tcpdump Command in Linux with Examples

manav014

tcpdump is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux. It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system. It is many times used as a security tool as well. It saves the captured information in a pcap file, these pcap files can then be opened through Wireshark or through the command tool itself.

Installing tcpdump tool in Linux

Many Operating Systems have tcpdump command pre-installed but to install it, use the following commands. **For RedHat based linux OS**

```
yum install tcpdump
```

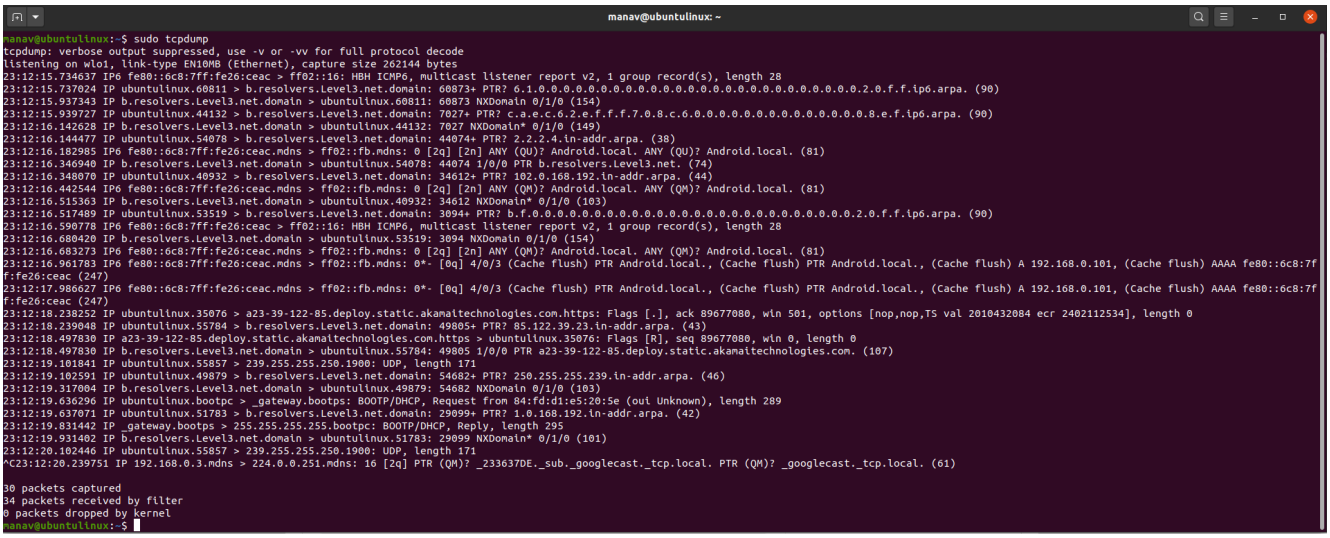
For Ubuntu/Debian OS

```
apt install tcpdump
```

Working with tcpdump command

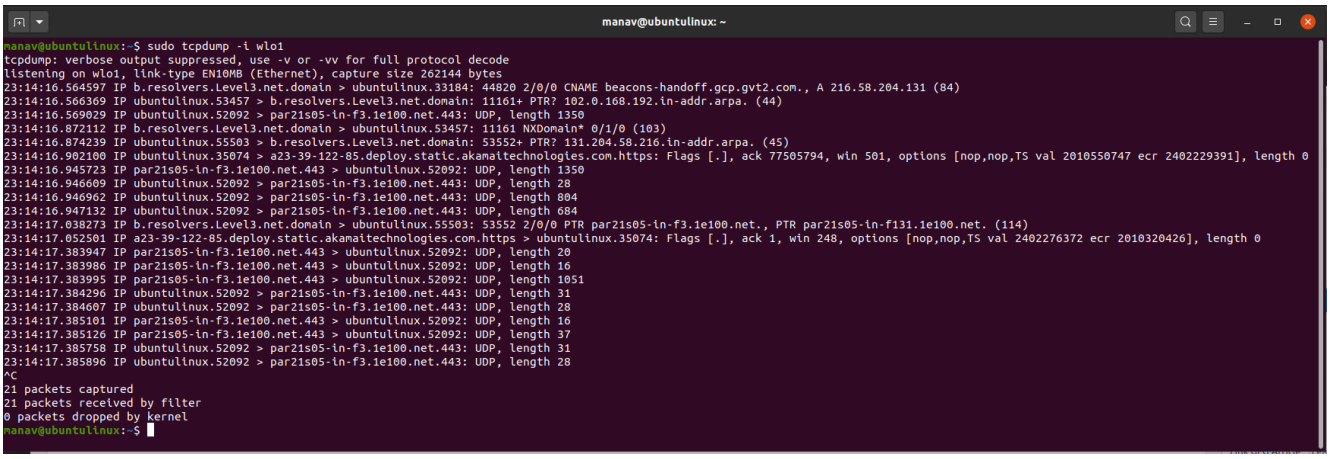
1. To capture the packets of current network interface

```
sudo tcpdump
```



This will capture the packets from the current interface of the network through which the system is connected to the internet. **2.** To capture packets from a specific network interface

```
sudo tcpdump -i wlo1
```



This command will now capture the packets from wlo1 network interface. **3.** To capture specific number of packets

```
sudo tcpdump -c 4 -i wlo1
```

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ sudo tcpdump -c 4 -i wlo1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
23:15:20.257784 IP 192.168.0.3.mdns > 224.0.0.251.mdns: 25 [2q] PTR (QM)? _233637DE._sub._googlecast._tcp.local. PTR (QM)? _googlecast._tcp.local. (61)
23:15:20.259572 IP ubuntulinux.50749 > b.resolvers.Level3.net.domain: 37963+ PTR? 251.0.0.224.in-addr.arpa. (42)
23:15:20.461763 IP b.resolvers.Level3.net.domain > ubuntulinux.50749: 37963 NXDomain 0/1/0 (99)
23:15:20.463051 IP ubuntulinux.54591 > b.resolvers.Level3.net.domain: 7530+ PTR? 3.0.168.192.in-addr.arpa. (42)
4 packets captured
7 packets received by filter
0 packets dropped by kernel
manav@ubuntulinux:~$
```

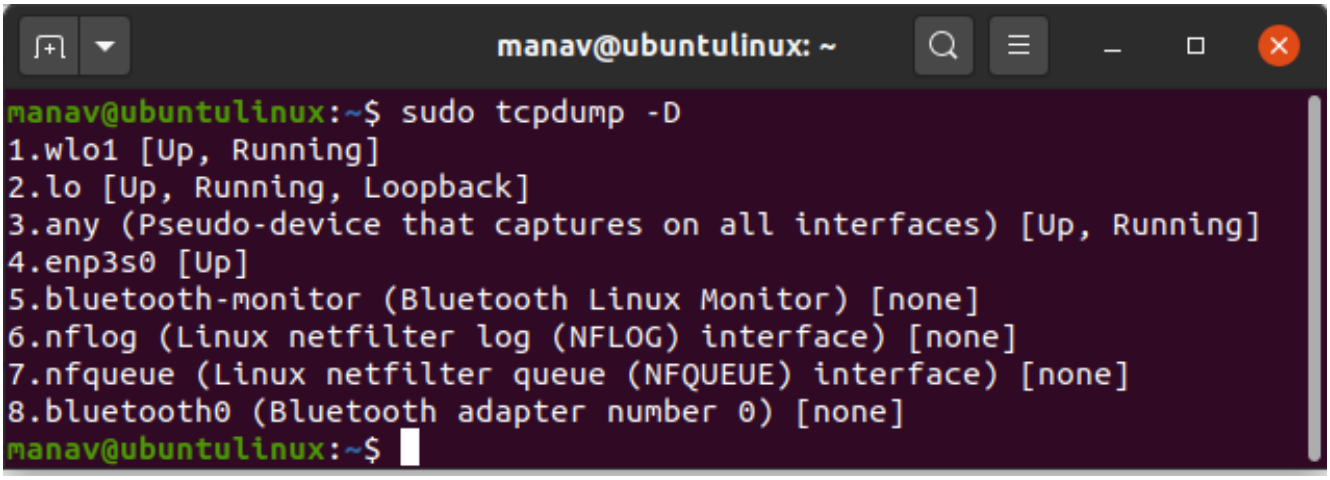
This command will capture only 4 packets from the wlo1 interface. **4.** To print captured packets in ASCII format

