

WIRESHARK

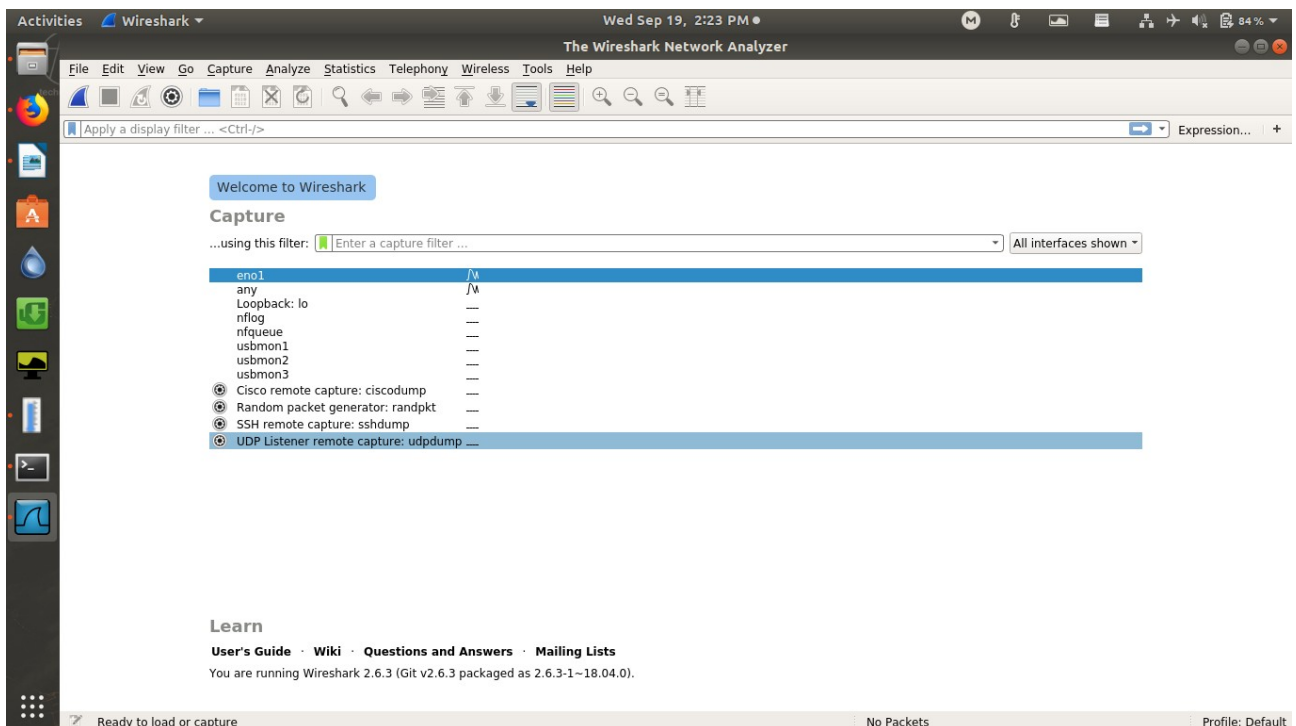
Introduction :

- It is the most popular open source network sniffer and packet / protocol analyzer solutions.
- It was previously known as ethereal . But renamed as wireshark.

Features :

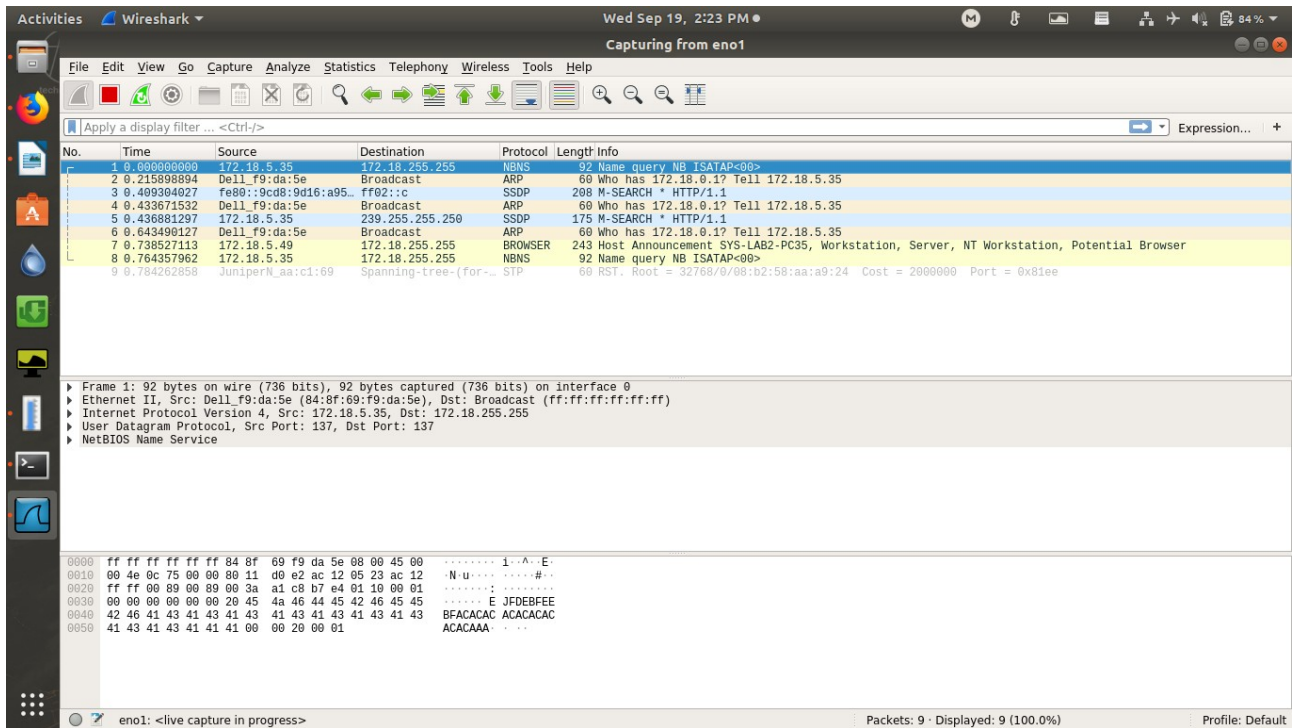
- Live data capture
- support for offline protocol analysis
- Enriched UI
- Supports almost all network , application and transport protocols.
- Display packets with very detailed protocol information
- Save captured packet data.

wireshark main window :

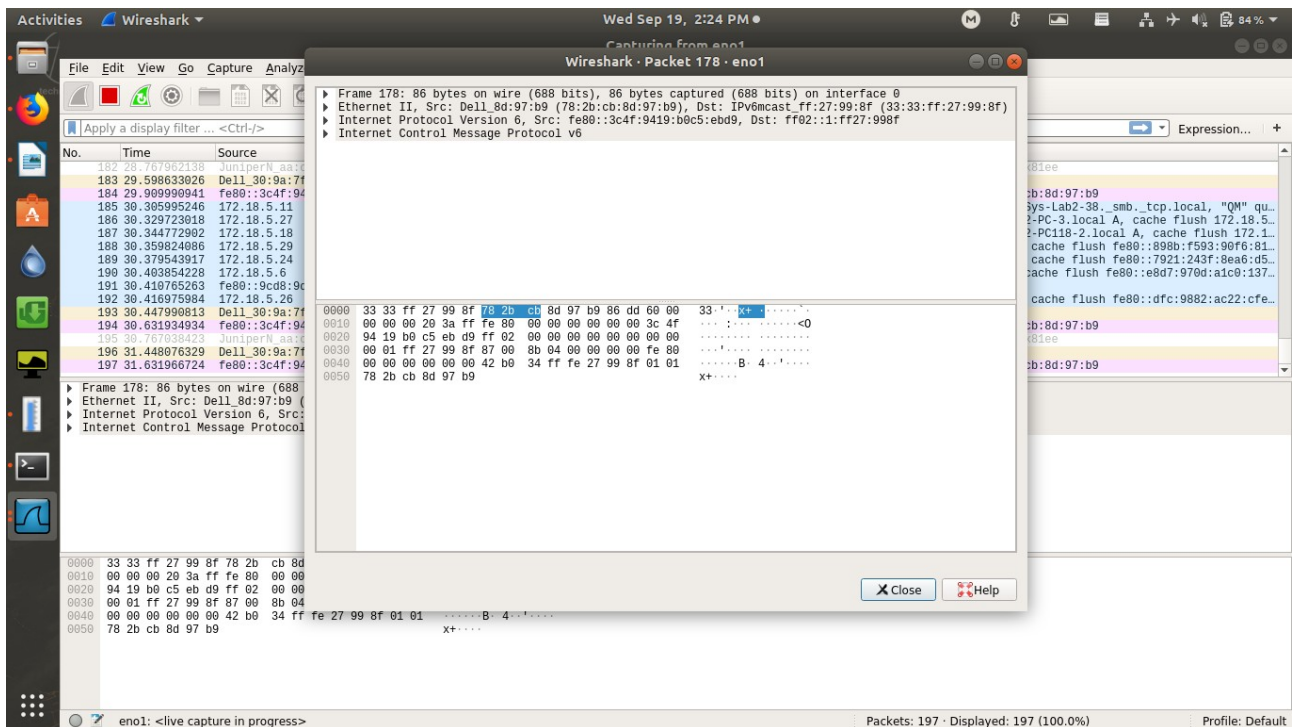


WIRESHARK

Ethernet interface monitoring :



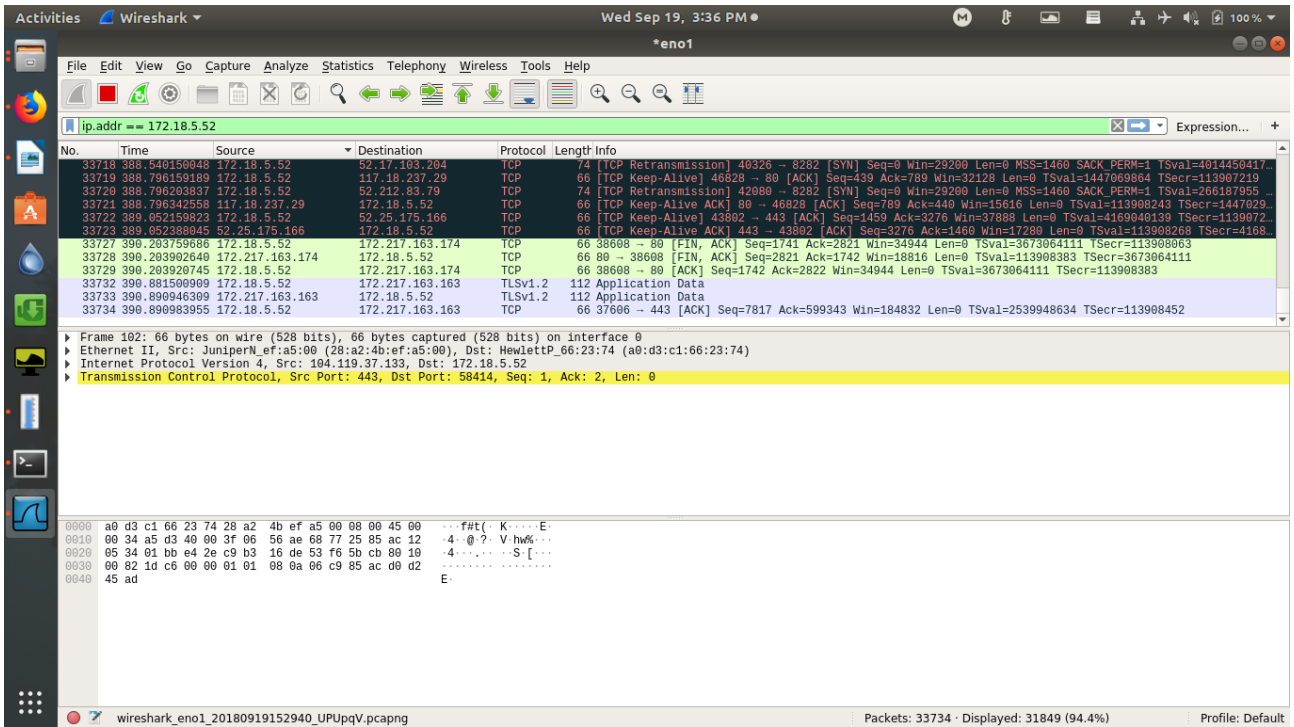
Packet details :



WIRESHARK

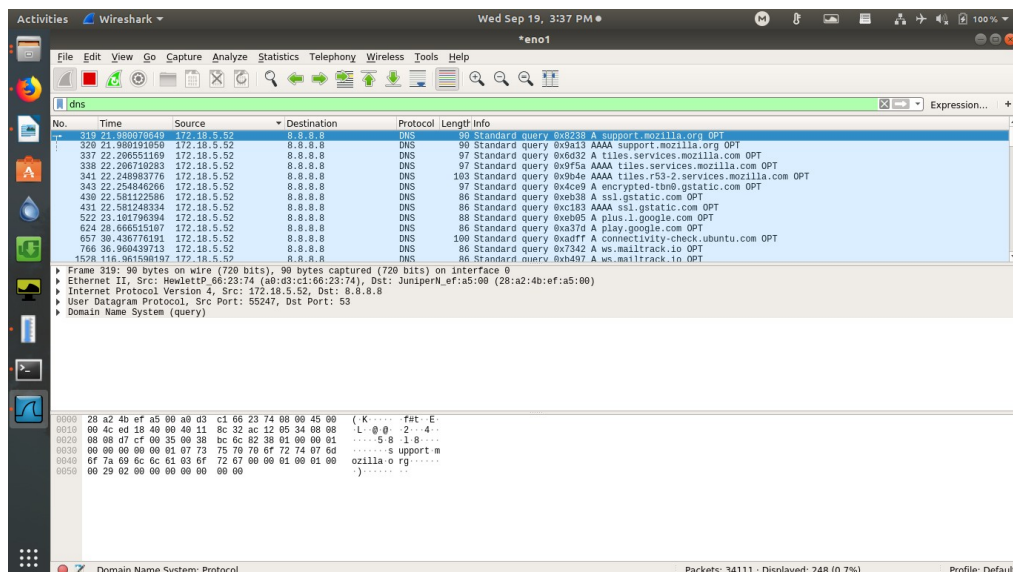
filter packet by ip address

syntax :ip.addr == <ip_addr> -> put this in display filter



filter packet by protocol name

syntax : <protocol> -> put this in display filter

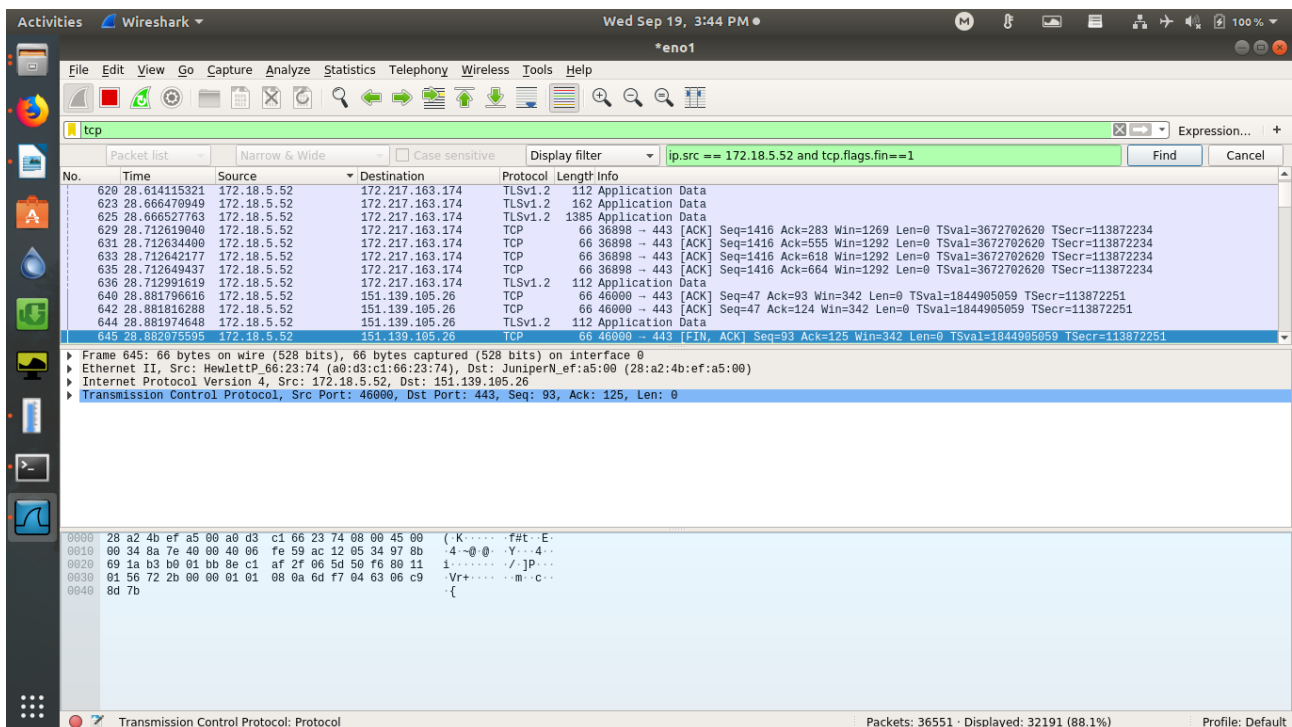


WIRESHARK

FIND Packet :

if you want find the syn packet for some specific ip address then go to EDIT --> Find packet then enter

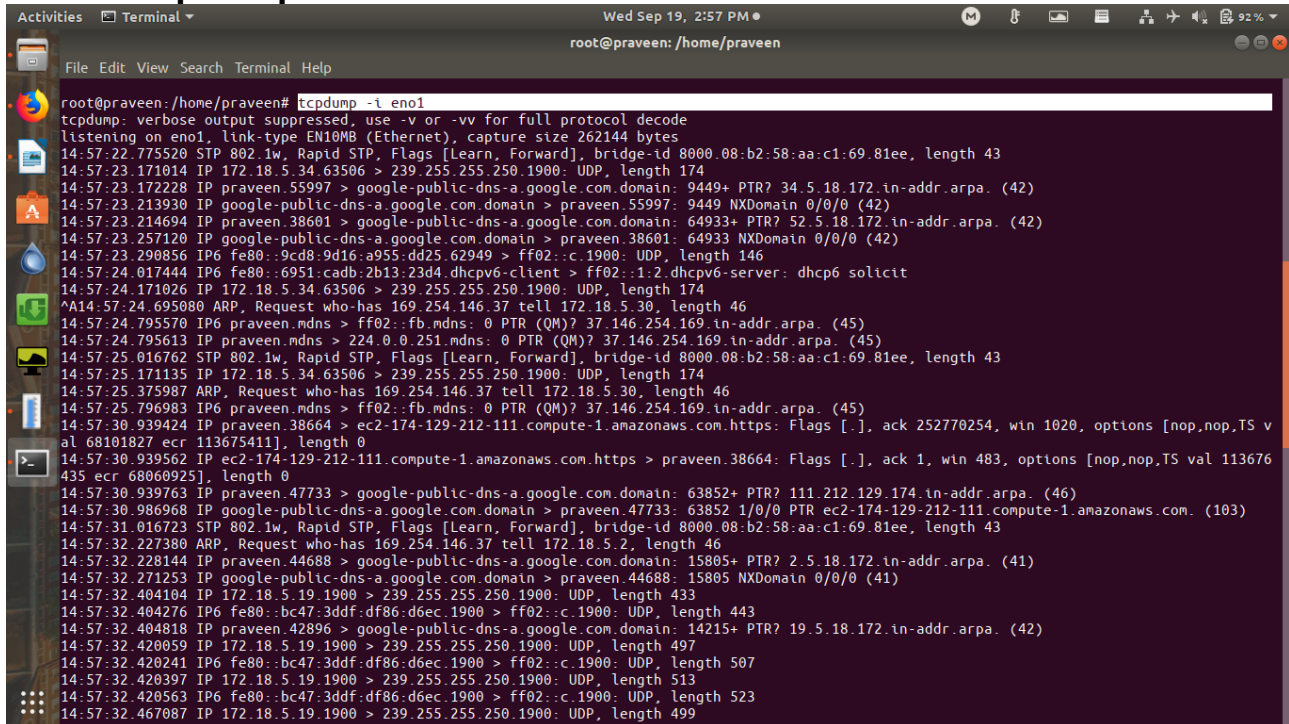
syntax : `ip.src == <ip.addr> and tcp.flags.syn==1`



```
root@praveen: /home/praveen
File Edit View Search Terminal Help
praveen@praveen:~$ tcpdump -i any
tcpdump: any: You don't have permission to capture on that device
(socket: Operation not permitted)
praveen@praveen:~$ sudo su
[sudo] password for praveen:
root@praveen:/home/praveen# tcpdump -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
14:49:51.221998 IP 172.18.5.38.59449 > 255.255.255.255.1947: UDP, length 40
14:49:51.224631 ARP, Request who-has 169.254.146.37 tell 172.18.5.2, length 46
14:49:51.227118 IP localhost.44388 > localhost.domain: 24968+ PTR? 255.255.255.255.in-addr.arpa. (46)
14:49:51.227621 IP localhost.domain > localhost.44388: 24968 ServFail 0/0/0 (46)
14:49:51.372741 IP6 praveen.mdns > ff02::fb.mdns: 0 PTR (QM)? 37.146.254.169.in-addr.arpa. (45)
14:49:56.318451 IP localhost.35683 > localhost.domain: 45021+ PTR? 53.0.0.127.in-addr.arpa. (41)
14:49:56.318699 IP localhost.55249 > localhost.domain: 45706+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
14:49:56.318960 IP praveen.41032 > google-public-dns-a.google.com.domain: 14246+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
14:49:56.362345 IP google-public-dns-a.google.com.domain > praveen.41032: 14246 NXDomain 0/1/0 (154)
14:49:56.363280 IP localhost.41469 > localhost.domain: 44965+ PTR? 8.8.8.8.in-addr.arpa. (38)
14:49:56.363400 IP praveen.53625 > google-public-dns-a.google.com.domain: 59950+ PTR? 8.8.8.8.in-addr.arpa. (38)
14:49:56.495069 IP google-public-dns-a.google.com.domain > praveen.53625: 59950 1/0/0 PTR google-public-dns-a.google.com. (82)
14:49:56.463677 ARP, Request who-has_gateway tell 172.18.5.19, length 46
14:49:56.463823 IP localhost.37004 > localhost.domain: 28653+ PTR? 1.0.18.172.in-addr.arpa. (41)
14:49:56.464014 IP praveen.41269 > google-public-dns-a.google.com.domain: 64882+ PTR? 1.0.18.172.in-addr.arpa. (41)
14:49:56.472523 ARP, Request who-has_gateway tell 172.18.5.19, length 46
14:49:56.506229 IP google-public-dns-a.google.com.domain > praveen.41269: 64882 NXDomain 0/0/0 (41)
14:49:56.872624 ARP, Request who-has 169.254.146.37 tell 172.18.5.2, length 46
14:49:57.723983 ARP, Request who-has 169.254.146.37 tell 172.18.5.2, length 46
14:49:57.791025 ARP, Request who-has 169.254.146.37 tell 172.18.5.30, length 46
14:49:57.791162 IP localhost.56762 > localhost.domain: 64263+ PTR? 30.5.18.172.in-addr.arpa. (42)
14:49:57.791371 IP praveen.54595 > google-public-dns-a.google.com.domain: 3753+ PTR? 30.5.18.172.in-addr.arpa. (42)
14:49:57.832143 IP google-public-dns-a.google.com.domain > praveen.54595: 3753 NXDomain 0/0/0 (42)
14:49:57.832346 IP localhost.domain > localhost.56762: 64263 NXDomain 0/0/0 (42)
14:49:58.383907 ARP, Request who-has 169.254.146.37 tell 172.18.5.30, length 46
14:49:58.724072 ARP, Request who-has 169.254.146.37 tell 172.18.5.2, length 46
14:49:59.316591 IP 172.18.5.58.60284 > 224.0.0.252.hostmon: UDP, length 38
14:49:59.316772 IP localhost.33401 > localhost.domain: 62049+ PTR? 252.0.0.224.in-addr.arpa. (42)
```

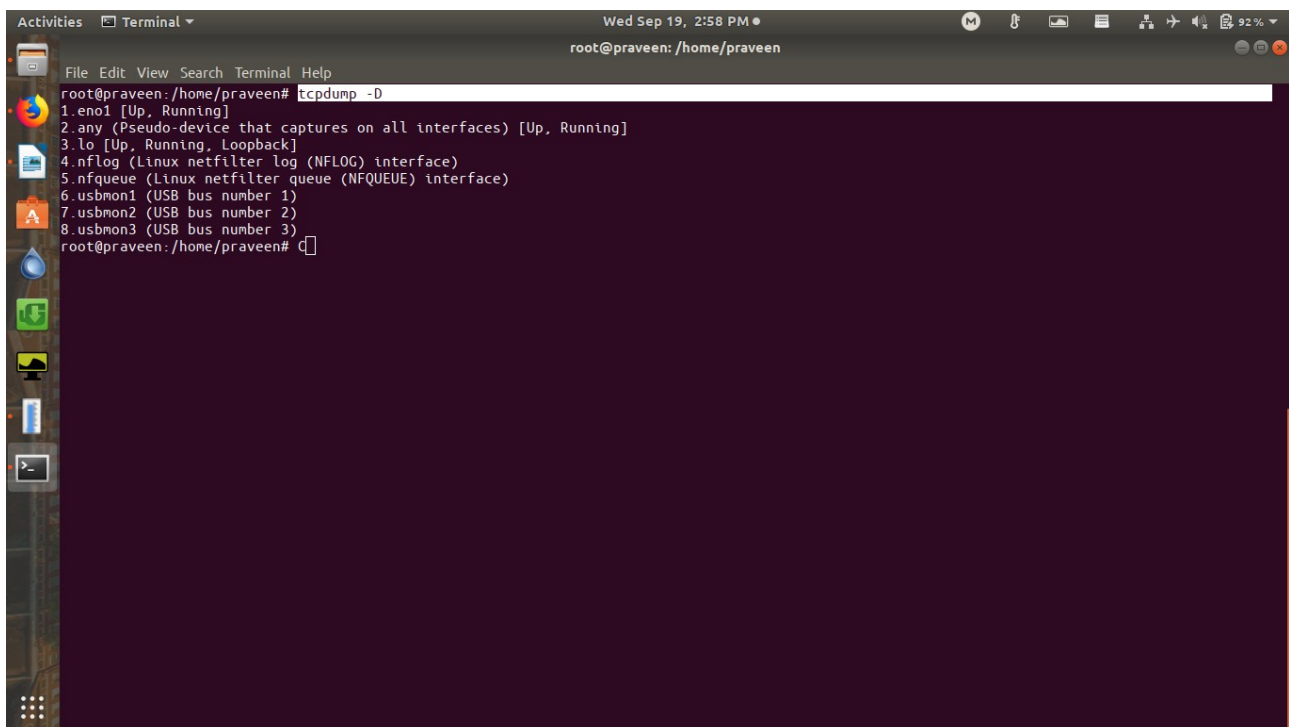

TCP DUMP

2. tcpdump -i eno1 : Listen on the eno1 interface



A terminal window titled 'Terminal' with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Wed Sep 19, 2:57 PM, root@praveen: /home/praveen). The prompt is root@praveen:/home/praveen#. The command tcpdump -i eno1 has been executed. The output shows a list of network packets captured on the eno1 interface, including STP, ARP, and HTTP traffic. The first few lines of output are: tcpdump: verbose output suppressed, use -v or -vv for full protocol decode; listening on eno1, link-type EN10MB (Ethernet), capture size 262144 bytes; 14-57:22.775520 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 8000.08:b2:58:aa:c1:69.81ee, length 43; 14-57:23.171014 IP 172.18.5.34.63506 > 239.255.255.250.1900: UDP, length 174; 14-57:23.172228 IP praveen.55997 > google-public-dns-a.google.com.domain: 9449+ PTR? 34.5.18.172.in-addr.arpa. (42); 14-57:23.213930 IP google-public-dns-a.google.com.domain > praveen.55997: 9449 NXDomain 0/0/0 (42); 14-57:23.214694 IP praveen.38601 > google-public-dns-a.google.com.domain: 64933+ PTR? 52.5.18.172.in-addr.arpa. (42); 14-57:23.257120 IP google-public-dns-a.google.com.domain > praveen.38601: 64933 NXDomain 0/0/0 (42); 14-57:23.290856 IP6 fe80::9cd8:9d16:a955:dd25.62949 > ff02::c.1900: UDP, length 146; 14-57:24.017444 IP6 fe80::6951:cadb:2b13:23d4.dhcpv6-client > ff02::1:2.dhcpv6-server: dhcp6 solicit; 14-57:24.171026 IP 172.18.5.34.63506 > 239.255.255.250.1900: UDP, length 174; 14-57:24.695080 ARP, Request who-has 169.254.146.37 tell 172.18.5.30, length 46; 14-57:24.795570 IP6 praveen.mdns > ff02::fb.mdns: 0 PTR (QM)? 37.146.254.169.in-addr.arpa. (45); 14-57:24.795613 IP praveen.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 37.146.254.169.in-addr.arpa. (45); 14-57:25.016762 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 8000.08:b2:58:aa:c1:69.81ee, length 43; 14-57:25.171135 IP 172.18.5.34.63506 > 239.255.255.250.1900: UDP, length 174; 14-57:25.375987 ARP, Request who-has 169.254.146.37 tell 172.18.5.30, length 46; 14-57:25.796983 IP6 praveen.mdns > ff02::fb.mdns: 0 PTR (QM)? 37.146.254.169.in-addr.arpa. (45); 14-57:30.939424 IP praveen.38664 > ec2-174-129-212-111.compute-1.amazonaws.com.https: Flags [.], ack 252770254, win 1020, options [nop,nop,TS val 68101827 ecr 113675411], length 0; 14-57:30.939562 IP ec2-174-129-212-111.compute-1.amazonaws.com.https > praveen.38664: Flags [.], ack 1, win 483, options [nop,nop,TS val 113676435 ecr 68060925], length 0; 14-57:30.939763 IP praveen.47733 > google-public-dns-a.google.com.domain: 63852+ PTR? 111.212.129.174.in-addr.arpa. (46); 14-57:30.986968 IP google-public-dns-a.google.com.domain > praveen.47733: 63852 1/0/0 PTR ec2-174-129-212-111.compute-1.amazonaws.com. (103); 14-57:31.016723 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 8000.08:b2:58:aa:c1:69.81ee, length 43; 14-57:32.227380 ARP, Request who-has 169.254.146.37 tell 172.18.5.2, length 46; 14-57:32.228144 IP praveen.44688 > google-public-dns-a.google.com.domain: 15805+ PTR? 2.5.18.172.in-addr.arpa. (41); 14-57:32.271253 IP google-public-dns-a.google.com.domain > praveen.44688: 15805 NXDomain 0/0/0 (41); 14-57:32.404104 IP 172.18.5.19.1900 > 239.255.255.250.1900: UDP, length 433; 14-57:32.404276 IP6 fe80::bc47:3ddf:df86:d6ec.1900 > ff02::c.1900: UDP, length 443; 14-57:32.404818 IP praveen.42896 > google-public-dns-a.google.com.domain: 14215+ PTR? 19.5.18.172.in-addr.arpa. (42); 14-57:32.420059 IP 172.18.5.19.1900 > 239.255.255.250.1900: UDP, length 497; 14-57:32.420241 IP6 fe80::bc47:3ddf:df86:d6ec.1900 > ff02::c.1900: UDP, length 507; 14-57:32.420397 IP 172.18.5.19.1900 > 239.255.255.250.1900: UDP, length 513; 14-57:32.420563 IP6 fe80::bc47:3ddf:df86:d6ec.1900 > ff02::c.1900: UDP, length 523; 14-57:32.467087 IP 172.18.5.19.1900 > 239.255.255.250.1900: UDP, length 499;

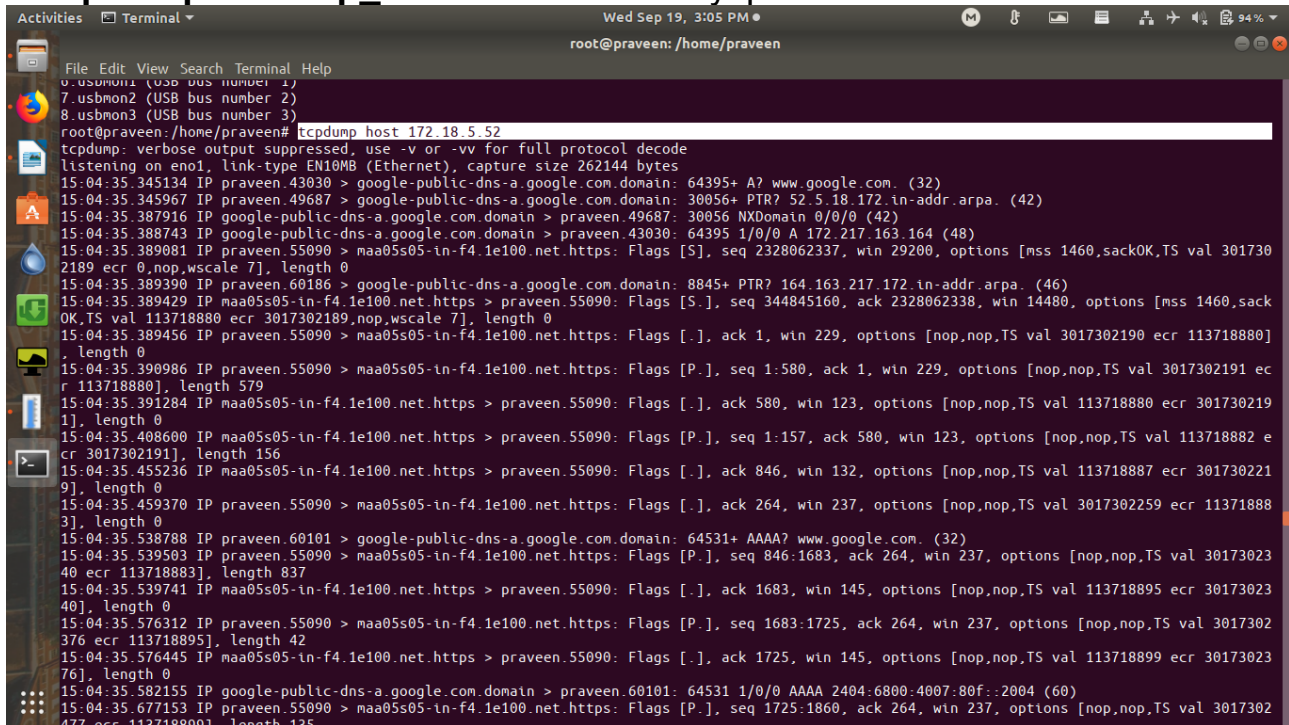
3 . tcpdump -D : show the list of available interfaces



A terminal window titled 'Terminal' with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Wed Sep 19, 2:58 PM, root@praveen: /home/praveen). The prompt is root@praveen:/home/praveen#. The command tcpdump -D has been executed. The output shows a list of available interfaces for tcpdump to listen on: 1.eno1 [Up, Running]; 2.any (Pseudo-device that captures on all interfaces) [Up, Running]; 3.lo [Up, Running, Loopback]; 4.nflog (Linux netfilter log (NFLOG) interface); 5.nfqueue (Linux netfilter queue (NFQUEUE) interface); 6.usbmon1 (USB bus number 1); 7.usbmon2 (USB bus number 2); 8.usbmon3 (USB bus number 3); The prompt is now root@praveen:/home/praveen#.

TCP DUMP

4. tcpdump host <ip_addr> - find traffic by ip address



The screenshot shows a terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Wed Sep 19, 3:05 PM, root@praveen: /home/praveen). The terminal content shows the command `tcpdump host 172.18.5.52` being executed. The output displays network traffic captured on the `eno1` interface, showing various IP addresses and protocols. The output is as follows:

```
File Edit View Search Terminal Help
0.usbmon1 (USB bus number 1)
7.usbmon2 (USB bus number 2)
8.usbmon3 (USB bus number 3)
root@praveen:/home/praveen# tcpdump host 172.18.5.52
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eno1, link-type EN10MB (Ethernet), capture size 262144 bytes
15:04:35.345134 IP praveen.43030 > google-public-dns-a.google.com.domain: 64395+ A? www.google.com. (32)
15:04:35.345967 IP praveen.49687 > google-public-dns-a.google.com.domain: 30056+ PTR? 52.5.18.172.in-addr.arpa. (42)
15:04:35.387916 IP google-public-dns-a.google.com.domain > praveen.49687: 30056 NXDomain 0/0/0 (42)
15:04:35.388743 IP google-public-dns-a.google.com.domain > praveen.43030: 64395 1/0/0 A 172.217.163.164 (48)
15:04:35.389081 IP praveen.55090 > maa05s05-in-f4.1e100.net.https: Flags [S], seq 2328062337, win 29200, options [mss 1460,sackOK,TS val 3017302189 ecr 0,nop,wscale 7], length 0
15:04:35.389390 IP praveen.60186 > google-public-dns-a.google.com.domain: 8845+ PTR? 164.163.217.172.in-addr.arpa. (46)
15:04:35.389429 IP maa05s05-in-f4.1e100.net.https > praveen.55090: Flags [S.], seq 344845160, ack 2328062338, win 14480, options [mss 1460,sackOK,TS val 113718880 ecr 3017302189,nop,wscale 7], length 0
15:04:35.389456 IP praveen.55090 > maa05s05-in-f4.1e100.net.https: Flags [.], ack 1, win 229, options [nop,nop,TS val 3017302190 ecr 113718880], length 0
15:04:35.390986 IP praveen.55090 > maa05s05-in-f4.1e100.net.https: Flags [P.], seq 1:580, ack 1, win 229, options [nop,nop,TS val 3017302191 ecr 113718880], length 579
15:04:35.391284 IP maa05s05-in-f4.1e100.net.https > praveen.55090: Flags [.], ack 580, win 123, options [nop,nop,TS val 113718880 ecr 3017302191], length 0
15:04:35.408600 IP maa05s05-in-f4.1e100.net.https > praveen.55090: Flags [P.], seq 1:157, ack 580, win 123, options [nop,nop,TS val 113718882 ecr 3017302191], length 156
15:04:35.455236 IP maa05s05-in-f4.1e100.net.https > praveen.55090: Flags [.], ack 846, win 132, options [nop,nop,TS val 113718887 ecr 3017302219], length 0
15:04:35.459370 IP praveen.55090 > maa05s05-in-f4.1e100.net.https: Flags [.], ack 264, win 237, options [nop,nop,TS val 3017302259 ecr 113718883], length 0
15:04:35.538788 IP praveen.60101 > google-public-dns-a.google.com.domain: 64531+ AAAA? www.google.com. (32)
15:04:35.539503 IP praveen.55090 > maa05s05-in-f4.1e100.net.https: Flags [P.], seq 846:1683, ack 264, win 237, options [nop,nop,TS val 3017302340 ecr 113718883], length 837
15:04:35.539741 IP maa05s05-in-f4.1e100.net.https > praveen.55090: Flags [.], ack 1683, win 145, options [nop,nop,TS val 113718895 ecr 3017302340], length 0
15:04:35.576312 IP praveen.55090 > maa05s05-in-f4.1e100.net.https: Flags [P.], seq 1683:1725, ack 264, win 237, options [nop,nop,TS val 3017302376 ecr 113718895], length 42
15:04:35.576445 IP maa05s05-in-f4.1e100.net.https > praveen.55090: Flags [.], ack 1725, win 145, options [nop,nop,TS val 113718899 ecr 3017302376], length 0
15:04:35.582155 IP google-public-dns-a.google.com.domain > praveen.60101: 64531 1/0/0 AAAA 2404:6800:4007:80f::2004 (60)
15:04:35.677153 IP praveen.55090 > maa05s05-in-f4.1e100.net.https: Flags [P.], seq 1725:1860, ack 264, win 237, options [nop,nop,TS val 3017302477 ecr 113718899], length 135
```

5 . tcpdump net <subnet_mask> - find packets by subnet

6 . tcpdump port <number> - filter traffic by port number

TCP DUMP

```
Activities Terminal Wed Sep 19, 3:09 PM root@praveen: /home/praveen
File Edit View Search Terminal Help
15:08:32.711579 IP 117.18.237.29.http > praveen.46224: Flags [.], ack 879, win 130, options [nop,nop,TS val 113742612 ecr 1445403556], length 0
^Z
[16]+ Stopped tcpdump port 80
root@praveen:/home/praveen# tcpdump port 21
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eno1, link-type EN10MB (Ethernet), capture size 262144 bytes
^Z
[17]+ Stopped tcpdump port 21
root@praveen:/home/praveen# tcpdump port 22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eno1, link-type EN10MB (Ethernet), capture size 262144 bytes
^Z
[18]+ Stopped tcpdump port 22
root@praveen:/home/praveen# tcpdump port 53
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eno1, link-type EN10MB (Ethernet), capture size 262144 bytes
15:09:45.992519 IP praveen.50532 > google-public-dns-a.google.com.domain: 45713+ A? tiles.services.mozilla.com. (44)
15:09:45.992721 IP praveen.45258 > google-public-dns-a.google.com.domain: 25077+ AAAA? tiles.services.mozilla.com. (44)
15:09:45.993458 IP praveen.38318 > google-public-dns-a.google.com.domain: 51157+ PTR? 52.5.18.172.in-addr.arpa. (42)
15:09:46.034786 IP google-public-dns-a.google.com.domain > praveen.38318: 51157 NXDomain 0/0/0 (42)
15:09:46.035180 IP google-public-dns-a.google.com.domain > praveen.45258: 25077 1/1/0 CNAME tiles.r53-2.services.mozilla.com. (152)
15:09:46.037623 IP google-public-dns-a.google.com.domain > praveen.50532: 45713 9/0/0 CNAME tiles.r53-2.services.mozilla.com., A 52.39.131.77, A 52.41.78.152, A 34.209.108.219, A 34.210.116.46, A 54.148.200.51, A 54.200.49.36, A 54.244.12.88, A 54.70.186.116 (198)
15:09:46.112403 IP praveen.58708 > google-public-dns-a.google.com.domain: 27183+ A? safebrowsing.googleapis.com. (45)
15:09:46.156988 IP google-public-dns-a.google.com.domain > praveen.58708: 27183 1/0/0 A 172.217.163.138 (61)
15:09:46.342378 IP praveen.34151 > google-public-dns-a.google.com.domain: 46846+ A? www.gstatic.com. (33)
15:09:46.387495 IP google-public-dns-a.google.com.domain > praveen.34151: 46846 1/0/0 A 172.217.163.131 (49)
15:09:47.088690 IP praveen.47532 > google-public-dns-a.google.com.domain: 53548+ A? plus.l.google.com. (35)
15:09:47.087074 IP praveen.57154 > google-public-dns-a.google.com.domain: 3825+ AAAA? plus.l.google.com. (35)
15:09:47.103802 IP praveen.55260 > google-public-dns-a.google.com.domain: 22713+ A? www3.l.google.com. (35)
15:09:47.103260 IP praveen.34839 > google-public-dns-a.google.com.domain: 34749+ AAAA? www3.l.google.com. (35)
15:09:47.130916 IP google-public-dns-a.google.com.domain > praveen.47532: 53548 1/0/0 A 172.217.163.174 (51)
15:09:47.131184 IP google-public-dns-a.google.com.domain > praveen.57154: 3825 1/0/0 AAAA 2404:6800:4007:80e::200e (63)
15:09:47.148305 IP google-public-dns-a.google.com.domain > praveen.55260: 22713 1/0/0 A 172.217.163.142 (51)
15:09:47.969439 IP praveen.34839 > google-public-dns-a.google.com.domain: 34749+ AAAA? www3.l.google.com. (35)
15:09:49.719441 IP praveen.34839 > google-public-dns-a.google.com.domain: 34749+ AAAA? www3.l.google.com. (35)
15:09:52.151996 IP google-public-dns-a.google.com.domain > praveen.34839: 34749 1/0/0 AAAA 2404:6800:4007:80e::200e (63)
```

7 . tcpdump <protocol> - filter traffic by protocol

```
Activities Terminal Wed Sep 19, 3:11 PM root@praveen: /home/praveen
File Edit View Search Terminal Help
^Z
[20]+ Stopped tcpdump icmp
root@praveen:/home/praveen# tcpdump tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eno1, link-type EN10MB (Ethernet), capture size 262144 bytes
15:11:09.995993 IP praveen.48494 > 151.101.192.228.https: Flags [P.], seq 3527081222:3527081268, ack 856085495, win 237, options [nop,nop,TS val 749937342 ecr 113758341], length 46
15:11:09.996157 IP 151.101.192.228.https > praveen.48494: Flags [.], ack 46, win 131, options [nop,nop,TS val 113758341 ecr 749937342], length 0
15:11:09.996272 IP praveen.48494 > 151.101.192.228.https: Flags [P.], seq 46:77, ack 1, win 237, options [nop,nop,TS val 749937342 ecr 113758341], length 31
15:11:09.996289 IP praveen.48494 > 151.101.192.228.https: Flags [F.], seq 77, ack 1, win 237, options [nop,nop,TS val 749937342 ecr 113758341], length 0
15:11:09.996408 IP 151.101.192.228.https > praveen.48494: Flags [.], ack 77, win 131, options [nop,nop,TS val 113758341 ecr 749937342], length 0
15:11:09.996441 IP 151.101.192.228.https > praveen.48494: Flags [F.], seq 1, ack 78, win 131, options [nop,nop,TS val 113758341 ecr 749937342], length 0
15:11:09.996453 IP praveen.48494 > 151.101.192.228.https: Flags [.], ack 2, win 237, options [nop,nop,TS val 749937343 ecr 113758341], length 0
15:11:13.996604 IP praveen.36622 > maa05s05-in-f14.1e100.net.https: Flags [P.], seq 3335474684:3335474730, ack 2027592295, win 237, options [nop,nop,TS val 3671567681 ecr 113753312], length 46
15:11:13.996714 IP praveen.37106 > maa05s05-in-f3.1e100.net.https: Flags [P.], seq 3184048930:3184048976, ack 1244970467, win 336, options [nop,nop,TS val 2538451517 ecr 113753312], length 46
15:11:13.996932 IP praveen.37106 > maa05s05-in-f3.1e100.net.https: Flags [P.], seq 46:77, ack 1, win 336, options [nop,nop,TS val 2538451517 ecr 113753312], length 31
15:11:13.996950 IP praveen.37106 > maa05s05-in-f3.1e100.net.https: Flags [F.], seq 77, ack 1, win 336, options [nop,nop,TS val 2538451517 ecr 113753312], length 0
15:11:13.997061 IP maa05s05-in-f3.1e100.net.https > praveen.37106: Flags [.], ack 78, win 141, options [nop,nop,TS val 113758741 ecr 2538451517], length 0
15:11:13.997097 IP maa05s05-in-f3.1e100.net.https > praveen.37106: Flags [F.], seq 1, ack 78, win 141, options [nop,nop,TS val 113758741 ecr 2538451517], length 0
15:11:13.997112 IP praveen.37106 > maa05s05-in-f3.1e100.net.https: Flags [.], ack 2, win 336, options [nop,nop,TS val 2538451517 ecr 113758741], length 0
15:11:13.997172 IP praveen.36622 > maa05s05-in-f14.1e100.net.https: Flags [P.], seq 46:77, ack 1, win 237, options [nop,nop,TS val 3671567681 ecr 113753312], length 31
15:11:13.997299 IP maa05s05-in-f14.1e100.net.https > praveen.36622: Flags [.], ack 78, win 144, options [nop,nop,TS val 113758741 ecr 3671567681], length 0
15:11:13.997330 IP maa05s05-in-f14.1e100.net.https > praveen.36622: Flags [F.], seq 1, ack 78, win 144, options [nop,nop,TS val 113758741 ecr 3671567681], length 0
```