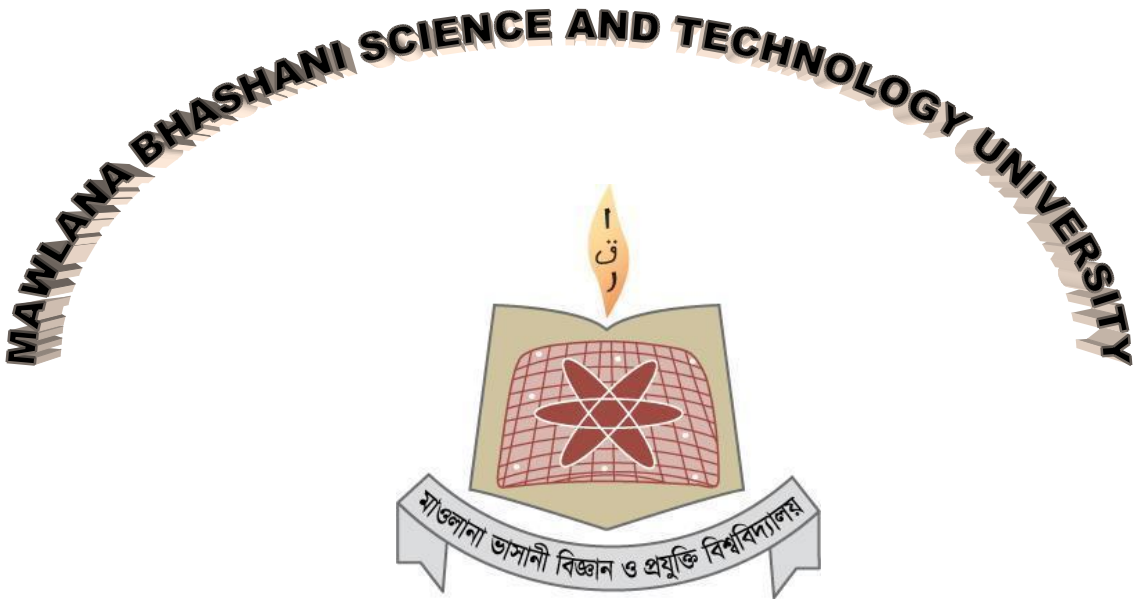


Assignment

Assignment Name: LINUX commands.

Course code: ICT-3208

Course title: Computer Network Lab

Date of Performance: 09/11/2020

Date of Submission: 19/11/2020

SUBMITTED BY

Name: Shakhera khanom

ID: IT-18033

3rd year 2nd semester

Session: 2017-18

Department of ICT,

MBSTU.

SUBMITTED TO

Nazrul Islam

Assistant Professor

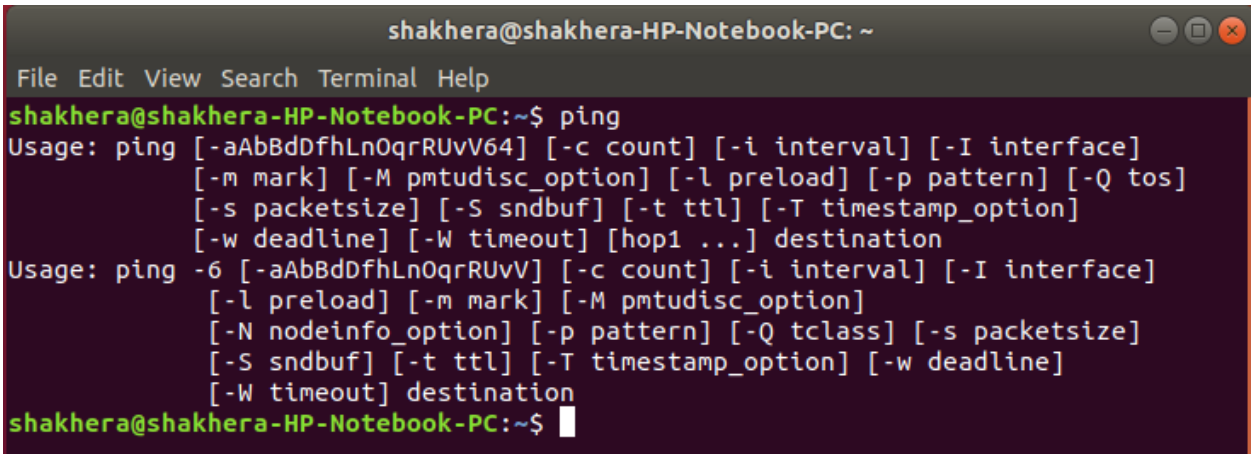
Department of ICT,

MBSTU.

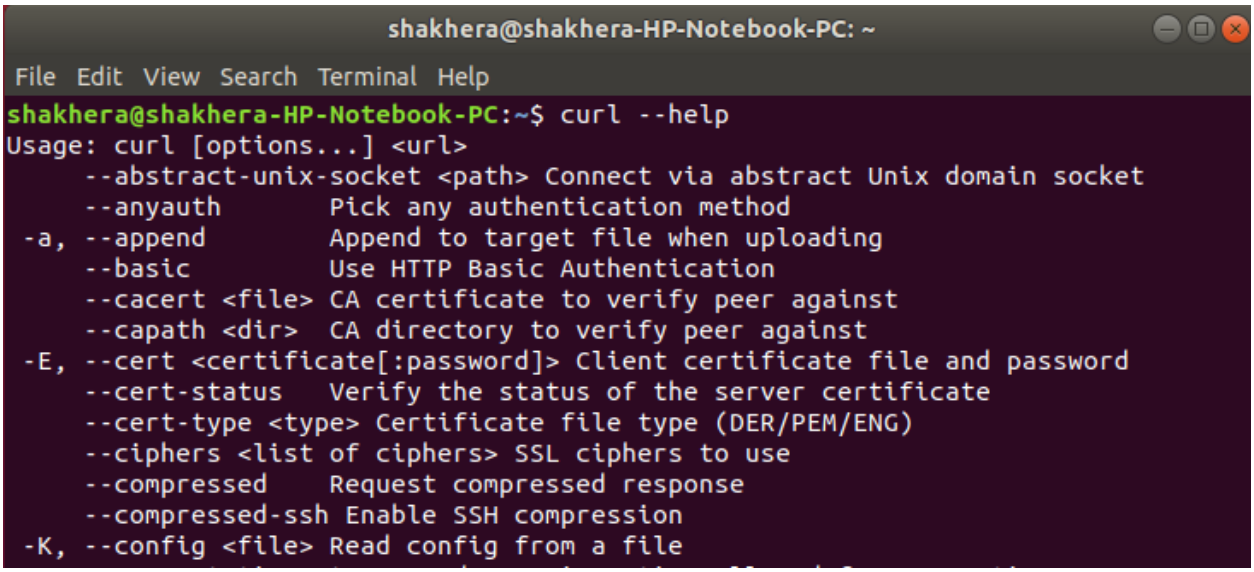
Assignment No: 01

Assignment Name: LINUX commands.

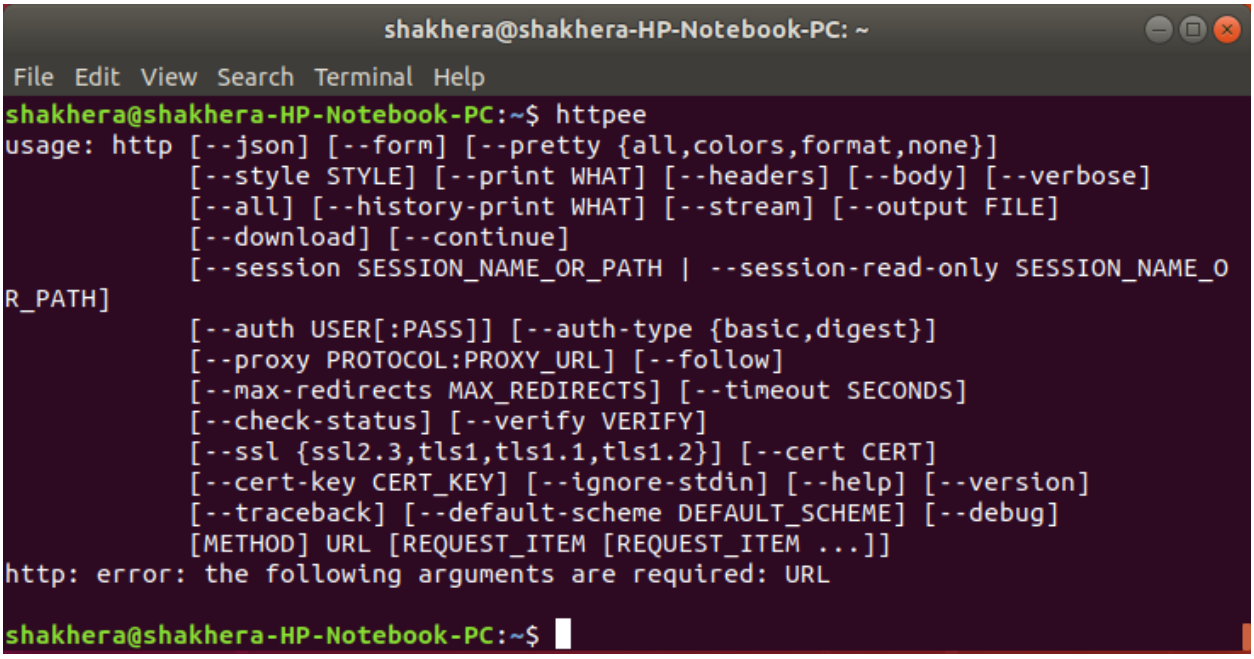
PING: Linux "*ping*" command stands for (Packet Internet Groper). It checks connectivity between two nodes to see if a server is available. It sends ICMP ECHO_REQUEST packets to network hosts and displays the data on the remote server's response. It checks if a remote host is up, or that network interfaces can be reached. Further, it is used to check if a network connection is available between two devices. It is also handy tool for checking your network connection and verifying network issues.



CURL: Linux "*curl*" command is used to download or upload data to a server via supported protocols such as HTTP, FTP, IMAP, SFTP, TFTP, IMAP, POP3, SCP, etc. It is a remote utility, so it works without user interaction.

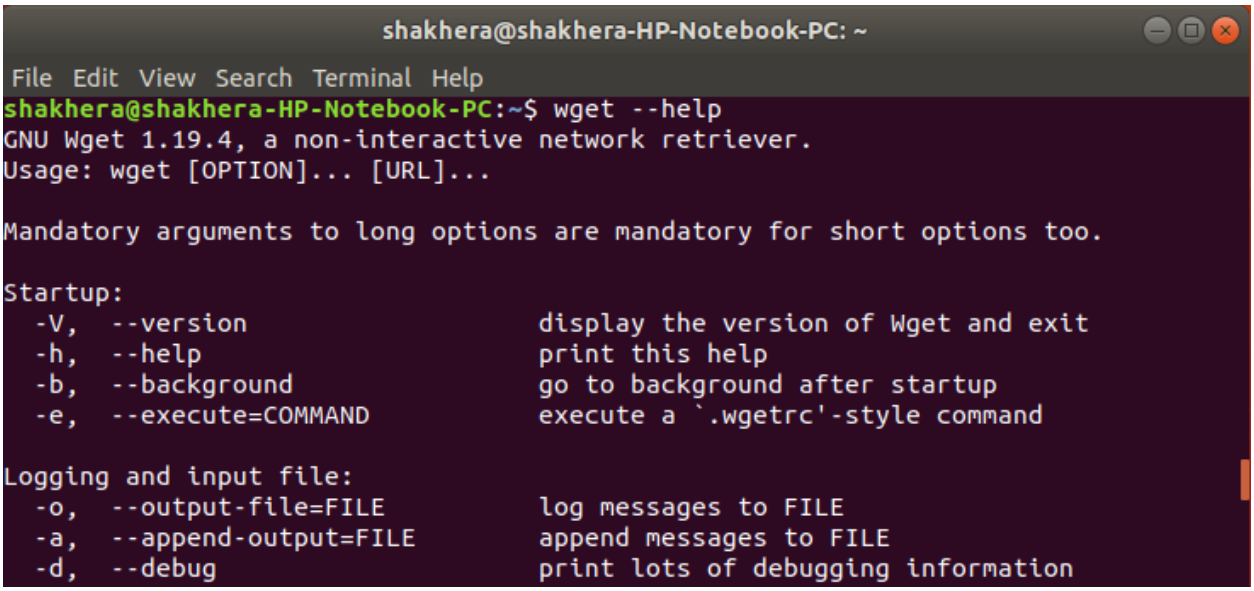


HTTPIE: Linux *"httpie"* aitch-tee-tee-pie is a user friendly command-line http client for the api era. It comes with JSON support, system highlighting, persisten sessions, wget-line downloads, plugins, and more.

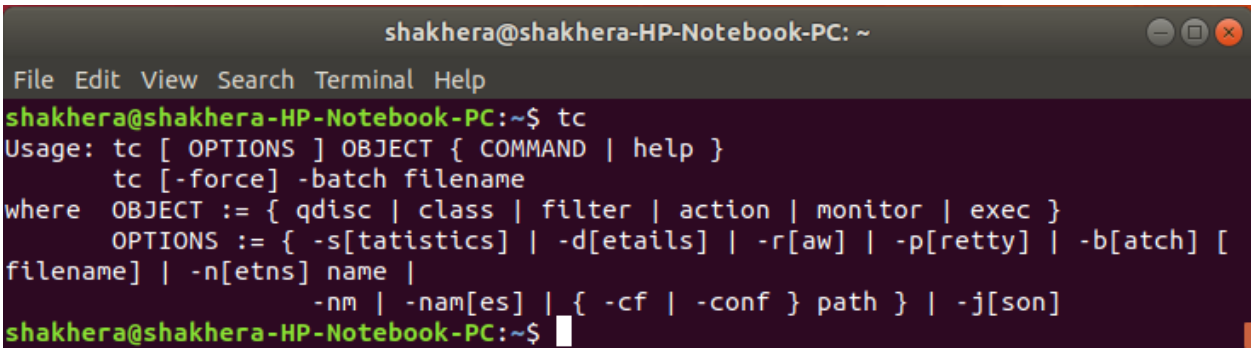


WGET: Linux command *wget* stands for web get**.** The *wget* is a free non-interactive file downloader command. Non-interactive means it can work in background when user is not logged in. This allows user to get disconnected with the system while *wget* finish its work. It can even download entire website as a

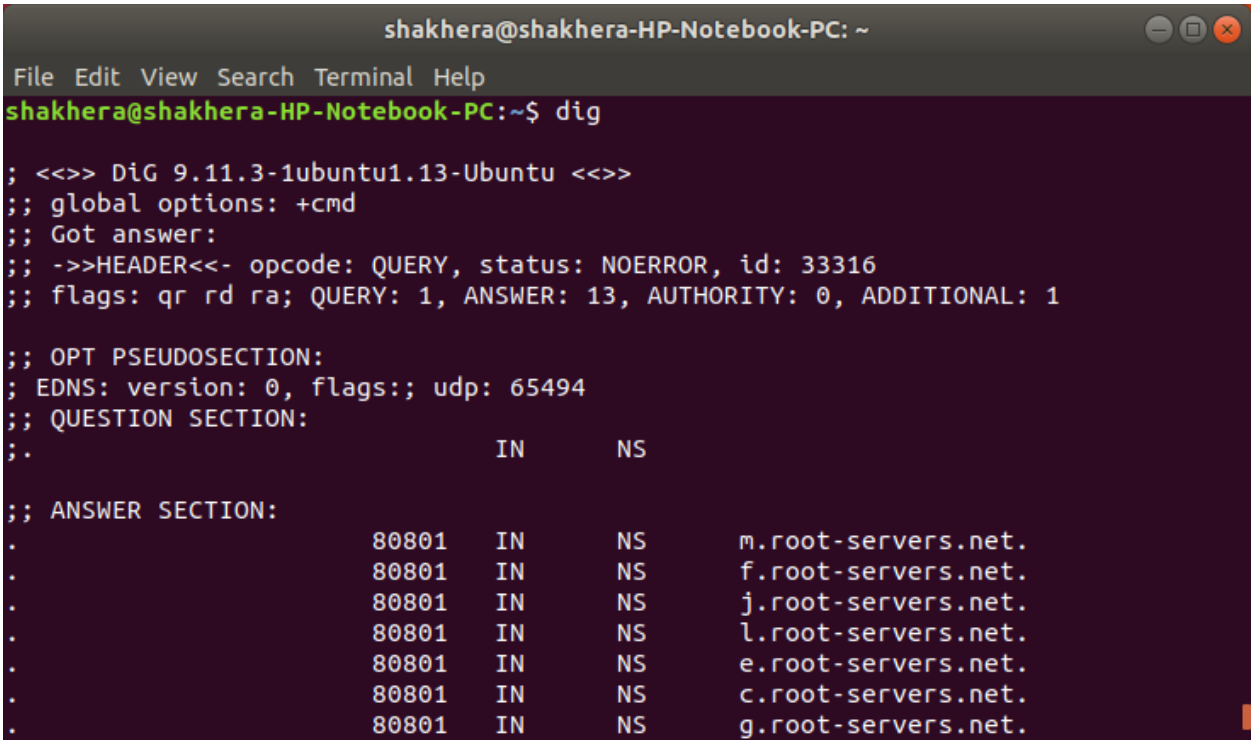
local version of remote websites, fully recreating the structure of original website. In short, you can mirror an entire website with *wget.*



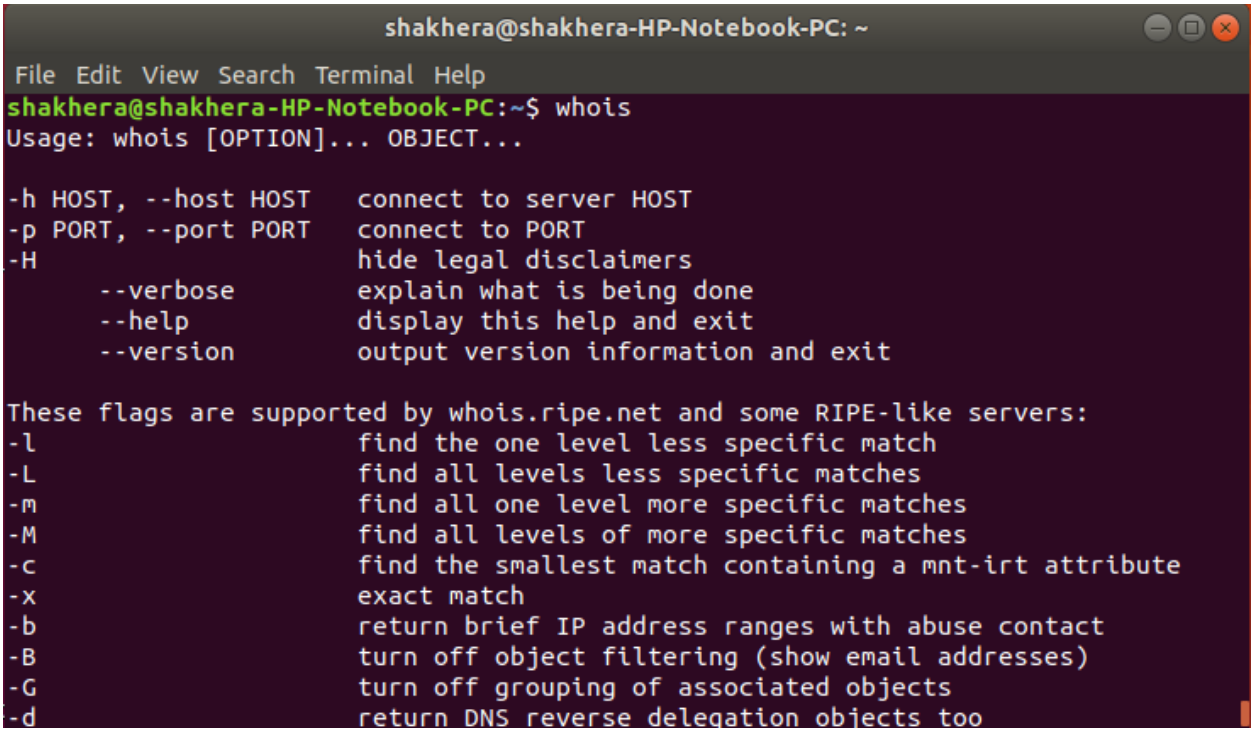
TC: Linux **"***tc"* (traffic control) is the user-space utility program used to configure the Linux kernel packet scheduler.



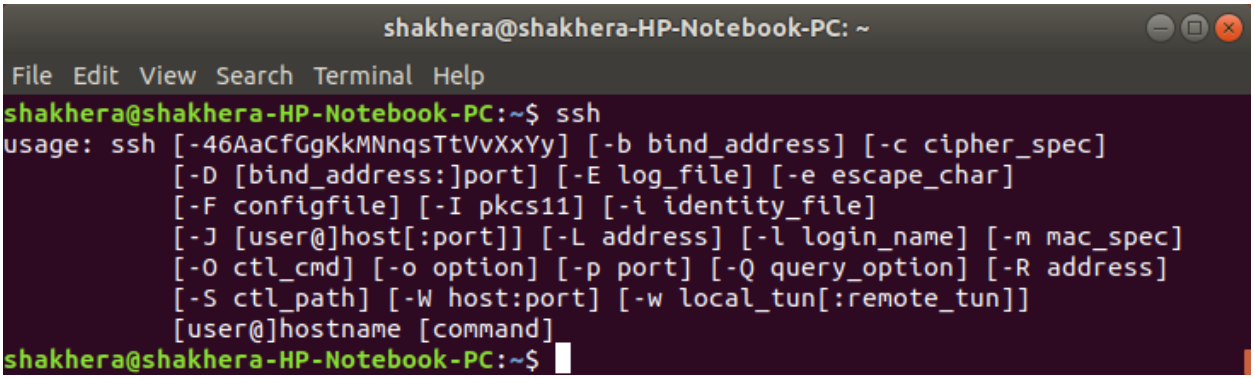
DIG/NSLOOKUP: Linux *"dig"* command stands for Domain Information Groper. This command is used for tasks related to DNS lookup to query DNS name servers.



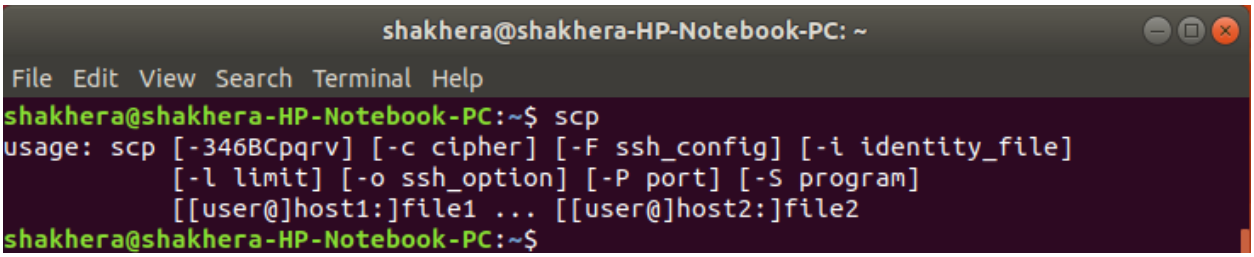
WHOIS: Linux *"whois"* command displays information about a website's record. You may get all the information about a website regarding its registration and owner's information.



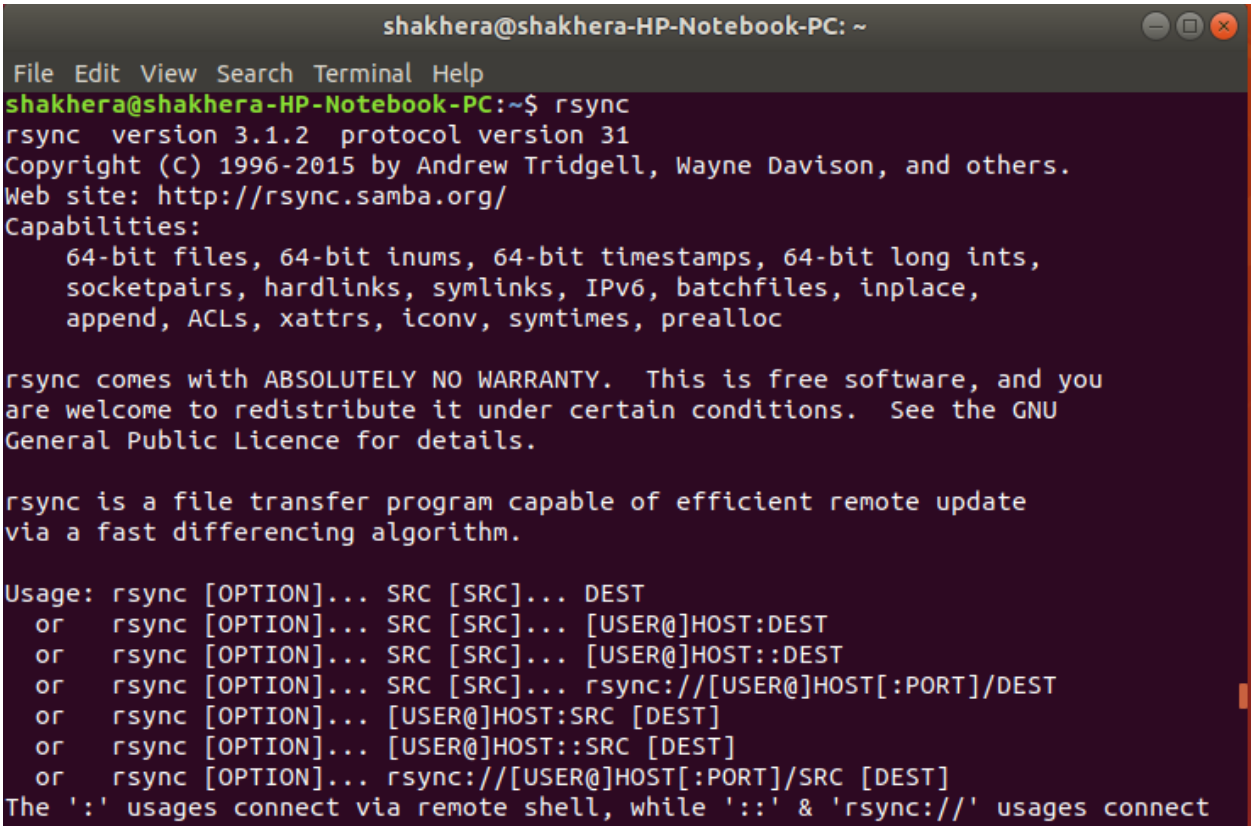
SSH: Linux **"***ssh"* (Secure SHell) command is a Network protocol used for communication between two networked computer. It is different from other protocols in way that it provide security while accessing other system. Hence anyone on network will see only encrypted data and not the plain data.



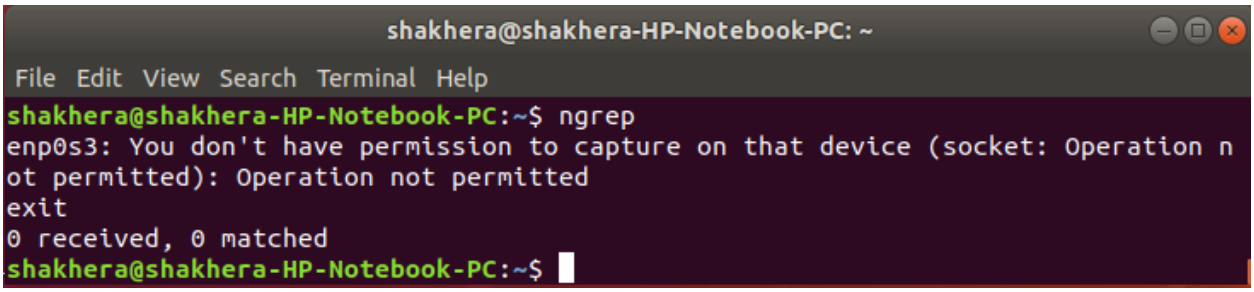
SCP: Linux **"***scp"* (secure copy) command in Linux system is used to copy file(s) between servers in a secure way. The SCP command or secure copy allows secure transferring of files in between the local host and the remote host or between two remote hosts. It uses the same authentication and security as it is used in the Secure Shell (SSH) protocol. SCP is known for its simplicity, security and pre-installed availability.



