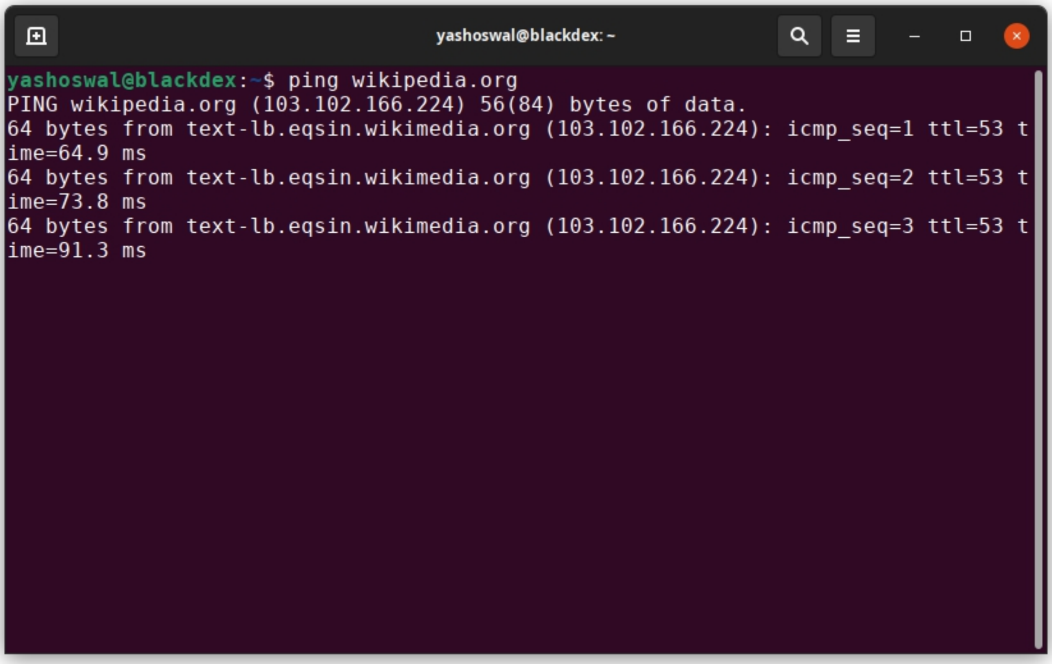
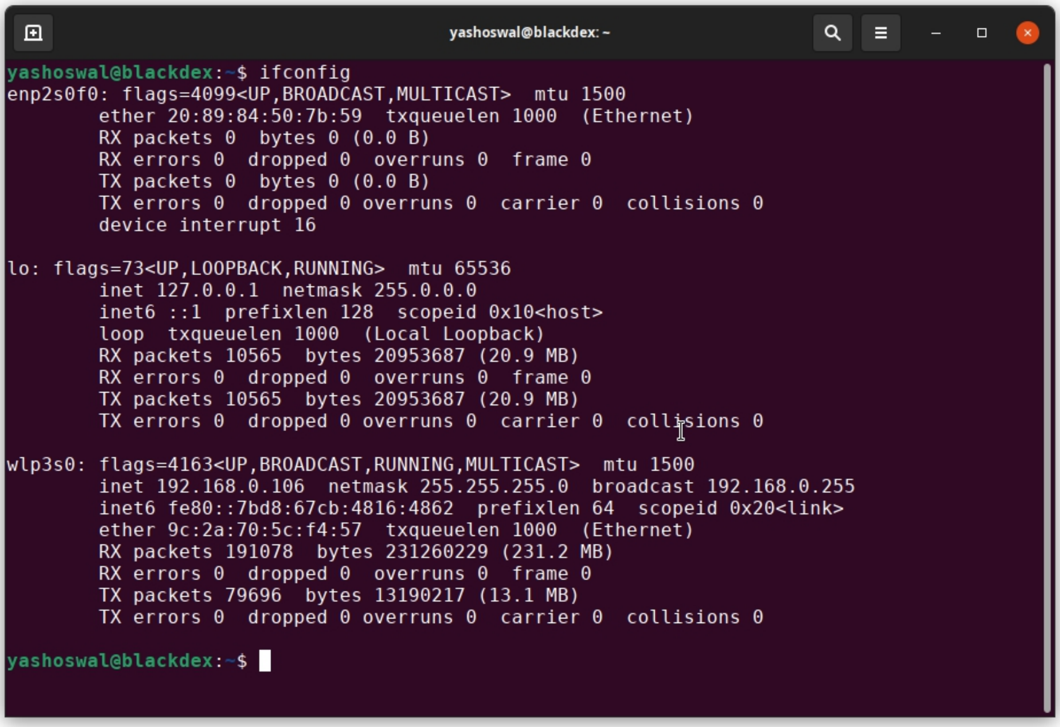
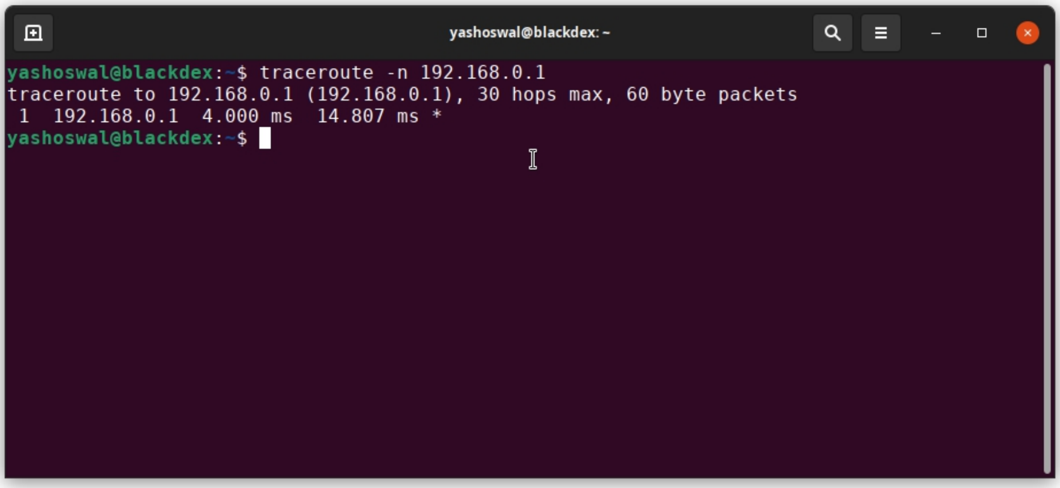
Assignment 3
Roll no: 38
Div: B



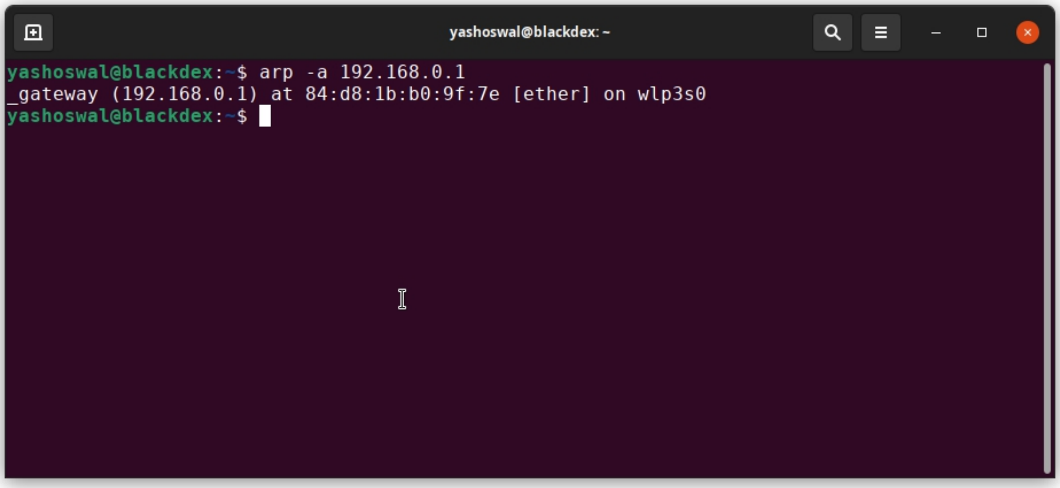
```
yashoswal@blackdex:~$ ping wikipedia.org
PING wikipedia.org (103.102.166.224) 56(84) bytes of data.
64 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=1 ttl=53 t
ime=64.9 ms
64 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=2 ttl=53 t
ime=73.8 ms
64 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=3 ttl=53 t
ime=91.3 ms
```



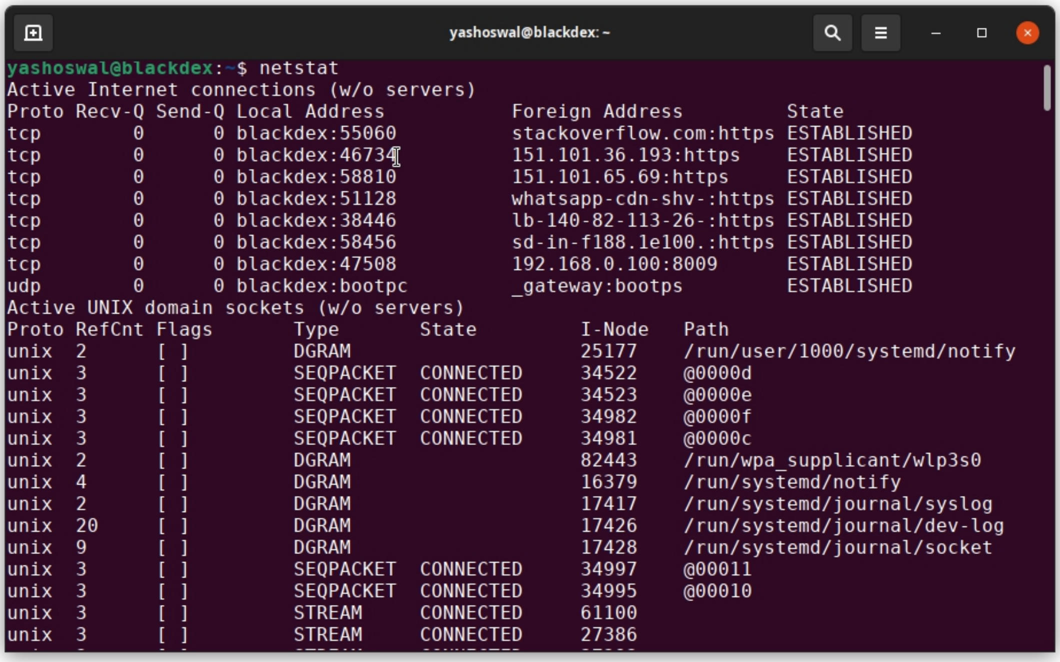
```
yashoswal@blackdex:~$ ifconfig
enp2s0f0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 20:89:84:50:7b:59  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 10565  bytes 20953687 (20.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10565  bytes 20953687 (20.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.106  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::7bd8:67cb:4816:4862  prefixlen 64  scopeid 0x20<link>
        ether 9c:2a:70:5c:f4:57  txqueuelen 1000  (Ethernet)
        RX packets 191078  bytes 231260229 (231.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 79696  bytes 13190217 (13.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

yashoswal@blackdex:~$
```



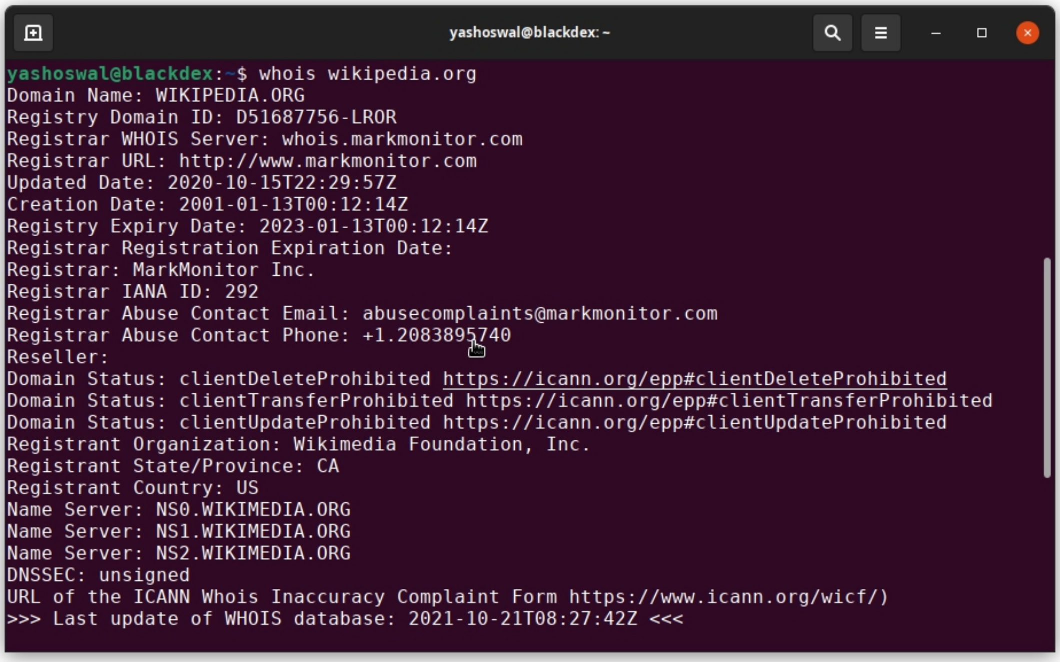
```
yashoswal@blackdex:~$ traceroute -n 192.168.0.1
traceroute to 192.168.0.1 (192.168.0.1), 30 hops max, 60 byte packets
 1  192.168.0.1  4.000 ms  14.807 ms *
yashoswal@blackdex:~$ 
```



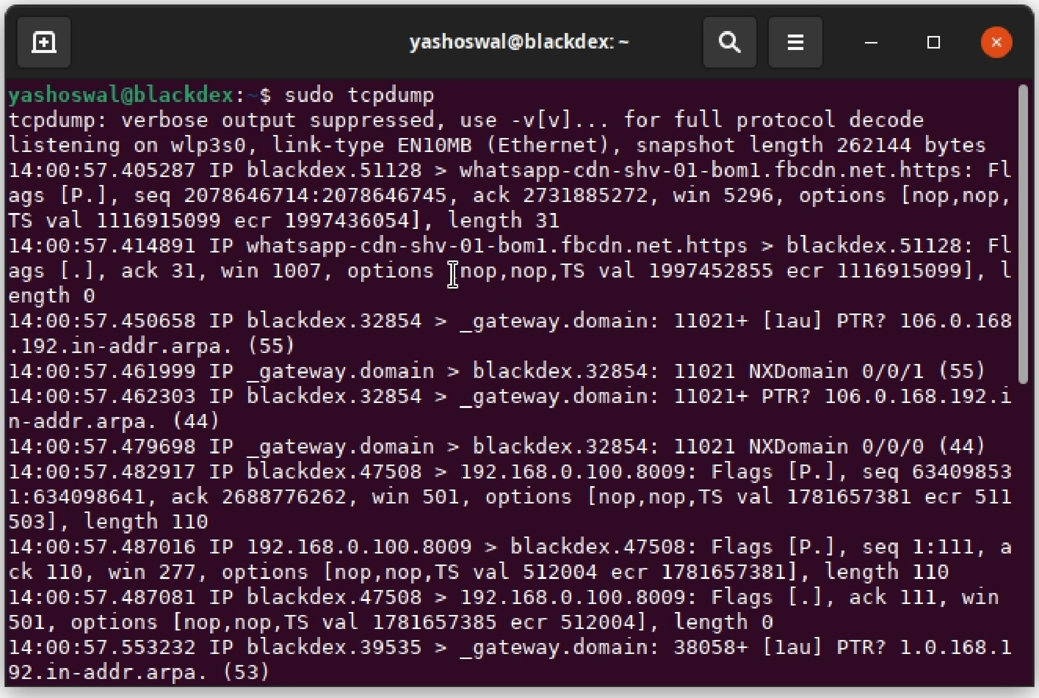
```
yashoswal@blackdex:~$ arp -a 192.168.0.1
_gateway (192.168.0.1) at 84:d8:1b:b0:9f:7e [ether] on wlp3s0
yashoswal@blackdex:~$ 
```



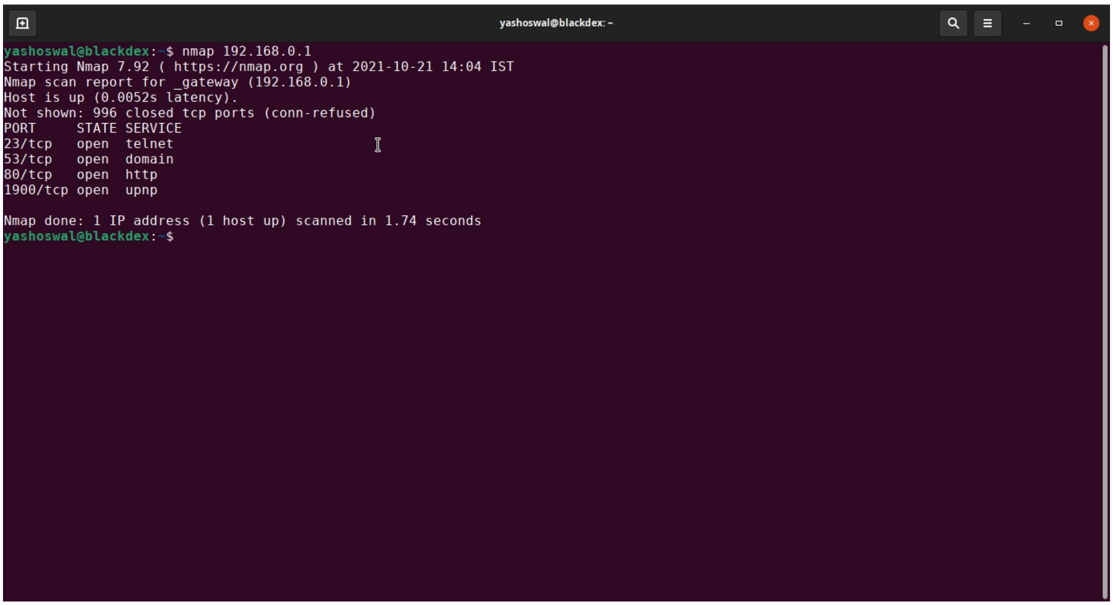
```
yashoswal@blackdex:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 blackdex:55060          stackoverflow.com:https ESTABLISHED
tcp        0      0 blackdex:46734          151.101.36.193:https    ESTABLISHED
tcp        0      0 blackdex:58810          151.101.65.69:https     ESTABLISHED
tcp        0      0 blackdex:51128          whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 blackdex:38446          lb-140-82-113-26-:https ESTABLISHED
tcp        0      0 blackdex:58456          sd-in-f188.1e100.:https ESTABLISHED
tcp        0      0 blackdex:47508          192.168.0.100:8009      ESTABLISHED
udp        0      0 blackdex:bootpc         _gateway:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    25177    /run/user/1000/systemd/notify
unix  3      [ ]         SEQPACKET  CONNECTED     34522    @0000d
unix  3      [ ]         SEQPACKET  CONNECTED     34523    @0000e
unix  3      [ ]         SEQPACKET  CONNECTED     34982    @0000f
unix  3      [ ]         SEQPACKET  CONNECTED     34981    @0000c
unix  2      [ ]         DGRAM                    82443    /run/wpa_supplicant/wlp3s0
unix  4      [ ]         DGRAM                    16379    /run/systemd/notify
unix  2      [ ]         DGRAM                    17417    /run/systemd/journal/syslog
unix  20     [ ]         DGRAM                    17426    /run/systemd/journal/dev-log
unix  9      [ ]         DGRAM                    17428    /run/systemd/journal/socket
unix  3      [ ]         SEQPACKET  CONNECTED     34997    @00011
