tcpdump is a data-network packet analyzer computer program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

Tcpdump uses libpcap library to capture the network packets & is available on almost all Linux/Unix flavors.

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
```

1. To capture the packets of current network interface

```
sudo tcpdump
```

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
23:12:15.734637 IP6 fe80::6c8:7ff:fe26:ceac > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
23:12:15.737024 IP ubuntulinux.60811 > b.resolvers.Level3.net.domain: 60873+ PTR? 6.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
23:12:15.937343 IP b.resolvers.Level3.net.domain > ubuntulinux.60811: 60873 NXDomain 0/1/0 (154)
23:12:15.939727 IP ubuntulinux.44132 > b.resolvers.Level3.net.domain: 7027+ PTR? c.a.e.c.6.2.e.f.f.f.7.0.8.c.6.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
23:12:16.142628 IP b.resolvers.Level3.net.domain > ubuntulinux.44132: 7027 NXDomain* 0/1/0 (149)
23:12:16.144477 IP ubuntulinux.54078 > b.resolvers.Level3.net.domain: 44074+ PTR? 2.2.2.4.in-addr.arpa. (38)
23:12:16.182985 IP6 fe80::6c8:7ff:fe26:ceac.mdns > ff02::fb.mdns: 0 [2q] [2n] ANY (QU)? Android.local. ANY (QU)? Android.local. (81)
23:12:16.346940 IP b.resolvers.Level3.net.domain > ubuntulinux.54078: 44074 1/0/0 PTR b.resolvers.Level3.net. (74)
23:12:16.348070 IP ubuntulinux.40932 > b.resolvers.Level3.net.domain: 34612+ PTR? 102.0.168.192.in-addr.arpa. (44)
23:12:16.442544 IP6 fe80::6c8:7ff:fe26:ceac.mdns > ff02::fb.mdns: 0 [2q] [2n] ANY (QM)? Android.local. ANY (QM)? Android.local. (81)
23:12:16.515363 IP b.resolvers.Level3.net.domain > ubuntulinux.40932: 34612 NXDomain* 0/1/0 (103)
23:12:16.517489 IP ubuntulinux.53519 > b.resolvers.Level3.net.domain: 3094+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
23:12:16.590778 IP6 fe80::6c8:7ff:fe26:ceac > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
23:12:16.680420 IP b.resolvers.Level3.net.domain > ubuntulinux.53519: 3094 NXDomain 0/1/0 (154)
23:12:16.683273 IP6 fe80::6c8:7ff:fe26:ceac.mdns > ff02::fb.mdns: 0 [2q] [2n] ANY (QM)? Android.local. ANY (QM)? Android.local. (81)
23:12:16.961783 IP6 fe80::6c8:7ff:fe26:ceac.mdns > ff02::fb.mdns: 0*- [0q] 4/0/3 (Cache flush) PTR Android.local., (Cache flush) PTR Android.local., (Cache flush) A 192.168.0.101, (Cache flush) AAAA fe80::6c8:7f
f:fe26:ceac (247)
23:12:17.986627 IP6 fe80::6c8:7ff:fe26:ceac.mdns > ff02::fb.mdns: 0*- [0q] 4/0/3 (Cache flush) PTR Android.local., (Cache flush) PTR Android.local., (Cache flush) A 192.168.0.101, (Cache flush) AAAA fe80::6c8:7f
f:fe26:ceac (247)
23:12:18.238252 IP ubuntulinux.35076 > a23-39-122-85.deploy.static.akamaitechnologies.com.https: Flags [.], ack 89677080, win 501, options [nop,nop,TS val 2010432084 ecr 2402112534], length 0
23:12:18.239048 IP ubuntulinux.55784 > b.resolvers.Level3.net.domain: 49805+ PTR? 85.122.39.23.in-addr.arpa. (43)
23:12:18.497830 IP a23-39-122-85.deploy.static.akamaitechnologies.com.https > ubuntulinux.35076: Flags [R], seq 89677080, win 0, length 0
23:12:18.497830 IP b.resolvers.Level3.net.domain > ubuntulinux.55784: 49805 1/0/0 PTR a23-39-122-85.deploy.static.akamaitechnologies.com. (107)
23:12:19.101841 IP ubuntulinux.55857 > 239.255.255.250.1900: UDP, length 171
23:12:19.102591 IP ubuntulinux.49879 > b.resolvers.Level3.net.domain: 54682+ PTR? 250.255.255.239.in-addr.arpa. (46)
23:12:19.317004 IP b.resolvers.Level3.net.domain > ubuntulinux.49879: 54682 NXDomain 0/1/0 (103)
23:12:19.636296 IP ubuntulinux.bootpc > _gateway.bootps: BOOTP/DHCP, Request from 84:fd:d1:e5:20:5e (oui Unknown), length 289
23:12:19.637071 IP ubuntulinux.51783 > b.resolvers.Level3.net.domain: 29099+ PTR? 1.0.168.192.in-addr.arpa. (42)
23:12:19.831442 IP _gateway.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply, length 295
23:12:19.931402 IP b.resolvers.Level3.net.domain > ubuntulinux.51783: 29099 NXDomain* 0/1/0 (101)
23:12:20.102446 IP ubuntulinux.55857 > 239.255.255.250.1900: UDP, length 171
^C23:12:20.239751 IP 192.168.0.3.mdns > 224.0.0.251.mdns: 16 [2q] PTR (QM)? _233637DE._sub._googlecast._tcp.local. PTR (QM)? _googlecast._tcp.local. (61)

30 packets captured
34 packets received by filter
0 packets dropped by kernel
manav@ubuntulinux:~$
```

