NETWORKING & SYSTEM ADMINISTRATION LAB

Name: ALLEN S PHILIP

Roll No: 20

Batch: RMCA- A

Date: 03/06/2022

Experiment No.: 1

Aim

Analyzing network packets stream using tcpdump, wireshark and netcat.

Procedure

1. Tcpdump

$sudo apt install tcpdump :Installation

Packet-Listing

$sudo tcpdump :To list all packets

$sudo tcpdump -D : To list network cards(devies)

$sudo tcpdump -i <device_name> : To list packets from specific device

$sudo tcpdump -c 5 -i <device_name> : To list first five packets from specified device

Filtering-Options

$sudo tcpdump -c 5 -i <device_name> port <port_no> : List packets from port 80

$sudo tcpdump -i <device_name> not <protocol> : To avoid packets from specified protocol.

$sudo tcpdump -i <device_name> -c 10 -w <file_name>.pcap : Write captured details to file

$sudo tcpdump -r <file_name>.pcap : Display Captured Details

2. Wireshark

$sudo apt install wireshark   :Installation

$sudo usermod -aG wireshark allensphilip : Giving user acess permission of wireshark

$sudo wireshark : To open wireshark

3. NetCat

- Known as the swiss knife of network admiinnistrators
- In ubuntu nc or netcat both valid

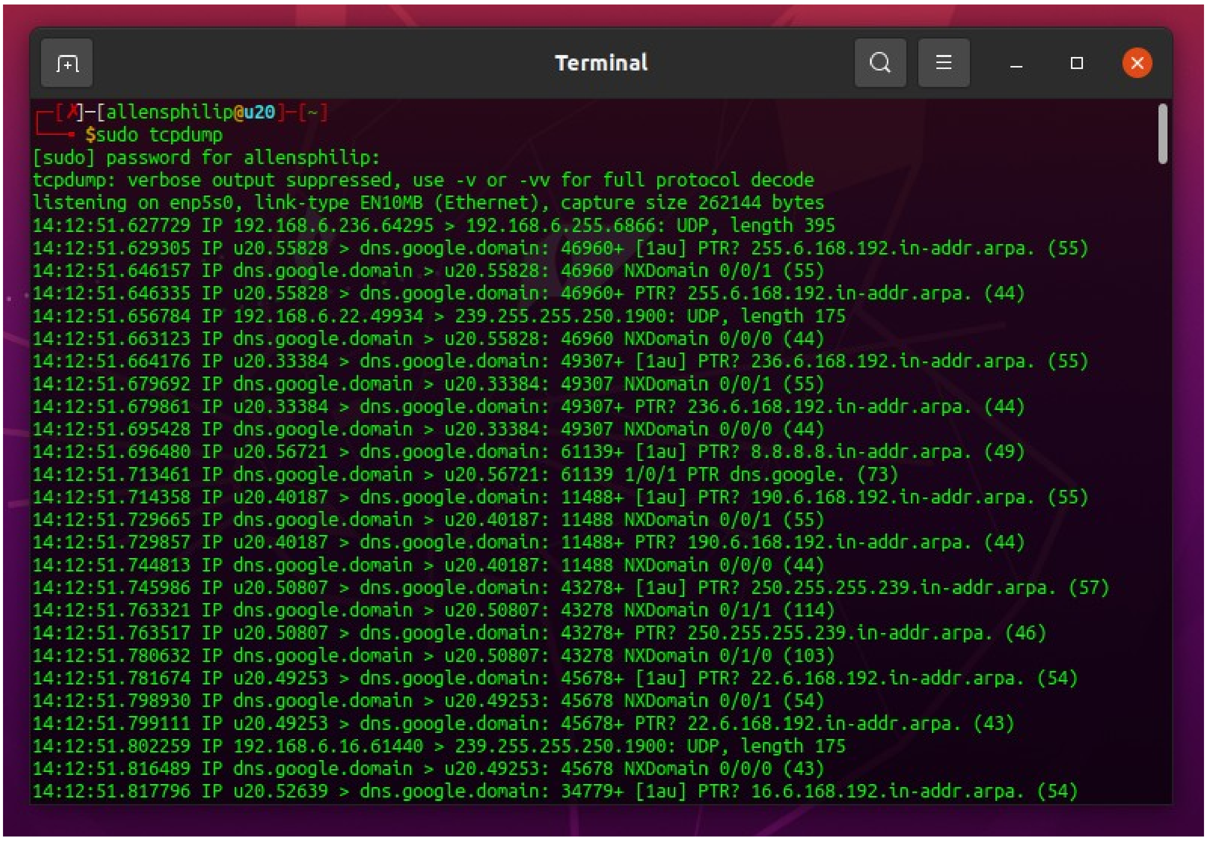
Syntax:

```
nc [option] host port
```

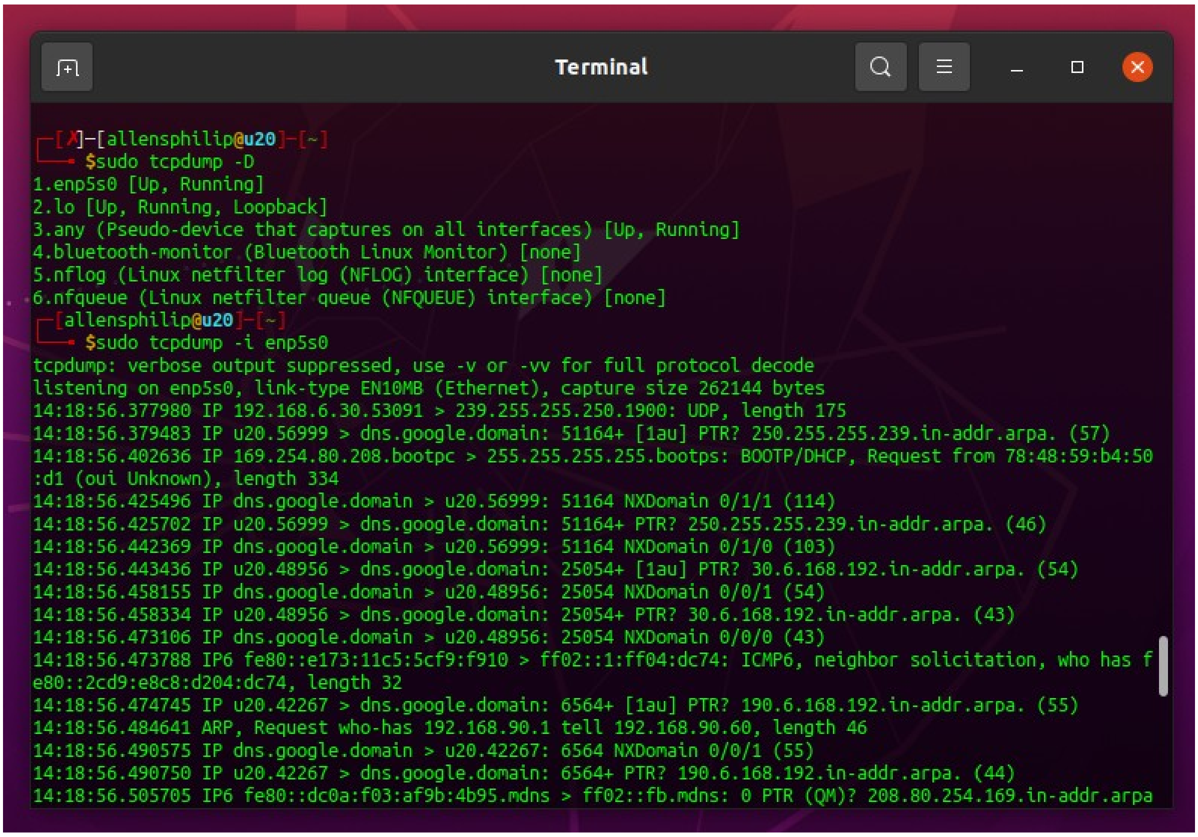
```
$sudo apt-get install netcat   :  Installation
 $nc -l -p <port_no>     : Opening listener,
                           -l  : listining,  -p :port
$nc <host> <port>         : Opening listener
$nc -i <intervel_count> <host> :  send with an intervel
```