unix  3      [ ]         SEQPACKET  CONNECTED     34995    @00010
unix  3      [ ]         STREAM     CONNECTED     61100
unix  3      [ ]         STREAM     CONNECTED     27386
```



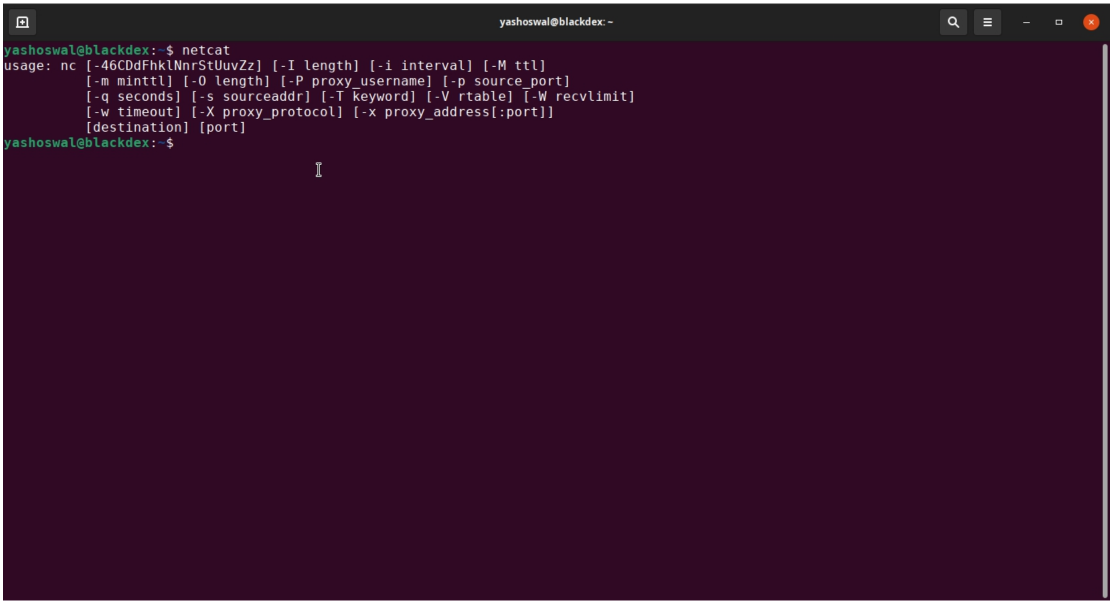
```
yashoswal@blackdex:~$ whois wikipedia.org
Domain Name: WIKIPEDIA.ORG
Registry Domain ID: D51687756-LROR
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-10-15T22:29:57Z
Creation Date: 2001-01-13T00:12:14Z
Registry Expiry Date: 2023-01-13T00:12:14Z
Registrar Registration Expiration Date:
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Organization: Wikimedia Foundation, Inc.
Registrant State/Province: CA
Registrant Country: US
Name Server: NS0.WIKIMEDIA.ORG
Name Server: NS1.WIKIMEDIA.ORG
Name Server: NS2.WIKIMEDIA.ORG
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2021-10-21T08:27:42Z <<<
```



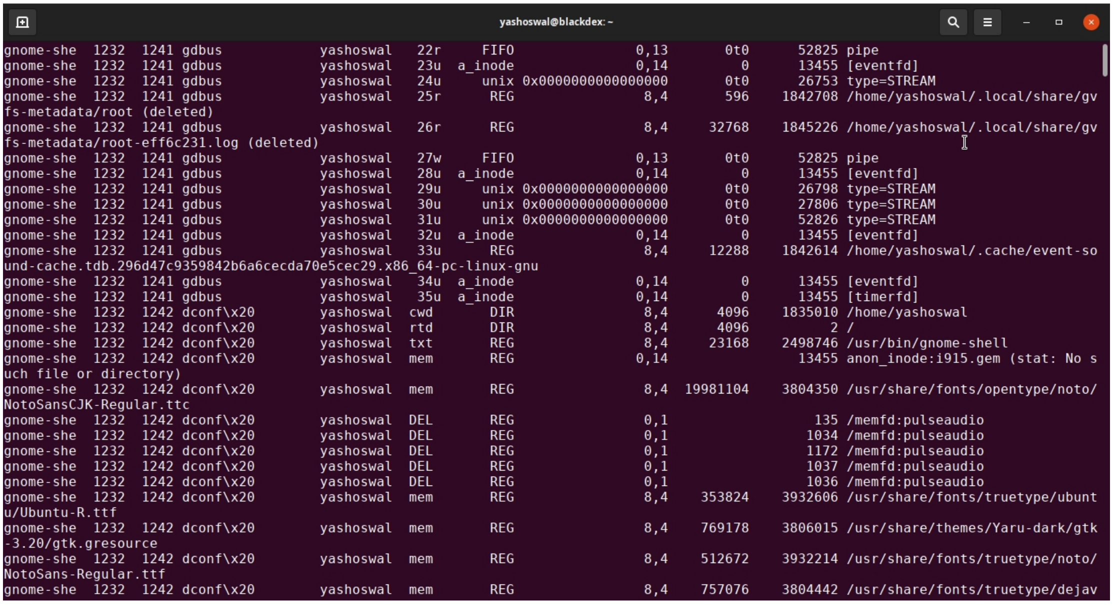
```
yashoswal@blackdex:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp3s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
14:00:57.405287 IP blackdex.51128 > whatsapp-cdn-shv-01-bom1.fbcdn.net.https: Fl
ags [P.], seq 2078646714:2078646745, ack 2731885272, win 5296, options [nop,nop,
TS val 1116915099 ecr 1997436054], length 31
14:00:57.414891 IP whatsapp-cdn-shv-01-bom1.fbcdn.net.https > blackdex.51128: Fl
ags [.], ack 31, win 1007, options [nop,nop,TS val 1997452855 ecr 1116915099], l
ength 0
14:00:57.450658 IP blackdex.32854 > _gateway.domain: 11021+ [1au] PTR? 106.0.168
.192.in-addr.arpa. (55)
14:00:57.461999 IP _gateway.domain > blackdex.32854: 11021 NXDomain 0/0/1 (55)
14:00:57.462303 IP blackdex.32854 > _gateway.domain: 11021+ PTR? 106.0.168.192.i
n-addr.arpa. (44)
14:00:57.479698 IP _gateway.domain > blackdex.32854: 11021 NXDomain 0/0/0 (44)
14:00:57.482917 IP blackdex.47508 > 192.168.0.100.8009: Flags [P.], seq 63409853
1:634098641, ack 2688776262, win 501, options [nop,nop,TS val 1781657381 ecr 511
503], length 110
14:00:57.487016 IP 192.168.0.100.8009 > blackdex.47508: Flags [P.], seq 1:111, a
ck 110, win 277, options [nop,nop,TS val 512004 ecr 1781657381], length 110
14:00:57.487081 IP blackdex.47508 > 192.168.0.100.8009: Flags [.], ack 111, win
501, options [nop,nop,TS val 1781657385 ecr 512004], length 0
14:00:57.553232 IP blackdex.39535 > _gateway.domain: 38058+ [1au] PTR? 1.0.168.1
92.in-addr.arpa. (53)
```



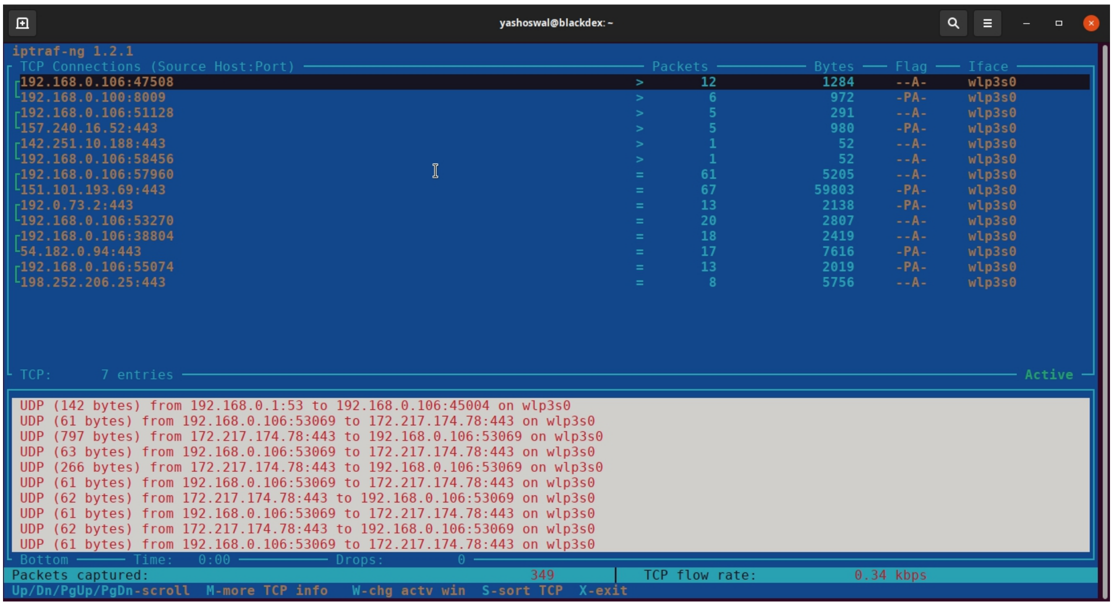
```
yashoswal@blackdex:~$ nmap 192.168.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-21 14:04 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.0052s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
yashoswal@blackdex:~$
```



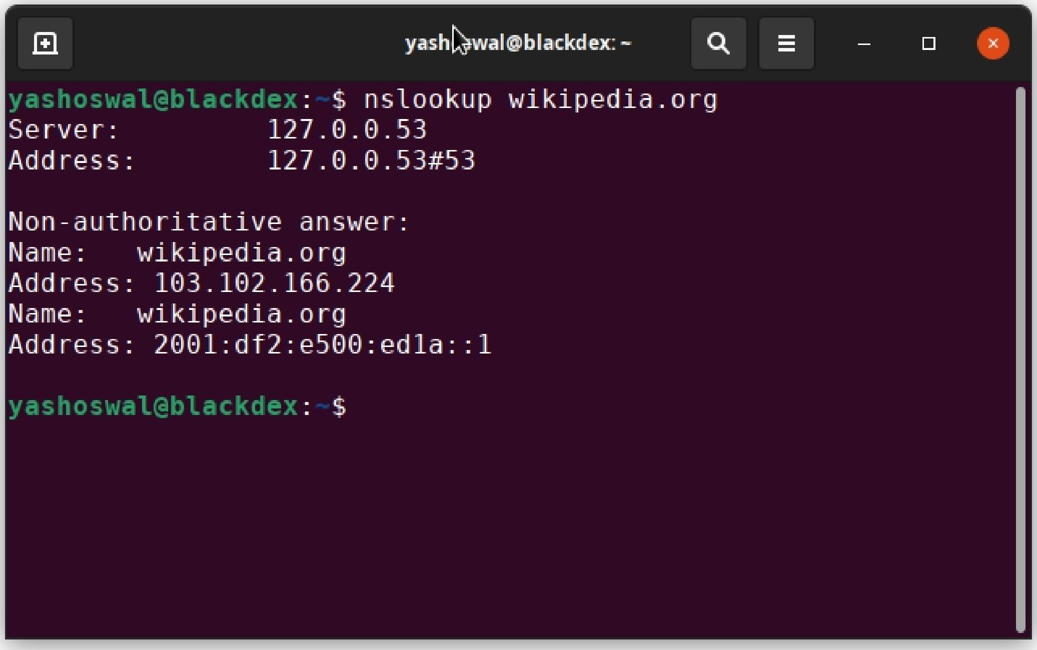
```
yashoswal@blackdex:~$ netcat
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s sourceaddr] [-T keyword] [-V rtable] [-W recvlimit]
          [-w timeout] [-X proxy_protocol] [-x proxy_address[:port]]
          [destination] [port]
yashoswal@blackdex:~$
```



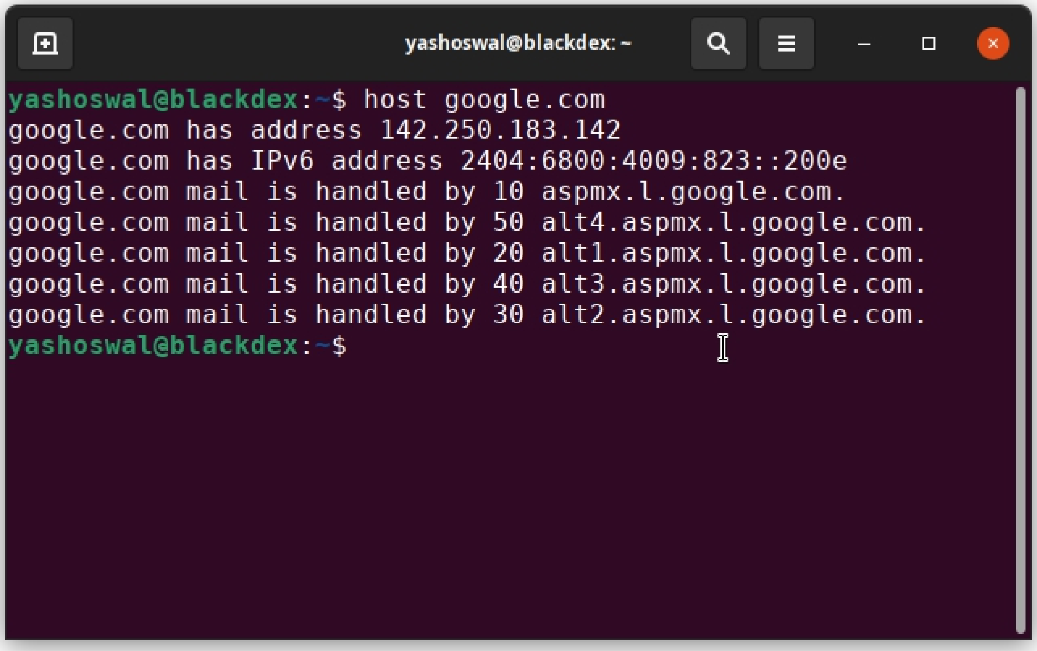
```
gnome-she  1232  1241 gdbus            yashoswal   22r      FIFO               0,13       0t0      52825 pipe
gnome-she  1232  1241 gdbus            yashoswal   23u  a_inode               0,14         0      13455 [eventfd]
gnome-she  1232  1241 gdbus            yashoswal   24u     unix 0x0000000000000000       0t0      26753 type=STREAM
gnome-she  1232  1241 gdbus            yashoswal   25r      REG                8,4       596    1842708 /home/yashoswal/.local/share/gv
fs-metadata/root (deleted)
gnome-she  1232  1241 gdbus            yashoswal   26r      REG                8,4     32768    1845226 /home/yashoswal/.local/share/gv
fs-metadata/root-eff6c231.log (deleted)
gnome-she  1232  1241 gdbus            yashoswal   27w      FIFO               0,13       0t0      52825 pipe
gnome-she  1232  1241 gdbus            yashoswal   28u  a_inode               0,14         0      13455 [eventfd]
gnome-she  1232  1241 gdbus            yashoswal   29u     unix 0x0000000000000000       0t0      26798 type=STREAM
gnome-she  1232  1241 gdbus            yashoswal   30u     unix 0x0000000000000000       0t0      27806 type=STREAM
gnome-she  1232  1241 gdbus            yashoswal   31u     unix 0x0000000000000000       0t0      52826 type=STREAM
gnome-she  1232  1241 gdbus            yashoswal   32u  a_inode               0,14         0      13455 [eventfd]
gnome-she  1232  1241 gdbus            yashoswal   33u      REG                8,4     12288    1842614 /home/yashoswal/.cache/event-so
und-cache.tdb.296d47c9359842b6a6cecda70e5cec29.x86_64-pc-linux-gnu
gnome-she  1232  1241 gdbus            yashoswal   34u  a_inode               0,14         0      13455 [eventfd]
gnome-she  1232  1241 gdbus            yashoswal   35u  a_inode               0,14         0      13455 [timerfd]
gnome-she  1232  1242 dconf\x20        yashoswal  cwd       DIR                8,4      4096    1835010 /home/yashoswal
gnome-she  1232  1242 dconf\x20        yashoswal  rtd       DIR                8,4      4096          2 /
gnome-she  1232  1242 dconf\x20        yashoswal  txt       REG                8,4     23168    2498746 /usr/bin/gnome-shell
gnome-she  1232  1242 dconf\x20        yashoswal  mem       REG               0,14                13455 anon_inode:i915.gem (stat: No s
uch file or directory)
gnome-she  1232  1242 dconf\x20        yashoswal  mem       REG                8,4  19981104    3804350 /usr/share/fonts/opentype/noto/
NotoSansCJK-Regular.ttc
gnome-she  1232  1242 dconf\x20        yashoswal  DEL       REG                0,1                  135 /memfd:pulseaudio
gnome-she  1232  1242 dconf\x20        yashoswal  DEL       REG                0,1                 1034 /memfd:pulseaudio
gnome-she  1232  1242 dconf\x20        yashoswal  DEL       REG                0,1                 1172 /memfd:pulseaudio
gnome-she  1232  1242 dconf\x20        yashoswal  DEL       REG                0,1                 1037 /memfd:pulseaudio
gnome-she  1232  1242 dconf\x20        yashoswal  DEL       REG                0,1                 1036 /memfd:pulseaudio
gnome-she  1232  1242 dconf\x20        yashoswal  mem       REG                8,4    353824    3932606 /usr/share/fonts/truetype/ubunt
u/Ubuntu-R.ttf
gnome-she  1232  1242 dconf\x20        yashoswal  mem       REG                8,4    769178    3806015 /usr/share/themes/Yaru-dark/gtk
-3.20/gtk.gresource
gnome-she  1232  1242 dconf\x20        yashoswal  mem       REG                8,4    512672    3932214 /usr/share/fonts/truetype/noto/
NotoSans-Regular.ttf
gnome-she  1232  1242 dconf\x20        yashoswal  mem       REG                8,4    757076    3804442 /usr/share/fonts/truetype/dejav
```



```
iptraf-ng 1.2.1
┌ TCP Connections (Source Host:Port) ──────────────────────────── Packets ──────────── Bytes ── Flag ── Iface ──
┌192.168.0.106:47508                                             >      12            1284   --A-     wlp3s0
└192.168.0.100:8009                                              >       6             972   -PA-     wlp3s0
┌192.168.0.106:51128                                             >       5             291   --A-     wlp3s0
└157.240.16.52:443                                               >       5             980   -PA-     wlp3s0
┌142.251.10.188:443                                              >       1              52   --A-     wlp3s0
└192.168.0.106:58456                                             >       1              52   --A-     wlp3s0
┌192.168.0.106:57960                                             =      61            5205   --A-     wlp3s0
└151.101.193.69:443                                              =      67           59803   -PA-     wlp3s0
┌192.0.73.2:443                                                  =      13            2138   -PA-     wlp3s0
└192.168.0.106:53270                                             =      20            2807   --A-     wlp3s0
┌192.168.0.106:38804                                             =      18            2419   --A-     wlp3s0
└54.182.0.94:443                                                 =      17            7616   -PA-     wlp3s0
┌192.168.0.106:55074                                             =      13            2019   -PA-     wlp3s0
└198.252.206.25:443                                              =       8            5756   --A-     wlp3s0



└ TCP:      7 entries ─────────────────────────────────────────────────────────────────────────── Active ─
 UDP (142 bytes) from 192.168.0.1:53 to 192.168.0.106:45004 on wlp3s0
 UDP (61 bytes) from 192.168.0.106:53069 to 172.217.174.78:443 on wlp3s0
 UDP (797 bytes) from 172.217.174.78:443 to 192.168.0.106:53069 on wlp3s0
 UDP (63 bytes) from 192.168.0.106:53069 to 172.217.174.78:443 on wlp3s0
 UDP (266 bytes) from 172.217.174.78:443 to 192.168.0.106:53069 on wlp3s0
 UDP (61 bytes) from 192.168.0.106:53069 to 172.217.174.78:443 on wlp3s0
 UDP (62 bytes) from 172.217.174.78:443 to 192.168.0.106:53069 on wlp3s0
 UDP (61 bytes) from 192.168.0.106:53069 to 172.217.174.78:443 on wlp3s0
 UDP (62 bytes) from 172.217.174.78:443 to 192.168.0.106:53069 on wlp3s0
 UDP (61 bytes) from 192.168.0.106:53069 to 172.217.174.78:443 on wlp3s0
└ Bottom ────── Time:   0:00 ────────── Drops:        0 ──────────────────────────────────────────────────
Packets captured:                                   349  │  TCP flow rate:          0.34 kbps
Up/Dn/PgUp/PgDn-scroll  M-more TCP info   W-chg actv win  S-sort TCP  X-exit
```



```
yashoswal@blackdex:~$ nslookup wikipedia.org
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   wikipedia.org
Address: 103.102.166.224
Name:   wikipedia.org
Address: 2001:df2:e500:ed1a::1

yashoswal@blackdex:~$
```



```
yashoswal@blackdex:~$ host google.com
google.com has address 142.250.183.142
google.com has IPv6 address 2404:6800:4009:823::200e
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
yashoswal@blackdex:~$
```