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
```

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ sudo tcpdump -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
23:14:16.564597 IP b.resolvers.Level3.net.domain > ubuntulinux.33184: 44820 2/0/0 CNAME beacons-handoff.gcp.gvt2.com., A 216.58.204.131 (84)
23:14:16.566369 IP ubuntulinux.53457 > b.resolvers.Level3.net.domain: 11161+ PTR? 102.0.168.192.in-addr.arpa. (44)
23:14:16.569029 IP ubuntulinux.52092 > par21s05-in-f3.1e100.net.443: UDP, length 1350
23:14:16.872112 IP b.resolvers.Level3.net.domain > ubuntulinux.53457: 11161 NXDomain* 0/1/0 (103)
23:14:16.874239 IP ubuntulinux.55503 > b.resolvers.Level3.net.domain: 53552+ PTR? 131.204.58.216.in-addr.arpa. (45)
23:14:16.902100 IP ubuntulinux.35074 > a23-39-122-85.deploy.static.akamaitechnologies.com.https: Flags [.], ack 77505794, win 501, options [nop,nop,TS val 2010550747 ecr 2402229391], length 0
23:14:16.945723 IP par21s05-in-f3.1e100.net.443 > ubuntulinux.52092: UDP, length 1350
23:14:16.946609 IP ubuntulinux.52092 > par21s05-in-f3.1e100.net.443: UDP, length 28
23:14:16.946962 IP ubuntulinux.52092 > par21s05-in-f3.1e100.net.443: UDP, length 804
23:14:16.947132 IP ubuntulinux.52092 > par21s05-in-f3.1e100.net.443: UDP, length 684
23:14:17.038273 IP b.resolvers.Level3.net.domain > ubuntulinux.55503: 53552 2/0/0 PTR par21s05-in-f3.1e100.net., PTR par21s05-in-f131.1e100.net. (114)
23:14:17.052501 IP a23-39-122-85.deploy.static.akamaitechnologies.com.https > ubuntulinux.35074: Flags [.], ack 1, win 248, options [nop,nop,TS val 2402276372 ecr 2010320426], length 0
23:14:17.383947 IP par21s05-in-f3.1e100.net.443 > ubuntulinux.52092: UDP, length 20
23:14:17.383986 IP par21s05-in-f3.1e100.net.443 > ubuntulinux.52092: UDP, length 16
23:14:17.383995 IP par21s05-in-f3.1e100.net.443 > ubuntulinux.52092: UDP, length 1051
23:14:17.384296 IP ubuntulinux.52092 > par21s05-in-f3.1e100.net.443: UDP, length 31
23:14:17.384607 IP ubuntulinux.52092 > par21s05-in-f3.1e100.net.443: UDP, length 28
23:14:17.385101 IP par21s05-in-f3.1e100.net.443 > ubuntulinux.52092: UDP, length 16
23:14:17.385126 IP par21s05-in-f3.1e100.net.443 > ubuntulinux.52092: UDP, length 37
23:14:17.385758 IP ubuntulinux.52092 > par21s05-in-f3.1e100.net.443: UDP, length 31
23:14:17.385896 IP ubuntulinux.52092 > par21s05-in-f3.1e100.net.443: UDP, length 28
^C
21 packets captured
21 packets received by filter
0 packets dropped by kernel
manav@ubuntulinux:~$
```

This command will now capture the packets from wlo1 network interface.

