



tcpdump Command in Linux with Examples



manav014

[Read](#)[Discuss](#)

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

[illegible]

```
manav@ubuntu19:~$ 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 > ubuntu19linux.33184: 44820 2/0/0 CNAME beacons-handoff.gcp.gvt2.com., A 216.58.204.131 (84)
23:14:16.566369 IP ubuntu19linux.53457 > b.resolvers.Level3.net.domain: 11161+ PTR? 102.0.168.192.in-addr.arpa. (44)
23:14:16.569029 IP ubuntu19linux.52092 > par21s05-lin-f3.1e100.net.443: UDP, length 1350
23:14:16.571112 IP b.resolvers.Level3.net.domain > ubuntu19linux.53457: 11161 NXDomain 0/1/0 (103)
23:14:16.874239 IP ubuntu19linux.55583 > b.resolvers.Level3.net.domain: 53552+ PTR? 131.204.58.216.in-addr.arpa. (45)
23:14:16.902100 IP ubuntu19linux.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-lin-f3.1e100.net.443 > ubuntu19linux.52092: UDP, length 1350
23:14:16.946609 IP ubuntu19linux.52092 > par21s05-lin-f3.1e100.net.443: UDP, length 28
23:14:16.946962 IP ubuntu19linux.52092 > par21s05-lin-f3.1e100.net.443: UDP, length 804
23:14:16.947132 IP ubuntu19linux.52092 > par21s05-lin-f3.1e100.net.443: UDP, length 684
23:14:17.052501 IP a23-39-122-85.deploy.static.akamaitechnologies.com.https > ubuntu19linux.53552: 2/0/0 PTR par21s05-lin-f3.1e100.net., PTR par21s05-lin-f311.1e100.net. (114)
23:14:17.052501 IP a23-39-122-85.deploy.static.akamaitechnologies.com.https > ubuntu19linux.35074: Flags [.] , ack 1, win 248, options [nop,nop,TS val 2402276372 ecr 2010320426], length 0
23:14:17.383947 IP par21s05-lin-f3.1e100.net.443 > ubuntu19linux.52092: UDP, length 20
23:14:17.383986 IP par21s05-lin-f3.1e100.net.443 > ubuntu19linux.52092: UDP, length 16
23:14:17.383995 IP par21s05-lin-f3.1e100.net.443 > ubuntu19linux.52092: UDP, length 1051
23:14:17.384296 IP ubuntu19linux.52092 > par21s05-lin-f3.1e100.net.443: UDP, length 31
23:14:17.384007 IP ubuntu19linux.52092 > par21s05-lin-f3.1e100.net.443: UDP, length 28
23:14:17.385101 IP par21s05-lin-f3.1e100.net.443 > ubuntu19linux.52092: UDP, length 37
23:14:17.385126 IP par21s05-lin-f3.1e100.net.443 > ubuntu19linux.52092: UDP, length 37
23:14:17.385758 IP ubuntu19linux.52092 > par21s05-lin-f3.1e100.net.443: UDP, length 31
23:14:17.385896 IP ubuntu19linux.52092 > par21s05-lin-f3.1e100.net.443: UDP, length 28
^C
21 packets captured
21 packets received by filter
0 packets dropped by kernel
manav@ubuntu19:~$
```

```
manav@ubuntu:~$ 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 ubuntu: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 > ubuntu:50749: 37963 NXDomain 0/1/0 (99)
23:15:20.463051 IP ubuntu: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@ubuntu:~$
```

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@ubuntu:~$ 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 > ubuntu:49890: Flags [P.], seq 3549039789:3549039820, ack 1122930302, win 282, options [nop,nop,TS val 1076801243 ecr 2330761273], length 31
E..S.7%.#..l..f.....B.....
0.....9.....f.....q...je...k.....
23:16:40.134280 IP ubuntu:49890 > ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https: Flags [F.], seq 31, win 501, options [nop,nop,TS val 2330766296 ecr 1076801243], length 0
E..4...@.0.3....f#..l...B.....
....0...
23:16:40.134317 IP ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https > ubuntu:49890: Flags [F.], seq 31, ack 1, win 282, options [nop,nop,TS val 1076801243 ecr 2330761273], length 0
E..4.0%.#..l..f.....B.....@.....
0.....9.....
23:16:40.135955 IP ubuntu:51470 > b.resolvers.Level3.net.domain: 30561+ PTR? 102.0.168.192.in-addr.arpa. (44)
E..H.58.0..j...f.....5.4.Mwa.....102.0.168.192.in-addr.arpa....
23:16:40.178214 IP ubuntu:49890 > ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https: Flags [F.], seq 32, win 501, options [nop,nop,TS val 2330766340 ecr 1076801243], length 0
E..4...@.0.3....f#..l...B.....
....0...
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..0.....E3....._233637DE._sub._googlecast._tcp.local.....
23:16:40.334162 IP b.resolvers.Level3.net.domain > ubuntu:51470: 30561 NXDomain* 0/1/0 (103)
E...0.5.-B.....f.5..o# wa.....102.0.168.192.in-addr.arpa.....*0./ localhost..nobody.invalid.....:..*0
23:16:40.337133 IP ubuntu:50547 > b.resolvers.Level3.net.domain: 61778+ PTR? 251.0.0.224.in-addr.arpa. (42)
E..F.W0.0.....f.....5.2.U.R.....251.0.0.224.in-addr.arpa....
23:16:40.538940 IP b.resolvers.Level3.net.domain > ubuntu:50547: 61778 NXDomain 0/1/0 (99)
E...0.5.-@.....f.5.s.k3.R.....251.0.0.224.in-addr.arpa.....
h...sns.dns.icann.org..noc..xYZ.... :....
23:16:40.540226 IP ubuntu:58407 > b.resolvers.Level3.net.domain: 39497+ PTR? 3.0.168.192.in-addr.arpa. (42)
E..F.f0.0.....f.....5.2.U.I.....3.0.168.192.in-addr.arpa....
23:16:40.743759 IP b.resolvers.Level3.net.domain > ubuntu:58407: 39497 NXDomain* 0/1/0 (101)
E...0.5.-@.....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@ubuntu:~$
```

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. **6.** To display packets in HEX and ASCII values

`sudo tcpdump -XX -i wlo1`

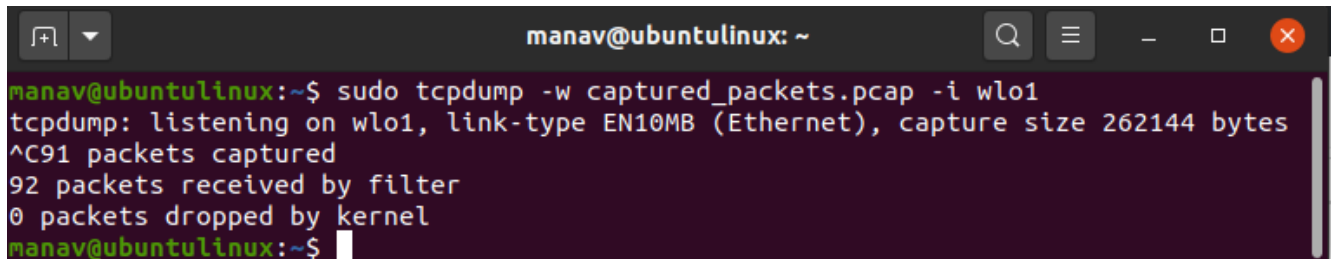
