Parshvanath Charitable Trust's
A. P. SHAH INSTITUTE OF TECHNOLOGY
(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

Department of Information Technology

Semester: V **Name of Student: Vishal Bangar**
Academic Year: 2021-22 **Student ID: 20104084**
Class / Branch: TE IT
Subject: Security Lab (SL)
Name of Instructor: Prof. Kiran Deshpande

EXPERIMENT NO. 3B

Aim: To study analysis of network packets by sing open source sniffing tools like tcpdump and Wireshark in promiscuous and non-promiscuous mode.

tcpdump -D : display all available interfaces

```
apsit@apsit-HP-Notebook:/$ tcpdump -D
1.wlo1 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.enp1s0 [Up]
5.bluetooth0 (Bluetooth adapter number 0)
6.nflog (Linux netfilter log (NFLOG) interface)
7.nfqueue (Linux netfilter queue (NFQUEUE) interface)
8.usbmon1 (USB bus number 1)
9.usbmon2 (USB bus number 2)
apsit@apsit-HP-Notebook:/$
```

tcpdump -i wlo1 : capture traffic at the interface “wlo1”

```
apsit@apsit-HP-Notebook:/$ sudo tcpdump -i wlo1
[sudo] password for apsit:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
01:08:57.072974 IP 192.168.0.3.39146 > ec2-23-22-162-56.compute-1.amazonaws.com.https: F
lags [.], ack 3368797950, win 1444, options [nop,nop,TS val 142745535 ecr 2122488719], l
ength 0
01:08:57.162523 IP 192.168.0.3.38352 > domain.name.dlink.com.domain: 20947+ PTR? 56.162.
22.23.in-addr.arpa. (43)
01:08:57.230722 IP domain.name.dlink.com.domain > 192.168.0.3.38352: 20947 1/0/0 PTR ec2
-23-22-162-56.compute-1.amazonaws.com. (97)
01:08:57.231672 IP 192.168.0.3.38352 > domain.name.dlink.com.domain: 8090+ PTR? 3.0.168.
192.in-addr.arpa. (42)
01:08:57.236148 IP domain.name.dlink.com.domain > 192.168.0.3.38352: 8090 NXDomain 0/0/0
 (42)
01:08:57.236893 IP 192.168.0.3.38352 > domain.name.dlink.com.domain: 32152+ PTR? 1.0.168
.192.in-addr.arpa. (42)
01:08:57.245049 IP domain.name.dlink.com.domain > 192.168.0.3.38352: 32152* 1/0/0 PTR do
main.name.dlink.com. (77)
01:08:57.322531 IP ec2-23-22-162-56.compute-1.amazonaws.com.https > 192.168.0.3.39146: F
lags [.], ack 1, win 422, options [nop,nop,TS val 2122491308 ecr 142745535], length 0
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
apsit@apsit-HP-Notebook:/$
```

tcpdump -i wlo1 port 80 : capture traffic at the interface “wlo1” on port 80

```
apsit@apsit-HP-Notebook:/$ sudo tcpdump -i wlo1 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
01:10:08.961873 IP 192.168.0.3.59832 > vz01-phx.stablehost.com.http: Flags [S], seq 9326
85527, win 29200, options [mss 1460,sackOK,TS val 1388467646 ecr 0,nop,wscale 7], length
 0
01:10:09.215356 IP vz01-phx.stablehost.com.http > 192.168.0.3.59832: Flags [S.], seq 211
8994519, ack 932685528, win 14480, options [mss 1452,sackOK,TS val 620956985 ecr 1388467
646,nop,wscale 7], length 0
01:10:09.215393 IP 192.168.0.3.59832 > vz01-phx.stablehost.com.http: Flags [.], ack 1, w
in 229, options [nop,nop,TS val 1388467900 ecr 620956985], length 0
01:10:09.215841 IP 192.168.0.3.59832 > vz01-phx.stablehost.com.http: Flags [P.], seq 1:5
01, ack 1, win 229, options [nop,nop,TS val 1388467900 ecr 620956985], length 500: HTTP:
 GET /capture-tcp-syn-ack-fin-packets-tcpdump.html HTTP/1.1
01:10:09.469501 IP vz01-phx.stablehost.com.http > 192.168.0.3.59832: Flags [.], ack 501,
 win 122, options [nop,nop,TS val 620957239 ecr 1388467900], length 0
01:10:11.007879 IP vz01-phx.stablehost.com.http > 192.168.0.3.59832: Flags [.], seq 1441
:2881, ack 501, win 122, options [nop,nop,TS val 620958776 ecr 1388467900], length 1440:
 HTTP
```

