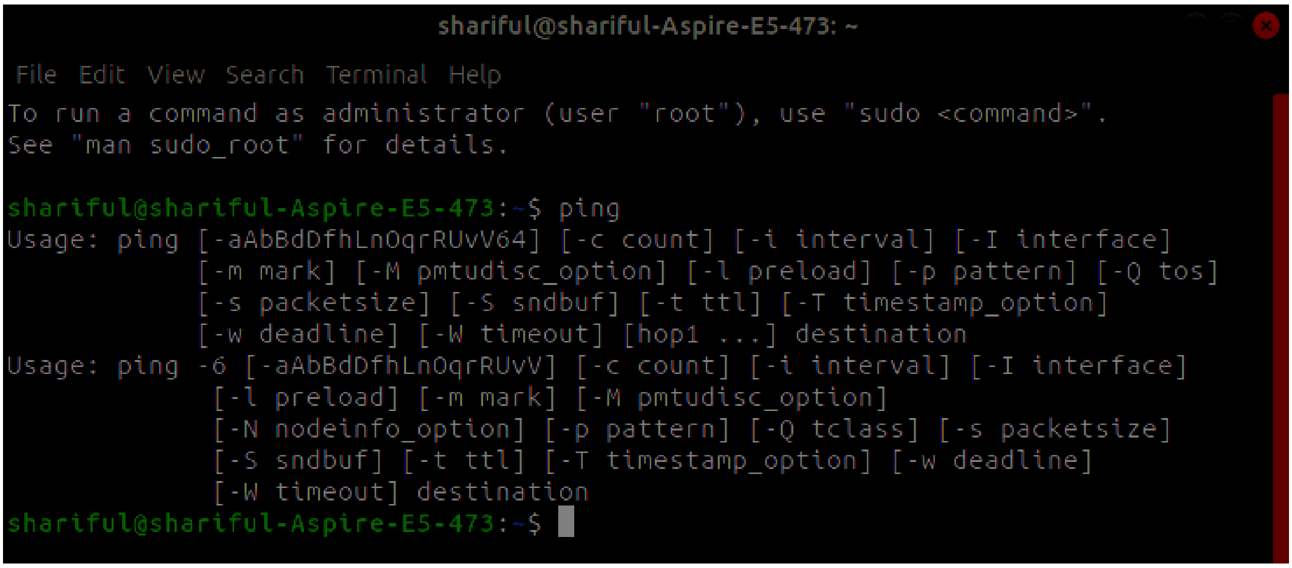
Assignment No: 01
Assignment Name: LINUX commands.
Name: Md. Shariful Islam
ID: IT-17013

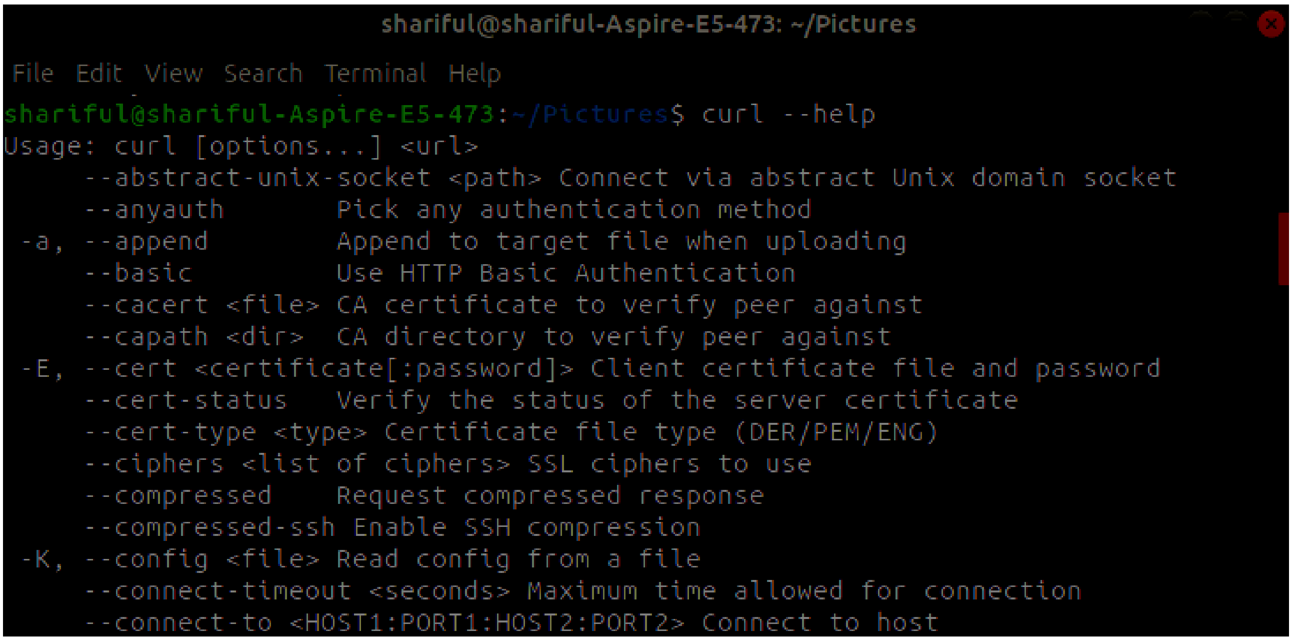
Run the commands given below:

PING: The ping command is one of the most used tools for troubleshooting, testing, and diagnosing network connectivity issues. Ping works by sending one or more ICMP (Internet Control Message Protocol) Echo Request packages to a specified destination IP on the network and waits for a reply.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

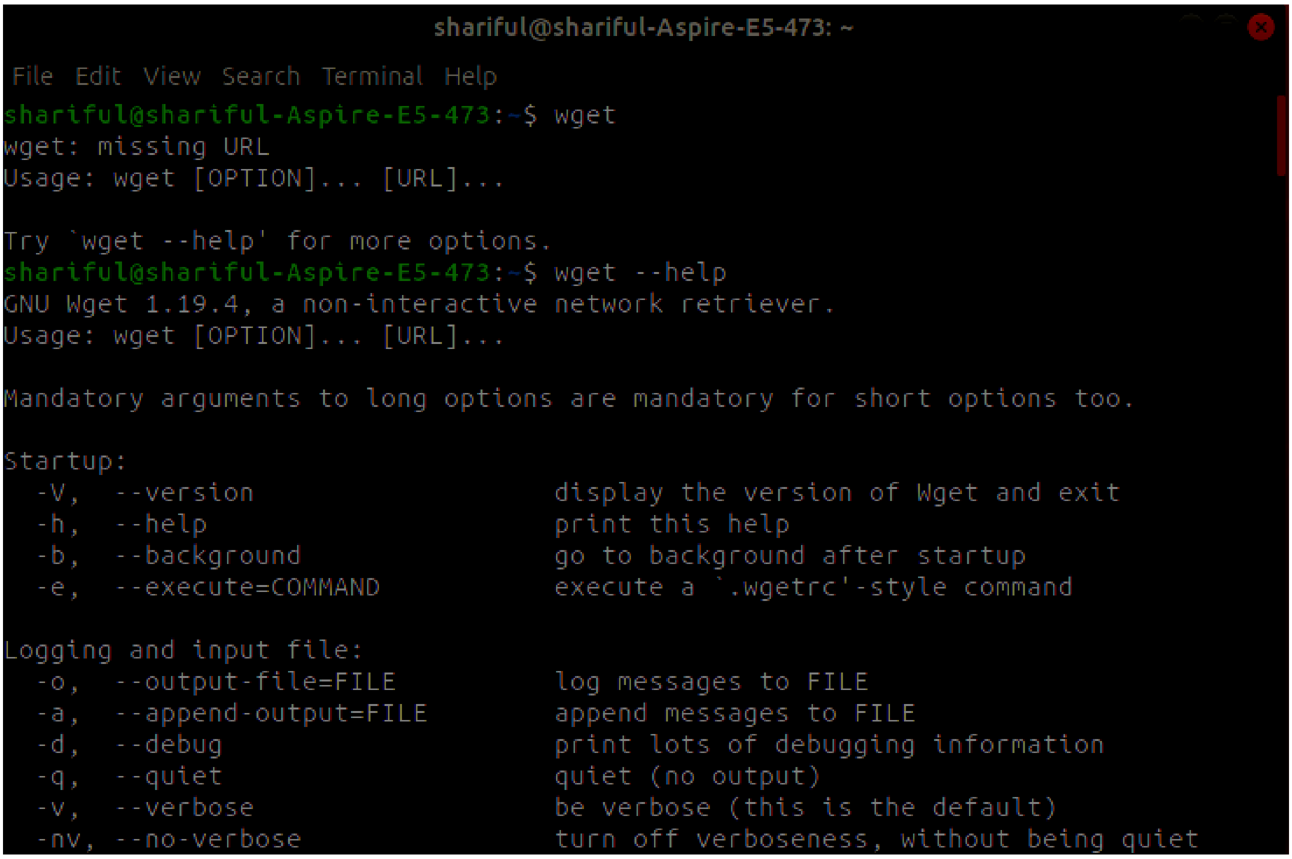
```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

shariful@shariful-Aspire-E5-473:~$ ping
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
            [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
            [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
            [-w deadline] [-W timeout] [hop1 ...] destination
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
             [-l preload] [-m mark] [-M pmtudisc_option]
             [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize]
             [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline]
             [-W timeout] destination
shariful@shariful-Aspire-E5-473:~$ 
```

CURL: curl is a command line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP or FILE). curl is powered by Libcurl. This tool is preferred for automation, since it is designed to work without user interaction.


shariful@shariful-Aspire-E5-473: ~/Pictures
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~/Pictures$ curl --help
Usage: curl [options...] <url>
     --abstract-unix-socket <path> Connect via abstract Unix domain socket
     --anyauth       Pick any authentication method
 -a, --append        Append to target file when uploading
     --basic         Use HTTP Basic Authentication
     --cacert <file> CA certificate to verify peer against
     --capath <dir>  CA directory to verify peer against
 -E, --cert <certificate[:password]> Client certificate file and password
     --cert-status   Verify the status of the server certificate
     --cert-type <type> Certificate file type (DER/PEM/ENG)
     --ciphers <list of ciphers> SSL ciphers to use
     --compressed    Request compressed response
     --compressed-ssh Enable SSH compression
 -K, --config <file> Read config from a file
     --connect-timeout <seconds> Maximum time allowed for connection
     --connect-to <HOST1:PORT1:HOST2:PORT2> Connect to host
```

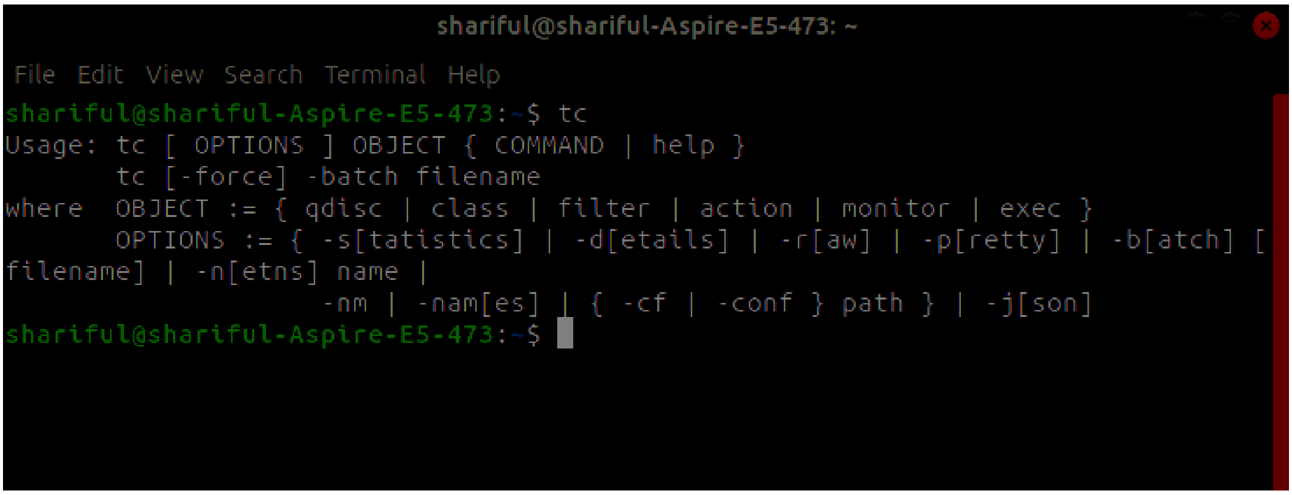
WGET: wget is a free utility for non-interactive download of files from the web.It
supports HTTP,HTTPS, and FTP protocols.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ wget
wget: missing URL
Usage: wget [OPTION]... [URL]...

Try `wget --help' for more options.
shariful@shariful-Aspire-E5-473:~$ wget --help
GNU Wget 1.19.4, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:
  -V,  --version                   display the version of Wget and exit
  -h,  --help                      print this help
  -b,  --background                go to background after startup
  -e,  --execute=COMMAND           execute a `.wgetrc'-style command

Logging and input file:
  -o,  --output-file=FILE          log messages to FILE
  -a,  --append-output=FILE        append messages to FILE
  -d,  --debug                     print lots of debugging information
  -q,  --quiet                     quiet (no output)
  -v,  --verbose                   be verbose (this is the default)
  -nv, --no-verbose                turn off verboseness, without being quiet
```

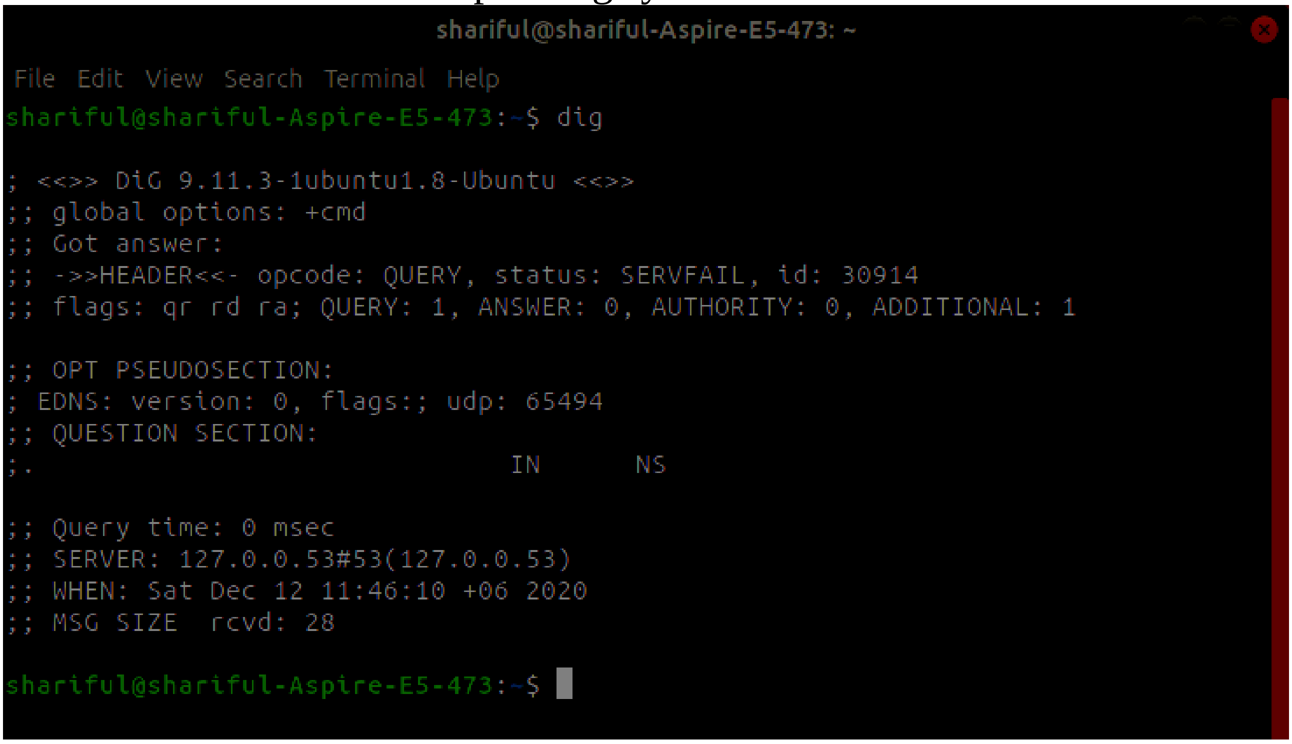
TC: Tc is used to configure Traffic Control in the Linux kernel. Traffic

Control consists of the following: SHAPING When traffic is shaped, its rate of transmission is under control. Shaping may be more than lowering the available bandwidth - it is also used to smooth out bursts in traffic for better network behaviour.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ tc
Usage: tc [ OPTIONS ] OBJECT { COMMAND | help }
       tc [-force] -batch filename
where  OBJECT := { qdisc | class | filter | action | monitor | exec }
       OPTIONS := { -s[tatistics] | -d[etails] | -r[aw] | -p[retty] | -b[atch] [
filename] | -n[etns] name |
                    -nm | -nam[es] | { -cf | -conf } path } | -j[son]
shariful@shariful-Aspire-E5-473:~$
```

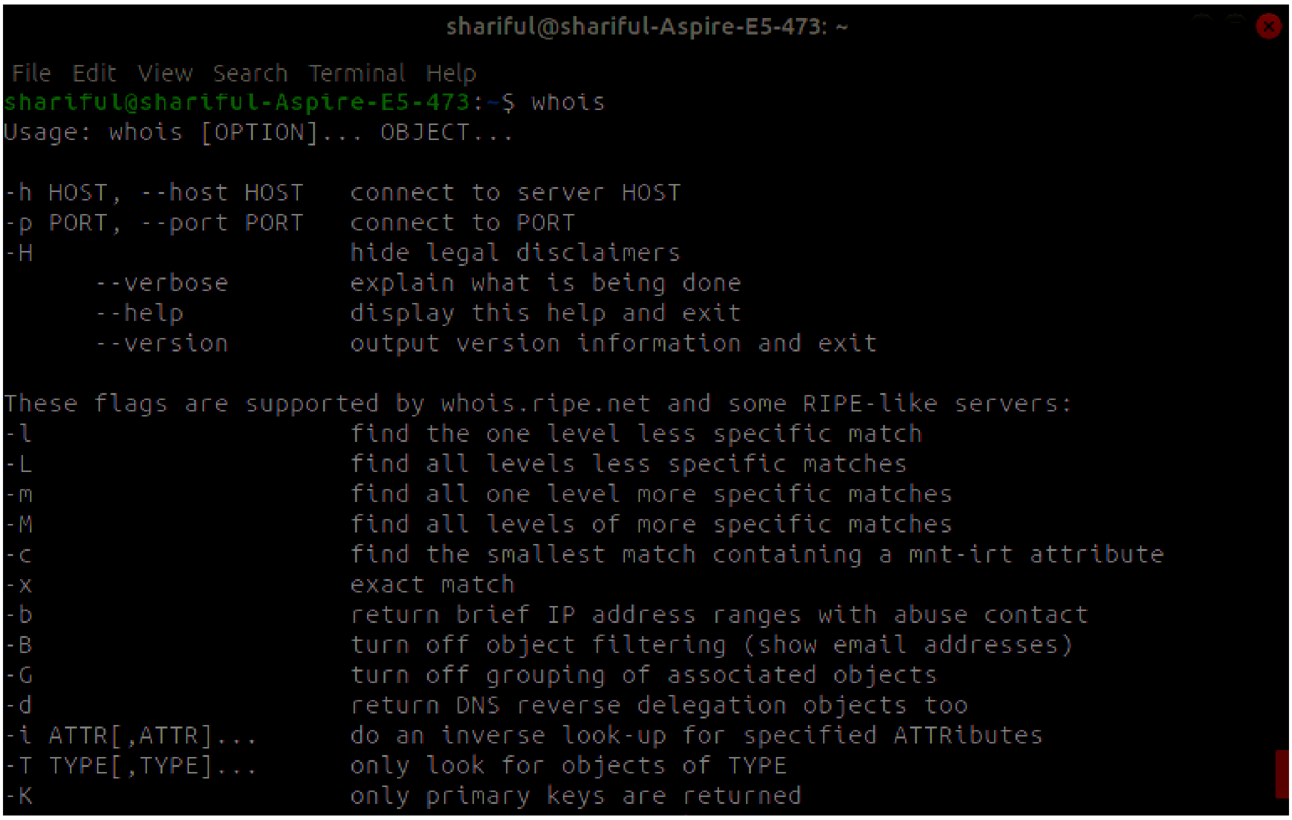
DIG/NSLOOKUP: Dig (Domain Information Groper) is a command line utility that performs DNS lookup by querying name servers and displaying the
result to you. In this tutorial, you'll find all the basic uses of the command you
should know in the Linux operating system.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ dig

; <<>> DiG 9.11.3-1ubuntu1.8-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 30914
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;.                              IN      NS

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Dec 12 11:46:10 +06 2020
;; MSG SIZE  rcvd: 28

shariful@shariful-Aspire-E5-473:~$
```

WHOIS: In Linux, the whois command line utility is a WHOIS client for

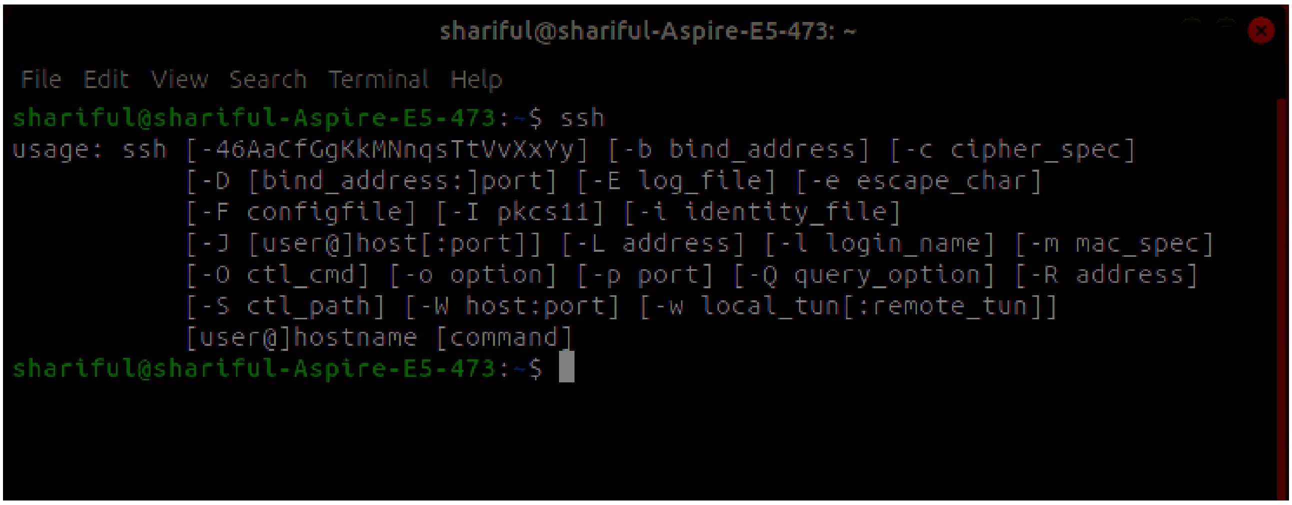
communicating with the WHOIS server (or database host) which listen to requests on the well-known port number 43, which stores and delivers database
content in a human-readable format.



shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

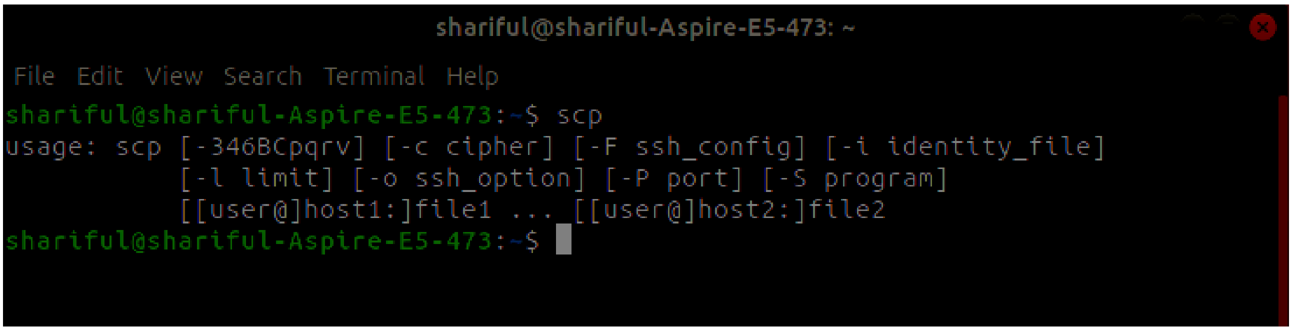
```
shariful@shariful-Aspire-E5-473:~$ whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST   connect to server HOST
-p PORT, --port PORT   connect to PORT
-H                     hide legal disclaimers
      --verbose        explain what is being done
      --help           display this help and exit
      --version        output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                     find the one level less specific match
-L                     find all levels less specific matches
-m                     find all one level more specific matches
-M                     find all levels of more specific matches
-c                     find the smallest match containing a mnt-irt attribute
-x                     exact match
-b                     return brief IP address ranges with abuse contact
-B                     turn off object filtering (show email addresses)
-G                     turn off grouping of associated objects
-d                     return DNS reverse delegation objects too
-i ATTR[,ATTR]...      do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...      only look for objects of TYPE
-K                     only primary keys are returned
```

SSH: ssh command provides a secure encrypted connection between two hosts
over an insecure network. This connection can also be used for terminal access,
file transfers, and for tunneling other applications. Graphical X11 applications
can also be run securely over SSH from a remote location.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

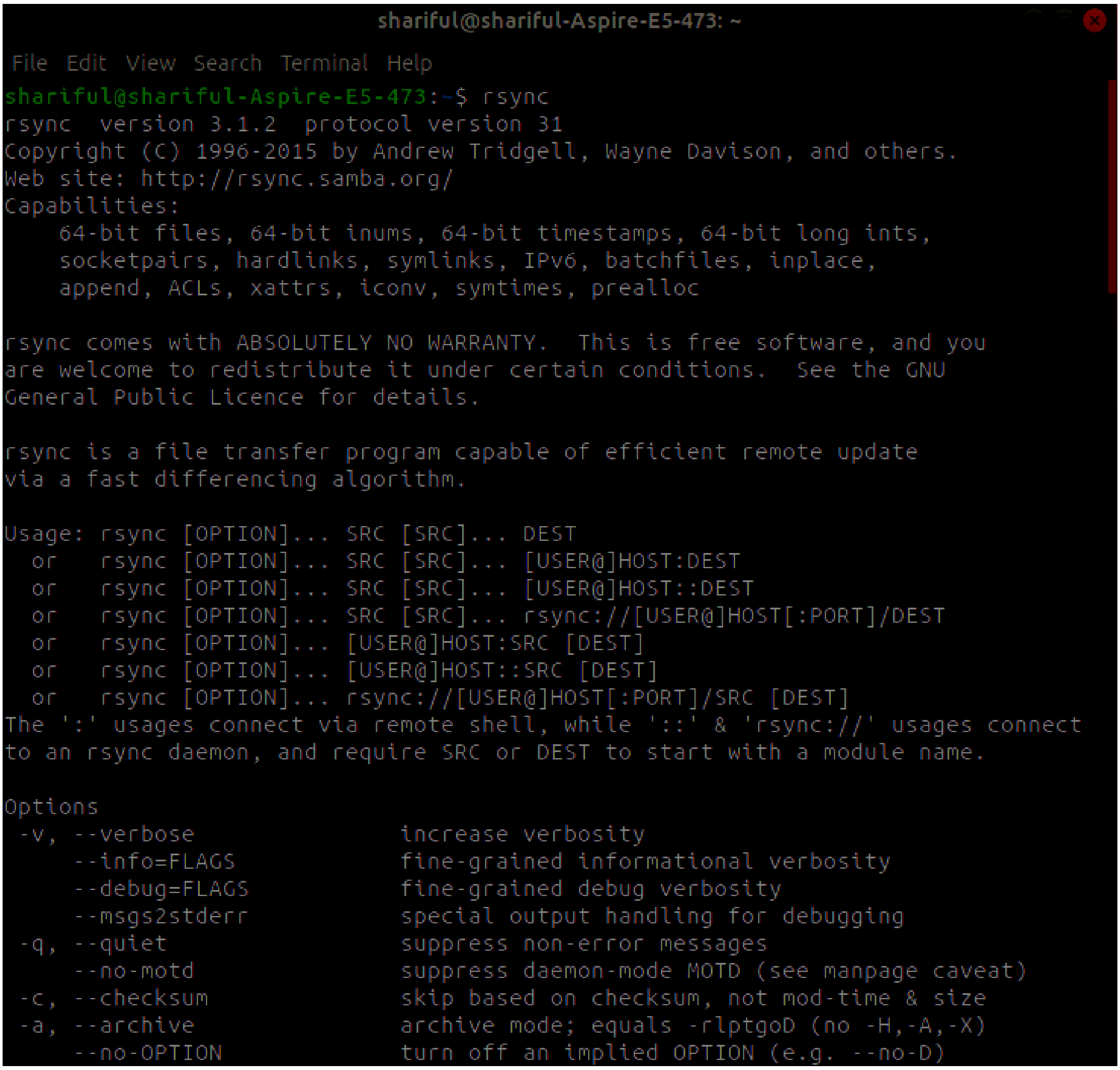
```
shariful@shariful-Aspire-E5-473:~$ ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-E log_file] [-e escape_char]
           [-F configfile] [-I pkcs11] [-i identity_file]
           [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]
           [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
           [user@]hostname [command]
shariful@shariful-Aspire-E5-473:~$
```

SCP: scp (secure copy) command in Linux system is used to copy file(s) between servers in a secure way. The SCP command or secure copy allows secure transferring of files in between the local host and the remote host or between two remote hosts.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

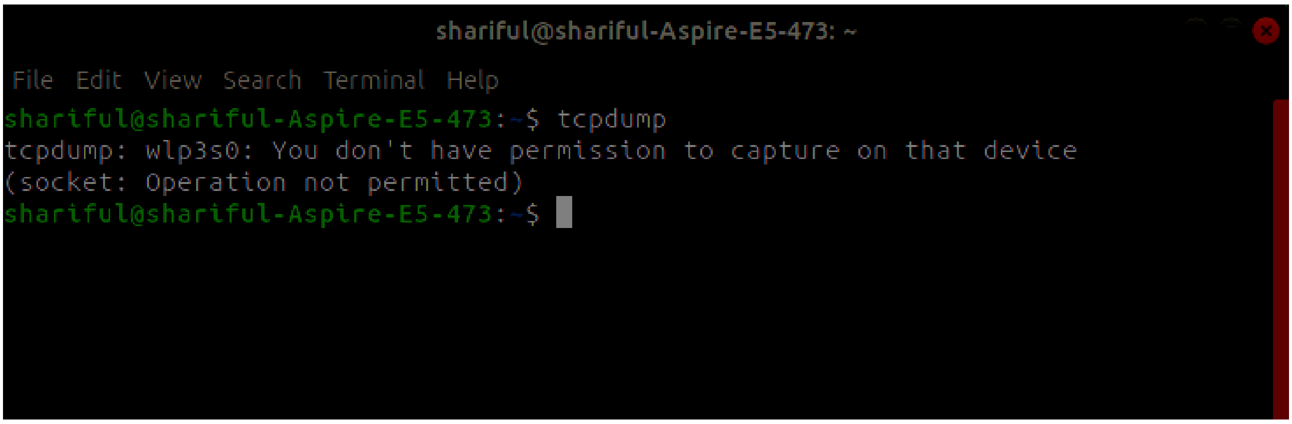
```
shariful@shariful-Aspire-E5-473:~$ scp
usage: scp [-346BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file]
           [-l limit] [-o ssh_option] [-P port] [-S program]
           [[user@]host1:]file1 ... [[user@]host2:]file2
shariful@shariful-Aspire-E5-473:~$
```

RSYNC: rsync is a fast and versatile command-line utility for synchronizing
files and directories between two locations over a remote shell, or from/to a
remote Rsync daemon. It provides fast incremental file transfer by transferring
only the differences between the source and the destination.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ rsync
rsync  version 3.1.2  protocol version 31
Copyright (C) 1996-2015 by Andrew Tridgell, Wayne Davison, and others.
Web site: http://rsync.samba.org/
Capabilities:
    64-bit files, 64-bit inums, 64-bit timestamps, 64-bit long ints,
    socketpairs, hardlinks, symlinks, IPv6, batchfiles, inplace,
    append, ACLs, xattrs, iconv, symtimes, prealloc

rsync comes with ABSOLUTELY NO WARRANTY.  This is free software, and you
are welcome to redistribute it under certain conditions.  See the GNU
General Public Licence for details.

rsync is a file transfer program capable of efficient remote update
via a fast differencing algorithm.

Usage: rsync [OPTION]... SRC [SRC]... DEST
  or   rsync [OPTION]... SRC [SRC]... [USER@]HOST:DEST
  or   rsync [OPTION]... SRC [SRC]... [USER@]HOST::DEST
  or   rsync [OPTION]... SRC [SRC]... rsync://[USER@]HOST[:PORT]/DEST
  or   rsync [OPTION]... [USER@]HOST:SRC [DEST]
  or   rsync [OPTION]... [USER@]HOST::SRC [DEST]
  or   rsync [OPTION]... rsync://[USER@]HOST[:PORT]/SRC [DEST]
The ':' usages connect via remote shell, while '::' & 'rsync://' usages connect
to an rsync daemon, and require SRC or DEST to start with a module name.

Options
 -v, --verbose               increase verbosity
     --info=FLAGS            fine-grained informational verbosity
     --debug=FLAGS           fine-grained debug verbosity
     --msgs2stderr           special output handling for debugging
 -q, --quiet                 suppress non-error messages
     --no-motd               suppress daemon-mode MOTD (see manpage caveat)
 -c, --checksum              skip based on checksum, not mod-time & size
 -a, --archive               archive mode; equals -rlptgoD (no -H,-A,-X)
     --no-OPTION             turn off an implied OPTION (e.g. --no-D)
```

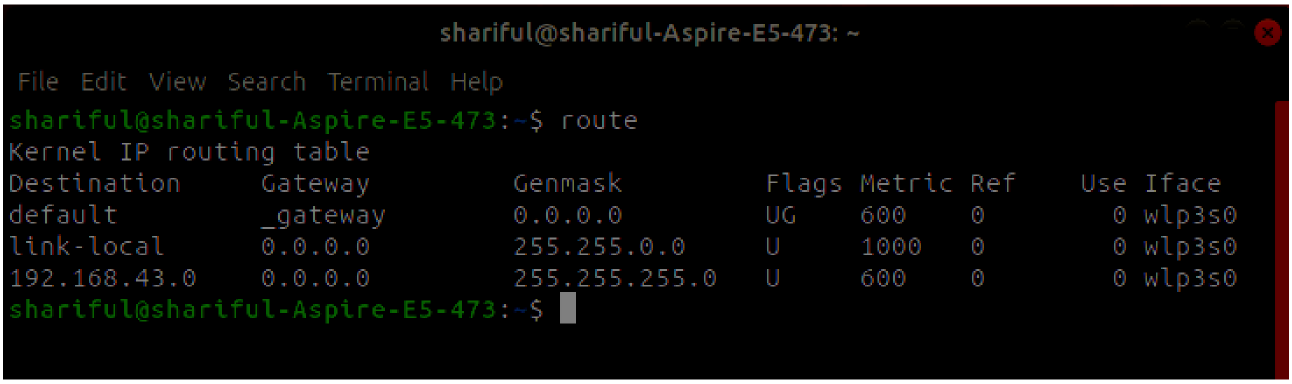
TCPDUMP: tcpdump is a most powerful and widely used command-line packets sniffer or package analyzer tool which is used to capture or filter TCP/IP packets that received or transferred over a network on a specific interface. It is available under most of the Linux/Unix based operating systems



shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

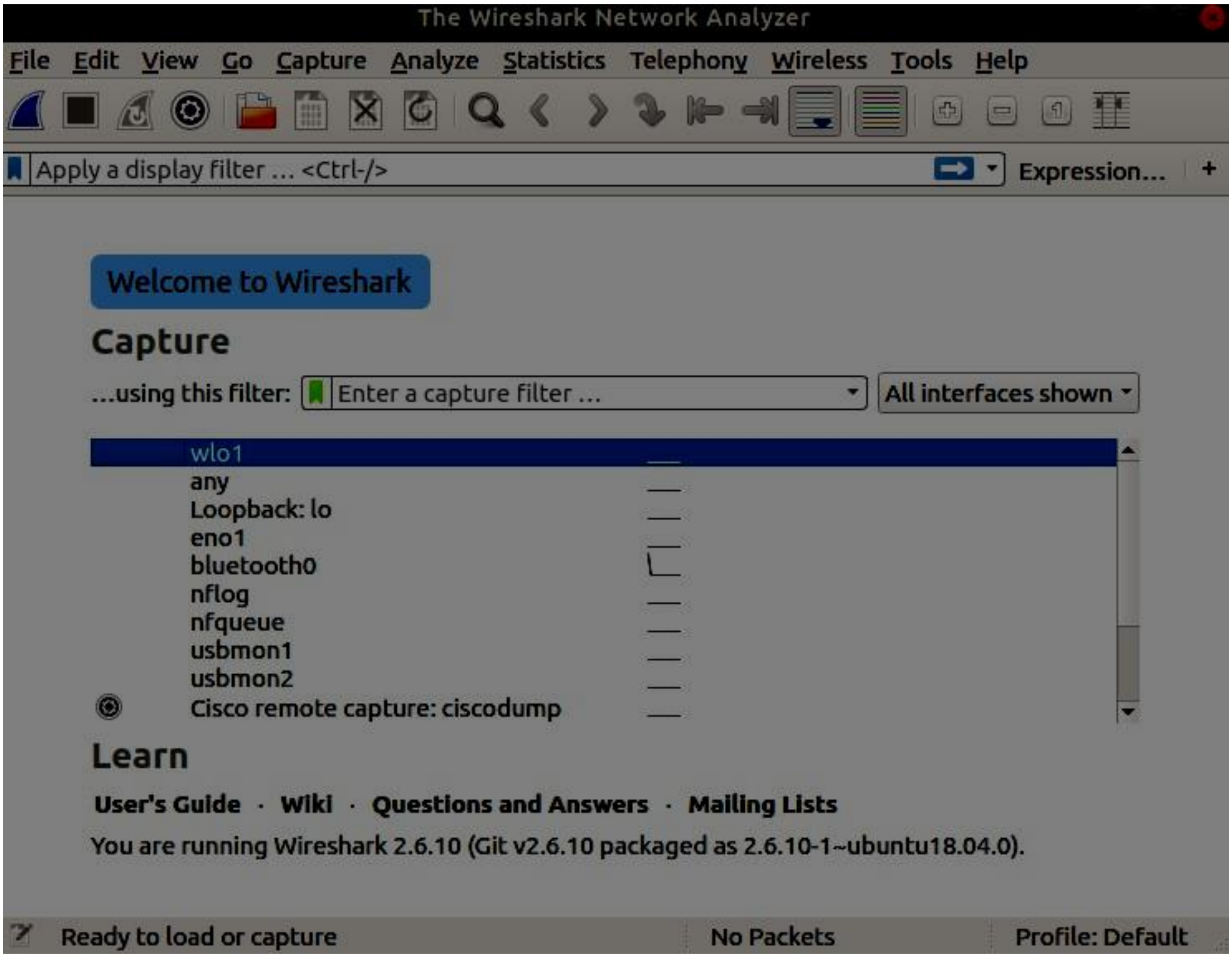
```
shariful@shariful-Aspire-E5-473:~$ tcpdump
tcpdump: wlp3s0: You don't have permission to capture on that device
(socket: Operation not permitted)
shariful@shariful-Aspire-E5-473:~$
```

WIRESHARK:



shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlp3s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlp3s0
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlp3s0
shariful@shariful-Aspire-E5-473:~$
```



Apply a display filter … <Ctrl-/>

Welcome to Wireshark

Capture

…using this filter: Enter a capture filter …   All interfaces shown

```
wlo1
any
Loopback: lo
eno1
bluetooth0
nflog
nfqueue
usbmon1
usbmon2
Cisco remote capture: ciscodump
```

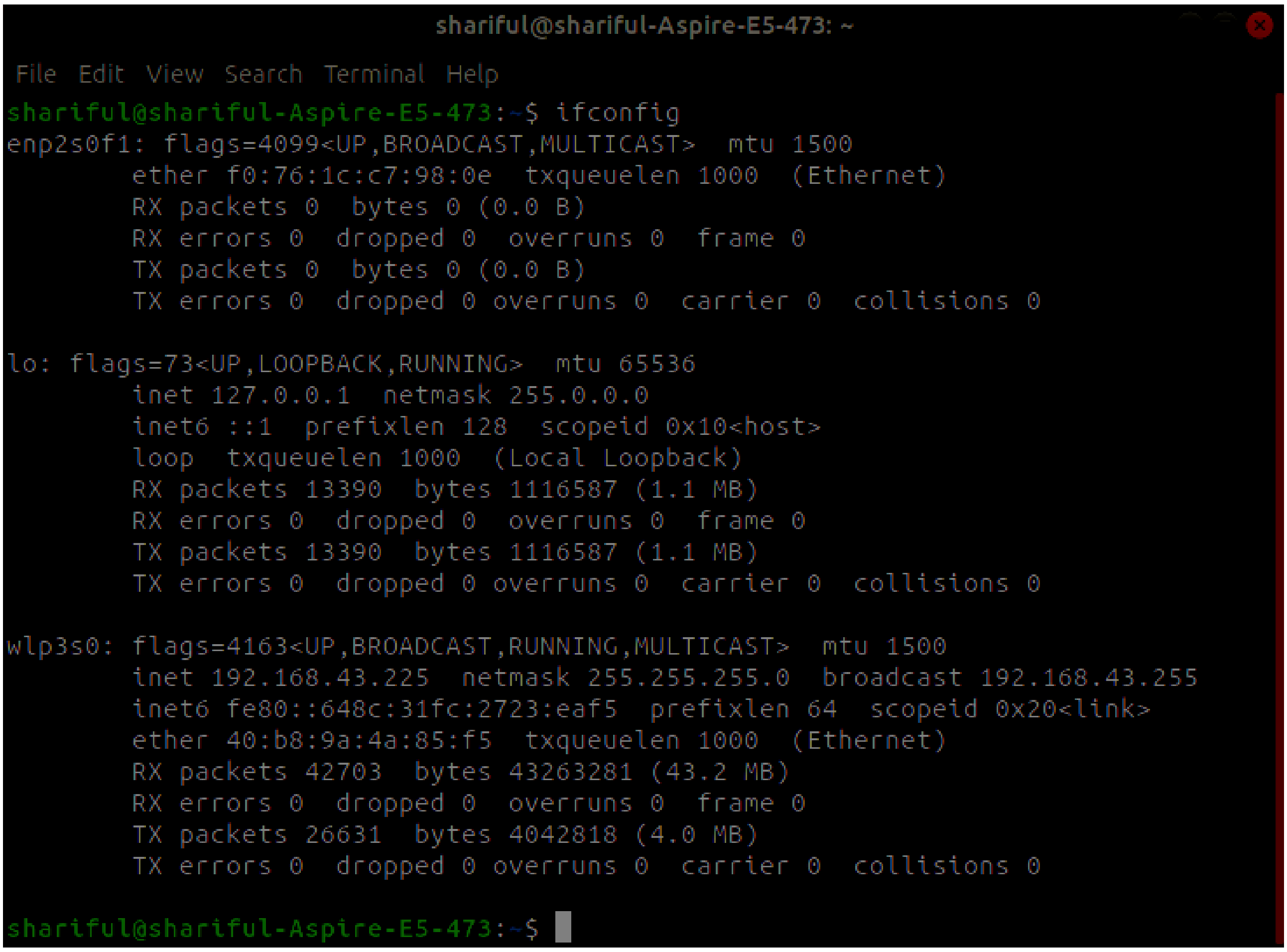
Learn

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

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

Ready to load or capture   No Packets   Profile: Default

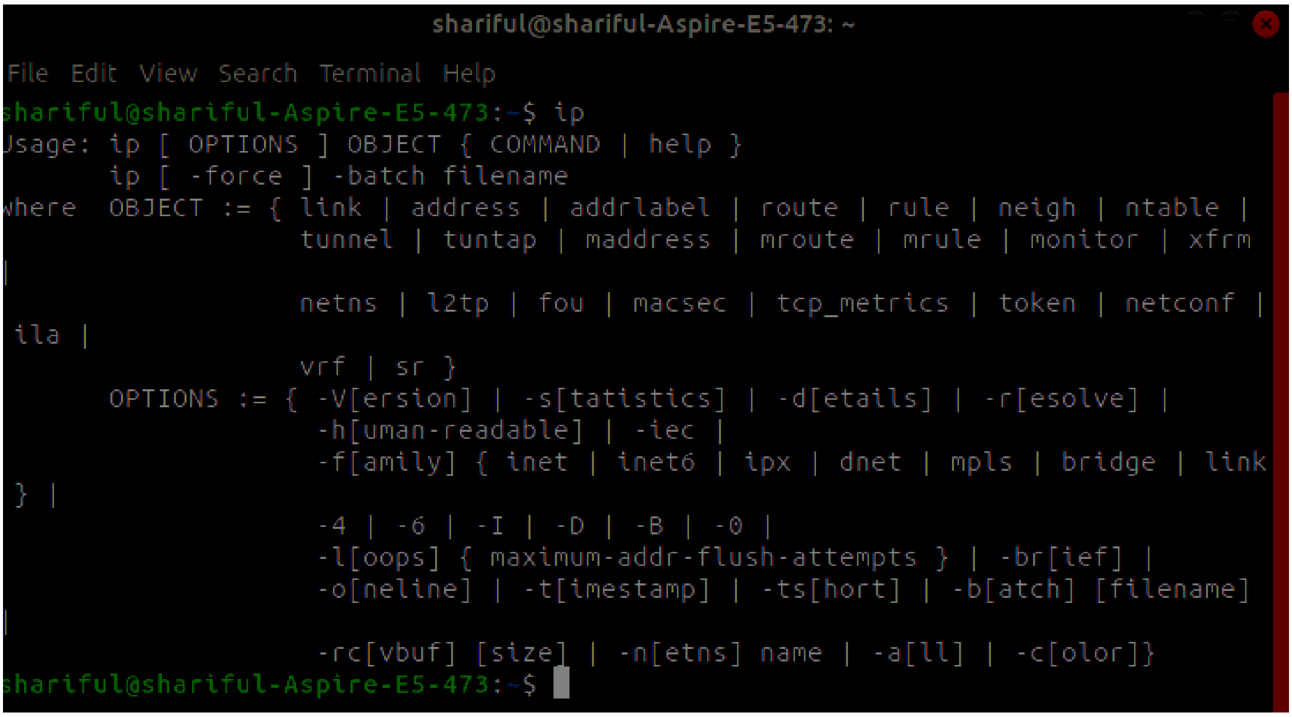
IFCONFIG: stands for "interface configuration." It is used to view and change the configuration of the network interfaces on your system.



shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

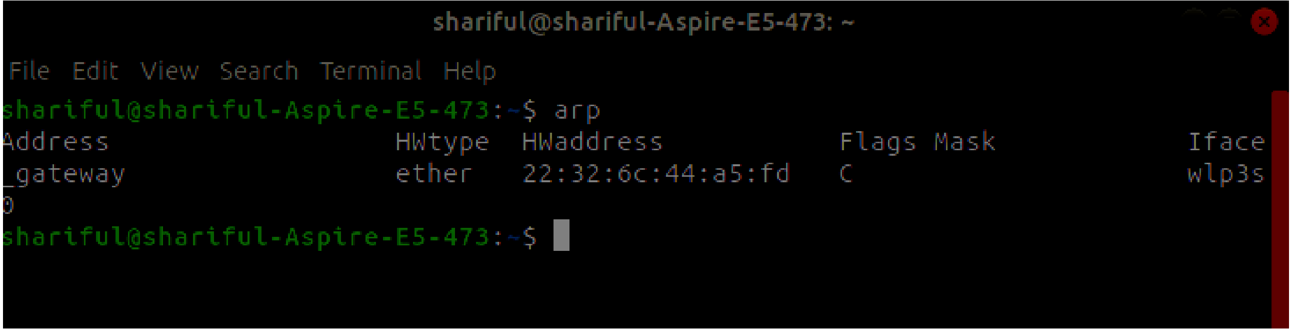
```
shariful@shariful-Aspire-E5-473:~$ ifconfig
enp2s0f1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether f0:76:1c:c7:98:0e  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 13390  bytes 1116587 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13390  bytes 1116587 (1.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.225  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 fe80::648c:31fc:2723:eaf5  prefixlen 64  scopeid 0x20<link>
        ether 40:b8:9a:4a:85:f5  txqueuelen 1000  (Ethernet)
        RX packets 42703  bytes 43263281 (43.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26631  bytes 4042818 (4.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

shariful@shariful-Aspire-E5-473:~$ 
```

IP: The ip command is a Linux net-tool for system and network administrators.
IP stands for Internet Protocol and as the name suggests, the tool is used for
configuring network interfaces. Older Linux distributions used the ifconfig command, which operates similarly.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | address | addrlabel | route | rule | neigh | ntable |
                   tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm
|
                   netns | l2tp | fou | macsec | tcp_metrics | token | netconf |
 ila |
                   vrf | sr }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -h[uman-readable] | -iec |
                    -f[amily] { inet | inet6 | ipx | dnet | mpls | bridge | link
 } |
                    -4 | -6 | -I | -D | -B | -0 |
                    -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                    -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename]
|
                    -rc[vbuf] [size] | -n[etns] name | -a[ll] | -c[olor]}
shariful@shariful-Aspire-E5-473:~$
```

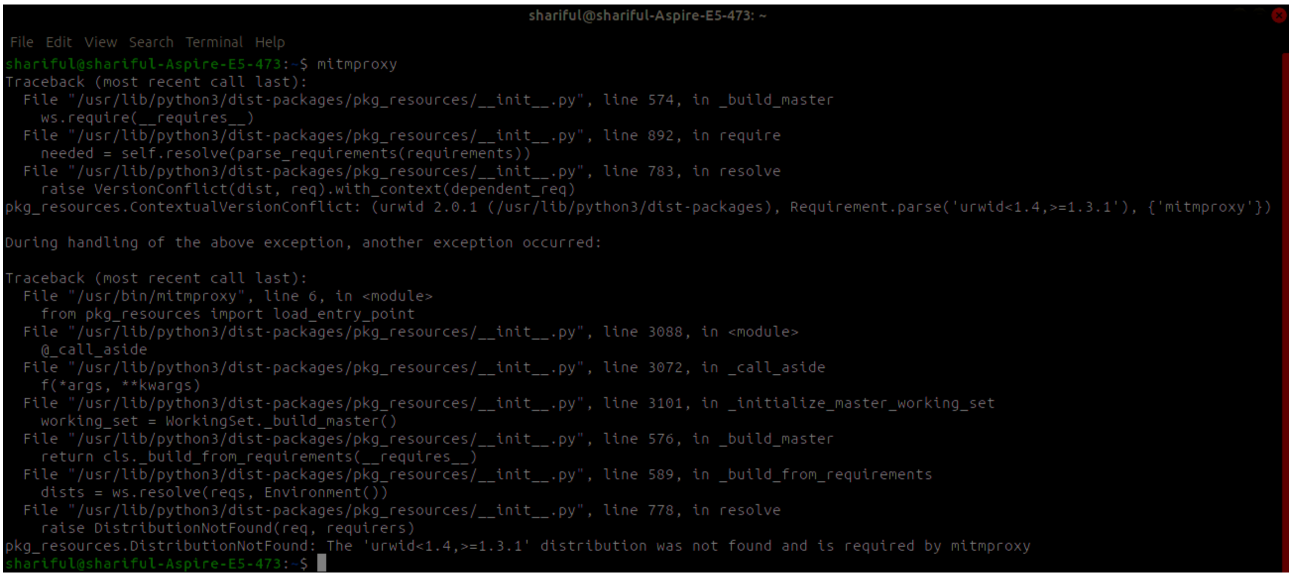
ARP: arp command manipulates the System’s ARP cache. It also allows a complete dump of the ARP cache. ARP stands for Address Resolution Protocol.
The primary function of this protocol is to resolve the IP address of a system to
its mac address, and hence it works between level 2(Data link layer) and level
3(Network layer).


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   22:32:6c:44:a5:fd   C                     wlp3s
0
shariful@shariful-Aspire-E5-473:~$
```

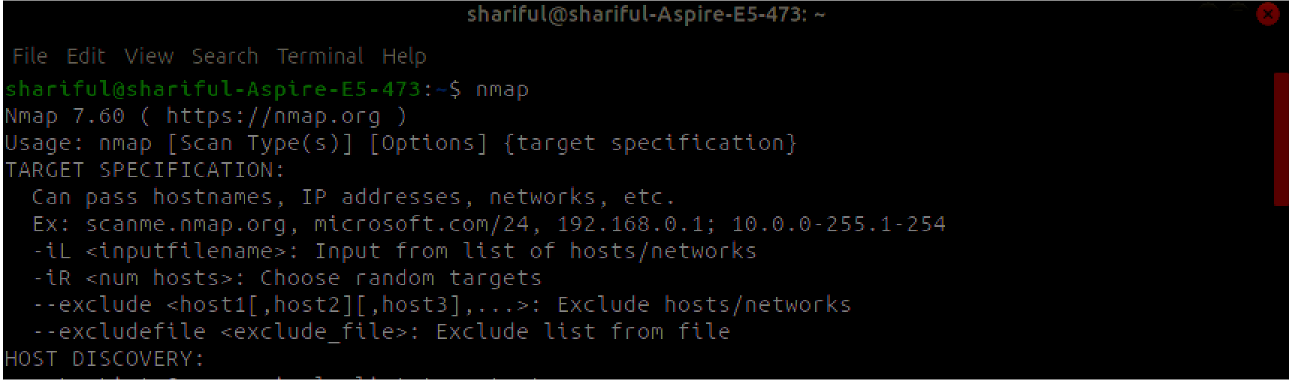
MITMPROXY: mitmproxy is an SSL-capable man-in-the-middle HTTP proxy. It provides a console interface that allows traffic flows to be inspected
and edited on the fly. Also shipped is mitmdump, the command-line version of
mitmproxy, with the same functionality but without the frills. Think tcpdump

for HTTP.

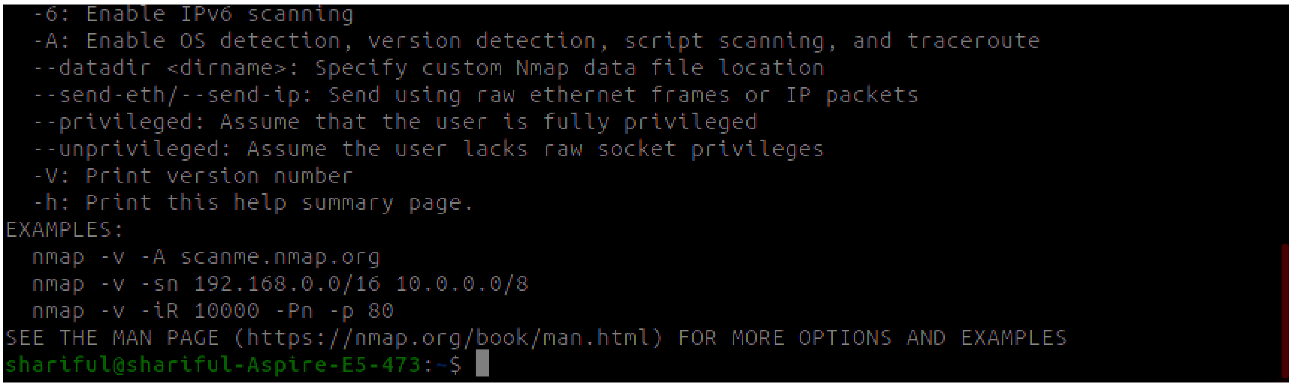

shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ mitmproxy
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 574, in _build_master
    ws.require(__requires__)
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 892, in require
    needed = self.resolve(parse_requirements(requirements))
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 783, in resolve
    raise VersionConflict(dist, req).with_context(dependent_req)
pkg_resources.ContextualVersionConflict: (urwid 2.0.1 (/usr/lib/python3/dist-packages), Requirement.parse('urwid<1.4,>=1.3.1'), {'mitmproxy'})

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/usr/bin/mitmproxy", line 6, in <module>
    from pkg_resources import load_entry_point
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 3088, in <module>
    @_call_aside
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 3072, in _call_aside
    f(*args, **kwargs)
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 3101, in _initialize_master_working_set
    working_set = WorkingSet._build_master()
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 576, in _build_master
    return cls._build_from_requirements(__requires__)
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 589, in _build_from_requirements
    dists = ws.resolve(reqs, Environment())
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 778, in resolve
    raise DistributionNotFound(req, requirers)
pkg_resources.DistributionNotFound: The 'urwid<1.4,>=1.3.1' distribution was not found and is required by mitmproxy
shariful@shariful-Aspire-E5-473:~$
```

NMAP: Nmap is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators.

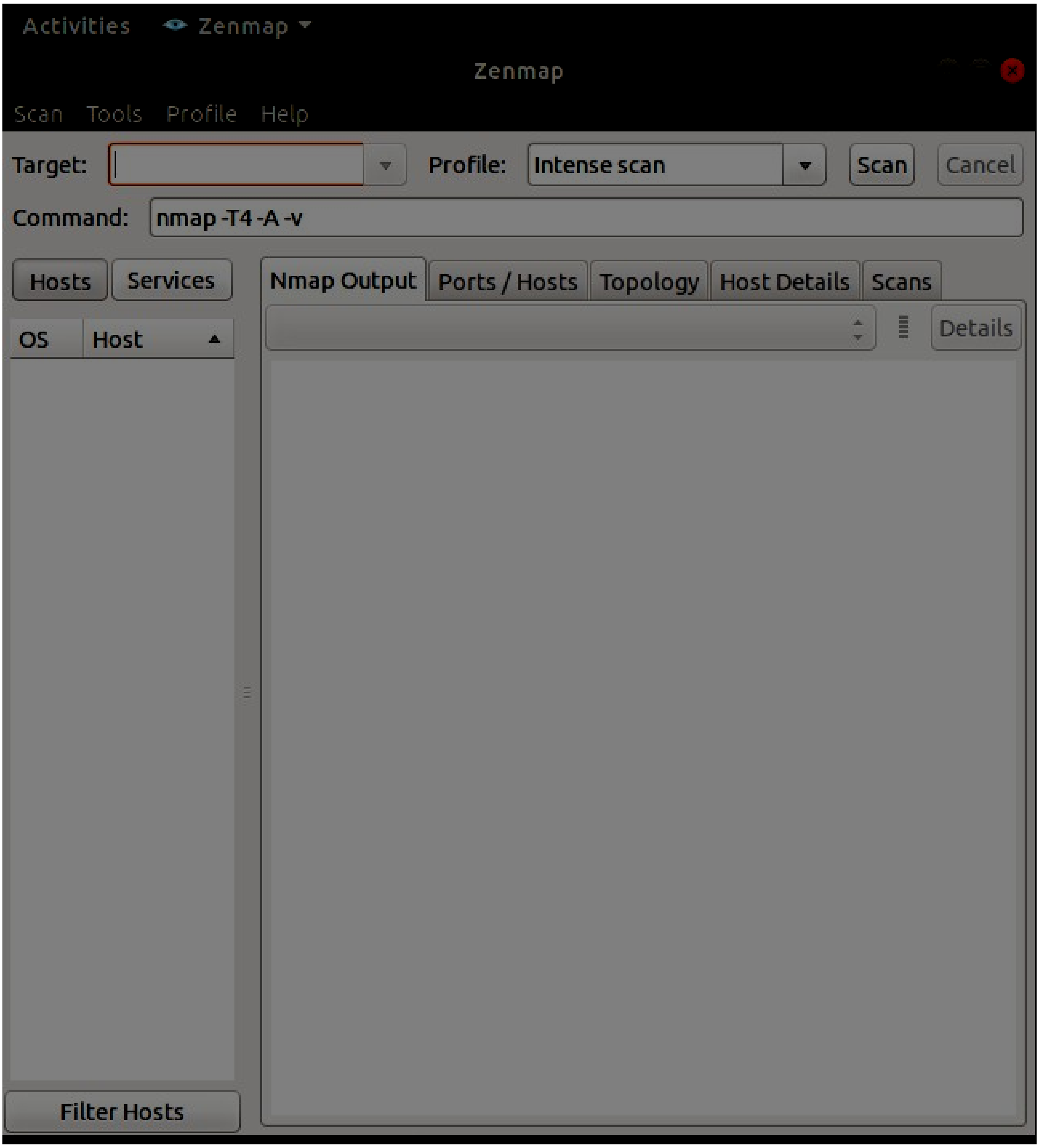

shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ nmap
Nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
```



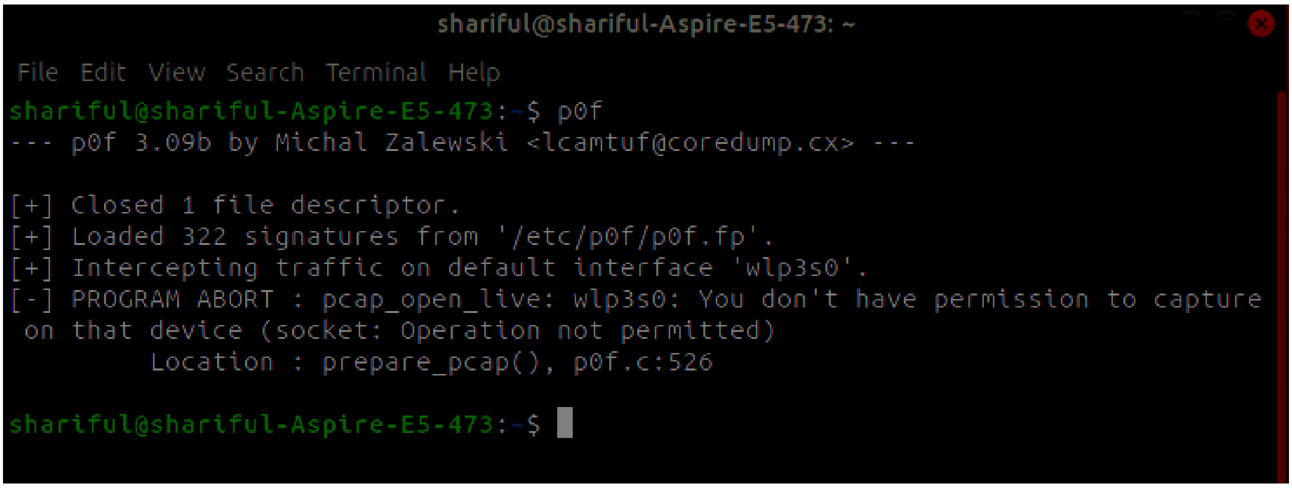
```
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
shariful@shariful-Aspire-E5-473:~$
```

ZENMAP:



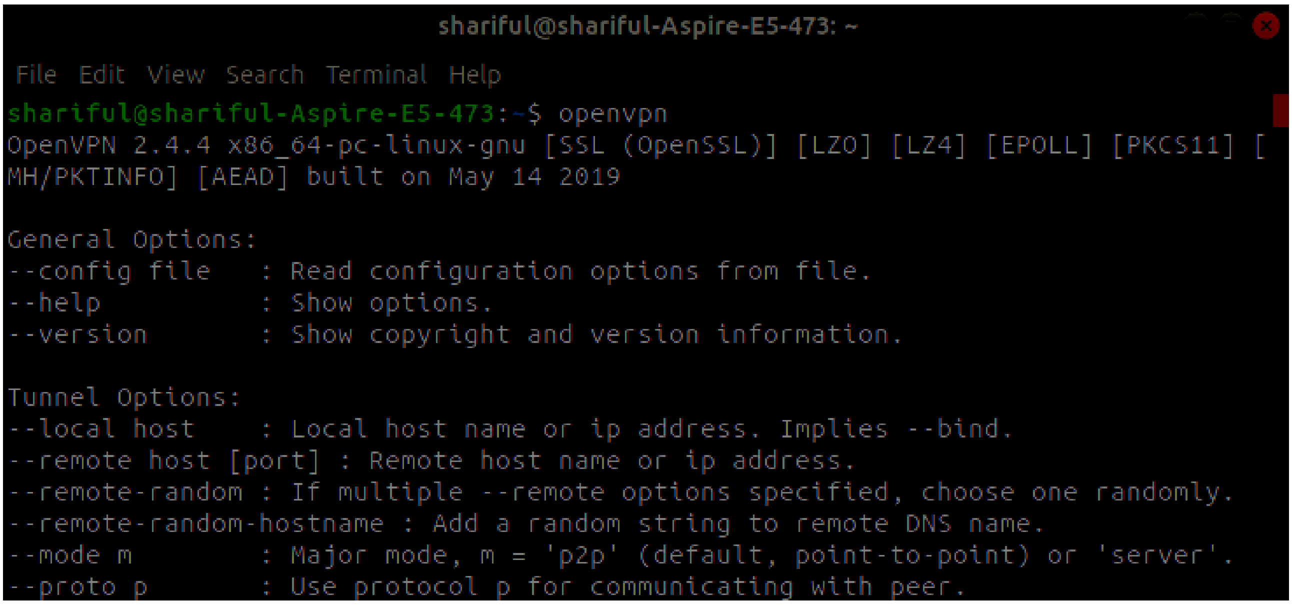
Command: nmap -T4 -A -v

P0F: p0f is a passive TCP/IP stack fingerprinting tool. p0f can attempt to identify the system running on machines that send network traffic to the box it
is running on, or to a machine that shares a medium with the machine it is running on. p0f can also assist in analysing other aspects of the remote system.

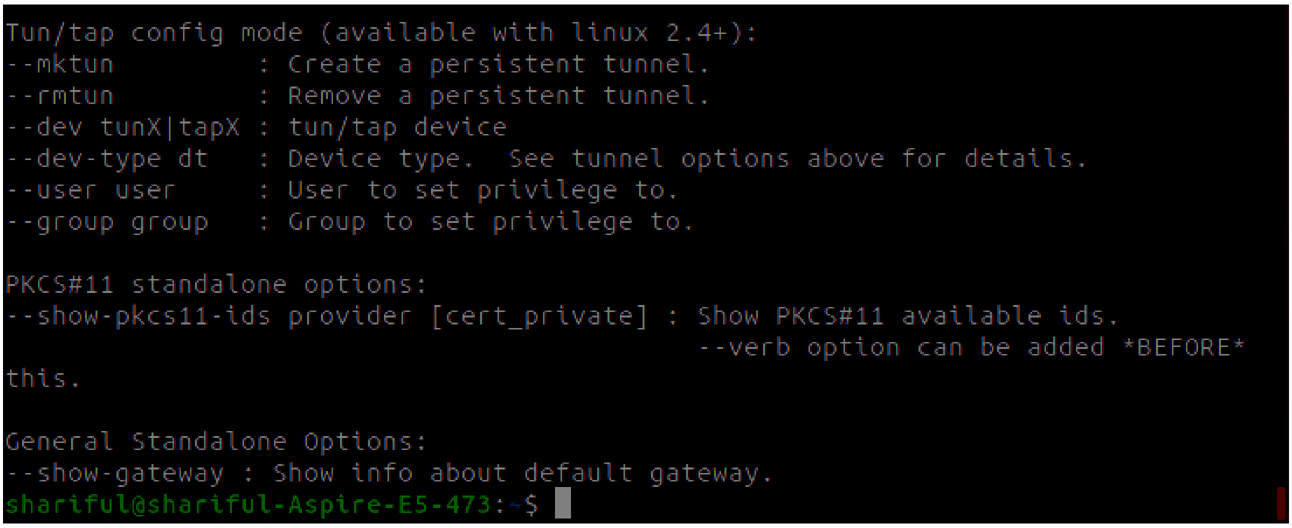

shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ p0f
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'wlp3s0'.
[-] PROGRAM ABORT : pcap_open_live: wlp3s0: You don't have permission to capture
 on that device (socket: Operation not permitted)
         Location : prepare_pcap(), p0f.c:526

shariful@shariful-Aspire-E5-473:~$
```

OPENVPN:


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

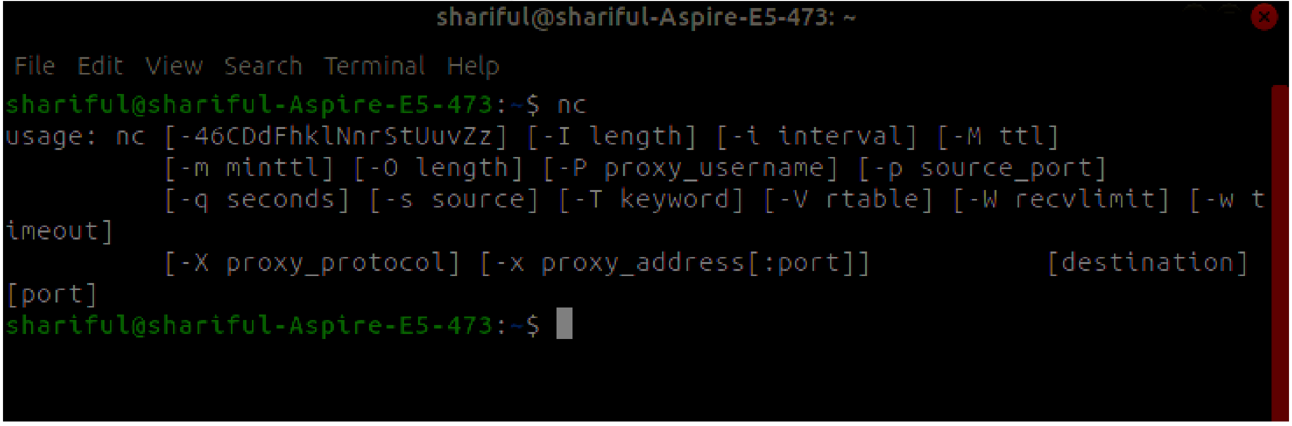
```
shariful@shariful-Aspire-E5-473:~$ openvpn
OpenVPN 2.4.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [
MH/PKTINFO] [AEAD] built on May 14 2019

General Options:
--config file   : Read configuration options from file.
--help          : Show options.
--version       : Show copyright and version information.

Tunnel Options:
--local host    : Local host name or ip address. Implies --bind.
--remote host [port] : Remote host name or ip address.
--remote-random : If multiple --remote options specified, choose one randomly.
--remote-random-hostname : Add a random string to remote DNS name.
--mode m        : Major mode, m = 'p2p' (default, point-to-point) or 'server'.
--proto p       : Use protocol p for communicating with peer.
```



```
Tun/tap config mode (available with linux 2.4+):
--mktun         : Create a persistent tunnel.
--rmtun         : Remove a persistent tunnel.
--dev tunX|tapX : tun/tap device
--dev-type dt   : Device type.  See tunnel options above for details.
--user user     : User to set privilege to.
--group group   : Group to set privilege to.

PKCS#11 standalone options:
--show-pkcs11-ids provider [cert_private] : Show PKCS#11 available ids.
                                            --verb option can be added *BEFORE*
this.

General Standalone Options:
--show-gateway : Show info about default gateway.
shariful@shariful-Aspire-E5-473:~$
```

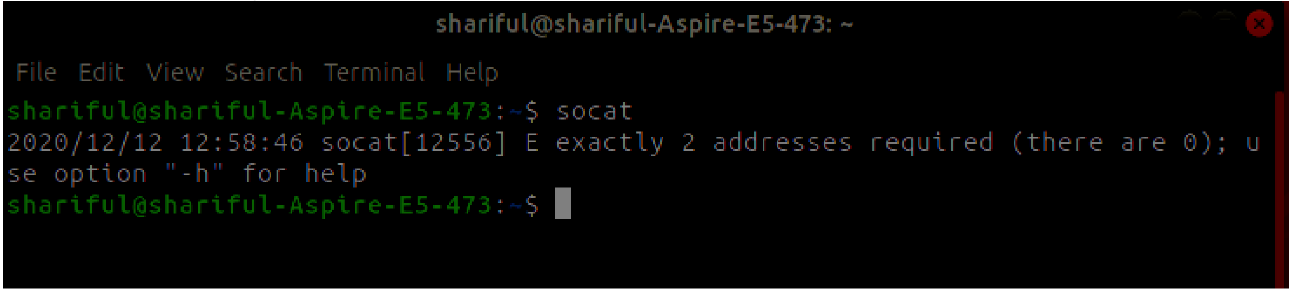
WIREGUARD:

NC: ncat or nc is networking utility with functionality similar to cat command but for network. It is a general purpose CLI tool for reading, writing, redirecting data across a network. It is designed to be a reliable back-end tool that can be used with scripts or other programs.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ nc
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w t
imeout]
          [-X proxy_protocol] [-x proxy_address[:port]]          [destination]
[port]
shariful@shariful-Aspire-E5-473:~$ 
```

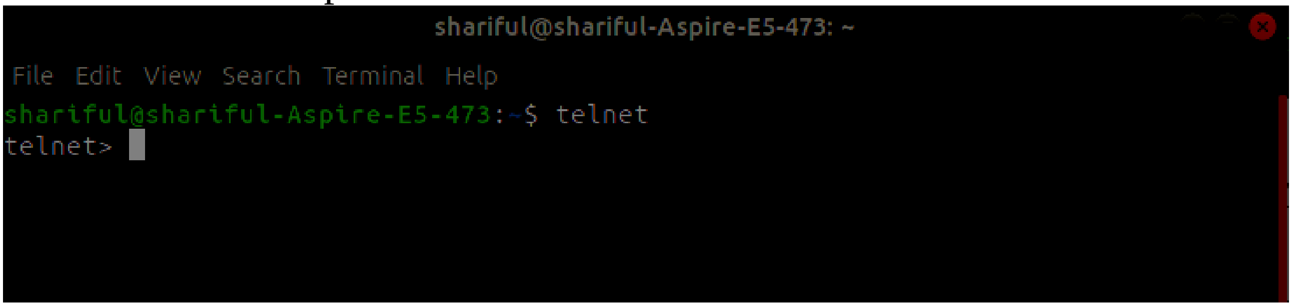
SOCAT: Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ socat
2020/12/12 12:58:46 socat[12556] E exactly 2 addresses required (there are 0); u
se option "-h" for help
shariful@shariful-Aspire-E5-473:~$ 
```

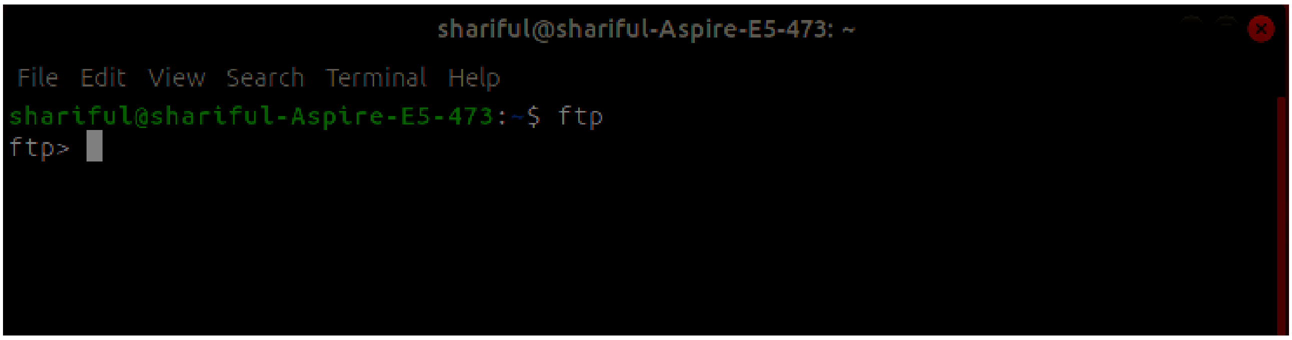
TELNET: In Linux, the telnet command is used to create a remote connection with a system over a TCP/IP network. It allows us to administrate other systems by the terminal. We can run a program to conduct administration.

It uses a TELNET protocol.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

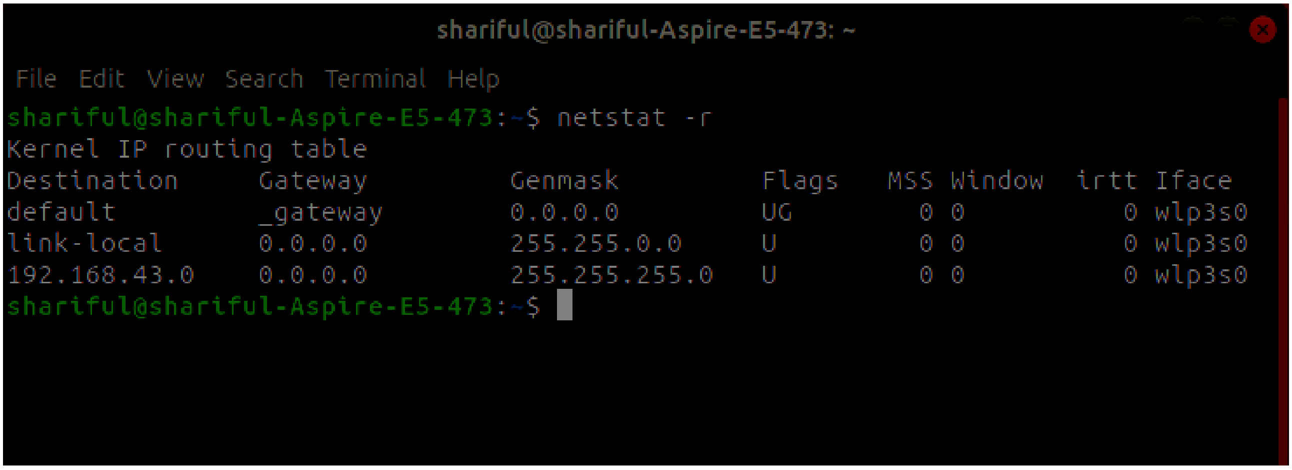
```
shariful@shariful-Aspire-E5-473:~$ telnet
telnet> 
```

FTP/SFTP: FTP (File Transfer Protocol) is a standard network protocol used to transfer files to and from a remote network. ... However, the ftp command is useful when you work on a server without GUI and you want to transfer files over FTP to or from a remote server.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

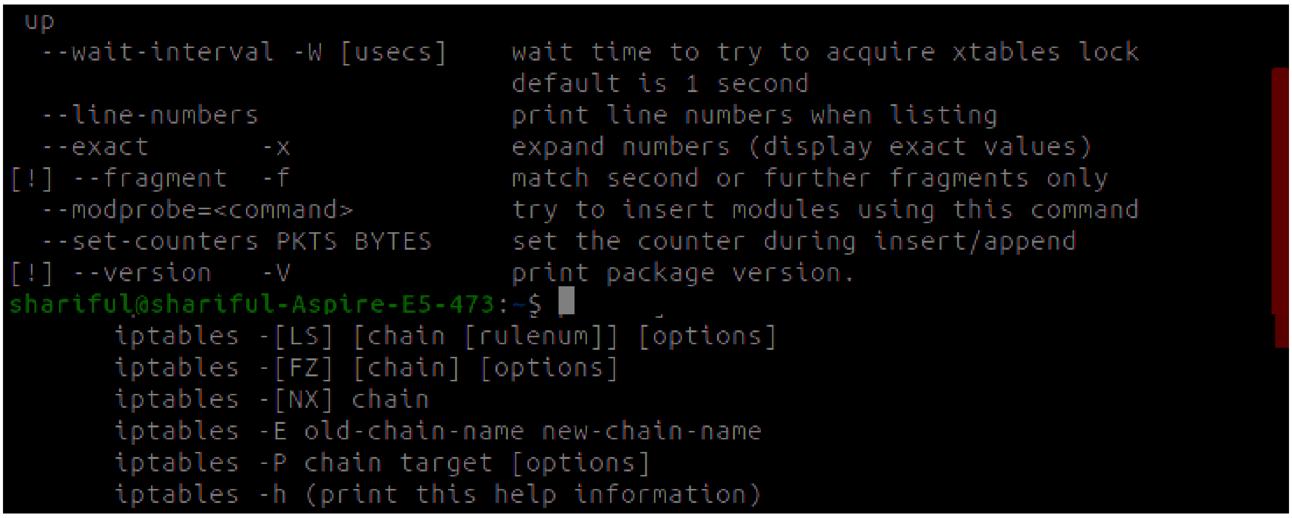
```
shariful@shariful-Aspire-E5-473:~$ ftp
ftp> 
```

NETSTAT/SS/LSOF/FUSER: The netstat command generates displays that show network status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information, and interface information. The most frequently used options for determining network status are: s , r , and i .


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 wlp3s0
link-local      0.0.0.0         255.255.0.0     U         0 0          0 wlp3s0
192.168.43.0    0.0.0.0         255.255.255.0   U         0 0          0 wlp3s0
shariful@shariful-Aspire-E5-473:~$ 
```

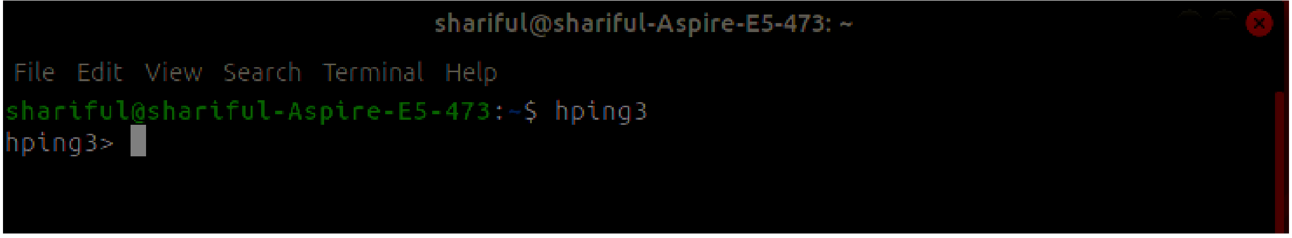
IPTABLES: iptables is a command line interface used to set up and maintain tables for the Netfilter firewall for IPv4, included in the Linux kernel. The firewall matches packets with rules defined in these tables and then takes the specified action on a possible match. Tables is the name for a set of chains.



```
 up
  --wait-interval -W [usecs]    wait time to try to acquire xtables lock
                                default is 1 second
  --line-numbers                print line numbers when listing
  --exact        -x             expand numbers (display exact values)
[!] --fragment   -f             match second or further fragments only
  --modprobe=<command>          try to insert modules using this command
  --set-counters PKTS BYTES     set the counter during insert/append
[!] --version    -V             print package version.
shariful@shariful-Aspire-E5-473:~$ 
       iptables -[LS] [chain [rulenum]] [options]
       iptables -[FZ] [chain] [options]
       iptables -[NX] chain
       iptables -E old-chain-name new-chain-name
       iptables -P chain target [options]
       iptables -h (print this help information)
```

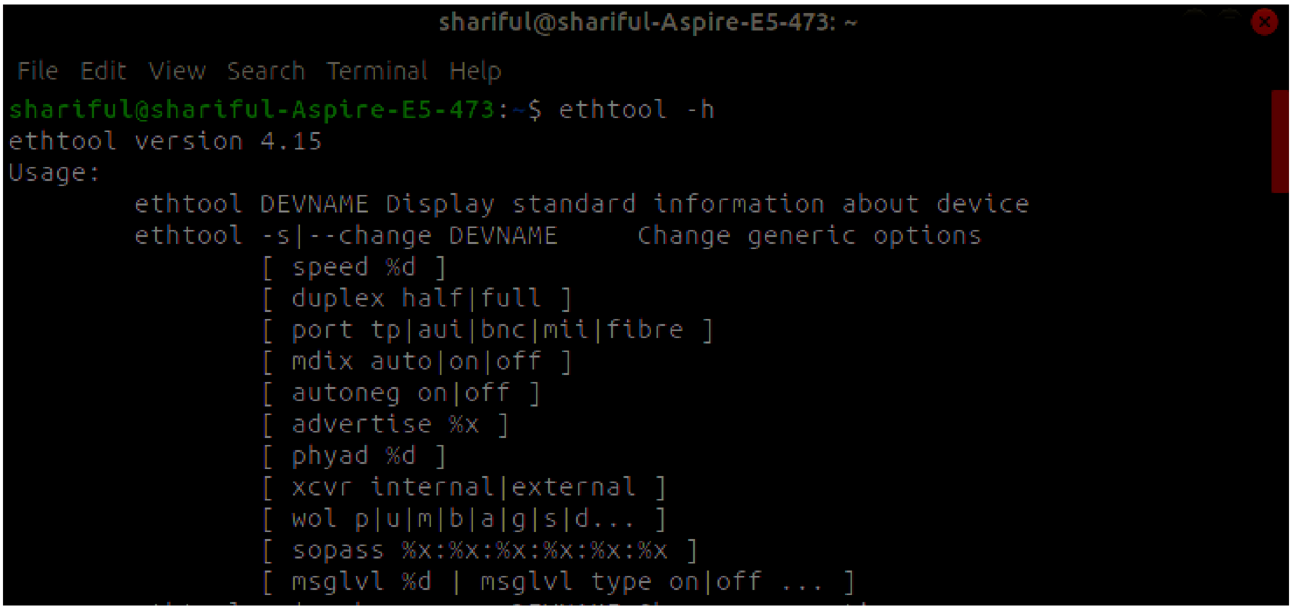
NFTABLES:

HPING3: hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn’t only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

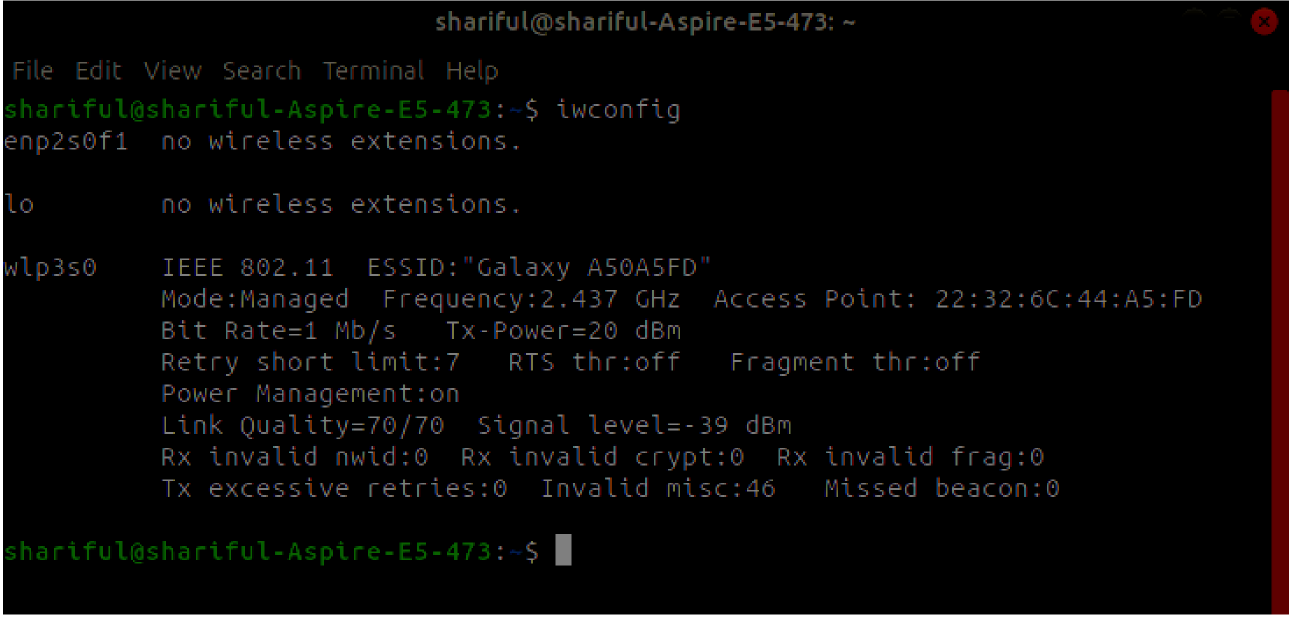
```
shariful@shariful-Aspire-E5-473:~$ hping3
hping3> 
```

ETHTOOL: The ethtool command is used to display/change Ethernet adapter settings. You can change network card speed, auto-negotiation, wake on LAN setting, duplex mode using this tool in Linux.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

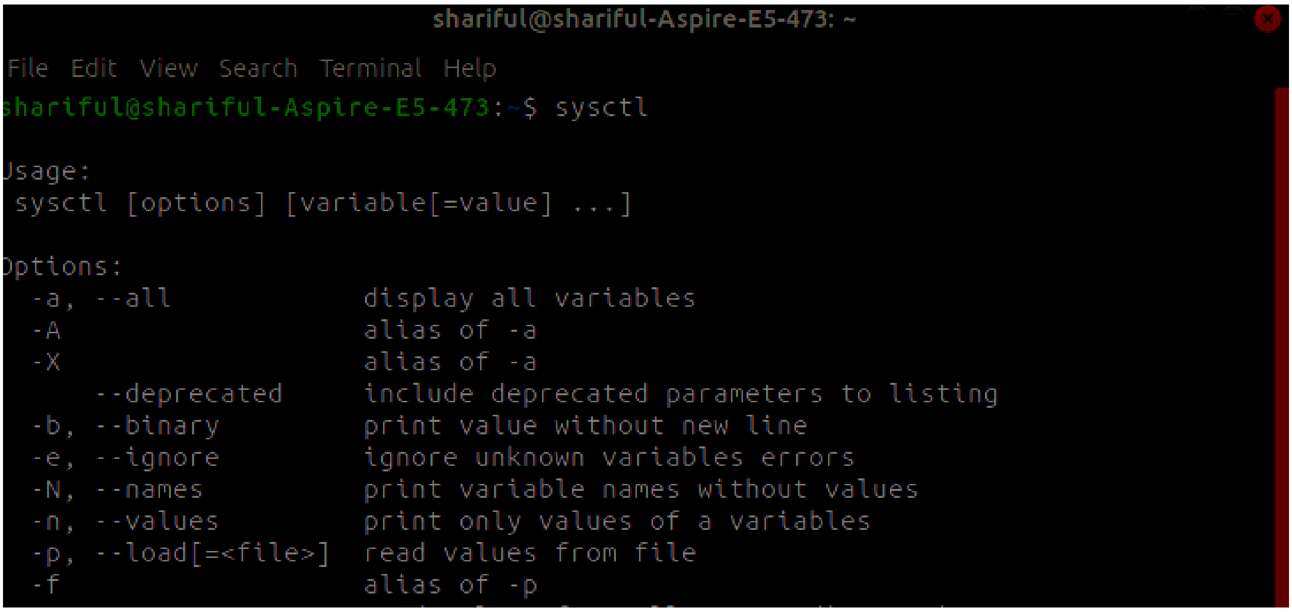
```
shariful@shariful-Aspire-E5-473:~$ ethtool -h
ethtool version 4.15
Usage:
        ethtool DEVNAME Display standard information about device
        ethtool -s|--change DEVNAME     Change generic options
                [ speed %d ]
                [ duplex half|full ]
                [ port tp|aui|bnc|mii|fibre ]
                [ mdix auto|on|off ]
                [ autoneg on|off ]
                [ advertise %x ]
                [ phyad %d ]
                [ xcvr internal|external ]
                [ wol p|u|m|b|a|g|s|d... ]
                [ sopass %x:%x:%x:%x:%x:%x ]
                [ msglvl %d | msglvl type on|off ... ]
```

IW/IWCONFIG: iwconfig command in Linux is like ifconfig command, in the sense it works with kernel-resident network interface but it is dedicated to
wireless networking interfaces only. It is used to set the parameters of the network interface that are particular to the wireless operation like SSID, frequency etc.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

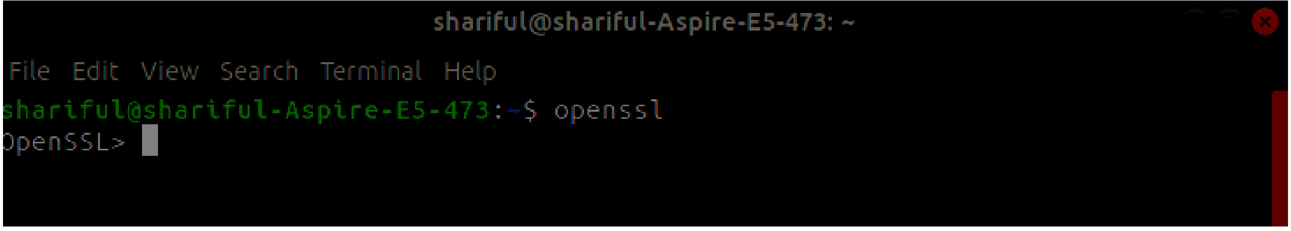
```
shariful@shariful-Aspire-E5-473:~$ iwconfig
enp2s0f1  no wireless extensions.

lo        no wireless extensions.

wlp3s0    IEEE 802.11  ESSID:"Galaxy A50A5FD"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 22:32:6C:44:A5:FD
          Bit Rate=1 Mb/s   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=70/70  Signal level=-39 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:46   Missed beacon:0

shariful@shariful-Aspire-E5-473:~$ 
```

SYSCTL: The sysctl command reads the information from the /proc/sys directory. /proc/sys is a virtual directory that contains file objects that can be
used to view and set the current kernel parameters. You can also view a parameter value by displaying the content of the appropriate file.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

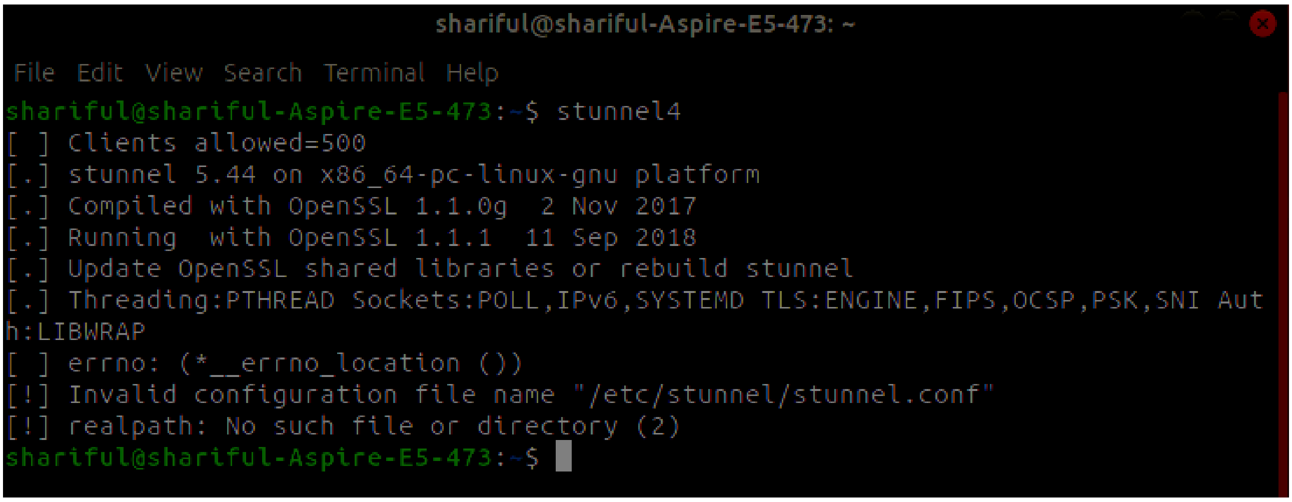
```
shariful@shariful-Aspire-E5-473:~$ sysctl

Usage:
 sysctl [options] [variable[=value] ...]

Options:
  -a, --all            display all variables
  -A                   alias of -a
  -X                   alias of -a
      --deprecated     include deprecated parameters to listing
  -b, --binary         print value without new line
  -e, --ignore         ignore unknown variables errors
  -N, --names          print variable names without values
  -n, --values         print only values of a variables
  -p, --load[=<file>]  read values from file
  -f                   alias of -p
```

OPENSSL: OpenSSL is a versatile command line tool that can be used for a large variety of tasks ... This includes OpenSSL examples of generating private keys, certificate signing requests, and certificate format conversion.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ openssl
OpenSSL>
```

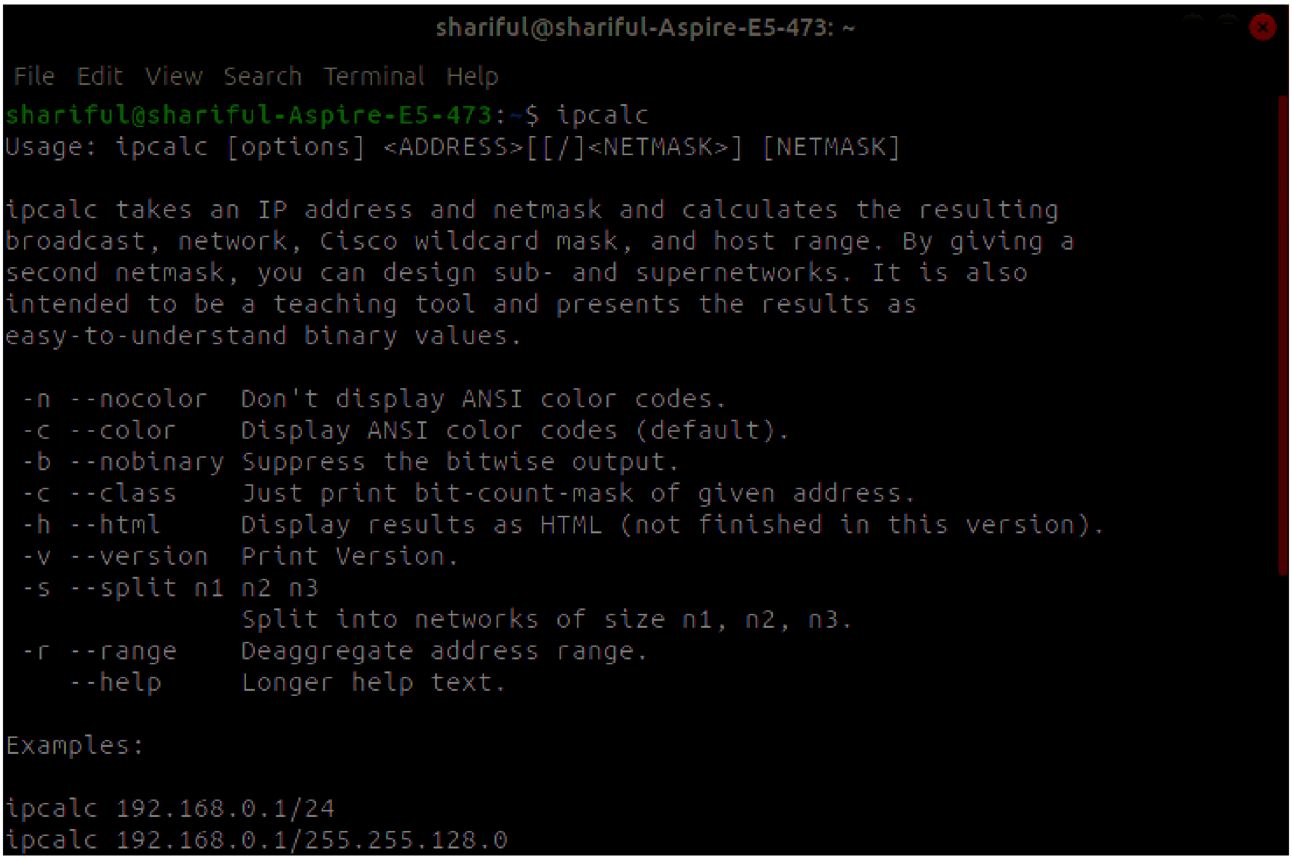
STUNNEL: Stunnel is an open-source multi-platform application used to provide a universal TLS/SSL tunneling service. Stunnel can be used to provide secure encrypted connections for clients or servers that do not speak TLS or SSL natively.



shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ stunnel4
[ ] Clients allowed=500
[.] stunnel 5.44 on x86_64-pc-linux-gnu platform
[.] Compiled with OpenSSL 1.1.0g  2 Nov 2017
[.] Running  with OpenSSL 1.1.1  11 Sep 2018
[.] Update OpenSSL shared libraries or rebuild stunnel
[.] Threading:PTHREAD Sockets:POLL,IPv6,SYSTEMD TLS:ENGINE,FIPS,OCSP,PSK,SNI Aut
h:LIBWRAP
[ ] errno: (*__errno_location ())
[!] Invalid configuration file name "/etc/stunnel/stunnel.conf"
[!] realpath: No such file or directory (2)
shariful@shariful-Aspire-E5-473:~$ 
```

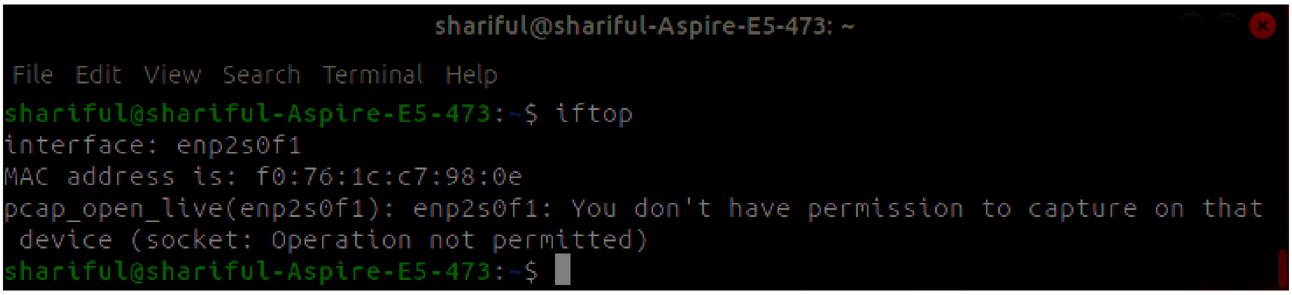
IPCALC:The ifcalc command listens to
network traffic on a named network interface, or on the first interface, it can
find which looks like an external interface if none is specified, and displays a
table of current bandwidth usage by pairs of hosts. The iftop is a perfect tool for
remote Linux server over an ssh based session



shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ ipcalc
Usage: ipcalc [options] <ADDRESS>[[/]<NETMASK>] [NETMASK]

ipcalc takes an IP address and netmask and calculates the resulting
broadcast, network, Cisco wildcard mask, and host range. By giving a
second netmask, you can design sub- and supernetworks. It is also
intended to be a teaching tool and presents the results as
easy-to-understand binary values.

 -n --nocolor  Don't display ANSI color codes.
 -c --color    Display ANSI color codes (default).
 -b --nobinary Suppress the bitwise output.
 -c --class    Just print bit-count-mask of given address.
 -h --html     Display results as HTML (not finished in this version).
 -v --version  Print Version.
 -s --split n1 n2 n3
               Split into networks of size n1, n2, n3.
 -r --range    Deaggregate address range.
    --help     Longer help text.

Examples:

ipcalc 192.168.0.1/24
ipcalc 192.168.0.1/255.255.128.0
```

IPTRAF/NETHOGS/IFTOP/NTOP: The iftop command listens to network traffic on a named network interface, or on the first interface, it can find which looks like an external interface if none is specified, and displays a table of current bandwidth usage by pairs of hosts. The iftop is a perfect tool for remote Linux server over an ssh based session.


shariful@shariful-Aspire-E5-473: ~
File Edit View Search Terminal Help

```
shariful@shariful-Aspire-E5-473:~$ iftop
interface: enp2s0f1
MAC address is: f0:76:1c:c7:98:0e
pcap_open_live(enp2s0f1): enp2s0f1: You don't have permission to capture on that
 device (socket: Operation not permitted)
shariful@shariful-Aspire-E5-473:~$
```