```
manav@ubuntulinux:~$ sudo tcpdump -XX -i wlo1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
23:22:35.577734 ARP, Request who-has gateway tell 192.168.0.4, length 46
0x0000: ffff ffff ffff 9c8c ceda 4b4a 0800 0001 .....n.KD...
0x0010: 0800 0004 0001 9c8c ceda 4b4a cba8 0004 .....n.KD...
0x0020: 0000 0000 0000 cba8 0001 0000 0000 0000 .....
0x0030: 0000 0000 0000 0000 0000 0000 .....
0x0040: 0000 0000 0000 0000 0000 0000 .....
0x0050: 000c 0001 .....
23:22:35.579506 IP ubuntuLinux.54789 > b.resolvers.Level3.net.domain: 2880+ PTR? 1.0.168.192.in-addr.arpa. (42)
0x0000: 5d45 6e86 ffb4 84fd d1e5 205e 0800 4500 X.n.....f..
0x0010: 0046 d486 4000 4011 9f8c cba8 0866 0402 ..f..g..f...
0x0020: 0202 e9b0 0035 0032 c755 6963 0100 0001 .....5.2.Utc...
0x0030: 0000 0000 0000 0134 0130 0331 3638 0331 .....4.8.168.1
0x0040: 0000 0000 0000 0131 0130 0331 3638 0331 .....1.0.168.1
0x0050: 3932 0769 6e2d 6164 6472 0461 7270 6100 92.in-addr.arpa.
0x0060: 000c 0001 .....
23:22:35.783330 IP b.resolvers.Level3.net.domain > ubuntuLinux.54789: 2880 NXDomain* 0/1/0 (101)
0x0000: 84fd d1e5 205e 5d45 6e86 ffb4 0800 4520 ....X.n.....f..
0x0010: 0046 d486 4000 4011 9f8c cba8 0866 0402 ..f..g..f...
0x0020: 0000 0035 e9b0 000d 433f 6963 8583 0001 ..f..s...n.k.g...
0x0030: 0000 0001 0000 0134 0130 0331 3638 0331 .....4.8.168.1
0x0040: 3932 0769 6e2d 6164 6472 0461 7270 6100 92.in-addr.arpa.
0x0050: 000c 0001 c010 0800 0001 0800 2a30 082f .....*/
0x0060: 096c 6f63 616c 686f 7374 0000 6e6f 626f /localhost.nob...
0x0070: 6479 0769 6e76 616c 6964 0800 0000 0100 dy.invalid....
0x0080: 000e 1000 0004 b000 093a 0800 002a 30 .....*/
23:22:35.784699 IP ubuntuLinux.59659 > b.resolvers.Level3.net.domain: 26979+ PTR? 4.0.168.192.in-addr.arpa. (42)
0x0000: 5d45 6e86 ffb4 84fd d1e5 205e 0800 4500 X.n.....f..
0x0010: 0046 d486 4000 4011 9f8c cba8 0866 0402 ..f..g..f...
0x0020: 0202 e9b0 0035 0032 c755 6963 0100 0001 .....5.2.Utc...
0x0030: 0000 0000 0000 0134 0130 0331 3638 0331 .....4.8.168.1
0x0040: 3932 0769 6e2d 6164 6472 0461 7270 6100 92.in-addr.arpa.
0x0050: 000c 0001 .....
23:22:35.987294 IP b.resolvers.Level3.net.domain > ubuntuLinux.59659: 26979 NXDomain* 0/1/0 (101)
0x0000: 84fd d1e5 205e 5d45 6e86 ffb4 0800 4520 ....X.n.....f..
0x0010: 0046 d486 4000 4011 9f8c cba8 0866 0402 ..f..g..f...
0x0020: 0000 0035 e9b0 000d 433f 6963 8583 0001 ..f..s...n.k.g...
0x0030: 0000 0001 0000 0134 0130 0331 3638 0331 .....4.8.168.1
0x0040: 3932 0769 6e2d 6164 6472 0461 7270 6100 92.in-addr.arpa.
0x0050: 000c 0001 c010 0800 0001 0800 2a30 082f .....*/
0x0060: 096c 6f63 616c 686f 7374 0000 6e6f 626f /localhost.nob...
0x0070: 6479 0769 6e76 616c 6964 0800 0000 0100 dy.invalid....
0x0080: 000e 1000 0004 b000 093a 0800 002a 30 .....*/
23:22:35.989297 IP ubuntuLinux.41460 > b.resolvers.Level3.net.domain: 7622+ PTR? 102.0.168.192.in-addr.arpa. (44)
0x0000: 5d45 6e86 ffb4 84fd d1e5 205e 0800 4500 X.n.....f..
0x0010: 0046 d486 4000 4011 9f8c cba8 0866 0402 ..f..g..f...
0x0020: 0202 a1f4 0035 0034 c757 1d0c 0100 0001 .....5.4.w...
0x0030: 0000 0000 0000 0131 3632 0130 0331 3638 .....102.0.168
0x0040: 0131 3932 0769 6e2d 6164 6472 0461 7270 192.in-addr.arpa
0x0050: 0100 000c 0001 .....
23:22:36.192917 IP b.resolvers.Level3.net.domain > ubuntuLinux.41460: 7622 NXDomain* 0/1/0 (103)
0x0000: 84fd d1e5 205e 5d45 6e86 ffb4 0800 4520 ....X.n.....f..
0x0010: 0046 d486 4000 4011 9f8c cba8 0866 0402 ..f..g..f...
0x0020: 0000 0035 a1f4 000f a3be 1d0c 8583 0001 ..f..s...n.k.g...
0x0030: 0000 0001 0000 0131 3632 0130 0331 3638 .....102.0.168
0x0040: 0131 3932 0769 6e2d 6164 6472 0461 7270 192.in-addr.arpa
0x0050: 0100 000c 0001 c012 0800 0001 0800 2a30 .....*/
0x0060: 0000 .....
23:22:36.192917 IP b.resolvers.Level3.net.domain > ubuntuLinux.41460: 7622 NXDomain* 0/1/0 (103)
0x0000: 84fd d1e5 205e 5d45 6e86 ffb4 0800 4520 ....X.n.....f..
0x0010: 0046 d486 4000 4011 9f8c cba8 0866 0402 ..f..g..f...
0x0020: 0000 0035 a1f4 000f a3be 1d0c 8583 0001 ..f..s...n.k.g...
0x0030: 0000 0001 0000 0131 3632 0130 0331 3638 .....102.0.168
0x0040: 0131 3932 0769 6e2d 6164 6472 0461 7270 192.in-addr.arpa
0x0050: 0100 000c 0001 c012 0800 0001 0800 2a30 .....*/
0x0060: 0000 .....
23:22:37.625893 ARP, Request who-has gateway tell 192.168.0.4, length 46
0x0000: ffff ffff ffff 9c8c ceda 4b4a 0800 0001 .....n.KD...
0x0010: 0800 0004 0001 9c8c ceda 4b4a cba8 0004 .....n.KD...
0x0020: 0000 0000 0000 cba8 0001 0000 0000 0000 .....
0x0030: 0000 0000 0000 0000 0000 0000 .....
0 packets captured
0 packets received by filter
0 packets dropped by kernel
manav@ubuntulinux:~$
```

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

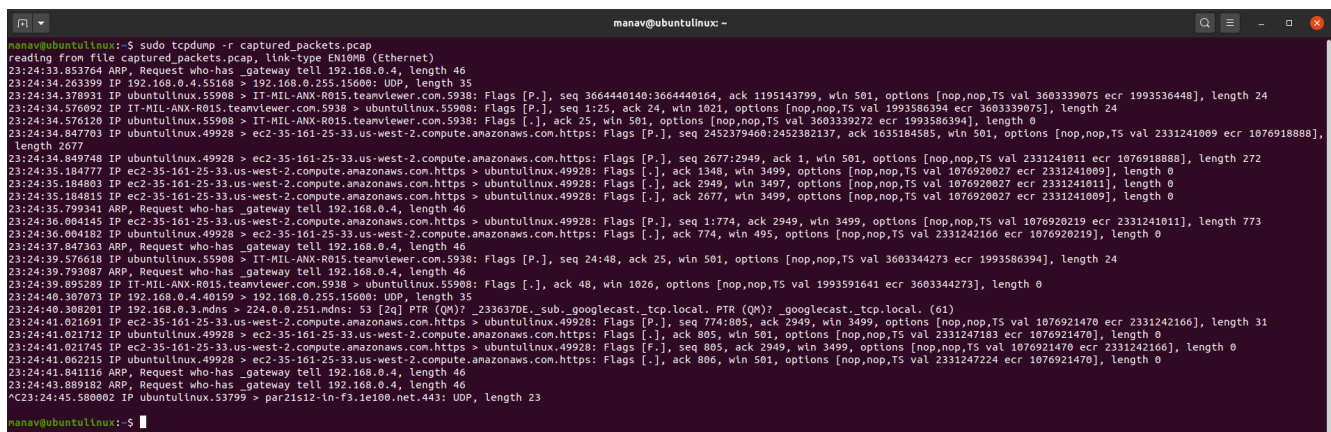
```
sudo tcpdump -w captured_packets.pcap -i wlo1
```



```
manav@ubuntulinux: ~$ sudo tcpdump -w captured_packets.pcap -i wlo1
tcpdump: listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C91 packets captured
92 packets received by filter
0 packets dropped by kernel
manav@ubuntulinux: ~$
```

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
```



```
manav@ubuntulinux: ~$ sudo tcpdump -r captured_packets.pcap
reading from file captured_packets.pcap, link-type EN10MB (Ethernet)
23:24:33.853764 ARP, Request who-has_gateway tell 192.168.0.4, length 46
23:24:34.263399 IP 192.168.0.4.55168 > 192.168.0.255.15600: UDP, length 35
23:24:34.378931 IP ubuntulinux.55908 > IT-MIL-ANX-R015.teamviewer.com.5938: Flags [P.], seq 3664440140:3664440164, ack 1195143799, win 501, options [nop,nop,TS val 3603339075 ecr 1993536448], length 24
23:24:34.576092 IP IT-MIL-ANX-R015.teamviewer.com.5938 > ubuntulinux.55908: Flags [P.], seq 1:25, ack 24, win 1021, options [nop,nop,TS val 1993586394 ecr 3603339075], length 24
23:24:34.576120 IP ubuntulinux.55908 > IT-MIL-ANX-R015.teamviewer.com.5938: Flags [.], ack 25, win 501, options [nop,nop,TS val 3603339272 ecr 1993586394], length 0
23:24:34.847703 IP ubuntulinux.49928 > ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https: Flags [P.], seq 2452379460:2452382137, ack 1635184585, win 501, options [nop,nop,TS val 2331241009 ecr 1076918888], length 2677
23:24:34.849748 IP ubuntulinux.49928 > ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https: Flags [P.], seq 2677:2949, ack 1, win 501, options [nop,nop,TS val 2331241011 ecr 1076918888], length 272
23:24:35.184777 IP ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https > ubuntulinux.49928: Flags [.], ack 1348, win 3499, options [nop,nop,TS val 1076920027 ecr 2331241009], length 0
23:24:35.184803 IP ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https > ubuntulinux.49928: Flags [.], ack 2949, win 3497, options [nop,nop,TS val 1076920027 ecr 2331241011], length 0
23:24:35.184815 IP ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https > ubuntulinux.49928: Flags [.], ack 2677, win 3499, options [nop,nop,TS val 1076920027 ecr 2331241009], length 0
23:24:35.799341 ARP, Request who-has_gateway tell 192.168.0.4, length 46
23:24:36.004145 IP ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https > ubuntulinux.49928: Flags [P.], seq 1:774, ack 2949, win 3499, options [nop,nop,TS val 1076920219 ecr 2331241011], length 773
23:24:36.004182 IP ubuntulinux.49928 > ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https: Flags [.], ack 774, win 495, options [nop,nop,TS val 2331242166 ecr 1076920219], length 0
23:24:37.847363 ARP, Request who-has_gateway tell 192.168.0.4, length 46
23:24:39.576618 IP ubuntulinux.55908 > IT-MIL-ANX-R015.teamviewer.com.5938: Flags [P.], seq 24:48, ack 25, win 501, options [nop,nop,TS val 3603344273 ecr 1993586394], length 24
23:24:39.793007 ARP, Request who-has_gateway tell 192.168.0.4, length 46
23:24:39.895289 IP IT-MIL-ANX-R015.teamviewer.com.5938 > ubuntulinux.55908: Flags [.], ack 48, win 1026, options [nop,nop,TS val 1993591641 ecr 3603344273], length 0
23:24:40.307073 IP 192.168.0.4.40159 > 192.168.0.255.15600: UDP, length 35
23:24:40.308201 IP 192.168.0.3.ndns > 224.0.0.251.ndns: 53 [2q] PTR (QM)? _233637DE._sub._googlecast._tcp.local. PTR (QM)? _googlecast._tcp.local. (61)
23:24:41.021691 IP ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https > ubuntulinux.49928: Flags [P.], seq 774:805, ack 2949, win 3499, options [nop,nop,TS val 1076921470 ecr 2331242166], length 31
23:24:41.021712 IP ubuntulinux.49928 > ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https: Flags [.], ack 805, win 501, options [nop,nop,TS val 2331247183 ecr 1076921470], length 0
23:24:41.021745 IP ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https > ubuntulinux.49928: Flags [F.], seq 805, ack 2949, win 3499, options [nop,nop,TS val 1076921470 ecr 2331242166], length 0
23:24:41.062215 IP ubuntulinux.49928 > ec2-35-161-25-33.us-west-2.compute.amazonaws.com.https: Flags [.], ack 806, win 501, options [nop,nop,TS val 2331247224 ecr 1076921470], length 0
23:24:41.841116 ARP, Request who-has_gateway tell 192.168.0.4, length 46
23:24:43.889182 ARP, Request who-has_gateway tell 192.168.0.4, length 46
^C23:24:45.580002 IP ubuntulinux.53759 > par21512-ln-f3.1e100.net.443: UDP, length 23
manav@ubuntulinux: ~$
```

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
```

```

manav@ubuntu:~$ 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
23:28:38.404165 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 2170722621 ecr 3655235039], 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 2170722660 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 2170722660,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 2170722660], 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@ubuntu:~$

```

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

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

```

manav@ubuntu:~$ 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 ubuntu: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 > ubuntu: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@ubuntu:~$

```

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



A-143, 9th Floor, Sovereign Corporate Tower,
Sector-136, Noida, Uttar Pradesh - 201305

feedback@geeksforgeeks.org

Company

About Us
Careers
In Media
Contact Us
Terms and Conditions
Privacy Policy
Copyright Policy
Third-Party Copyright Notices
Advertise with us

Languages

Python
Java
C++
GoLang
SQL
R Language
Android Tutorial

Algorithms

Sorting
Searching
Greedy
Dynamic Programming
Pattern Searching
Recursion
Backtracking

Data Science & ML

Data Science With Python
Data Science For Beginner
Machine Learning Tutorial
Maths For Machine Learning
Pandas Tutorial

Trending @GfG

Job Fair For Students
GfG Weekly #100
POTD: Revamped
Python Backend LIVE
Android App Development
DevOps LIVE
DSA in JavaScript

Data Structures

Array
String
Linked List
Stack
Queue
Tree
Graph

Web Development

HTML
CSS
JavaScript
Bootstrap
ReactJS
AngularJS
NodeJS

Interview Corner

Company Preparation
Preparation for SDE
Company Interview Corner
Experienced Interview
Internship Interview

[NumPy Tutorial](#)[NLP Tutorial](#)

Python

[Python Tutorial](#)[Python Programming Examples](#)[Django Tutorial](#)[Python Projects](#)[Python Tkinter](#)[OpenCV Python Tutorial](#)

UPSC/SSC/BANKING

[SSC CGL Syllabus](#)[SBI PO Syllabus](#)[IBPS PO Syllabus](#)[UPSC Ethics Notes](#)[UPSC Economics Notes](#)[UPSC History Notes](#)[Competitive Programming](#)[Aptitude](#)

GfG School

[CBSE Notes for Class 8](#)[CBSE Notes for Class 9](#)[CBSE Notes for Class 10](#)[CBSE Notes for Class 11](#)[CBSE Notes for Class 12](#)[English Grammar](#)

Write & Earn

[Write an Article](#)[Improve an Article](#)[Pick Topics to Write](#)[Write Interview Experience](#)[Internships](#)[Video Internship](#)

@geeksforgeeks , Some rights reserved