tcpdump -i wlo1 -c 5 : capture 5 packets at the interface "wlo1"

```
apsit@apsit-HP-Notebook:/$ sudo  tcpdump -i wlo1 -c 5
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
01:12:12.862633 IP 192.168.0.3.39666 > a23-35-33-226.deploy.static.akamaitechnologies.co
m.https: Flags [S], seq 1481548601, win 29200, options [mss 1460,sackOK,TS val 175521882
3 ecr 0,nop,wscale 7], length 0
01:12:12.863803 IP 192.168.0.3.38352 > domain.name.dlink.com.domain: 17570+ PTR? 226.33.
35.23.in-addr.arpa. (43)
01:12:12.891986 IP a23-35-33-226.deploy.static.akamaitechnologies.com.https > 192.168.0.
3.39666: Flags [S.], seq 2577026599, ack 1481548602, win 28960, options [mss 1452,sackOK
,TS val 137780409 ecr 1755218823,nop,wscale 7], length 0
01:12:12.892029 IP 192.168.0.3.39666 > a23-35-33-226.deploy.static.akamaitechnologies.co
m.https: Flags [.], ack 1, win 229, options [nop,nop,TS val 1755218852 ecr 137780409], l
ength 0
01:12:12.894756 IP 192.168.0.3.39666 > a23-35-33-226.deploy.static.akamaitechnologies.co
m.https: Flags [P.], seq 1:547, ack 1, win 229, options [nop,nop,TS val 1755218855 ecr 1
37780409], length 546
5 packets captured
17 packets received by filter
9 packets dropped by kernel
apsit@apsit-HP-Notebook:/$
```

tcpdump -i wlo1 tcp : capture only tcp traffic at interface "wlo1"

```
apsit@apsit-HP-Notebook:/$ 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
01:13:14.393309 IP 172.217.194.189.https > 192.168.0.3.51680: Flags [P.], seq 1402433658
:1402433718, ack 3397138618, win 255, options [nop,nop,TS val 855118485 ecr 1903280836],
 length 60
01:13:14.393367 IP 192.168.0.3.51680 > 172.217.194.189.https: Flags [.], ack 60, win 254
, options [nop,nop,TS val 1903306808 ecr 855118485], length 0
01:13:14.608977 IP 192.168.0.3.32920 > ec2-184-72-237-155.compute-1.amazonaws.com.https:
 Flags [.], ack 3310232932, win 319, options [nop,nop,TS val 1344348399 ecr 2589624678],
 length 0
01:13:14.865798 IP ec2-184-72-237-155.compute-1.amazonaws.com.https > 192.168.0.3.32920:
 Flags [.], ack 1, win 123, options [nop,nop,TS val 2589627302 ecr 1344306625], length 0
01:13:16.130666 IP 192.168.0.3.54928 > edge-star-z-mini-shv-01-bom1.facebook.com.https:
Flags [P.], seq 2423887626:2423887665, ack 502352641, win 515, options [nop,nop,TS val 1
49184123 ecr 768801575], length 39
01:13:16.131684 IP 192.168.0.3.44018 > ec2-13-112-136-133.ap-northeast-1.compute.amazona
ws.com.https: Flags [P.], seq 205128468:205128514, ack 3182194387, win 341, options [nop
,nop,TS val 182986181 ecr 100612615], length 46
```