3. To capture specific number of packets

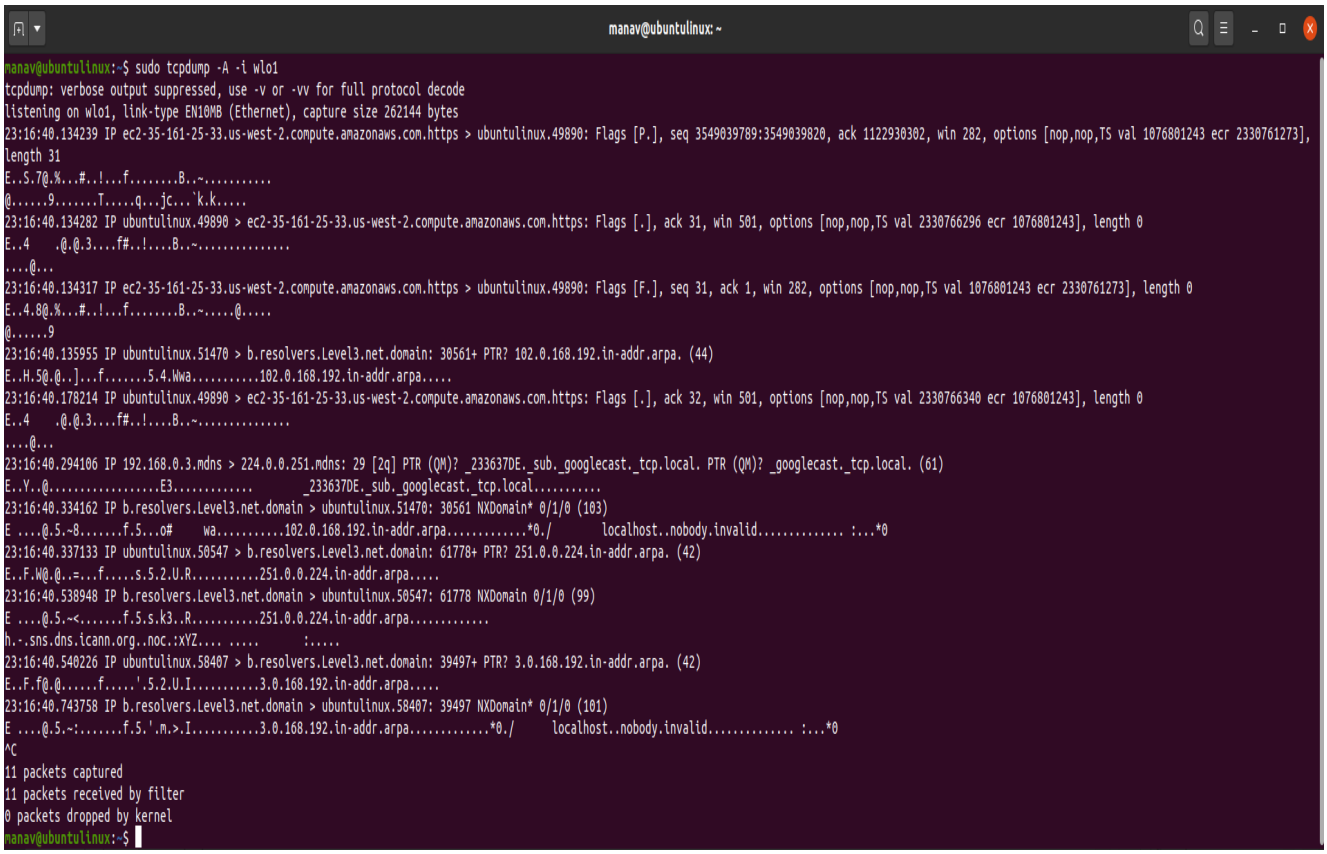
```
sudo tcpdump -c 4 -i wlo1
```

```
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.

To print captured packages 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@.%...#..!...f........B..~...........
@......9.......T.....q...jc...`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
```