Output Screenshot

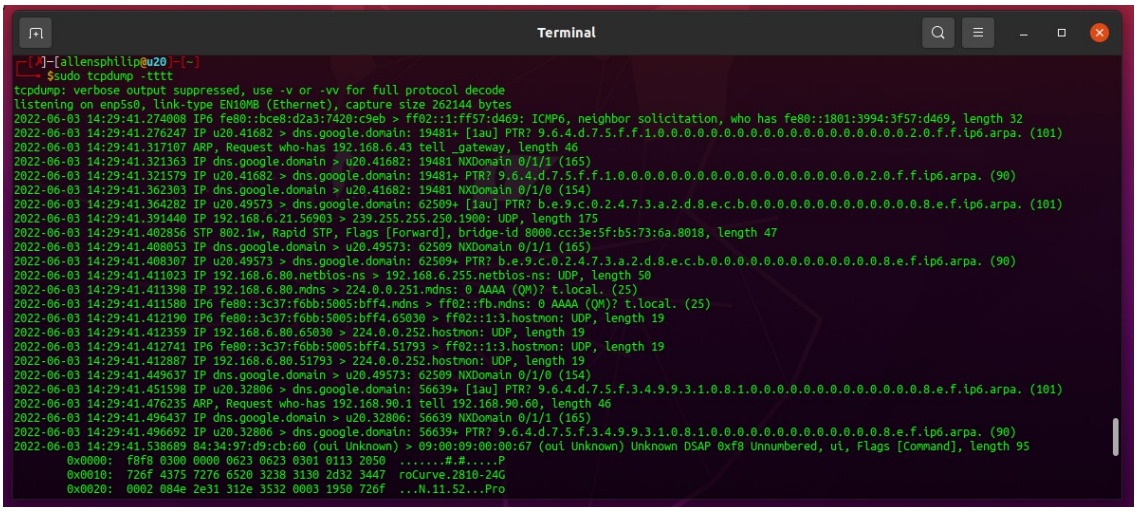
Tcpdump- Packet-Listing



```
┌─[✗]─[allensphilip@u20]─[~]
└──╼ $sudo tcpdump
[sudo] password for allensphilip:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:12:51.627729 IP 192.168.6.236.64295 > 192.168.6.255.6866: UDP, length 395
14:12:51.629305 IP u20.55828 > dns.google.domain: 46960+ [1au] PTR? 255.6.168.192.in-addr.arpa. (55)
14:12:51.646157 IP dns.google.domain > u20.55828: 46960 NXDomain 0/0/1 (55)
14:12:51.646335 IP u20.55828 > dns.google.domain: 46960+ PTR? 255.6.168.192.in-addr.arpa. (44)
14:12:51.656784 IP 192.168.6.22.49934 > 239.255.255.250.1900: UDP, length 175
14:12:51.663123 IP dns.google.domain > u20.55828: 46960 NXDomain 0/0/0 (44)
14:12:51.664176 IP u20.33384 > dns.google.domain: 49307+ [1au] PTR? 236.6.168.192.in-addr.arpa. (55)
14:12:51.679692 IP dns.google.domain > u20.33384: 49307 NXDomain 0/0/1 (55)
14:12:51.679861 IP u20.33384 > dns.google.domain: 49307+ PTR? 236.6.168.192.in-addr.arpa. (44)
14:12:51.695428 IP dns.google.domain > u20.33384: 49307 NXDomain 0/0/0 (44)
14:12:51.696480 IP u20.56721 > dns.google.domain: 61139+ [1au] PTR? 8.8.8.8.in-addr.arpa. (49)
14:12:51.713461 IP dns.google.domain > u20.56721: 61139 1/0/1 PTR dns.google. (73)
14:12:51.714358 IP u20.40187 > dns.google.domain: 11488+ [1au] PTR? 190.6.168.192.in-addr.arpa. (55)
14:12:51.729665 IP dns.google.domain > u20.40187: 11488 NXDomain 0/0/1 (55)
14:12:51.729857 IP u20.40187 > dns.google.domain: 11488+ PTR? 190.6.168.192.in-addr.arpa. (44)
14:12:51.744813 IP dns.google.domain > u20.40187: 11488 NXDomain 0/0/0 (44)
14:12:51.745986 IP u20.50807 > dns.google.domain: 43278+ [1au] PTR? 250.255.255.239.in-addr.arpa. (57)
14:12:51.763321 IP dns.google.domain > u20.50807: 43278 NXDomain 0/1/1 (114)
14:12:51.763517 IP u20.50807 > dns.google.domain: 43278+ PTR? 250.255.255.239.in-addr.arpa. (46)
14:12:51.780632 IP dns.google.domain > u20.50807: 43278 NXDomain 0/1/0 (103)
14:12:51.781674 IP u20.49253 > dns.google.domain: 45678+ [1au] PTR? 22.6.168.192.in-addr.arpa. (54)
14:12:51.798930 IP dns.google.domain > u20.49253: 45678 NXDomain 0/0/1 (54)
14:12:51.799111 IP u20.49253 > dns.google.domain: 45678+ PTR? 22.6.168.192.in-addr.arpa. (43)
14:12:51.802259 IP 192.168.6.16.61440 > 239.255.255.250.1900: UDP, length 175
14:12:51.816489 IP dns.google.domain > u20.49253: 45678 NXDomain 0/0/0 (43)
14:12:51.817796 IP u20.52639 > dns.google.domain: 34779+ [1au] PTR? 16.6.168.192.in-addr.arpa. (54)
```

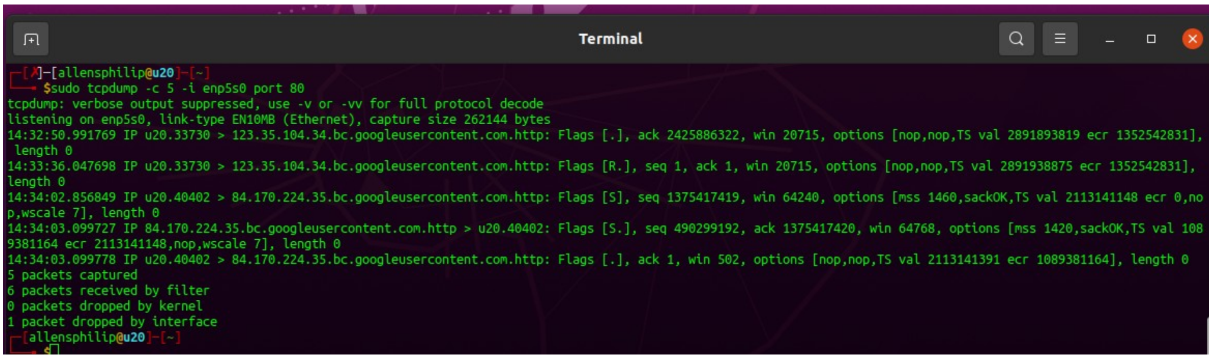


```
┌─[✗]─[allensphilip@u20]─[~]
└──╼ $sudo tcpdump -D
1.enp5s0 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
┌─[allensphilip@u20]─[~]
└──╼ $sudo tcpdump -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:18:56.377980 IP 192.168.6.30.53091 > 239.255.255.250.1900: UDP, length 175
14:18:56.379483 IP u20.56999 > dns.google.domain: 51164+ [1au] PTR? 250.255.255.239.in-addr.arpa. (57)
14:18:56.402636 IP 169.254.80.208.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 78:48:59:b4:50
:d1 (oui Unknown), length 334
14:18:56.425496 IP dns.google.domain > u20.56999: 51164 NXDomain 0/1/1 (114)
14:18:56.425702 IP u20.56999 > dns.google.domain: 51164+ PTR? 250.255.255.239.in-addr.arpa. (46)
14:18:56.442369 IP dns.google.domain > u20.56999: 51164 NXDomain 0/1/0 (103)
14:18:56.443436 IP u20.48956 > dns.google.domain: 25054+ [1au] PTR? 30.6.168.192.in-addr.arpa. (54)
14:18:56.458155 IP dns.google.domain > u20.48956: 25054 NXDomain 0/0/1 (54)
14:18:56.458334 IP u20.48956 > dns.google.domain: 25054+ PTR? 30.6.168.192.in-addr.arpa. (43)
14:18:56.473106 IP dns.google.domain > u20.48956: 25054 NXDomain 0/0/0 (43)
14:18:56.473788 IP6 fe80::e173:11c5:5cf9:f910 > ff02::1:ff04:dc74: ICMP6, neighbor solicitation, who has f
e80::2cd9:e8c8:d204:dc74, length 32
14:18:56.474745 IP u20.42267 > dns.google.domain: 6564+ [1au] PTR? 190.6.168.192.in-addr.arpa. (55)
14:18:56.484641 ARP, Request who-has 192.168.90.1 tell 192.168.90.60, length 46
14:18:56.490575 IP dns.google.domain > u20.42267: 6564 NXDomain 0/0/1 (55)
14:18:56.490750 IP u20.42267 > dns.google.domain: 6564+ PTR? 190.6.168.192.in-addr.arpa. (44)
14:18:56.505705 IP6 fe80::dc0a:f03:af9b:4b95.mdns > ff02::fb.mdns: 0 PTR (QM)? 208.80.254.169.in-addr.arpa
```

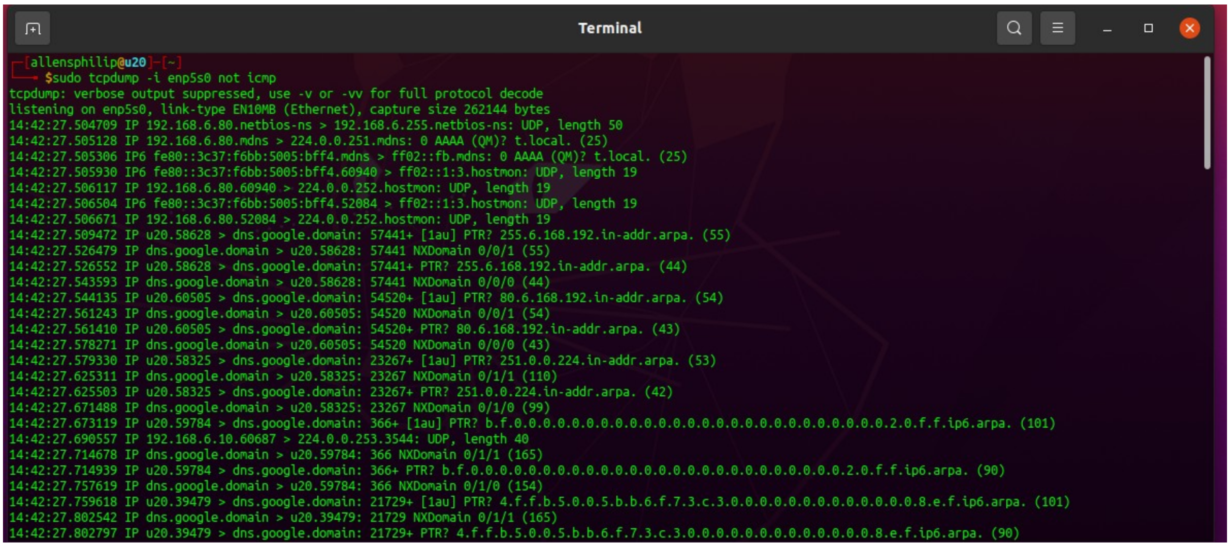


```
┌─[✗]─[allensphilip@u20]─[~]
└──╼ $sudo tcpdump -tttt
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
2022-06-03 14:29:41.274008 IP6 fe80::bce8:d2a3:7420:c9eb > ff02::1:ff57:d469: ICMP6, neighbor solicitation, who has fe80::1801:3994:3f57:d469, length 32
2022-06-03 14:29:41.276247 IP u20.41682 > dns.google.domain: 19481+ [1au] PTR? 9.6.4.d.7.5.f.f.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (101)
2022-06-03 14:29:41.317107 ARP, Request who-has 192.168.6.43 tell _gateway, length 46
2022-06-03 14:29:41.321363 IP dns.google.domain > u20.41682: 19481 NXDomain 0/1/1 (165)
2022-06-03 14:29:41.321579 IP u20.41682 > dns.google.domain: 19481+ PTR? 9.6.4.d.7.5.f.f.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
2022-06-03 14:29:41.362303 IP dns.google.domain > u20.41682: 19481 NXDomain 0/1/0 (154)
2022-06-03 14:29:41.364282 IP u20.49573 > dns.google.domain: 62509+ [1au] PTR? b.e.9.c.0.2.4.7.3.a.2.d.8.e.c.b.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (101)
2022-06-03 14:29:41.391440 IP 192.168.6.21.56903 > 239.255.255.250.1900: UDP, length 175
2022-06-03 14:29:41.402856 STP 802.1w, Rapid STP, Flags [Forward], bridge-id 8000.cc:3e:5f:b5:73:6a.8018, length 47
2022-06-03 14:29:41.408053 IP dns.google.domain > u20.49573: 62509 NXDomain 0/1/1 (165)
2022-06-03 14:29:41.408307 IP u20.49573 > dns.google.domain: 62509+ PTR? b.e.9.c.0.2.4.7.3.a.2.d.8.e.c.b.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
2022-06-03 14:29:41.411023 IP 192.168.6.80.netbios-ns > 192.168.6.255.netbios-ns: UDP, length 50
2022-06-03 14:29:41.411398 IP 192.168.6.80.mdns > 224.0.0.251.mdns: 0 AAAA (QM)? t.local. (25)
2022-06-03 14:29:41.411580 IP6 fe80::3c37:f6bb:5005:bff4.mdns > ff02::fb.mdns: 0 AAAA (QM)? t.local. (25)
2022-06-03 14:29:41.412190 IP6 fe80::3c37:f6bb:5005:bff4.65030 > ff02::1:3.hostmon: UDP, length 19
2022-06-03 14:29:41.412359 IP 192.168.6.80.65030 > 224.0.0.252.hostmon: UDP, length 19
2022-06-03 14:29:41.412741 IP6 fe80::3c37:f6bb:5005:bff4.51793 > ff02::1:3.hostmon: UDP, length 19
2022-06-03 14:29:41.412887 IP 192.168.6.80.51793 > 224.0.0.252.hostmon: UDP, length 19
2022-06-03 14:29:41.449637 IP dns.google.domain > u20.49573: 62509 NXDomain 0/1/0 (154)
2022-06-03 14:29:41.451598 IP u20.32806 > dns.google.domain: 56639+ [1au] PTR? 9.6.4.d.7.5.f.3.4.9.9.3.1.0.8.1.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (101)
2022-06-03 14:29:41.476235 ARP, Request who-has 192.168.90.1 tell 192.168.90.60, length 46
2022-06-03 14:29:41.496437 IP dns.google.domain > u20.32806: 56639 NXDomain 0/1/1 (165)
2022-06-03 14:29:41.496692 IP u20.32806 > dns.google.domain: 56639+ PTR? 9.6.4.d.7.5.f.3.4.9.9.3.1.0.8.1.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
2022-06-03 14:29:41.538689 84:34:97:d9:cb:60 (oui Unknown) > 09:00:09:00:00:67 (oui Unknown) Unknown DSAP 0xf8 Unnumbered, ui, Flags [Command], length 95
        0x0000:  f8f8 0300 0000 0623 0623 0301 0113 2050  .......#.#.....P
        0x0010:  726f 4375 7276 6520 3238 3130 2d32 3447  roCurve.2810-24G
        0x0020:  0002 084e 2e31 312e 3532 0003 1950 726f  ...N.11.52...Pro
```

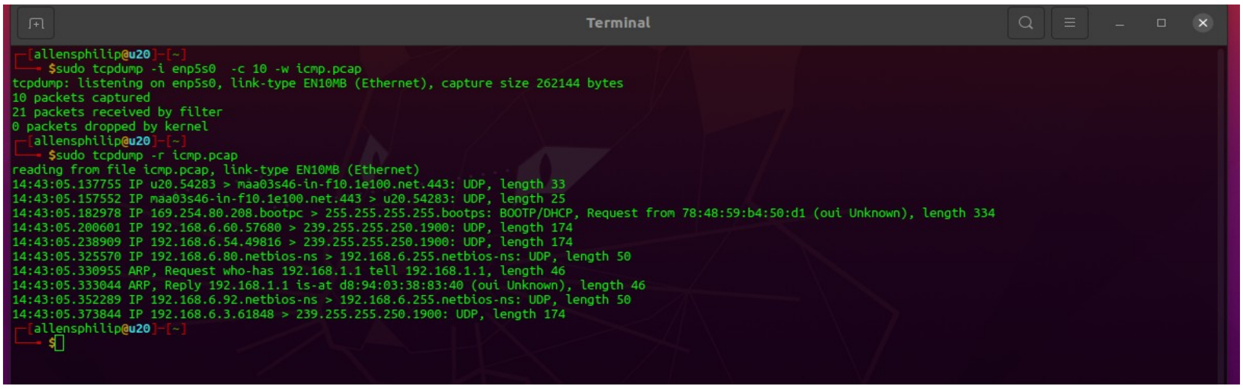
Tcpdump- Filtering-Options



```
┌─[✗]─[allensphilip@u20]─[~]
└──╼ $sudo tcpdump -c 5 -i enp5s0 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:32:50.991769 IP u20.33730 > 123.35.104.34.bc.googleusercontent.com.http: Flags [.], ack 2425886322, win 20715, options [nop,nop,TS val 2891893819 ecr 1352542831],
 length 0
14:33:36.047698 IP u20.33730 > 123.35.104.34.bc.googleusercontent.com.http: Flags [R.], seq 1, ack 1, win 20715, options [nop,nop,TS val 2891938875 ecr 1352542831],
length 0
14:34:02.856849 IP u20.40402 > 84.170.224.35.bc.googleusercontent.com.http: Flags [S], seq 1375417419, win 64240, options [mss 1460,sackOK,TS val 2113141148 ecr 0,no
p,wscale 7], length 0
14:34:03.099727 IP 84.170.224.35.bc.googleusercontent.com.http > u20.40402: Flags [S.], seq 490299192, ack 1375417420, win 64768, options [mss 1420,sackOK,TS val 108
9381164 ecr 2113141148,nop,wscale 7], length 0
14:34:03.099778 IP u20.40402 > 84.170.224.35.bc.googleusercontent.com.http: Flags [.], ack 1, win 502, options [nop,nop,TS val 2113141391 ecr 1089381164], length 0
5 packets captured
6 packets received by filter
0 packets dropped by kernel
1 packet dropped by interface
┌─[allensphilip@u20]─[~]
└──╼ $
```

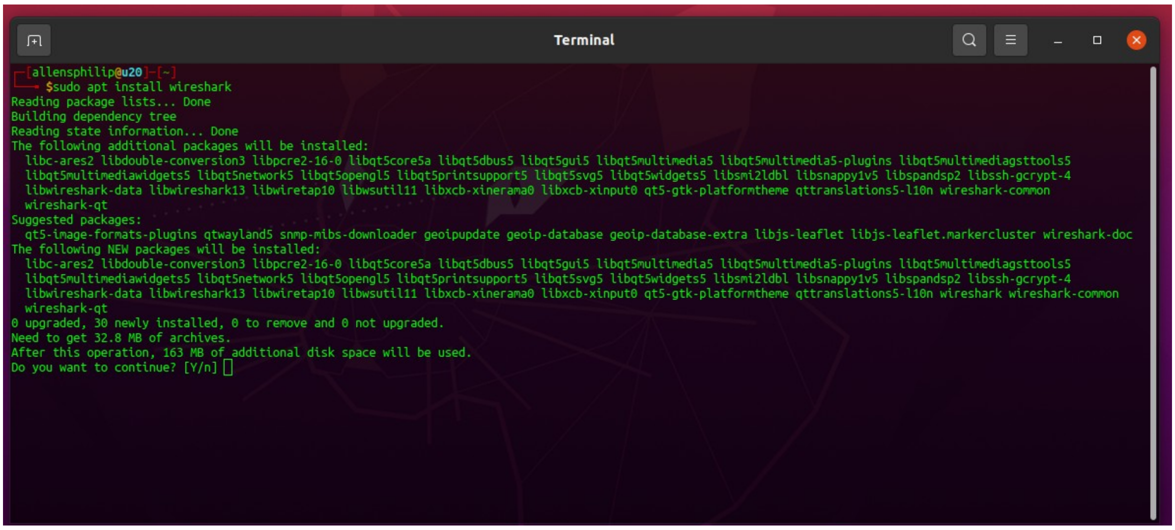


```
┌─[allensphilip@u20]─[~]
└──╼ $sudo tcpdump -i enp5s0 not icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:42:27.504709 IP 192.168.6.80.netbios-ns > 192.168.6.255.netbios-ns: UDP, length 50
14:42:27.505128 IP 192.168.6.80.mdns > 224.0.0.251.mdns: 0 AAAA (QM)? t.local. (25)
14:42:27.505306 IP6 fe80::3c37:f6bb:5005:bff4.mdns > ff02::fb.mdns: 0 AAAA (QM)? t.local. (25)
14:42:27.505930 IP6 fe80::3c37:f6bb:5005:bff4.60940 > ff02::1:3.hostmon: UDP, length 19
14:42:27.506117 IP 192.168.6.80.60940 > 224.0.0.252.hostmon: UDP, length 19
14:42:27.506504 IP6 fe80::3c37:f6bb:5005:bff4.52084 > ff02::1:3.hostmon: UDP, length 19
14:42:27.506671 IP 192.168.6.80.52084 > 224.0.0.252.hostmon: UDP, length 19
14:42:27.509472 IP u20.58628 > dns.google.domain: 57441+ [1au] PTR? 255.6.168.192.in-addr.arpa. (55)
14:42:27.526479 IP dns.google.domain > u20.58628: 57441 NXDomain 0/0/1 (55)
14:42:27.526552 IP u20.58628 > dns.google.domain: 57441+ PTR? 255.6.168.192.in-addr.arpa. (44)
14:42:27.543593 IP dns.google.domain > u20.58628: 57441 NXDomain 0/0/0 (44)
14:42:27.544135 IP u20.60505 > dns.google.domain: 54520+ [1au] PTR? 80.6.168.192.in-addr.arpa. (54)
14:42:27.561243 IP dns.google.domain > u20.60505: 54520 NXDomain 0/0/1 (54)
14:42:27.561410 IP u20.60505 > dns.google.domain: 54520+ PTR? 80.6.168.192.in-addr.arpa. (43)
14:42:27.578271 IP dns.google.domain > u20.60505: 54520 NXDomain 0/0/0 (43)
14:42:27.579330 IP u20.58325 > dns.google.domain: 23267+ [1au] PTR? 251.0.0.224.in-addr.arpa. (53)
14:42:27.625311 IP dns.google.domain > u20.58325: 23267 NXDomain 0/1/1 (110)
14:42:27.625503 IP u20.58325 > dns.google.domain: 23267+ PTR? 251.0.0.224.in-addr.arpa. (42)
14:42:27.671488 IP dns.google.domain > u20.58325: 23267 NXDomain 0/1/0 (99)
14:42:27.673119 IP u20.59784 > dns.google.domain: 366+ [1au] PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (101)
14:42:27.690557 IP 192.168.6.10.60687 > 224.0.0.253.3544: UDP, length 40
14:42:27.714678 IP dns.google.domain > u20.59784: 366 NXDomain 0/1/1 (165)
14:42:27.714939 IP u20.59784 > dns.google.domain: 366+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
14:42:27.757619 IP dns.google.domain > u20.59784: 366 NXDomain 0/1/0 (154)
14:42:27.759618 IP u20.39479 > dns.google.domain: 21729+ [1au] PTR? 4.f.f.b.5.0.0.5.b.b.6.f.7.3.c.3.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (101)
14:42:27.802542 IP dns.google.domain > u20.39479: 21729 NXDomain 0/1/1 (165)
14:42:27.802797 IP u20.39479 > dns.google.domain: 21729+ PTR? 4.f.f.b.5.0.0.5.b.b.6.f.7.3.c.3.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
```

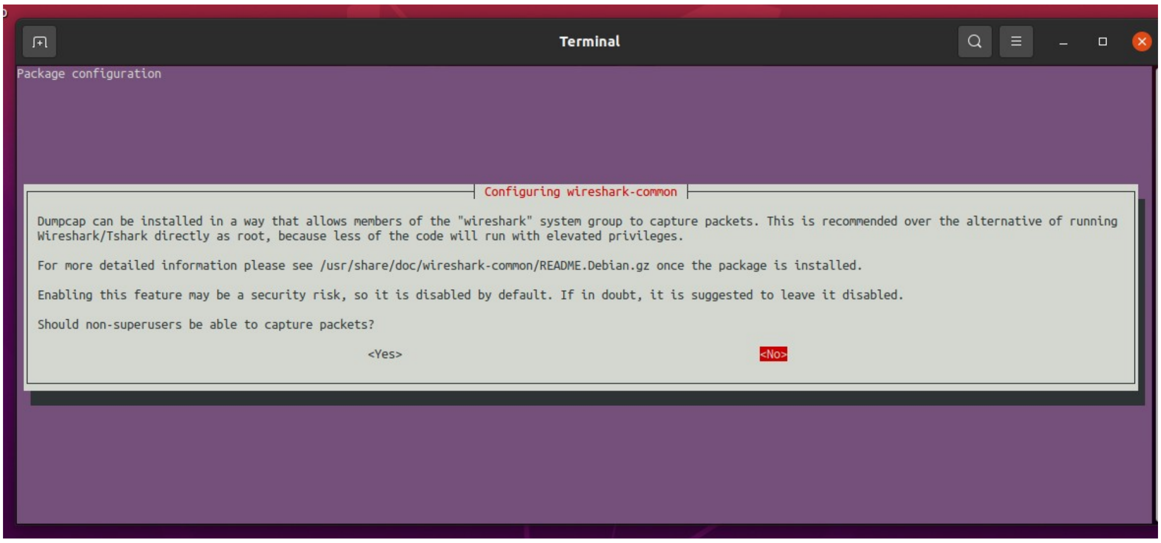


```
┌─[allensphilip@u20]─[~]
└──╼ $sudo tcpdump -i enp5s0  -c 10 -w icmp.pcap
tcpdump: listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
10 packets captured
21 packets received by filter
0 packets dropped by kernel
┌─[allensphilip@u20]─[~]
└──╼ $sudo tcpdump -r icmp.pcap
reading from file icmp.pcap, link-type EN10MB (Ethernet)
14:43:05.137755 IP u20.54283 > maa03s46-in-f10.1e100.net.443: UDP, length 33
14:43:05.157552 IP maa03s46-in-f10.1e100.net.443 > u20.54283: UDP, length 25
14:43:05.182978 IP 169.254.80.208.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 78:48:59:b4:50:d1 (oui Unknown), length 334
14:43:05.200601 IP 192.168.6.60.57680 > 239.255.255.250.1900: UDP, length 174
14:43:05.238909 IP 192.168.6.54.49816 > 239.255.255.250.1900: UDP, length 174
14:43:05.325570 IP 192.168.6.80.netbios-ns > 192.168.6.255.netbios-ns: UDP, length 50
14:43:05.330955 ARP, Request who-has 192.168.1.1 tell 192.168.1.1, length 46
14:43:05.333044 ARP, Reply 192.168.1.1 is-at d8:94:03:38:83:40 (oui Unknown), length 46
14:43:05.352289 IP 192.168.6.92.netbios-ns > 192.168.6.255.netbios-ns: UDP, length 50
14:43:05.373844 IP 192.168.6.3.61848 > 239.255.255.250.1900: UDP, length 174
┌─[allensphilip@u20]─[~]
└──╼ $
```

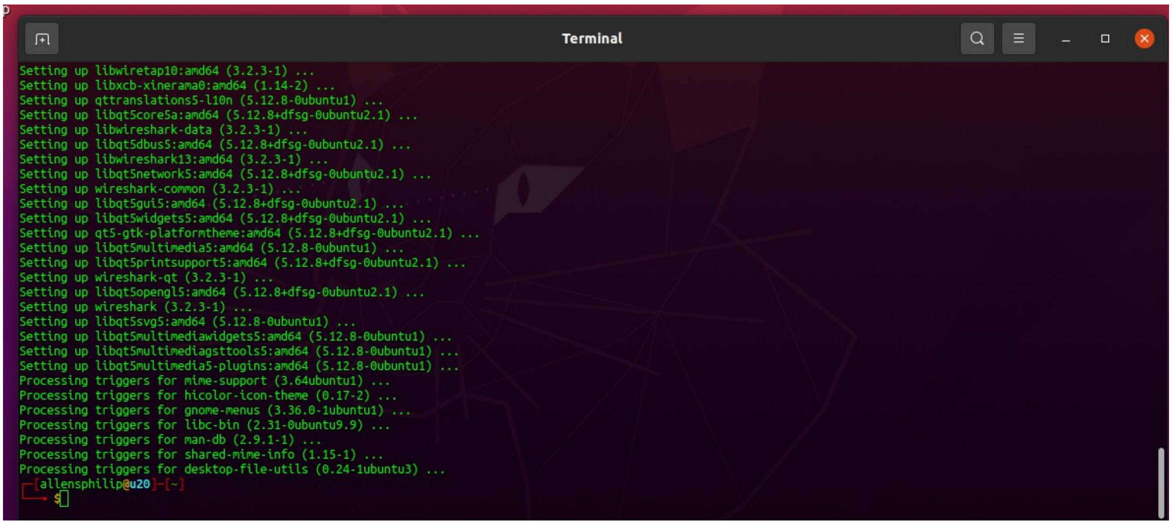
Wireshark



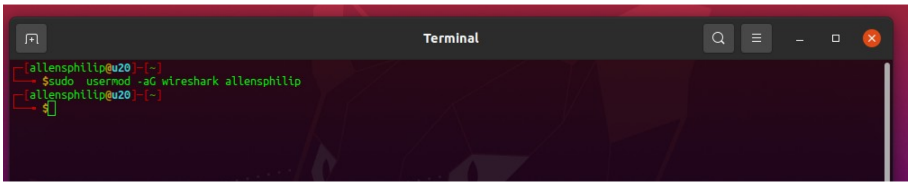
```
┌─[allensphilip@u20]─[~]
└──╼ $sudo apt install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libc-ares2 libdouble-conversion3 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5 libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4
  libwireshark-data libwireshark13 libwiretap10 libwsutil11 libxcb-xinerama0 libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n wireshark-common
  wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate geoip-database geoip-database-extra libjs-leaflet libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libdouble-conversion3 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5 libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4
  libwireshark-data libwireshark13 libwiretap10 libwsutil11 libxcb-xinerama0 libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common
  wireshark-qt
0 upgraded, 30 newly installed, 0 to remove and 0 not upgraded.
Need to get 32.8 MB of archives.
After this operation, 163 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```



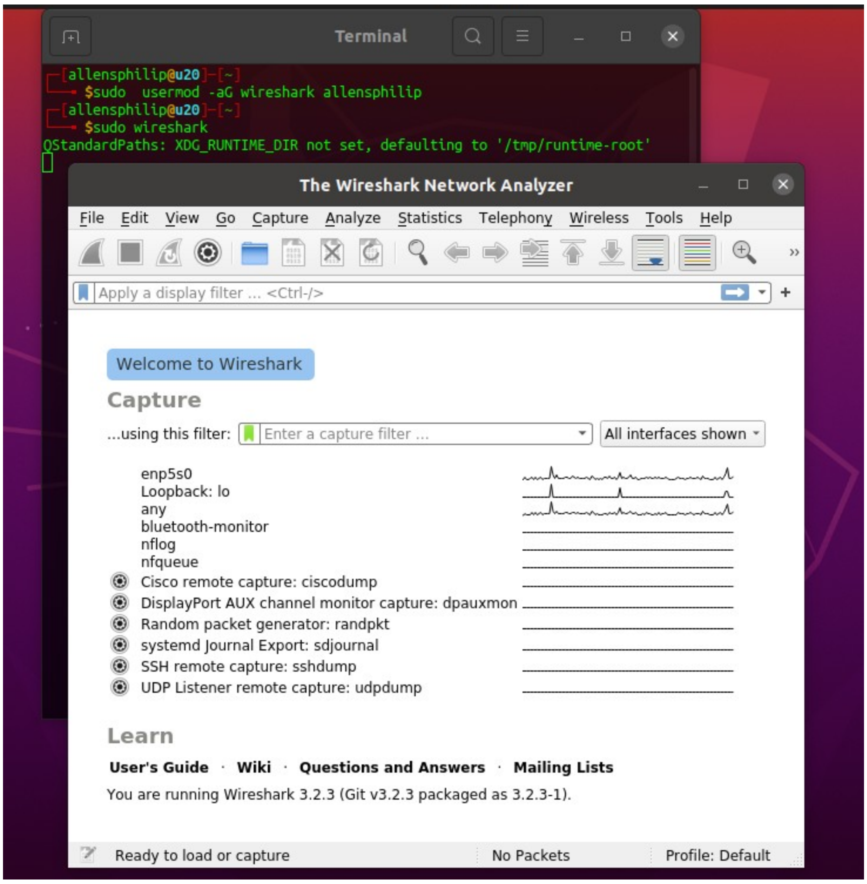
```
Package configuration

                    ┤ Configuring wireshark-common ├

 Dumpcap can be installed in a way that allows members of the "wireshark" system group to capture packets. This is recommended over the alternative of running
 Wireshark/Tshark directly as root, because less of the code will run with elevated privileges.

 For more detailed information please see /usr/share/doc/wireshark-common/README.Debian.gz once the package is installed.

 Enabling this feature may be a security risk, so it is disabled by default. If in doubt, it is suggested to leave it disabled.

 Should non-superusers be able to capture packets?

                         <Yes>                                        <No>
```



```
Setting up libwiretap10:amd64 (3.2.3-1) ...
Setting up libxcb-xinerama0:amd64 (1.14-2) ...
Setting up qttranslations5-l10n (5.12.8-0ubuntu1) ...
Setting up libqt5core5a:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Setting up libwireshark-data (3.2.3-1) ...
Setting up libqt5dbus5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Setting up libwireshark13:amd64 (3.2.3-1) ...
Setting up libqt5network5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Setting up wireshark-common (3.2.3-1) ...
Setting up libqt5gui5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Setting up libqt5widgets5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Setting up qt5-gtk-platformtheme:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Setting up libqt5multimedia5:amd64 (5.12.8-0ubuntu1) ...
Setting up libqt5printsupport5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Setting up wireshark-qt (3.2.3-1) ...
Setting up libqt5opengl5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Setting up wireshark (3.2.3-1) ...
Setting up libqt5svg5:amd64 (5.12.8-0ubuntu1) ...
Setting up libqt5multimediawidgets5:amd64 (5.12.8-0ubuntu1) ...
Setting up libqt5multimediagsttools5:amd64 (5.12.8-0ubuntu1) ...
Setting up libqt5multimedia5-plugins:amd64 (5.12.8-0ubuntu1) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.9) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for shared-mime-info (1.15-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
┌─[allensphilip@u20]─[~]
└──╼ $
```



```
┌─[allensphilip@u20]─[~]
└──╼ $sudo  usermod -aG wireshark allensphilip
┌─[allensphilip@u20]─[~]
└──╼ $
```


Terminal
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Enter a capture filter …
All interfaces shown

```
┌─[allensphilip@u20]─[~]
└──╼ $sudo  usermod -aG wireshark allensphilip
┌─[allensphilip@u20]─[~]
└──╼ $sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

Capture

…using this filter:

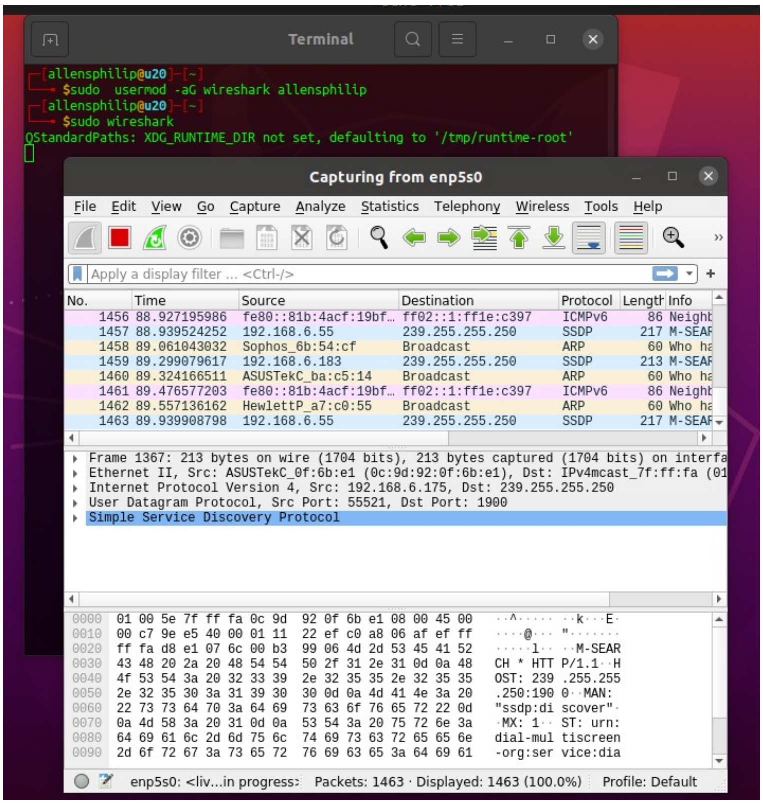
enp5s0
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).

Ready to load or capture | No Packets | Profile: Default


Terminal
Capturing from enp5s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

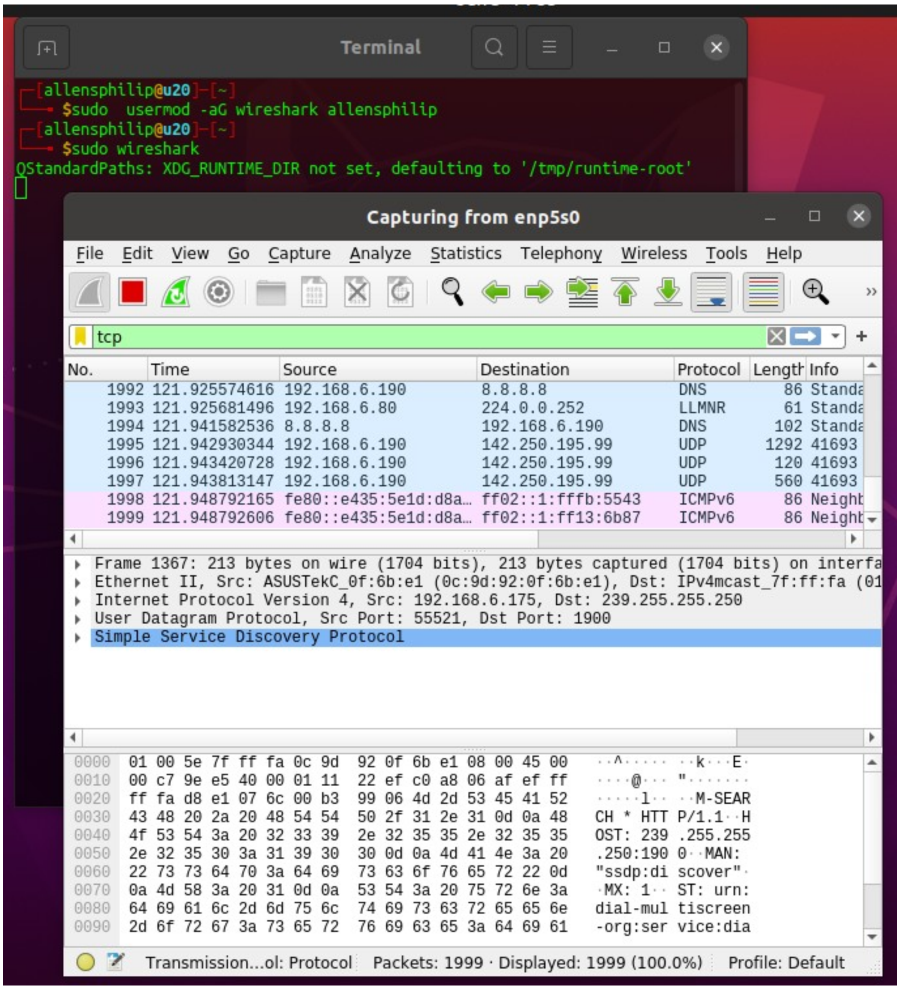
```
┌─[allensphilip@u20]─[~]
└──╼ $sudo  usermod -aG wireshark allensphilip
┌─[allensphilip@u20]─[~]
└──╼ $sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

```
No.     Time          Source                  Destination         Protocol Length Info
   1456 88.927195986  fe80::81b:4acf:19bf…   ff02::1:ff1e:c397   ICMPv6      86 Neighb
   1457 88.939524252  192.168.6.55            239.255.255.250     SSDP       217 M-SEAR
   1458 89.061043032  Sophos_6b:54:cf         Broadcast           ARP         60 Who ha
   1459 89.299079617  192.168.6.183           239.255.255.250     SSDP       213 M-SEAR
   1460 89.324166511  ASUSTekC_ba:c5:14       Broadcast           ARP         60 Who ha
   1461 89.476577203  fe80::81b:4acf:19bf…   ff02::1:ff1e:c397   ICMPv6      86 Neighb
   1462 89.557136162  HewlettP_a7:c0:55       Broadcast           ARP         60 Who ha
   1463 89.939908798  192.168.6.55            239.255.255.250     SSDP       217 M-SEAR
```

```
▸ Frame 1367: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interfa
▸ Ethernet II, Src: ASUSTekC_0f:6b:e1 (0c:9d:92:0f:6b:e1), Dst: IPv4mcast_7f:ff:fa (01
▸ Internet Protocol Version 4, Src: 192.168.6.175, Dst: 239.255.255.250
▸ User Datagram Protocol, Src Port: 55521, Dst Port: 1900
▸ Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 0c 9d  92 0f 6b e1 08 00 45 00   ··^····· ··k···E·
0010  00 c7 9e e5 40 00 01 11  22 ef c0 a8 06 af ef ff   ····@··· "·······
0020  ff fa d8 e1 07 6c 00 b3  99 06 4d 2d 53 45 41 52   ·····l·· ··M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN: 
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -org:ser vice:dia
```

enp5s0: <liv…in progress: | Packets: 1463 · Displayed: 1463 (100.0%) | Profile: Default


Terminal
Capturing from enp5s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
┌─[allensphilip@u20]─[~]
└──╼ $sudo  usermod -aG wireshark allensphilip
┌─[allensphilip@u20]─[~]
└──╼ $sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

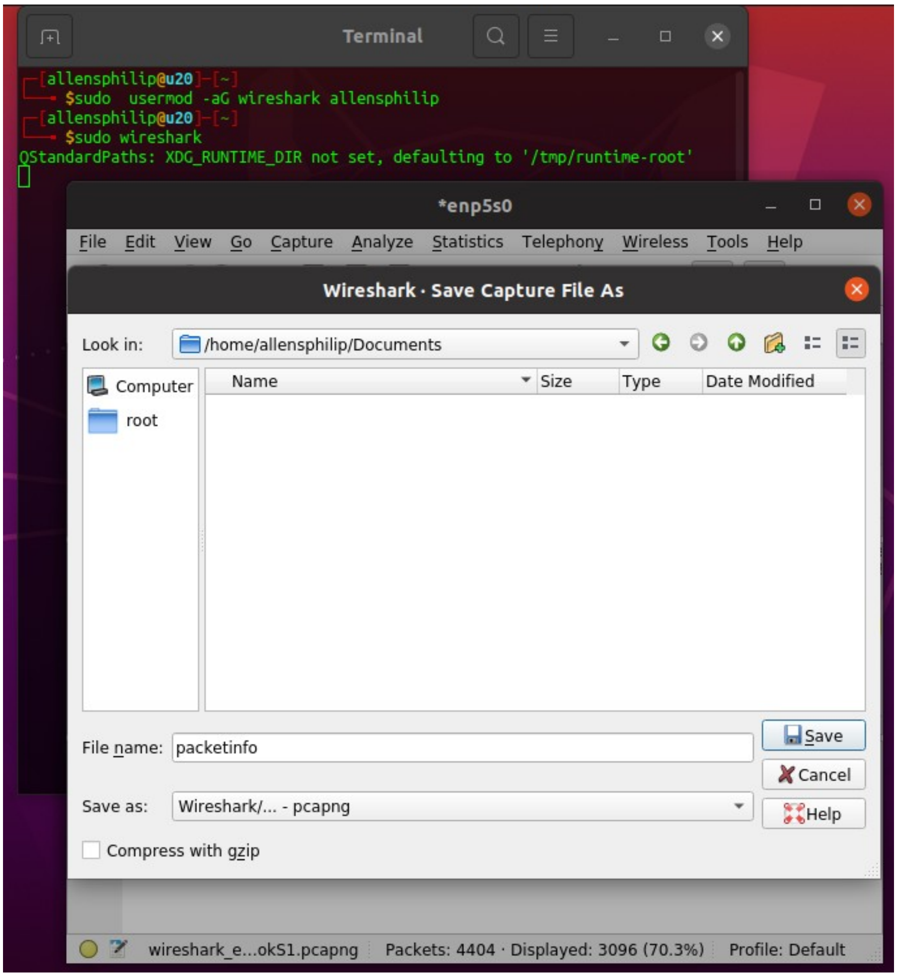
tcp

```
No.   Time           Source                 Destination        Protocol  Length Info
 1992 121.925574616 192.168.6.190          8.8.8.8            DNS         86 Standa
 1993 121.925681496 192.168.6.80           224.0.0.252        LLMNR       61 Standa
 1994 121.941582536 8.8.8.8                192.168.6.190      DNS        102 Standa
 1995 121.942930344 192.168.6.190          142.250.195.99     UDP       1292 41693
 1996 121.943420728 192.168.6.190          142.250.195.99     UDP        120 41693
 1997 121.943813147 192.168.6.190          142.250.195.99     UDP        560 41693
 1998 121.948792165 fe80::e435:5e1d:d8a…   ff02::1:fffb:5543  ICMPv6      86 Neight
 1999 121.948792606 fe80::e435:5e1d:d8a…   ff02::1:ff13:6b87  ICMPv6      86 Neight
```