To capture only TCP ACK packets:

sudo tcpdump -i wlo1 "tcp[tcpflags] & (tcp-ack) != 0" >/home/apsit/Desktop/ack.txt

```
1 01:34:00.950362 IP bom05s08-in-f14.1e100.net.https > apsit-HP-Notebook.45250: Flags [S.], seq
  2935813833, ack 3223070162, win 60192, options [mss 1380,sackOK,TS val 577951110 ecr
  4020449693,nop,wscale 8], length 0
2 01:34:00.950436 IP apsit-HP-Notebook.45250 > bom05s08-in-f14.1e100.net.https: Flags [.], ack 1,
  win 229, options [nop,nop,TS val 4020449795 ecr 577951110], length 0
3 01:34:00.956678 IP apsit-HP-Notebook.45250 > bom05s08-in-f14.1e100.net.https: Flags [P.], seq
  1:575, ack 1, win 229, options [nop,nop,TS val 4020449802 ecr 577951110], length 574
4 01:34:01.060352 IP bom05s08-in-f14.1e100.net.https > apsit-HP-Notebook.45250: Flags [.], ack
  575, win 240, options [nop,nop,TS val 577951219 ecr 4020449802], length 0
5 01:34:01.060399 IP bom05s08-in-f14.1e100.net.https > apsit-HP-Notebook.45250: Flags [P.], seq
  1:157, ack 575, win 240, options [nop,nop,TS val 577951219 ecr 4020449802], length 156
6 01:34:01.060432 IP apsit-HP-Notebook.45250 > bom05s08-in-f14.1e100.net.https: Flags [.], ack
  157, win 237, options [nop,nop,TS val 4020449905 ecr 577951219], length 0
```

```
1 01:35:57.791953 IP bom05s08-in-f10.1e100.net.https > 192.168.43.169.53626: Flags [F.], seq
  1046525628, ack 3550107812, win 244, options [nop,nop,TS val 4084820507 ecr 283862804], length 0
2 01:35:59.849334 IP 192.168.43.169.55630 > 117.18.232.12.https: Flags [F.], seq 2388221349, ack
  416919623, win 341, length 0
3 01:35:59.888280 IP 117.18.232.12.https > 192.168.43.169.55630: Flags [F.], seq 138, ack
  4294967265, win 290, length 0
4
```

To capture only TCP FIN packets:

To capture ssh packet:sudo tcpdump -i wlo1 -x -X -A -nvvv port 22 > ssh.txt

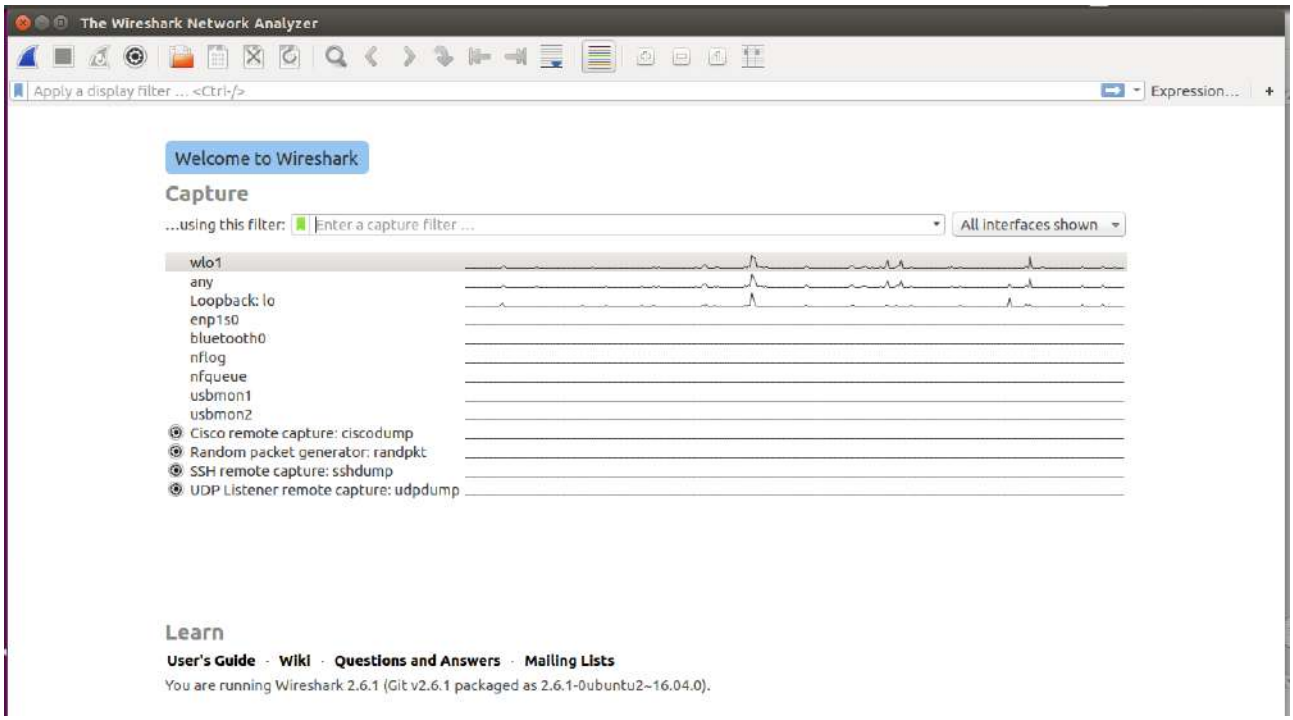
```
apsit@apsit-HP-Notebook:~$ sudo tcpdump -i wlan0 -x -X -A -nvvv port 22 > ssh.tx
t
[sudo] password for apsit:
tcpdump: wlan0: SIOCETHTOOL(ETHTOOL_GET_TS_INFO) ioctl failed: No such device
apsit@apsit-HP-Notebook:~$ sudo tcpdump -i wlo1 -x -X -A -nvvv port 22 > ssh.txt

tcpdump: listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 byt
es
^C78 packets captured
78 packets received by filter
0 packets dropped by kernel
apsit@apsit-HP-Notebook:~$
```

```
apsit@apsit-HP-Notebook:/$ ssh apsit@192.168.43.32
apsit@192.168.43.32's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic i686)

 * Documentation:  https://help.ubuntu.com/

Last login: Thu Aug 23 00:05:54 2018 from apsit-hp-notebook
apsit@apsit-Satellite-C660:~$ exit
logout
Connection to 192.168.43.32 closed.
apsit@apsit-HP-Notebook:/$ ssh apsit@192.168.43.32
apsit@192.168.43.32's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic i686)

 * Documentation:  https://help.ubuntu.com/

Last login: Thu Aug 23 01:46:18 2018 from apsit-hp-notebook
```

