    sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap
analyst@27f1a1a1be77:~$
```