```
sudo tcpdump -A -i wlo1
```

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ sudo tcpdump -A -i wlo1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
23:16:40.134239 IP ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https > ubuntulinux.49890: Flags [P.], seq 3549039789:3549039820, ack 1122930302, win 282, options [nop,nop,TS val 1076801243 ecr 2330761273],
length 31
E..S.7@.%...#..I...f........B..~.....
@......9......T....q...3C...'k.k.....
23:16:40.134282 IP ubuntulinux.49890 > ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https: Flags [.], ack 31, win 501, options [nop,nop,TS val 2330766296 ecr 1076801243], length 0
E..4    .@.@.3....f#..!....B..~.............
....@...
23:16:40.134317 IP ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https > ubuntulinux.49890: Flags [F.], seq 31, ack 1, win 282, options [nop,nop,TS val 1076801243 ecr 2330761273], length 0
E..4.8@.%...#..!...f........B..~.....@.....
@......9
23:16:40.135955 IP ubuntulinux.51470 > b.resolvers.Level3.net.domain: 30561+ PTR? 102.0.168.192.in-addr.arpa. (44)
E..H.5@.@..]...f.......5.4.Wwa...........102.0.168.192.in-addr.arpa.....
23:16:40.178214 IP ubuntulinux.49890 > ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https: Flags [.], ack 32, win 501, options [nop,nop,TS val 2330766340 ecr 1076801243], length 0
E..4    .@.@.3....f#..!....B..~.............
....@...
23:16:40.294106 IP 192.168.0.3.mdns > 224.0.0.251.mdns: 29 [2q] PTR (QM)? _233637DE._sub._googlecast._tcp.local. PTR (QM)? _googlecast._tcp.local. (61)
E..Y..@.................E3............        _233637DE._sub._googlecast._tcp.local..........
23:16:40.334162 IP b.resolvers.Level3.net.domain > ubuntulinux.51470: 30561 NXDomain* 0/1/0 (103)
E ....@.5.~8.......f.5...o#     wa...........102.0.168.192.in-addr.arpa............*0./        localhost..nobody.invalid............. :...*0
23:16:40.337133 IP ubuntulinux.50547 > b.resolvers.Level3.net.domain: 61778+ PTR? 251.0.0.224.in-addr.arpa. (42)
E..F.W@.@..=...f.....s.5.2.U.R...........251.0.0.224.in-addr.arpa.....
23:16:40.538948 IP b.resolvers.Level3.net.domain > ubuntulinux.50547: 61778 NXDomain 0/1/0 (99)
E ....@.5.~<........f.5.s.k3..R...........251.0.0.224.in-addr.arpa............
h..sns.dns.icann.org..noc.:xYZ.... .....        :.....
23:16:40.540226 IP ubuntulinux.58407 > b.resolvers.Level3.net.domain: 39497+ PTR? 3.0.168.192.in-addr.arpa. (42)
E..F.f@.@.....f.....'.5.2.U.I...........3.0.168.192.in-addr.arpa.....
23:16:40.743758 IP b.resolvers.Level3.net.domain > ubuntulinux.58407: 39497 NXDomain* 0/1/0 (101)
E ....@.5.~:.......f.5.'.m.>.I...........3.0.168.192.in-addr.arpa............*0./      localhost..nobody.invalid............. :...*0
^C
11 packets captured
11 packets received by filter
0 packets dropped by kernel
manav@ubuntulinux:~$
```

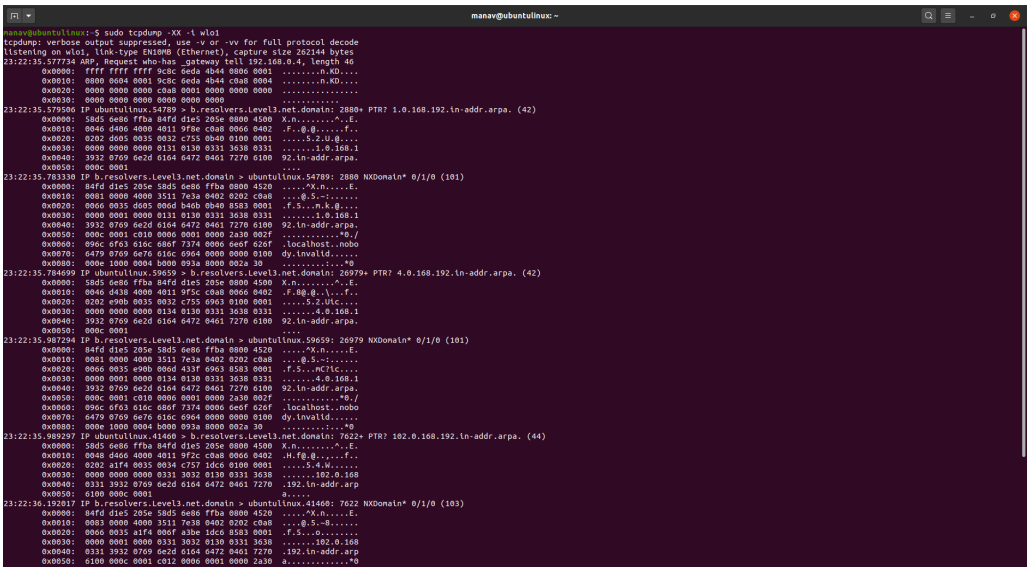
This command will now print the captured packets from wlo1 to ASCII value. **5.** To display all available interfaces

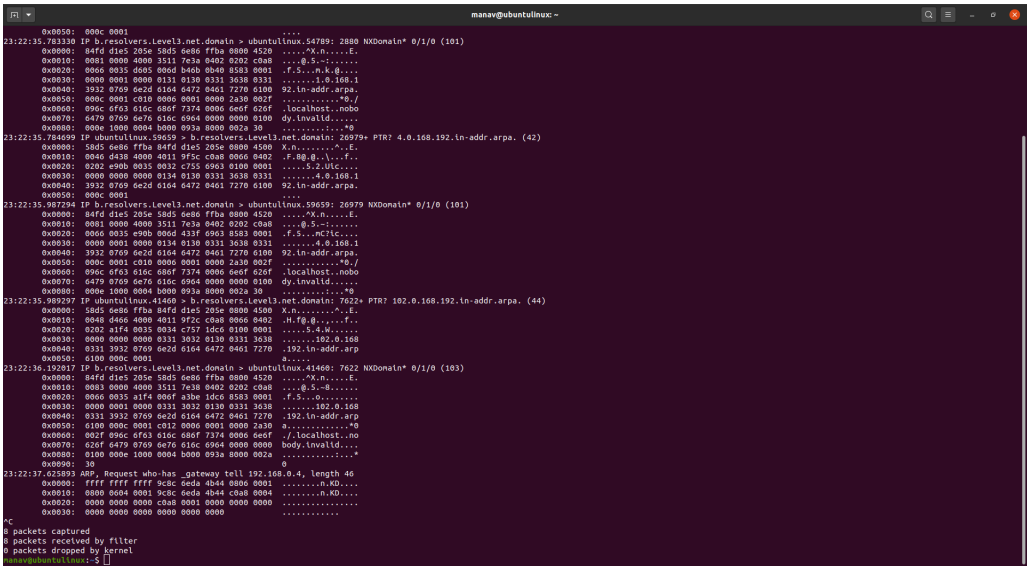
```
sudo tcpdump -D
```



This command will display all the interfaces that are available in the system. **6.** To display packets in HEX and ASCII values

```
sudo tcpdump -XX -i wlo1
```

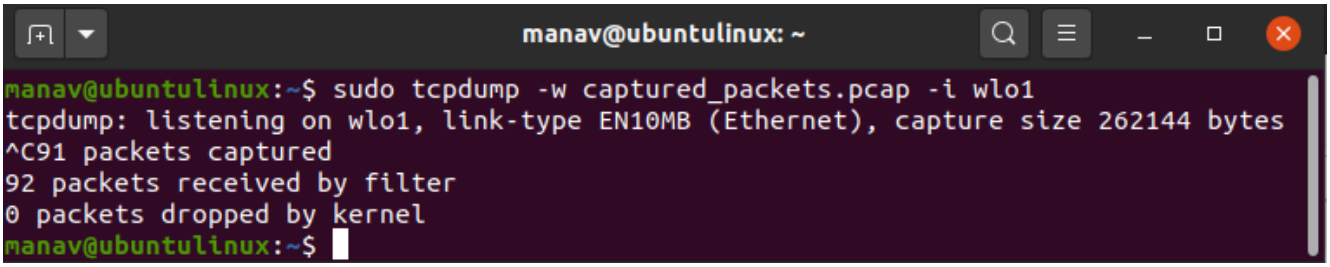




This command will

now print the packets captured from the wlo1 interface in the HEX and ASCII values. **7.** To save captured packets into a file

```
sudo tcpdump -w captured_packets.pcap -i wlo1
```

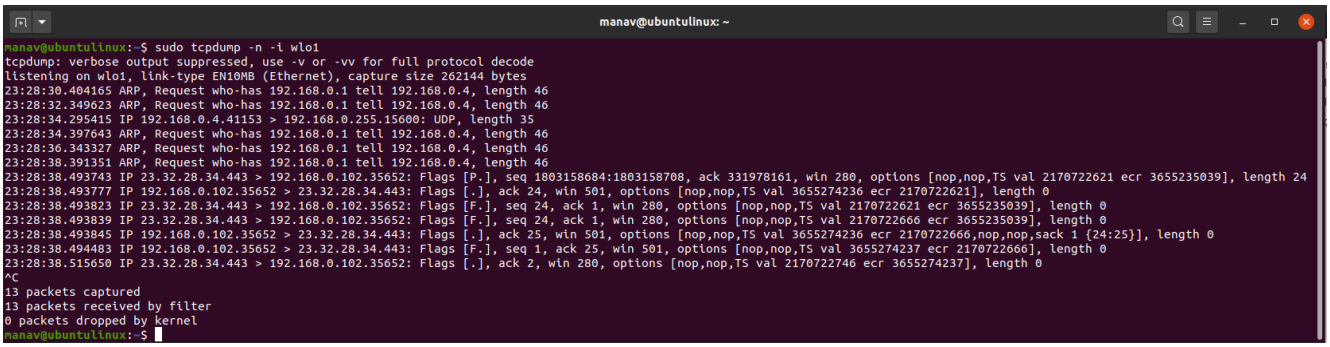


This command will now output all the captures packets in a file named as captured_packets.pcap. **8.** To read captured packets from a file

```
sudo tcpdump -r captured_packets.pcap
```

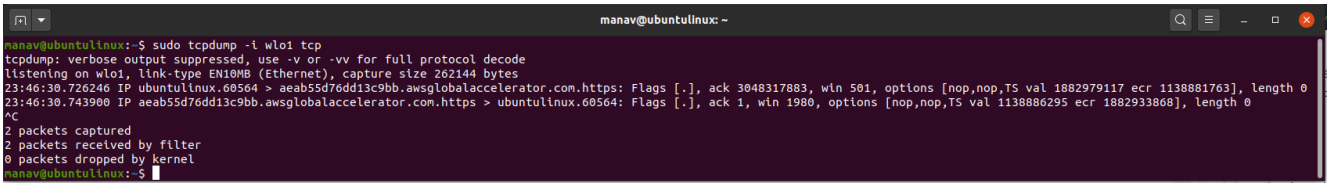
This command will now read the captured packets from the captured_packets.pcap file. **9.** To capture packets with ip address

```
sudo tcpdump -n -i wlo1
```



This command will now capture the packets with IP addresses. **10.** To capture only TCP packets

```
sudo tcpdump -i wlo1 tcp
```



This command will now capture only TCP packets from wlo1.

Last Updated : 14 Sep, 2022

6

Similar Reads

1. Ccat – Colorize Cat Command Output command in Linux with Examples
2. 'IPCS' command in Linux with examples
3. select command in Linux with examples
4. Sed Command in Linux/Unix with examples

5. ZIP command in Linux with examples
6. SORT command in Linux/Unix with examples
7. Cat command in Linux with examples
8. Head command in Linux with examples
9. Tail command in Linux with examples
10. wc command in Linux with examples

Next

traceroute command in Linux with Examples

Article Contributed By :

manav014
@manav014

Vote for difficulty

Current difficulty : Basic

Easy | Normal | Medium | Hard | Expert

Improved By : rohantimalsina

Article Tags : linux-command, Linux-networking-commands, Linux-Unix

Improve Article | Report Issue