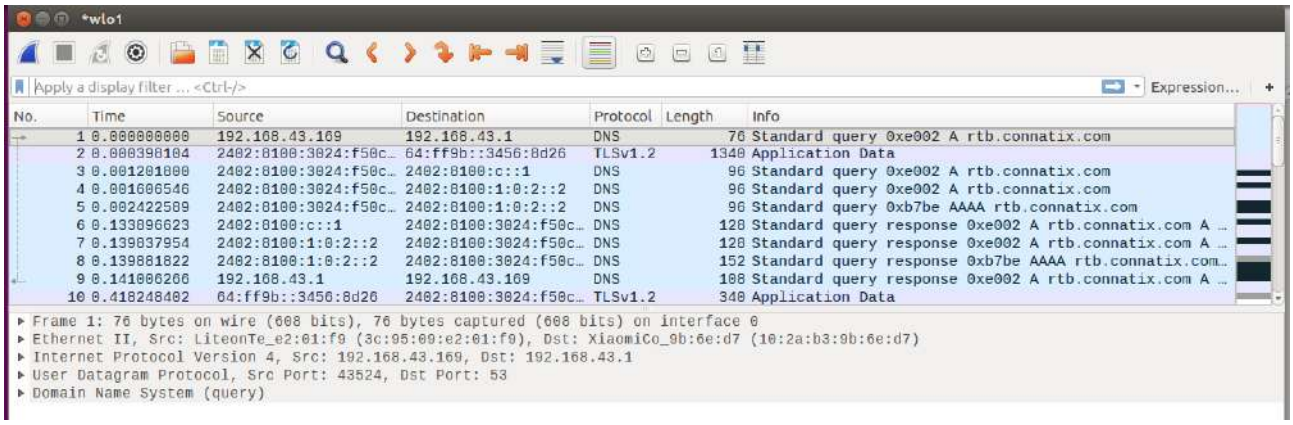
```
01:45:38.324806 IP (tos 0x0, ttl 64, id 4461, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.43.169.52974 > 192.168.43.32.22: Flags [S], cksum 0xa548 (correct), seq 480432837, win 29200, options [mss 1460,sackOK,TS val 607548906 ecr 0,nop,wscale 7], length 0
        0x0000:  4500 003c 116d 4000 4006 5135 c0a8 2ba9  E..<.m@.@.Q5..+.
        0x0010:  c0a8 2b20 ceee 0016 1ca2 d2c5 0000 0000  ..+.............
        0x0020:  a002 7210 a548 0000 0204 05b4 0402 080a  ..r..H..........
        0x0030:  2436 75ea 0000 0000 0103 0307            $6u.........
01:45:38.328105 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.43.32.22 > 192.168.43.169.52974: Flags [S.], cksum 0x09c0 (correct), seq 2957816868, ack 480432838, win 28960, options [mss 1460,sackOK,TS val 14326 ecr 607548906,nop,wscale 7], length 0
        0x0000:  4500 003c 0000 4000 4006 62a2 c0a8 2b20  E..<..@.@.b...+.
        0x0010:  c0a8 2ba9 0016 ceee b04c b424 1ca2 d2c6  ..+......L.$....
        0x0020:  a012 7120 09c0 0000 0204 05b4 0402 080a  ..q.............
        0x0030:  0000 37f6 2436 75ea 0103 0307            ..7.$6u.....
01:45:38.328151 IP (tos 0x0, ttl 64, id 4462, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.43.169.52974 > 192.168.43.32.22: Flags [.], cksum 0xa8c4 (correct), seq 1, ack 1, win 229, options [nop,nop,TS val 607548909 ecr 14326], length 0
        0x0000:  4500 0034 116e 4000 4006 513c c0a8 2ba9  E..4.n@.@.Q<..+.
        0x0010:  c0a8 2b20 ceee 0016 1ca2 d2c6 b04c b425  ..+..........L.%
        0x0020:  8010 00e5 a8c4 0000 0101 080a 2436 75ed  ............$6u.
        0x0030:  0000 37f6                                ..7.
01:45:38.329104 IP (tos 0x0, ttl 64, id 4463, offset 0, flags [DF], proto TCP (6), length 93)
    192.168.43.169.52974 > 192.168.43.32.22: Flags [P.], cksum 0x826a (correct), seq 1:42, ack 1, win 229, options [nop,nop,TS val 607548910 ecr 14326], length 41
        0x0000:  4500 005d 116f 4000 4006 5112 c0a8 2ba9  E..].o@.@.Q...+.
        0x0010:  c0a8 2b20 ceee 0016 1ca2 d2c6 b04c b425  ..+..........L.%
        0x0020:  8018 00e5 826a 0000 0101 080a 2436 75ee  .....j......$6u.
        0x0030:  0000 37f6 5353 482d 322e 302d 4f70 656e  ..7.SSH-2.0-Open
        0x0040:  5353 485f 372e 3270 3220 5562 756e 7475  SSH_7.2p2.Ubuntu
        0x0050:  2d34 7562 756e 7475 322e 340d 0a         -4ubuntu2.4..
01:45:38.420770 IP (tos 0x0, ttl 64, id 33756, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.43.32.22 > 192.168.43.169.52974: Flags [.], cksum 0xa899 (correct), seq 1, ack 42, win 227, options [nop,nop,TS val 14329 ecr 607548910], length 0
```

