Cybersecurity 701

tcpdump Lab

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

tcpdump Materials

- Materials needed
  - Kali Linux Virtual Machine

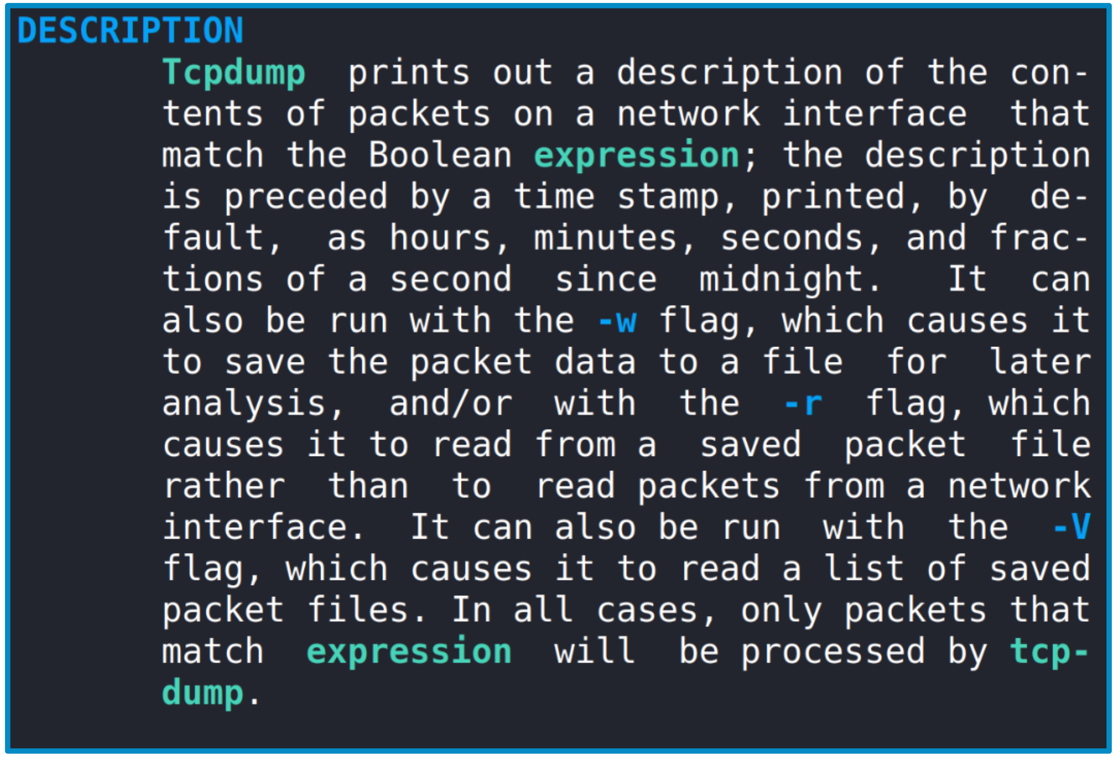
- Software Tools used (From Kali Linux OS)
  - tcpdump (TCP/IP Packet Analyzer)

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 4.9 – Given a scenario, use data sources to support an investigation.
    - Packet captures

What is TCPDump?

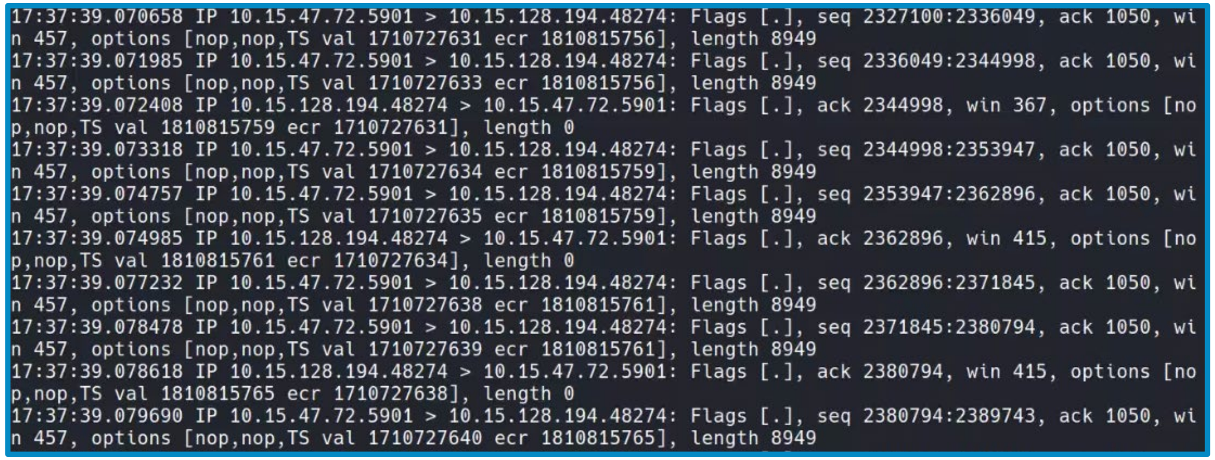
- Data-network packer analyzer program that runs inside the Terminal
  - Prints contents of network packets
  - Prints on screen or saved as text file



```
DESCRIPTION
       Tcpdump  prints out a description of the con-
       tents of packets on a network interface  that
       match the Boolean expression; the description
       is preceded by a time stamp, printed, by  de-
       fault,  as hours, minutes, seconds, and frac-
       tions of a second  since  midnight.   It  can
       also be run with the -w flag, which causes it
       to save the packet data to a file  for  later
       analysis,  and/or  with  the  -r  flag, which
       causes it to read from a  saved  packet  file
       rather  than  to  read packets from a network
       interface.  It can also be run  with  the  -V
       flag, which causes it to read a list of saved
       packet files. In all cases, only packets that
       match  expression  will  be processed by tcp-
       dump.
```

tcpdump Lab Overview

1. Set up the VM environment
2. Find your network interface
3. Capture packets
   - Contents of a Packet
4. Reduce packets dropped
5. Clean-up the output
   - Contents of a “Quiet” Packet
6. Expand output
7. Capture as a .txt file



```
17:37:39.070658 IP 10.15.47.72.5901 > 10.15.128.194.48274: Flags [.], seq 2327100:2336049, ack 1050, wi
n 457, options [nop,nop,TS val 1710727631 ecr 1810815756], length 8949
17:37:39.071985 IP 10.15.47.72.5901 > 10.15.128.194.48274: Flags [.], seq 2336049:2344998, ack 1050, wi
n 457, options [nop,nop,TS val 1710727633 ecr 1810815756], length 8949
17:37:39.072408 IP 10.15.128.194.48274 > 10.15.47.72.5901: Flags [.], ack 2344998, win 367, options [no
p,nop,TS val 1810815759 ecr 1710727631], length 0
17:37:39.073318 IP 10.15.47.72.5901 > 10.15.128.194.48274: Flags [.], seq 2344998:2353947, ack 1050, wi
n 457, options [nop,nop,TS val 1710727634 ecr 1810815759], length 8949
17:37:39.074757 IP 10.15.47.72.5901 > 10.15.128.194.48274: Flags [.], seq 2353947:2362896, ack 1050, wi
n 457, options [nop,nop,TS val 1710727635 ecr 1810815759], length 8949
17:37:39.074985 IP 10.15.128.194.48274 > 10.15.47.72.5901: Flags [.], ack 2362896, win 415, options [no
p,nop,TS val 1810815761 ecr 1710727634], length 0
17:37:39.077232 IP 10.15.47.72.5901 > 10.15.128.194.48274: Flags [.], seq 2362896:2371845, ack 1050, wi
n 457, options [nop,nop,TS val 1710727638 ecr 1810815761], length 8949
17:37:39.078478 IP 10.15.47.72.5901 > 10.15.128.194.48274: Flags [.], seq 2371845:2380794, ack 1050, wi
n 457, options [nop,nop,TS val 1710727639 ecr 1810815761], length 8949
17:37:39.078618 IP 10.15.128.194.48274 > 10.15.47.72.5901: Flags [.], ack 2380794, win 415, options [no
p,nop,TS val 1810815765 ecr 1710727638], length 0
17:37:39.079690 IP 10.15.47.72.5901 > 10.15.128.194.48274: Flags [.], seq 2380794:2389743, ack 1050, wi
n 457, options [nop,nop,TS val 1710727640 ecr 1810815765], length 8949
```

Set up Environment

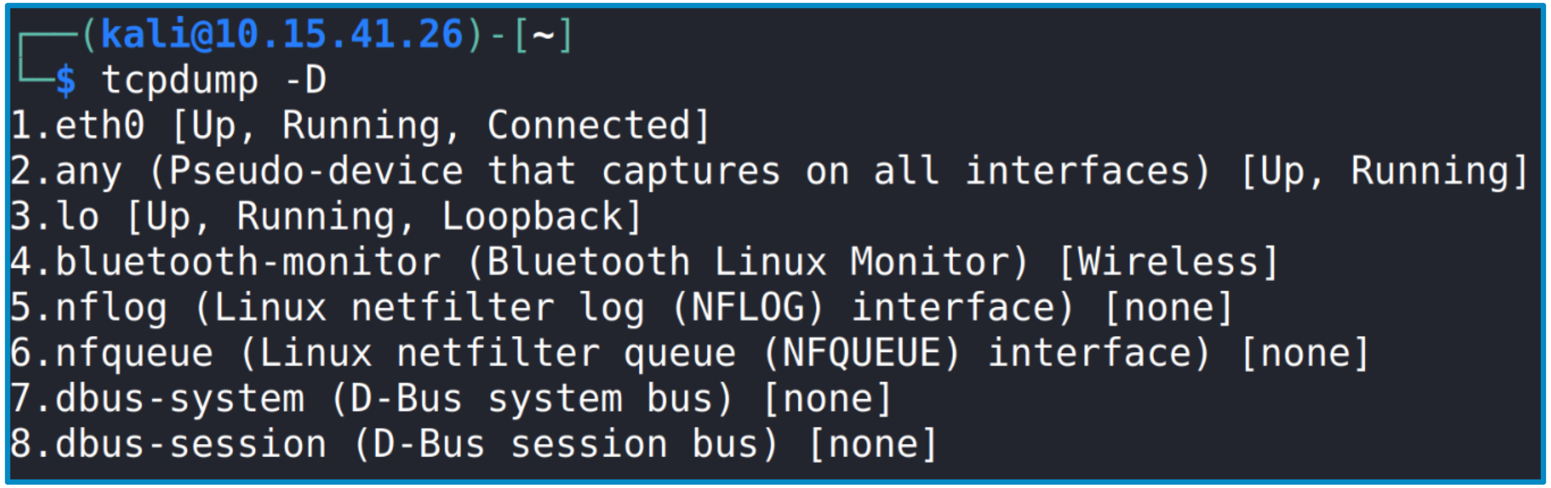
- Log into your range
- Open the Kali Linux Environment
  - You should be on your Kali Linux Desktop
  - Open a new Terminal session

Find Your Network Interface

- Use the following command to find all the available network interfaces

  `tcpdump -D`

- Your ethernet port should be eth0 (or similar) and is probably the first option
- Write this down, you will need to use this network interface throughout the lab



```
┌──(kali@10.15.41.26)-[~]
└─$ 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]
```

Capture Packets!

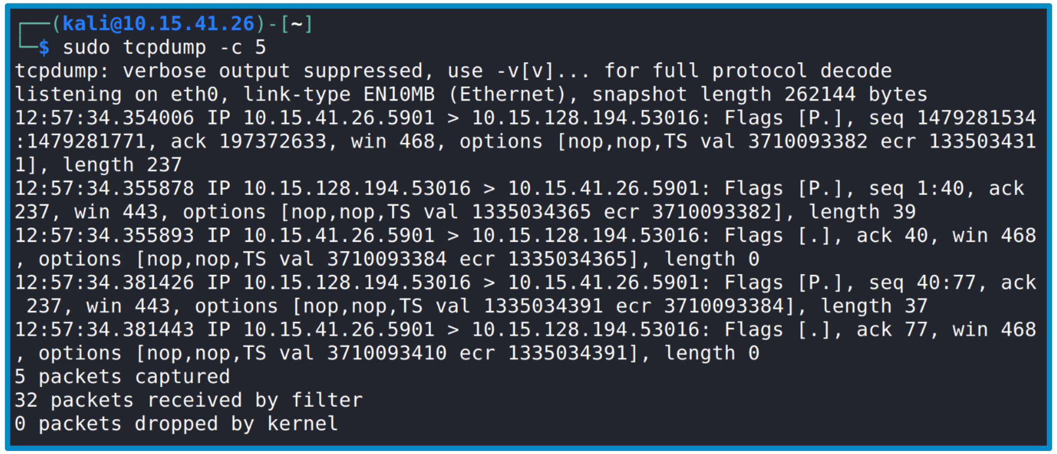
- To capture packets, use the following command:

  `sudo tcpdump -i eth0`

  - Here, i stands for interface
  - Thus, the command is run tcpdump on the interface of the network you specify
- Press CTRL+C to stop capturing packets
- To only capture 5 packets, use the following:

  `sudo tcpdump -c 5`

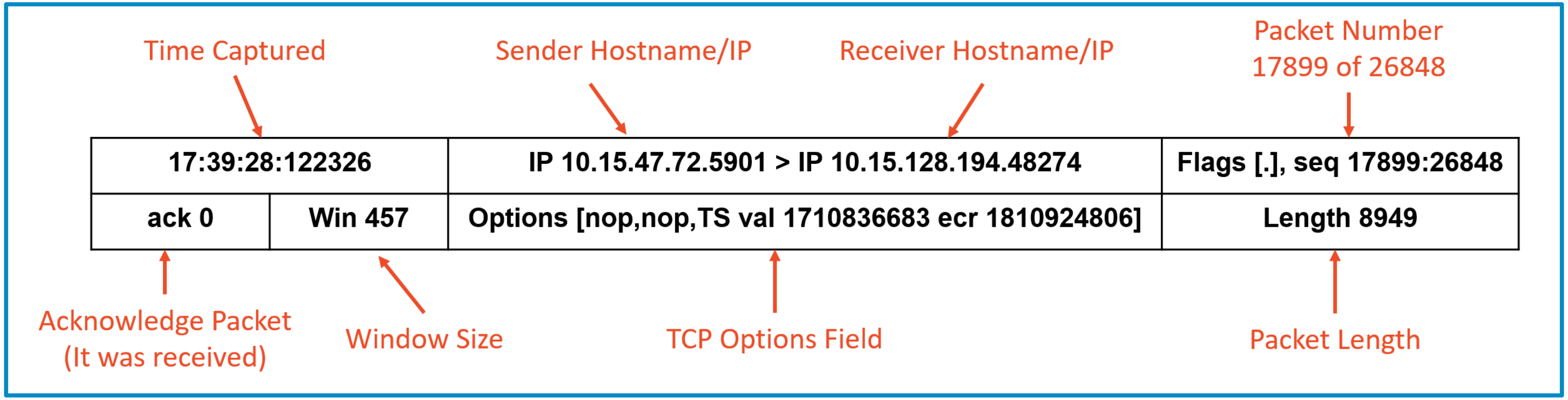
  - **`-c`** stands for *count*
  - tcpdump runs for a count of 5 times



```
┌──(kali@10.15.41.26)-[~]
└─$ sudo tcpdump -c 5
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:57:34.354006 IP 10.15.41.26.5901 > 10.15.128.194.53016: Flags [P.], seq 1479281534
:1479281771, ack 197372633, win 468, options [nop,nop,TS val 3710093382 ecr 133503431
1], length 237
12:57:34.355878 IP 10.15.128.194.53016 > 10.15.41.26.5901: Flags [P.], seq 1:40, ack
237, win 443, options [nop,nop,TS val 1335034365 ecr 3710093382], length 39
12:57:34.355893 IP 10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], ack 40, win 468
, options [nop,nop,TS val 3710093384 ecr 1335034365], length 0
12:57:34.381426 IP 10.15.128.194.53016 > 10.15.41.26.5901: Flags [P.], seq 40:77, ack
 237, win 443, options [nop,nop,TS val 1335034391 ecr 3710093384], length 37
12:57:34.381443 IP 10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], ack 77, win 468
, options [nop,nop,TS val 3710093410 ecr 1335034391], length 0
5 packets captured
32 packets received by filter
0 packets dropped by kernel
```

Contents of a Packet

- Take a look at one single packet and explore what it contains



Time Captured

Sender Hostname/IP

Receiver Hostname/IP

Packet Number 17899 of 26848

<table>
<tr><td colspan="2">17:39:28:122326</td><td>IP 10.15.47.72.5901 > IP 10.15.128.194.48274</td><td>Flags [.], seq 17899:26848</td></tr>
<tr><td>ack 0</td><td>Win 457</td><td>Options [nop,nop,TS val 1710836683 ecr 1810924806]</td><td>Length 8949</td></tr>
</table>

Acknowledge Packet (It was received)

Window Size

TCP Options Field

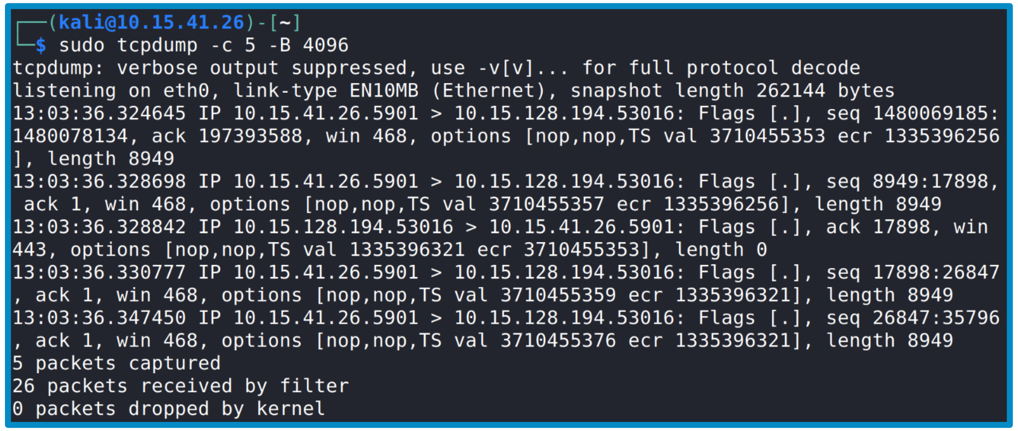
Packet Length

Reduce Packets Dropped

- What if you want to capture more packets? (e.g. decrease the number of packets dropped)
- Try the following command:

  `sudo tcpdump -c 5 -B 4096`

  - **`-B 4096`** stands for a *buffer* of 4096, thus reducing the number of packets dropped
- How many fewer packets were dropped when using this larger buffer?
  - What if you go higher?



```
┌──(kali@10.15.41.26)-[~]
└─$ sudo tcpdump -c 5 -B 4096
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:03:36.324645 IP 10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], seq 1480069185:
1480078134, ack 197393588, win 468, options [nop,nop,TS val 3710455353 ecr 1335396256
], length 8949
13:03:36.328698 IP 10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], seq 8949:17898,
 ack 1, win 468, options [nop,nop,TS val 3710455357 ecr 1335396256], length 8949
13:03:36.328842 IP 10.15.128.194.53016 > 10.15.41.26.5901: Flags [.], ack 17898, win
443, options [nop,nop,TS val 1335396321 ecr 3710455353], length 0
13:03:36.330777 IP 10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], seq 17898:26847
, ack 1, win 468, options [nop,nop,TS val 3710455359 ecr 1335396321], length 8949
13:03:36.347450 IP 10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], seq 26847:35796
, ack 1, win 468, options [nop,nop,TS val 3710455376 ecr 1335396321], length 8949
5 packets captured
26 packets received by filter
0 packets dropped by kernel
```

Clean-up the Output

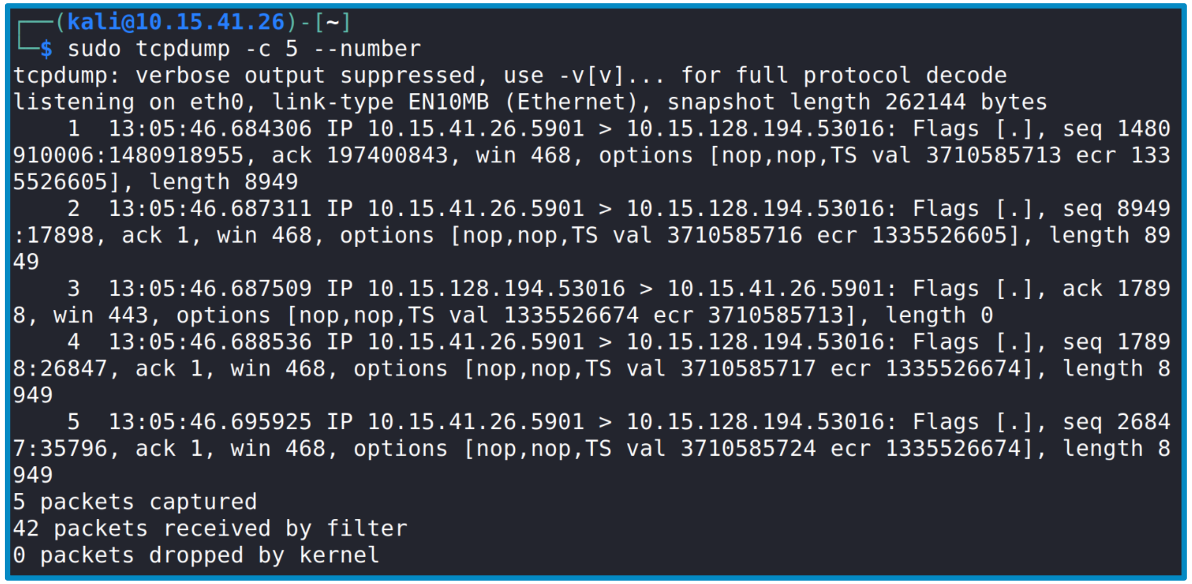
- To number the packets, use the `--number` option:

  `sudo tcpdump -c 5 --number`

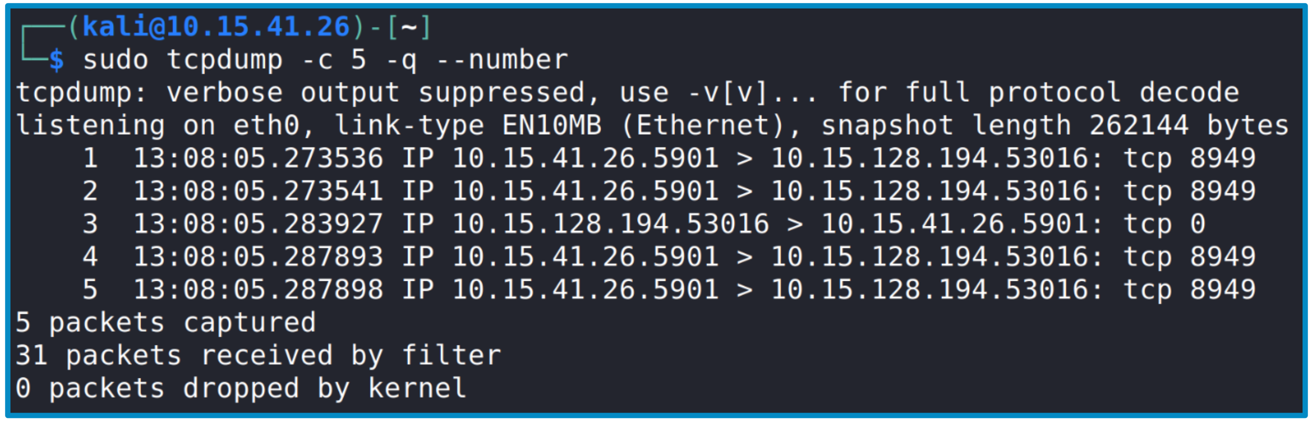
- To simplify the output, use the `-q` option:

  `sudo tcpdump -c 5 -q --number`

  - Here, `-q` stands for *quiet* output



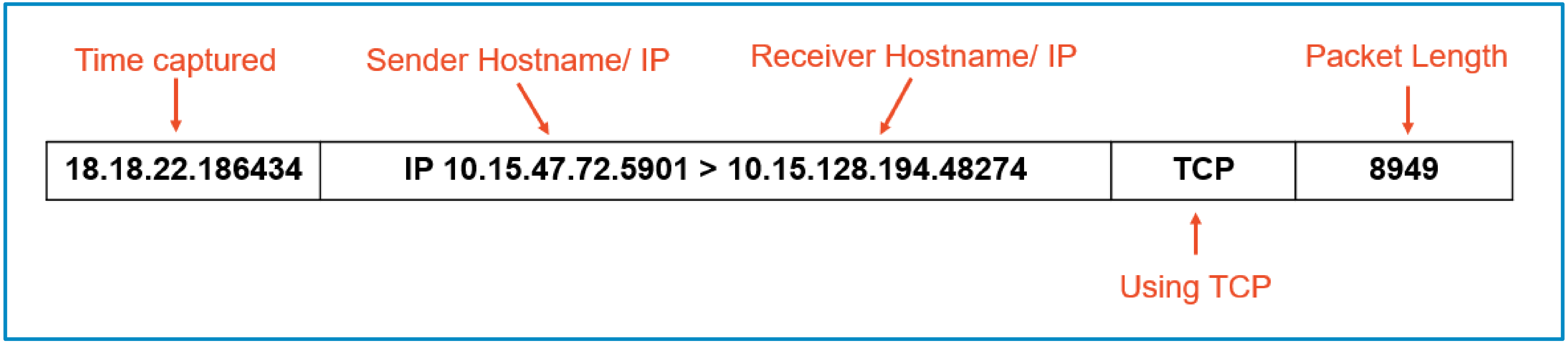
```
┌──(kali@10.15.41.26)-[~]
└─$ sudo tcpdump -c 5 --number
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
    1  13:05:46.684306 IP 10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], seq 1480
910006:1480918955, ack 197400843, win 468, options [nop,nop,TS val 3710585713 ecr 133
5526605], length 8949
    2  13:05:46.687311 IP 10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], seq 8949
:17898, ack 1, win 468, options [nop,nop,TS val 3710585716 ecr 1335526605], length 89
49
    3  13:05:46.687509 IP 10.15.128.194.53016 > 10.15.41.26.5901: Flags [.], ack 1789
8, win 443, options [nop,nop,TS val 1335526674 ecr 3710585713], length 0
    4  13:05:46.688536 IP 10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], seq 1789
8:26847, ack 1, win 468, options [nop,nop,TS val 3710585717 ecr 1335526674], length 8
949
    5  13:05:46.695925 IP 10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], seq 2684
7:35796, ack 1, win 468, options [nop,nop,TS val 3710585724 ecr 1335526674], length 8
949
5 packets captured
42 packets received by filter
0 packets dropped by kernel
```



```
┌──(kali@10.15.41.26)-[~]
└─$ sudo tcpdump -c 5 -q --number
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
    1  13:08:05.273536 IP 10.15.41.26.5901 > 10.15.128.194.53016: tcp 8949
    2  13:08:05.273541 IP 10.15.41.26.5901 > 10.15.128.194.53016: tcp 8949
    3  13:08:05.283927 IP 10.15.128.194.53016 > 10.15.41.26.5901: tcp 0
    4  13:08:05.287893 IP 10.15.41.26.5901 > 10.15.128.194.53016: tcp 8949
    5  13:08:05.287898 IP 10.15.41.26.5901 > 10.15.128.194.53016: tcp 8949
5 packets captured
31 packets received by filter
0 packets dropped by kernel
```

Contents of a “Quiet” Packet

- Let’s break down one of these quiet packets!
  - Notice how much less information is presented.



Time captured

Sender Hostname/ IP

Receiver Hostname/ IP

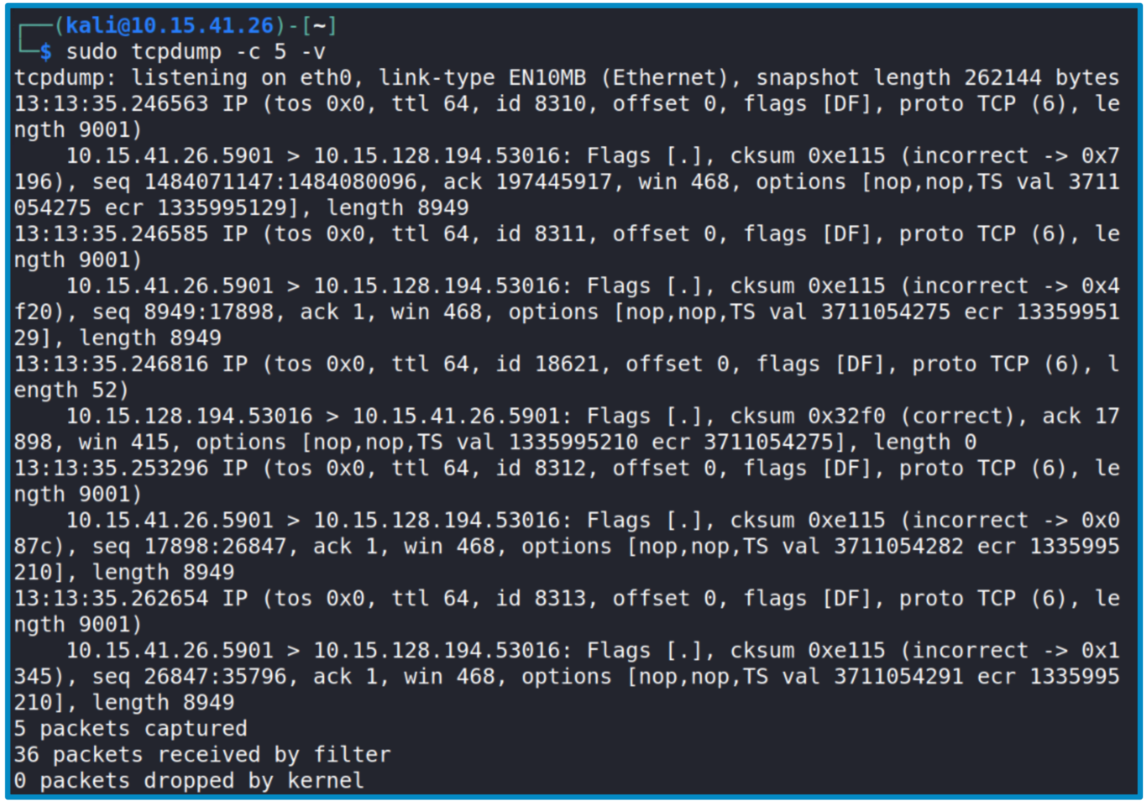
Packet Length

18.18.22.186434	IP 10.15.47.72.5901 > 10.15.128.194.48274	TCP	8949

Using TCP

Expand the Output

- To expand the output, use the **-v** option:
  - **`sudo tcpdump -c 5 -v`**
  - **`-v`** stands for *verbose*



```
┌──(kali@10.15.41.26)-[~]
└─$ sudo tcpdump -c 5 -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:13:35.246563 IP (tos 0x0, ttl 64, id 8310, offset 0, flags [DF], proto TCP (6), le
ngth 9001)
    10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], cksum 0xe115 (incorrect -> 0x7
196), seq 1484071147:1484080096, ack 197445917, win 468, options [nop,nop,TS val 3711
054275 ecr 1335995129], length 8949
13:13:35.246585 IP (tos 0x0, ttl 64, id 8311, offset 0, flags [DF], proto TCP (6), le
ngth 9001)
    10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], cksum 0xe115 (incorrect -> 0x4
f20), seq 8949:17898, ack 1, win 468, options [nop,nop,TS val 3711054275 ecr 13359951
29], length 8949
13:13:35.246816 IP (tos 0x0, ttl 64, id 18621, offset 0, flags [DF], proto TCP (6), l
ength 52)
    10.15.128.194.53016 > 10.15.41.26.5901: Flags [.], cksum 0x32f0 (correct), ack 17
898, win 415, options [nop,nop,TS val 1335995210 ecr 3711054275], length 0
13:13:35.253296 IP (tos 0x0, ttl 64, id 8312, offset 0, flags [DF], proto TCP (6), le
ngth 9001)
    10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], cksum 0xe115 (incorrect -> 0x0
87c), seq 17898:26847, ack 1, win 468, options [nop,nop,TS val 3711054282 ecr 1335995
210], length 8949
13:13:35.262654 IP (tos 0x0, ttl 64, id 8313, offset 0, flags [DF], proto TCP (6), le
ngth 9001)
    10.15.41.26.5901 > 10.15.128.194.53016: Flags [.], cksum 0xe115 (incorrect -> 0x1
345), seq 26847:35796, ack 1, win 468, options [nop,nop,TS val 3711054291 ecr 1335995
210], length 8949
5 packets captured
36 packets received by filter
0 packets dropped by kernel
```

Capture as a `.txt` File

- First, navigate to the Desktop directory using the following command:

  `cd Desktop`

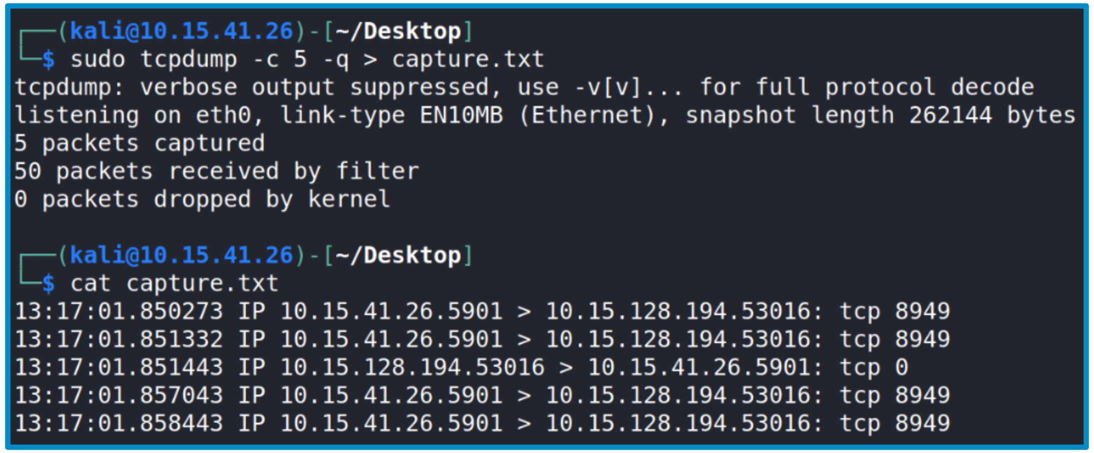
- Now, capture the packets as a txt file use the > redirection tool:

  `sudo tcpdump -c 5 -q > capture.txt`

  - `> capture.txt` is *redirecting* the output from the screen to a file named capture.txt

- To read the file, use the following command:

  `cat capture.txt`



```
┌──(kali@10.15.41.26)-[~/Desktop]
└─$ sudo tcpdump -c 5 -q > capture.txt
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
5 packets captured
50 packets received by filter
0 packets dropped by kernel

┌──(kali@10.15.41.26)-[~/Desktop]
└─$ cat capture.txt
13:17:01.850273 IP 10.15.41.26.5901 > 10.15.128.194.53016: tcp 8949
13:17:01.851332 IP 10.15.41.26.5901 > 10.15.128.194.53016: tcp 8949
13:17:01.851443 IP 10.15.128.194.53016 > 10.15.41.26.5901: tcp 0
13:17:01.857043 IP 10.15.41.26.5901 > 10.15.128.194.53016: tcp 8949
13:17:01.858443 IP 10.15.41.26.5901 > 10.15.128.194.53016: tcp 8949
```