```
▸ Frame 1367: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interfa
▸ Ethernet II, Src: ASUSTekC_0f:6b:e1 (0c:9d:92:0f:6b:e1), Dst: IPv4mcast_7f:ff:fa (01
▸ Internet Protocol Version 4, Src: 192.168.6.175, Dst: 239.255.255.250
▸ User Datagram Protocol, Src Port: 55521, Dst Port: 1900
▸ Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 0c 9d  92 0f 6b e1 08 00 45 00   ··^·····  ··k···E·
0010  00 c7 9e e5 40 00 01 11  22 ef c0 a8 06 af ef ff   ····@···  "·······
0020  ff fa d8 e1 07 6c 00 b3  99 06 4d 2d 53 45 41 52   ·····l··  ··M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN:
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -org:ser vice:dia
```

Transmission...ol: Protocol · Packets: 1999 · Displayed: 1999 (100.0%) · Profile: Default


Terminal
*enp5s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Save Capture File As
Computer
root
Name
Size
Type
Date Modified
Save
Cancel
Help

```
┌─[allensphilip@u20]─[~]
└──╼ $sudo  usermod -aG wireshark allensphilip
┌─[allensphilip@u20]─[~]
└──╼ $sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

Look in: /home/allensphilip/Documents

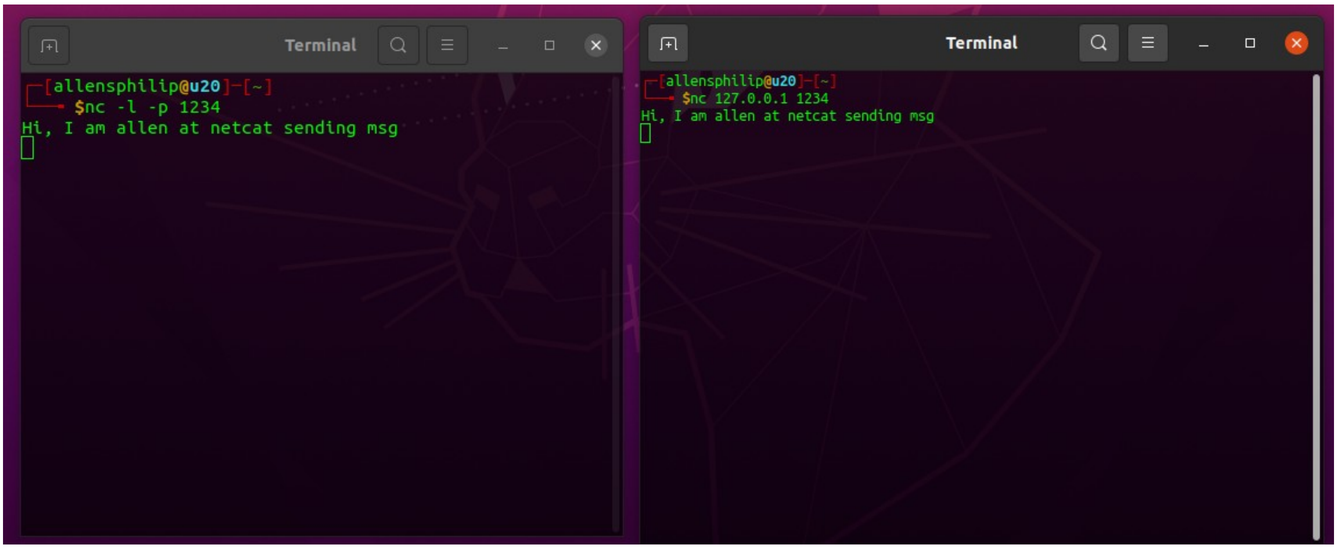
File name: packetinfo

Save as: Wireshark/... - pcapng

☐ Compress with gzip

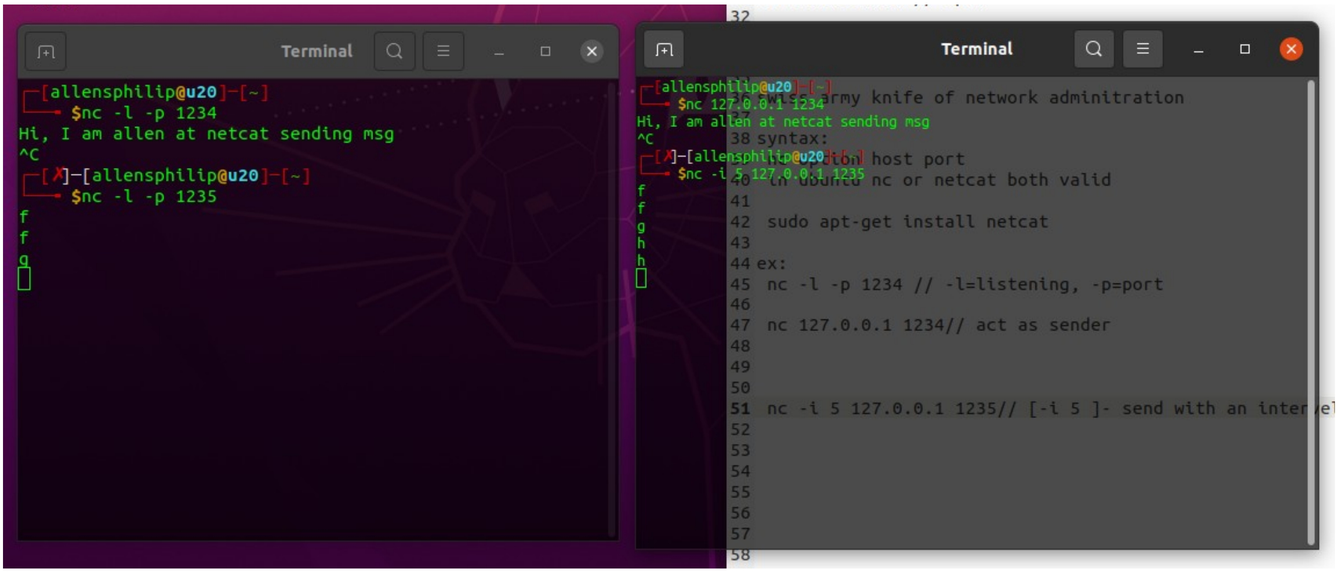
wireshark_e...okS1.pcapng · Packets: 4404 · Displayed: 3096 (70.3%) · Profile: Default

NetCat



```
┌─[allensphilip@u20]─[~]
└──╼ $nc -l -p 1234
Hi, I am allen at netcat sending msg
```

```
┌─[allensphilip@u20]─[~]
└──╼ $nc 127.0.0.1 1234
Hi, I am allen at netcat sending msg
```



```
┌─[allensphilip@u20]─[~]
└──╼ $nc -l -p 1234
Hi, I am allen at netcat sending msg
^C
┌─[✗]─[allensphilip@u20]─[~]
└──╼ $nc -l -p 1235
f
f
g
```

```
┌─[allensphilip@u20]─[~]
└──╼ $nc 127.0.0.1 1234
Hi, I am allen at netcat sending msg
^C
┌─[✗]─[allensphilip@u20]─[~]
└──╼ $nc -i 5 127.0.0.1 1235
f
f
g
h
h
```

```
swiss army knife of network adminitration

syntax:
 nc option host port
 in ubuntu nc or netcat both valid

 sudo apt-get install netcat

ex:
 nc -l -p 1234 // -l=listening, -p=port

 nc 127.0.0.1 1234// act as sender



 nc -i 5 127.0.0.1 1235// [-i 5 ]- send with an intervel
```