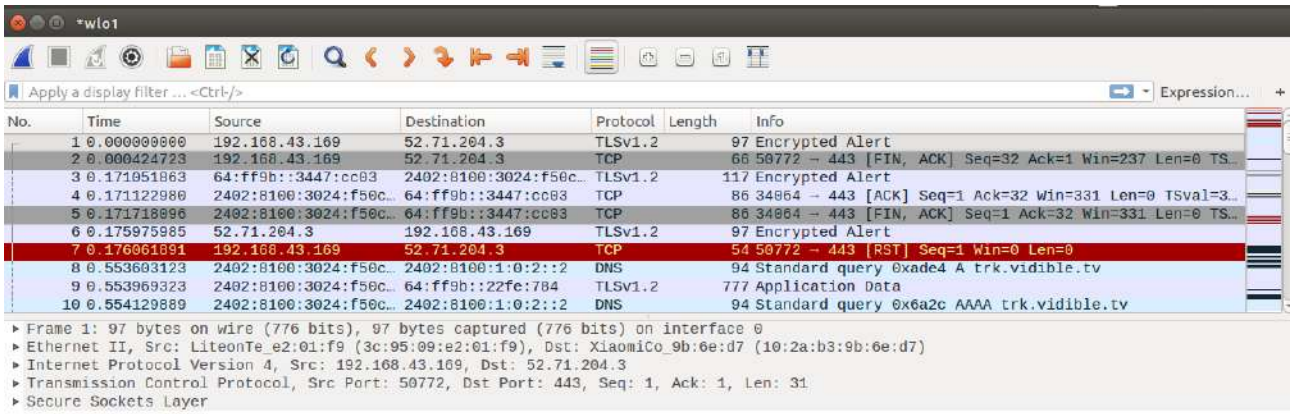
Wireshark:

Capture Data Packets in Wireshark:



To begin capturing, select the interface and click on Capture button at the top.





1. Start capturing packets in Wireshark. While in process initiate a telnet connection.

```
apsit@apsit-HP-Notebook:~$ sudo ip link set wlo1 promisc on
[sudo] password for apsit:
apsit@apsit-HP-Notebook:~$ netstat -i
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp1s0     1500 0        78      0      0 0          121      0      0      0 BMU
lo        65536 0     23791      0      0 0        23791      0      0      0 LRU
wlo1       1500 0    120989      0      0 0       119907      0      0      0 BMPRU
apsit@apsit-HP-Notebook:~$
```

Promiscuous and non promiscuous mode:

```
wlo1      Link encap:Ethernet  HWaddr 3c:95:09:e2:01:f9
          inet addr:192.168.43.169  Bcast:192.168.43.255  Mask:255.255.255.0
          inet6 addr: 2402:8100:3024:f50c:d977:f24e:259:fdda/64 Scope:Global
          inet6 addr: 2402:8100:3024:f50c:ae45:4d3d:2b1f:d265/64 Scope:Global
          inet6 addr: fe80::594c:3e55:695d:8a23/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:121102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:120038 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:84604559 (84.6 MB)  TX bytes:19875334 (19.8 MB)
```

```
apsit@apsit-HP-Notebook:~$ sudo ip link set wlo1 promisc off
apsit@apsit-HP-Notebook:~$ netstat -i
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp1s0     1500 0        78      0      0 0          121      0      0      0 BMU
lo        65536 0     23905      0      0 0        23905      0      0      0 LRU
wlo1       1500 0    122756      0      0 0       121294      0      0      0 BMRU
apsit@apsit-HP-Notebook:~$
```

Promiscous mode enable/disable in wireshark: