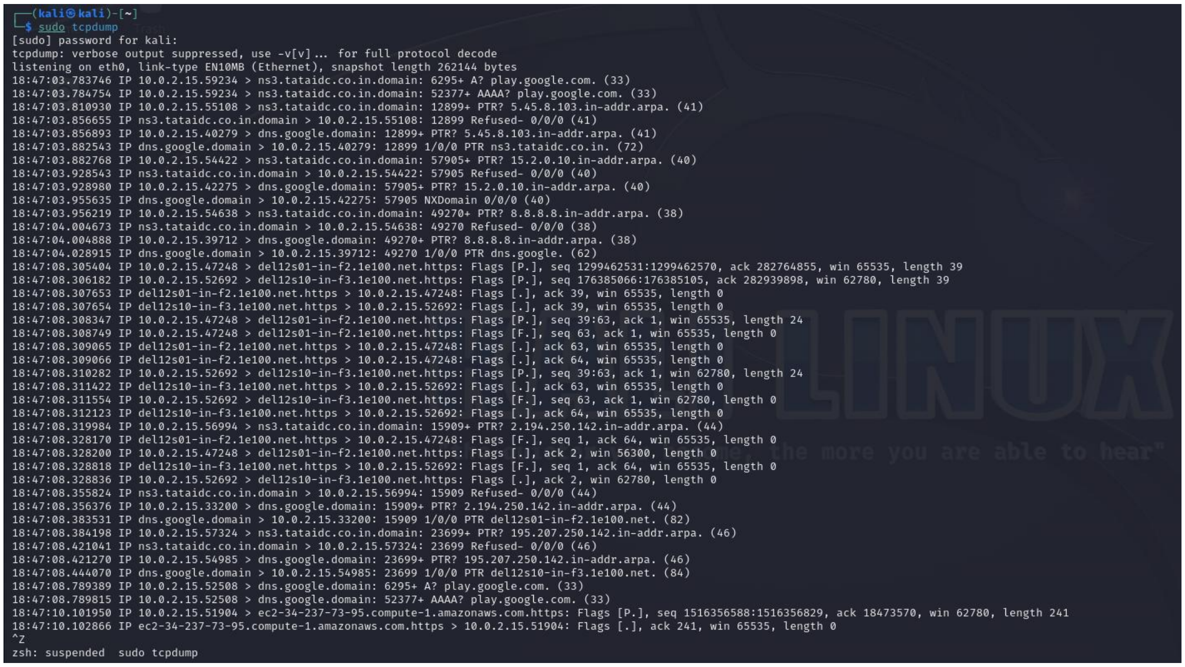
TCPdump

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.

- **Packet Capture**: tcpdump captures network packets from a specified network interface and displays the packet headers on the console. It can save captured packets to a file for later analysis using tools like Wireshark.
- **Filtering**: tcpdump uses the Berkeley Packet Filter (BPF) syntax to filter network traffic based on various criteria such as IP addresses, port numbers, protocols, and more. This allows users to focus on specific traffic of interest.
- **Protocol Analysis**: tcpdump can decode and display packet headers for various protocols, including TCP, UDP, ICMP, HTTP, DNS, and more, providing detailed insights into network communications.
- **Versatility**: tcpdump is versatile and can be used on many Unix-like operating systems, including Linux, macOS, and BSD. It requires root or sudo privileges to capture packets on network interfaces.

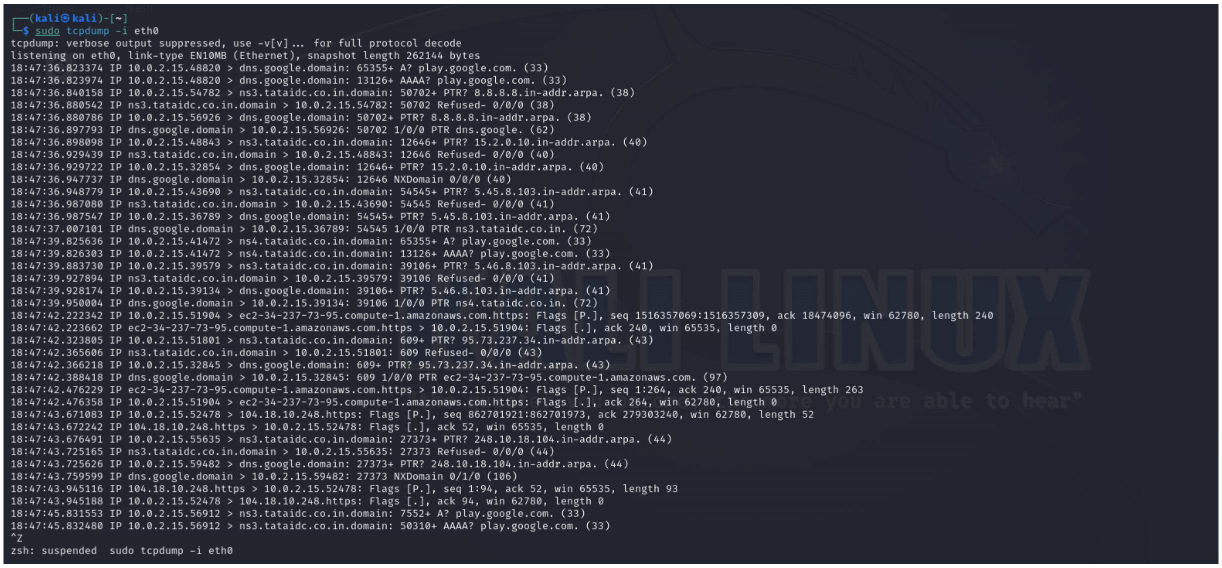
Examples: -

1. To capture the packets of current network interface



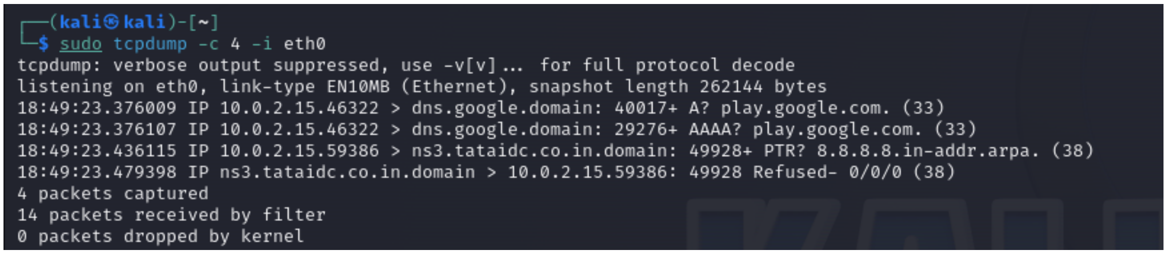
```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:47:03.783746 IP 10.0.2.15.59234 > ns3.tataidc.co.in.domain: 6295+ A? play.google.com. (33)
18:47:03.784754 IP 10.0.2.15.59234 > ns3.tataidc.co.in.domain: 52377+ AAAA? play.google.com. (33)
18:47:03.810930 IP 10.0.2.15.55108 > ns3.tataidc.co.in.domain: 12899+ PTR? 5.45.8.103.in-addr.arpa. (41)
18:47:03.856655 IP ns3.tataidc.co.in.domain > 10.0.2.15.55108: 12899 Refused- 0/0/0 (41)
18:47:03.856893 IP 10.0.2.15.40279 > dns.google.domain: 12899+ PTR? 5.45.8.103.in-addr.arpa. (41)
18:47:03.882543 IP dns.google.domain > 10.0.2.15.40279: 12899 1/0/0 PTR ns3.tataidc.co.in. (72)
18:47:03.882768 IP 10.0.2.15.54422 > ns3.tataidc.co.in.domain: 57905+ PTR? 15.2.0.10.in-addr.arpa. (40)
18:47:03.928543 IP ns3.tataidc.co.in.domain > 10.0.2.15.54422: 57905 Refused- 0/0/0 (40)
18:47:03.928980 IP 10.0.2.15.42275 > dns.google.domain: 57905+ PTR? 15.2.0.10.in-addr.arpa. (40)
18:47:03.955635 IP dns.google.domain > 10.0.2.15.42275: 57905 NXDomain 0/0/0 (40)
18:47:03.956219 IP 10.0.2.15.54638 > ns3.tataidc.co.in.domain: 49270+ PTR? 8.8.8.8.in-addr.arpa. (38)
18:47:04.004673 IP ns3.tataidc.co.in.domain > 10.0.2.15.54638: 49270 Refused- 0/0/0 (38)
18:47:04.004888 IP 10.0.2.15.39712 > dns.google.domain: 49270+ PTR? 8.8.8.8.in-addr.arpa. (38)
18:47:04.028915 IP dns.google.domain > 10.0.2.15.39712: 49270 1/0/0 PTR dns.google. (62)
18:47:08.305404 IP 10.0.2.15.47248 > del12s01-in-f2.1e100.net.https: Flags [P.], seq 1299462531:1299462570, ack 282764855, win 65535, length 39
18:47:08.306182 IP 10.0.2.15.52692 > del12s10-in-f3.1e100.net.https: Flags [P.], seq 176385066:176385105, ack 282939898, win 62780, length 39
18:47:08.307653 IP del12s01-in-f2.1e100.net.https > 10.0.2.15.47248: Flags [.], ack 39, win 65535, length 0
18:47:08.307654 IP del12s10-in-f3.1e100.net.https > 10.0.2.15.52692: Flags [.], ack 39, win 65535, length 0
18:47:08.308347 IP 10.0.2.15.47248 > del12s01-in-f2.1e100.net.https: Flags [P.], seq 39:63, ack 1, win 65535, length 24
18:47:08.308749 IP 10.0.2.15.47248 > del12s01-in-f2.1e100.net.https: Flags [F.], seq 63, ack 1, win 65535, length 0
18:47:08.309065 IP del12s01-in-f2.1e100.net.https > 10.0.2.15.47248: Flags [.], ack 63, win 65535, length 0
18:47:08.309066 IP del12s01-in-f2.1e100.net.https > 10.0.2.15.47248: Flags [.], ack 64, win 65535, length 0
18:47:08.310282 IP 10.0.2.15.52692 > del12s10-in-f3.1e100.net.https: Flags [P.], seq 39:63, ack 1, win 62780, length 24
18:47:08.311422 IP del12s10-in-f3.1e100.net.https > 10.0.2.15.52692: Flags [.], ack 63, win 65535, length 0
18:47:08.311554 IP 10.0.2.15.52692 > del12s10-in-f3.1e100.net.https: Flags [F.], seq 63, ack 1, win 62780, length 0
18:47:08.312123 IP del12s10-in-f3.1e100.net.https > 10.0.2.15.52692: Flags [.], ack 64, win 65535, length 0
18:47:08.319984 IP 10.0.2.15.56994 > ns3.tataidc.co.in.domain: 15909+ PTR? 2.194.250.142.in-addr.arpa. (44)
18:47:08.328170 IP del12s01-in-f2.1e100.net.https > 10.0.2.15.47248: Flags [F.], seq 1, ack 64, win 65535, length 0
18:47:08.328200 IP 10.0.2.15.47248 > del12s01-in-f2.1e100.net.https: Flags [.], ack 2, win 56300, length 0
18:47:08.328818 IP del12s10-in-f3.1e100.net.https > 10.0.2.15.52692: Flags [F.], seq 1, ack 64, win 65535, length 0
18:47:08.328836 IP 10.0.2.15.52692 > del12s10-in-f3.1e100.net.https: Flags [.], ack 2, win 62780, length 0
18:47:08.355824 IP ns3.tataidc.co.in.domain > 10.0.2.15.56994: 15909 Refused- 0/0/0 (44)
18:47:08.356376 IP 10.0.2.15.33200 > dns.google.domain: 15909+ PTR? 2.194.250.142.in-addr.arpa. (44)
18:47:08.383531 IP dns.google.domain > 10.0.2.15.33200: 15909 1/0/0 PTR del12s01-in-f2.1e100.net. (82)
18:47:08.384198 IP 10.0.2.15.57324 > ns3.tataidc.co.in.domain: 23699+ PTR? 195.207.250.142.in-addr.arpa. (46)
18:47:08.421041 IP ns3.tataidc.co.in.domain > 10.0.2.15.57324: 23699 Refused- 0/0/0 (46)
18:47:08.421270 IP 10.0.2.15.54985 > dns.google.domain: 23699+ PTR? 195.207.250.142.in-addr.arpa. (46)
18:47:08.444070 IP dns.google.domain > 10.0.2.15.54985: 23699 1/0/0 PTR del12s10-in-f3.1e100.net. (84)
18:47:08.789389 IP 10.0.2.15.52508 > dns.google.domain: 6295+ A? play.google.com. (33)
18:47:08.789815 IP 10.0.2.15.52508 > dns.google.domain: 52377+ AAAA? play.google.com. (33)
18:47:10.101950 IP 10.0.2.15.51904 > ec2-34-237-73-95.compute-1.amazonaws.com.https: Flags [P.], seq 1516356588:1516356829, ack 18473570, win 62780, length 241
18:47:10.102866 IP ec2-34-237-73-95.compute-1.amazonaws.com.https > 10.0.2.15.51904: Flags [.], ack 241, win 65535, length 0
^Z
zsh: suspended  sudo tcpdump
```

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



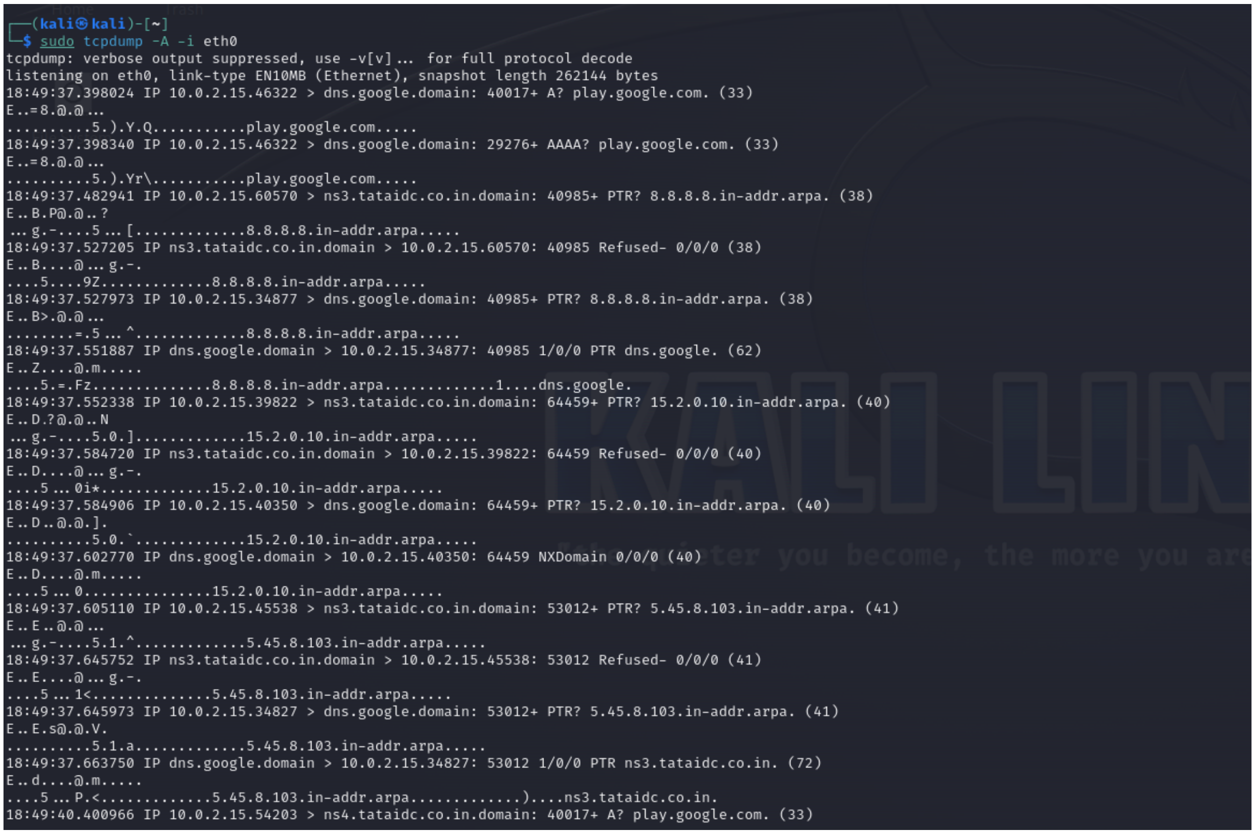
```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:47:36.823374 IP 10.0.2.15.48820 > dns.google.domain: 65355+ A? play.google.com. (33)
18:47:36.823974 IP 10.0.2.15.48820 > dns.google.domain: 13126+ AAAA? play.google.com. (33)
18:47:36.840158 IP 10.0.2.15.54782 > ns3.tataidc.co.in.domain: 50702+ PTR? 8.8.8.8.in-addr.arpa. (38)
18:47:36.880542 IP ns3.tataidc.co.in.domain > 10.0.2.15.54782: 50702 Refused- 0/0/0 (38)
18:47:36.880786 IP 10.0.2.15.56926 > dns.google.domain: 50702+ PTR? 8.8.8.8.in-addr.arpa. (38)
18:47:36.897793 IP dns.google.domain > 10.0.2.15.56926: 50702 1/0/0 PTR dns.google. (62)
18:47:36.898098 IP 10.0.2.15.48843 > ns3.tataidc.co.in.domain: 12646+ PTR? 15.2.0.10.in-addr.arpa. (40)
18:47:36.929439 IP ns3.tataidc.co.in.domain > 10.0.2.15.48843: 12646 Refused- 0/0/0 (40)
18:47:36.929722 IP 10.0.2.15.32854 > dns.google.domain: 12646+ PTR? 15.2.0.10.in-addr.arpa. (40)
18:47:36.947737 IP dns.google.domain > 10.0.2.15.32854: 12646 NXDomain 0/0/0 (40)
18:47:36.948779 IP 10.0.2.15.43690 > ns3.tataidc.co.in.domain: 54545+ PTR? 5.45.8.103.in-addr.arpa. (41)
18:47:36.987080 IP ns3.tataidc.co.in.domain > 10.0.2.15.43690: 54545 Refused- 0/0/0 (41)
18:47:36.987547 IP 10.0.2.15.36789 > dns.google.domain: 54545+ PTR? 5.45.8.103.in-addr.arpa. (41)
18:47:37.007101 IP dns.google.domain > 10.0.2.15.36789: 54545 1/0/0 PTR ns3.tataidc.co.in. (72)
18:47:39.825636 IP 10.0.2.15.41472 > ns4.tataidc.co.in.domain: 65355+ A? play.google.com. (33)
18:47:39.826303 IP 10.0.2.15.41472 > ns4.tataidc.co.in.domain: 13126+ AAAA? play.google.com. (33)
18:47:39.883730 IP 10.0.2.15.39579 > ns3.tataidc.co.in.domain: 39106+ PTR? 5.46.8.103.in-addr.arpa. (41)
18:47:39.927894 IP ns3.tataidc.co.in.domain > 10.0.2.15.39579: 39106 Refused- 0/0/0 (41)
18:47:39.928174 IP 10.0.2.15.39134 > dns.google.domain: 39106+ PTR? 5.46.8.103.in-addr.arpa. (41)
18:47:39.950004 IP dns.google.domain > 10.0.2.15.39134: 39106 1/0/0 PTR ns4.tataidc.co.in. (72)
18:47:42.222342 IP 10.0.2.15.51904 > ec2-34-237-73-95.compute-1.amazonaws.com.https: Flags [P.], seq 1516357069:1516357309, ack 18474096, win 62780, length 240
18:47:42.223662 IP ec2-34-237-73-95.compute-1.amazonaws.com.https > 10.0.2.15.51904: Flags [.], ack 240, win 65535, length 0
18:47:42.323805 IP 10.0.2.15.51801 > ns3.tataidc.co.in.domain: 609+ PTR? 95.73.237.34.in-addr.arpa. (43)
18:47:42.365606 IP ns3.tataidc.co.in.domain > 10.0.2.15.51801: 609 Refused- 0/0/0 (43)
18:47:42.366218 IP 10.0.2.15.32845 > dns.google.domain: 609+ PTR? 95.73.237.34.in-addr.arpa. (43)
18:47:42.388418 IP dns.google.domain > 10.0.2.15.32845: 609 1/0/0 PTR ec2-34-237-73-95.compute-1.amazonaws.com. (97)
18:47:42.476229 IP ec2-34-237-73-95.compute-1.amazonaws.com.https > 10.0.2.15.51904: Flags [P.], seq 1:264, ack 240, win 65535, length 263
18:47:42.476358 IP 10.0.2.15.51904 > ec2-34-237-73-95.compute-1.amazonaws.com.https: Flags [.], ack 264, win 62780, length 0
18:47:43.671083 IP 10.0.2.15.52478 > 104.18.10.248.https: Flags [P.], seq 862701921:862701973, ack 279303240, win 62780, length 52
18:47:43.672242 IP 104.18.10.248.https > 10.0.2.15.52478: Flags [.], ack 52, win 65535, length 0
18:47:43.676491 IP 10.0.2.15.55635 > ns3.tataidc.co.in.domain: 27373+ PTR? 248.10.18.104.in-addr.arpa. (44)
18:47:43.725165 IP ns3.tataidc.co.in.domain > 10.0.2.15.55635: 27373 Refused- 0/0/0 (44)
18:47:43.725626 IP 10.0.2.15.59482 > dns.google.domain: 27373+ PTR? 248.10.18.104.in-addr.arpa. (44)
18:47:43.759599 IP dns.google.domain > 10.0.2.15.59482: 27373 NXDomain 0/1/0 (106)
18:47:43.945116 IP 104.18.10.248.https > 10.0.2.15.52478: Flags [P.], seq 1:94, ack 52, win 65535, length 93
18:47:43.945188 IP 10.0.2.15.52478 > 104.18.10.248.https: Flags [.], ack 94, win 62780, length 0
18:47:45.831553 IP 10.0.2.15.56912 > ns3.tataidc.co.in.domain: 7552+ A? play.google.com. (33)
18:47:45.832480 IP 10.0.2.15.56912 > ns3.tataidc.co.in.domain: 50310+ AAAA? play.google.com. (33)
^Z
zsh: suspended  sudo tcpdump -i eth0
```

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



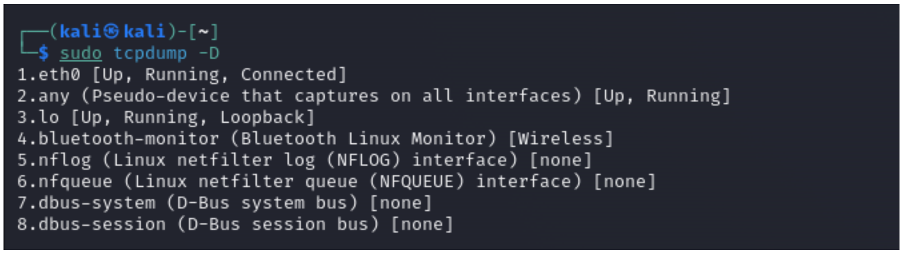
```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -c 4 -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:49:23.376009 IP 10.0.2.15.46322 > dns.google.domain: 40017+ A? play.google.com. (33)
18:49:23.376107 IP 10.0.2.15.46322 > dns.google.domain: 29276+ AAAA? play.google.com. (33)
18:49:23.436115 IP 10.0.2.15.59386 > ns3.tataidc.co.in.domain: 49928+ PTR? 8.8.8.8.in-addr.arpa. (38)
18:49:23.479398 IP ns3.tataidc.co.in.domain > 10.0.2.15.59386: 49928 Refused- 0/0/0 (38)
4 packets captured
14 packets received by filter
0 packets dropped by kernel
```

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



```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -A -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:49:37.398024 IP 10.0.2.15.46322 > dns.google.domain: 40017+ A? play.google.com. (33)
E..=8.@.@...
..........5.).Y.Q..........play.google.com.....
18:49:37.398340 IP 10.0.2.15.46322 > dns.google.domain: 29276+ AAAA? play.google.com. (33)
E..=8.@.@...
..........5.).Yr\..........play.google.com.....
18:49:37.482941 IP 10.0.2.15.60570 > ns3.tataidc.co.in.domain: 40985+ PTR? 8.8.8.8.in-addr.arpa. (38)
E..B.P@.@..?
...g.-....5...[............8.8.8.8.in-addr.arpa.....
18:49:37.527205 IP ns3.tataidc.co.in.domain > 10.0.2.15.60570: 40985 Refused- 0/0/0 (38)
E..B....@...g.-.
....5....9Z............8.8.8.8.in-addr.arpa.....
18:49:37.527973 IP 10.0.2.15.34877 > dns.google.domain: 40985+ PTR? 8.8.8.8.in-addr.arpa. (38)
E..B>.@.@...
........=.5...^............8.8.8.8.in-addr.arpa.....
18:49:37.551887 IP dns.google.domain > 10.0.2.15.34877: 40985 1/0/0 PTR dns.google. (62)
E..Z....@.m.....
....5.=.Fz.............8.8.8.8.in-addr.arpa............1....dns.google.
18:49:37.552338 IP 10.0.2.15.39822 > ns3.tataidc.co.in.domain: 64459+ PTR? 15.2.0.10.in-addr.arpa. (40)
E..D.?@.@..N
...g.-....5.0.]............15.2.0.10.in-addr.arpa.....
18:49:37.584720 IP ns3.tataidc.co.in.domain > 10.0.2.15.39822: 64459 Refused- 0/0/0 (40)
E..D....@...g.-.
....5...0i*............15.2.0.10.in-addr.arpa.....
18:49:37.584906 IP 10.0.2.15.40350 > dns.google.domain: 64459+ PTR? 15.2.0.10.in-addr.arpa. (40)
E..D..@.@.].
..........5.0.`............15.2.0.10.in-addr.arpa.....
18:49:37.602770 IP dns.google.domain > 10.0.2.15.40350: 64459 NXDomain 0/0/0 (40)
E..D....@.m.....
....5...0..............15.2.0.10.in-addr.arpa.....
18:49:37.605110 IP 10.0.2.15.45538 > ns3.tataidc.co.in.domain: 53012+ PTR? 5.45.8.103.in-addr.arpa. (41)
E..E..@.@...
...g.-....5.1.^............5.45.8.103.in-addr.arpa.....
18:49:37.645752 IP ns3.tataidc.co.in.domain > 10.0.2.15.45538: 53012 Refused- 0/0/0 (41)
E..E....@...g.-.
....5...1<.............5.45.8.103.in-addr.arpa.....
18:49:37.645973 IP 10.0.2.15.34827 > dns.google.domain: 53012+ PTR? 5.45.8.103.in-addr.arpa. (41)
E..E.s@.@.V.
..........5.1.a............5.45.8.103.in-addr.arpa.....
18:49:37.663750 IP dns.google.domain > 10.0.2.15.34827: 53012 1/0/0 PTR ns3.tataidc.co.in. (72)
E..d....@.m.....
....5...P.<............5.45.8.103.in-addr.arpa............)....ns3.tataidc.co.in.
18:49:40.400966 IP 10.0.2.15.54203 > ns4.tataidc.co.in.domain: 40017+ A? play.google.com. (33)
```

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



```
┌──(kali㉿kali)-[~]
└─$ sudo 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]
```