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ sudo tcpdump -D
1.wlo1 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.enp3s0 [Up]
5.bluetooth-monitor (Bluetooth Linux Monitor) [none]
6.nflog (Linux netfilter log (NFLOG) interface) [none]
7.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
8.bluetooth0 (Bluetooth adapter number 0) [none]
manav@ubuntulinux:~$
```

this command will display all the interfaces that are available in the system

To capture packets with ip address

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

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ sudo tcpdump -n -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
23:28:30.404165 ARP, Request who-has 192.168.0.1 tell 192.168.0.4, length 46
23:28:32.349623 ARP, Request who-has 192.168.0.1 tell 192.168.0.4, length 46
23:28:34.295415 IP 192.168.0.4.41153 > 192.168.0.255.15600: UDP, length 35
23:28:34.397643 ARP, Request who-has 192.168.0.1 tell 192.168.0.4, length 46
23:28:36.343327 ARP, Request who-has 192.168.0.1 tell 192.168.0.4, length 46
23:28:38.391351 ARP, Request who-has 192.168.0.1 tell 192.168.0.4, length 46
23:28:38.493743 IP 23.32.28.34.443 > 192.168.0.102.35652: Flags [P.], seq 1803158684:1803158708, ack 331978161, win 280, options [nop,nop,TS val 2170722621 ecr 3655235039], length 24
23:28:38.493777 IP 192.168.0.102.35652 > 23.32.28.34.443: Flags [.], ack 24, win 501, options [nop,nop,TS val 3655274236 ecr 2170722621], length 0
23:28:38.493823 IP 23.32.28.34.443 > 192.168.0.102.35652: Flags [F.], seq 24, ack 1, win 280, options [nop,nop,TS val 2170722621 ecr 3655235039], length 0
23:28:38.493839 IP 23.32.28.34.443 > 192.168.0.102.35652: Flags [F.], seq 24, ack 1, win 280, options [nop,nop,TS val 2170722666 ecr 3655235039], length 0
23:28:38.493845 IP 192.168.0.102.35652 > 23.32.28.34.443: Flags [.], ack 25, win 501, options [nop,nop,TS val 3655274236 ecr 2170722666,nop,nop,sack 1 {24:25}], length 0
23:28:38.494483 IP 192.168.0.102.35652 > 23.32.28.34.443: Flags [F.], seq 1, ack 25, win 501, options [nop,nop,TS val 3655274237 ecr 2170722666], length 0
23:28:38.515650 IP 23.32.28.34.443 > 192.168.0.102.35652: Flags [.], ack 2, win 280, options [nop,nop,TS val 2170722746 ecr 3655274237], length 0
^C
13 packets captured
13 packets received by filter
0 packets dropped by kernel
manav@ubuntulinux:~$
```

To capture only TCP packets

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

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ sudo tcpdump -i wlo1 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
23:46:30.726246 IP ubuntulinux.60564 > aeab55d76dd13c9bb.awsglobalaccelerator.com.https: Flags [.], ack 3048317883, win 501, options [nop,nop,TS val 1882979117 ecr 1138881763], length 0
23:46:30.743900 IP aeab55d76dd13c9bb.awsglobalaccelerator.com.https > ubuntulinux.60564: Flags [.], ack 1, win 1980, options [nop,nop,TS val 1138886295 ecr 1882933868], length 0
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
manav@ubuntulinux:~$
```

Get all the packets based on the IP address, whether source or destination or both, using the following command,

```
$ tcpdump host 192.168.1.100
```

To get packets based on source or destination of an IP address, use

```
$ tcpdump src 192.168.1.100
```

```
$ tcpdump dst 192.168.1.100
```

Dumpcap is a network traffic dump tool. It captures packet data from a live network and writes the packets to a file. Dumpcap's native capture file format is pcapng, which is also the format used by Wireshark.

By default, Dumpcap uses the pcap library to capture traffic from the first available network interface and writes the received raw packet data, along with the packets' time stamps into a pcapng file.

https://www.wireshark.org/docs/man-pages/dumpcap.html