RSYNC: The **"***rsync"* or remote synchronization is a software utility for Unix-Like systems that efficiently sync files and directories between two hosts or machines. One of them being the source or the local-host from which the files will be synced, the other one being the remote-host, on which synchronization will take place.

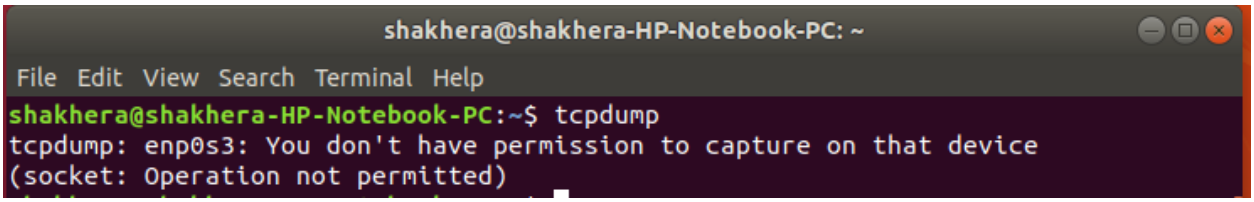


NGREP: The **"***ngrep"* strives to provide most of GNU grep's common features, applying them to the network layer. *ngrep* is a pcap-aware tool that will allow you to specify extended regular expressions to match against data payloads of packets.

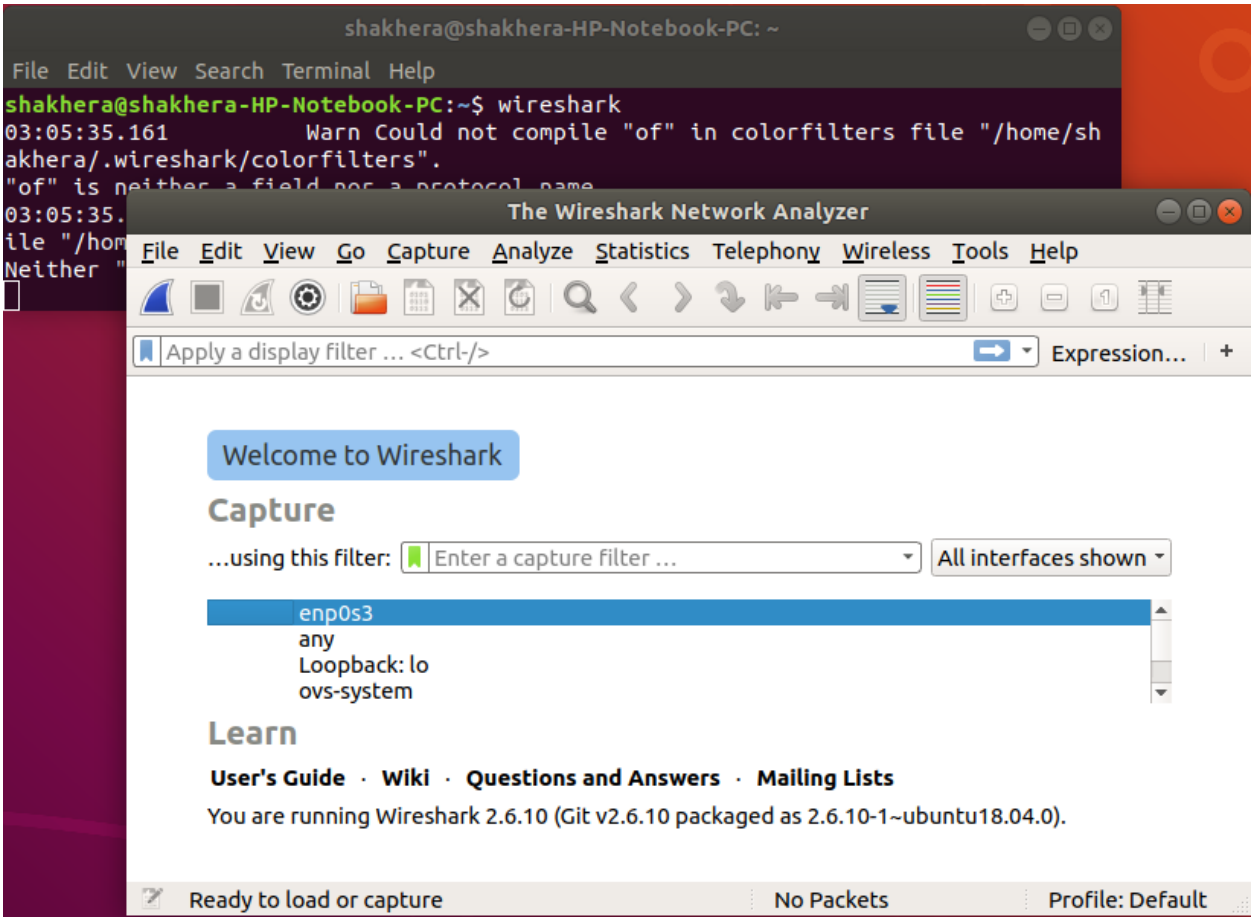


TCPDUMP: The **"***tcpdump"* is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux. It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system. It is many times used as a security tool as well. It saves the captured

information in a pcap file, these pcap files can then be opened through Wireshark or through the command tool itself.

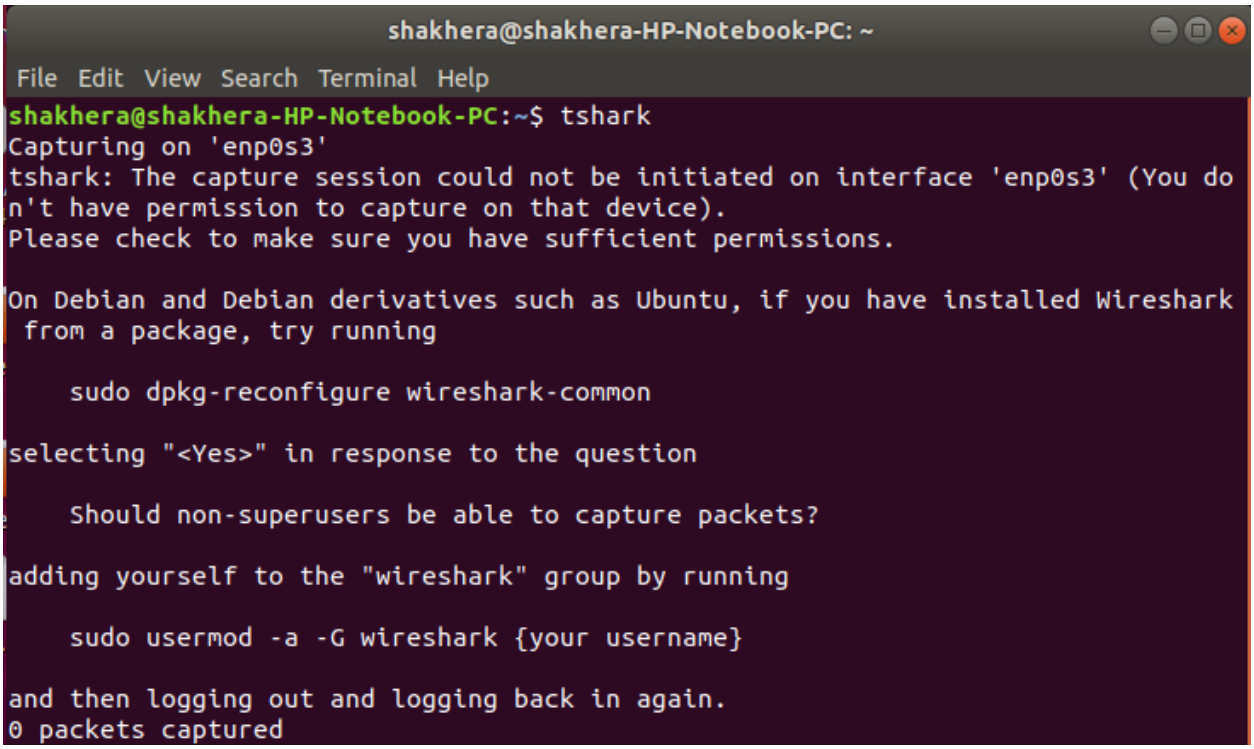


WIRESHARK: Linux **"***wireshark"* command is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting**.**

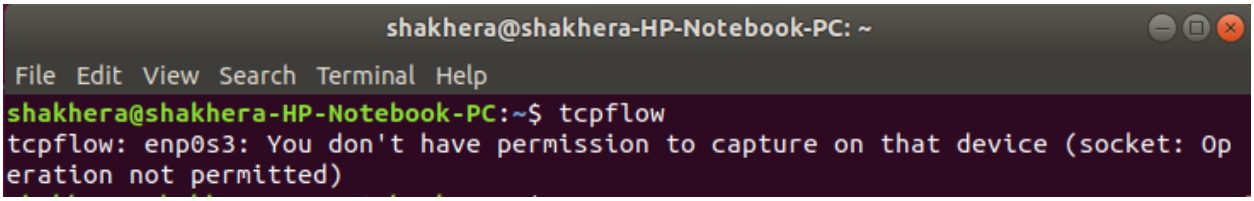


TSHARK: Linux **"***tshark"* is the command-line version of wireshark. It provide many useful commands and capture filters that can be used on terminal which

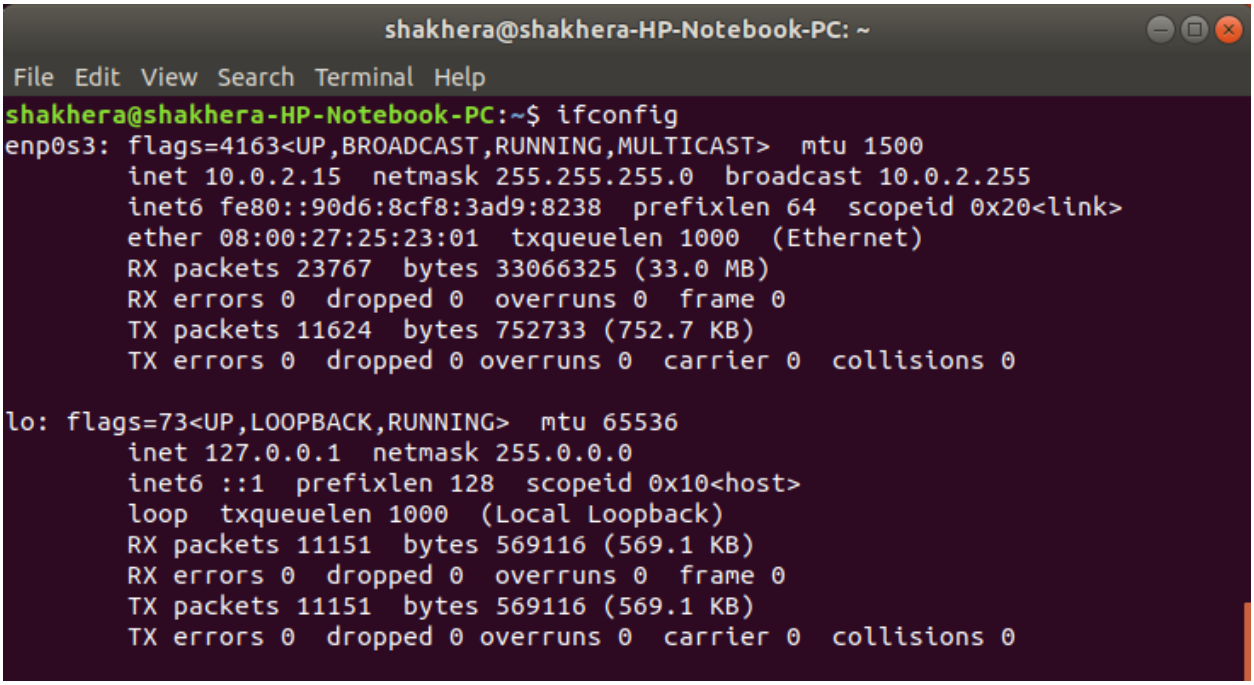
provides an efficient way to analyses the incoming traffic and capture the traffic in pcap. Let me give you a brief about the terminology we use in *tshark*.



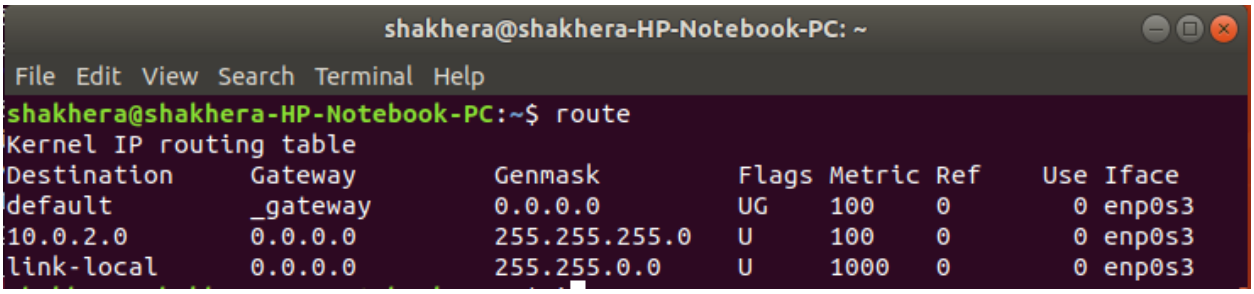
TCPFLOW: The "*tcpflow*" is a free, open source, powerful command line based tool for analyzing network traffic on Unix-like systems such as Linux. It captures data received or transferred over TCP connections, and stores it in a file for later analysis, in a useful format that allows for protocol analysis and debugging.



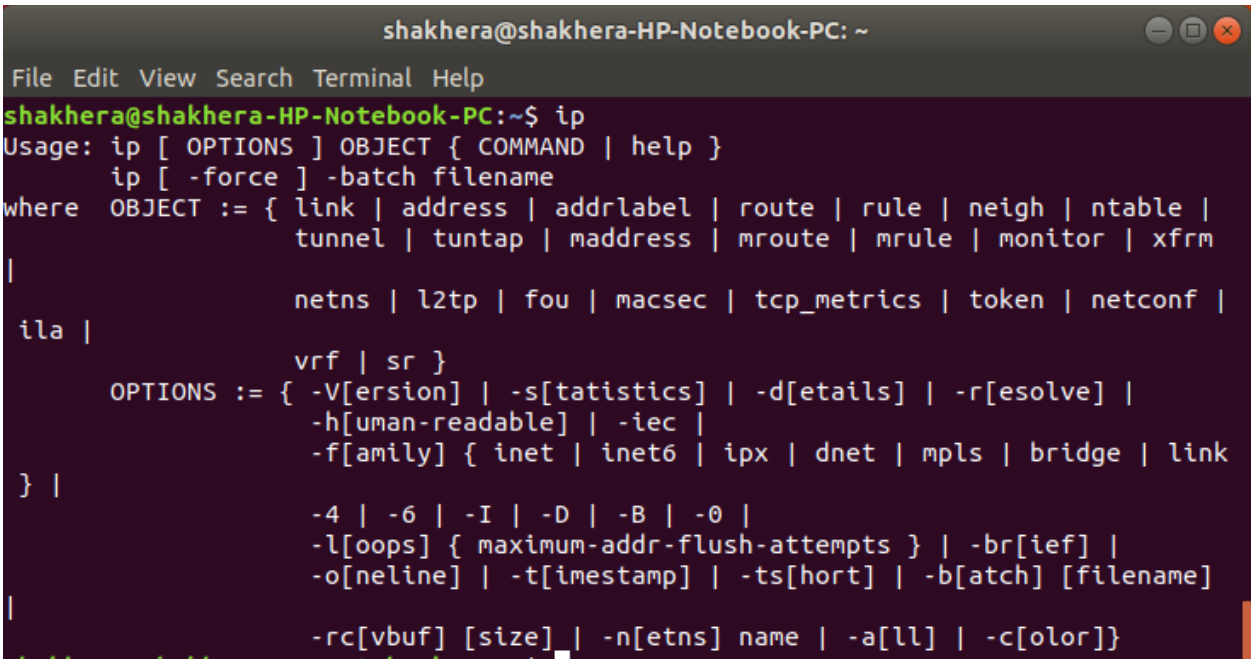
IFCONFIG: Linux "*ifconfig*" command is used for displaying current network configuration information, setting up an ip address, netmask or broadcast address to an network interface, creating an alias for network interface, setting up hardware address and enable or disable network interfaces.



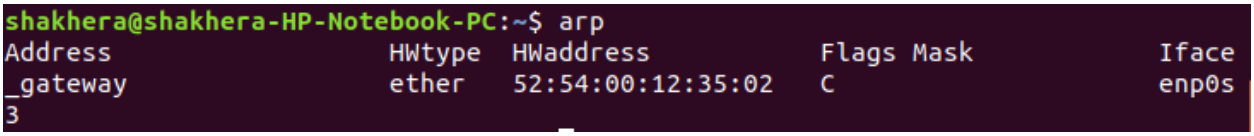
ROUTE: Linux **"***route"* command in Linux is used when you want to work with the IP/kernel routing table. It is mainly used to set up static routes to specific hosts or networks via an interface. It is used for showing or update the IP/kernel routing table



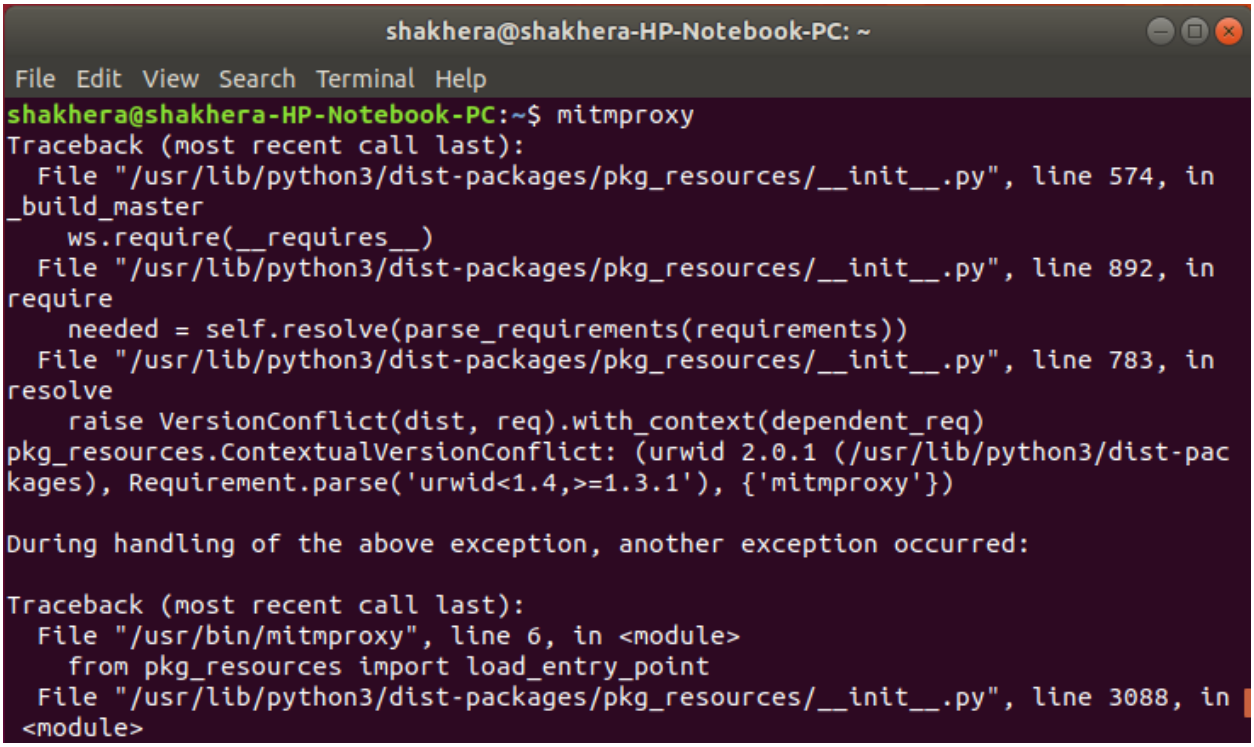
IP: Linux "*ip***"** command in Linux is present in the net-tools which is used for performing several network administration tasks. IP stands for Internet Protocol. This command is used to show or manipulate routing, devices, and tunnels.



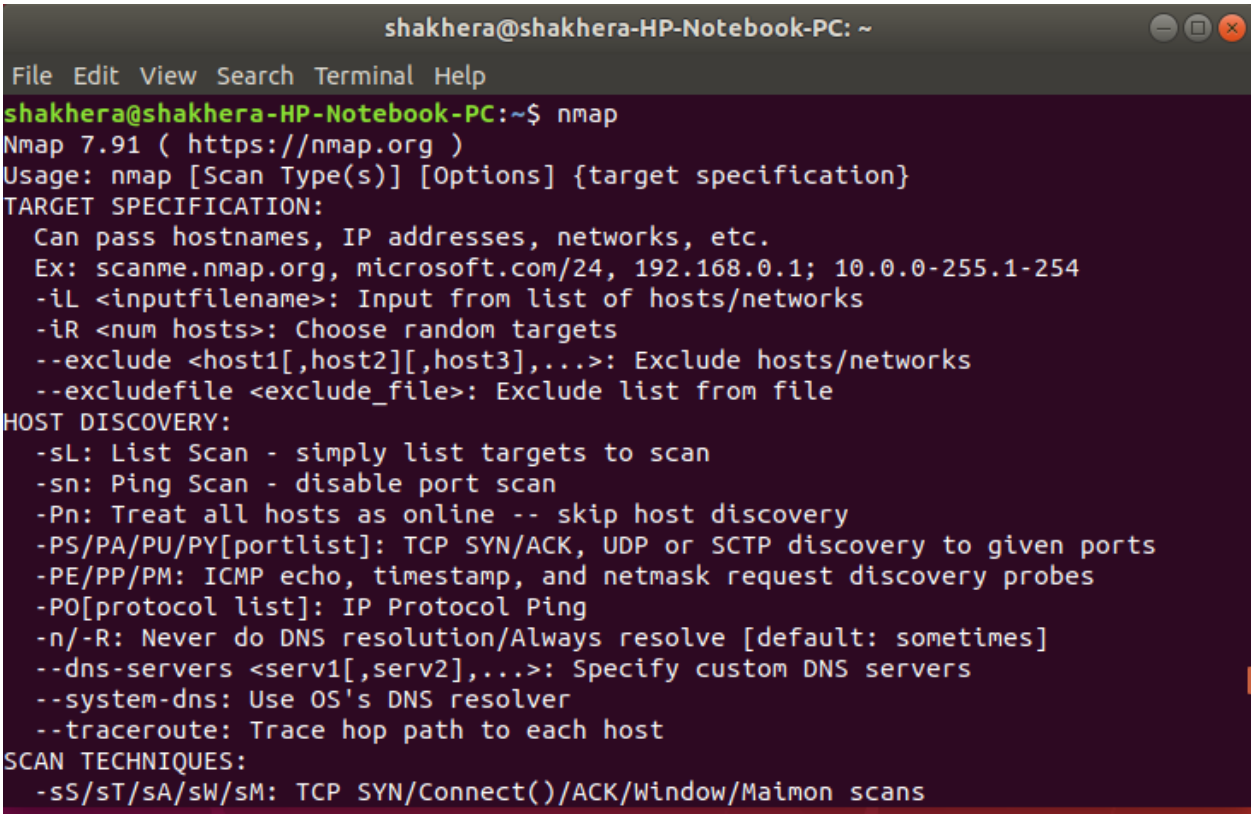
ARP: Linux *"arp"* command manipulates the System's ARP cache. It also allows a complete dump of the ARP cache. ARP stands for Address Resolution Protocol. The primary function of this protocol is to resolve the IP address of a system to its mac address, and hence it works between level 2(Data link layer)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



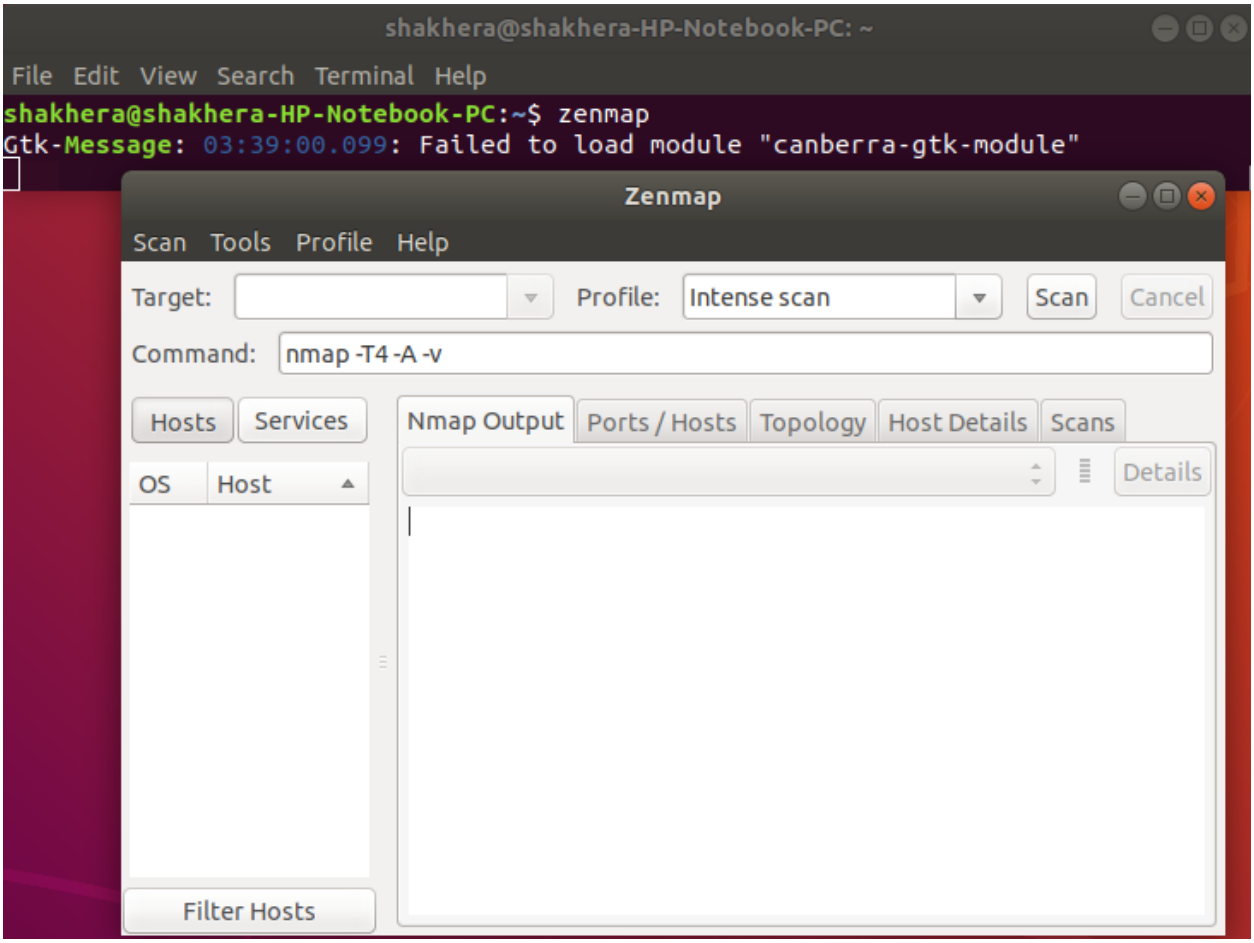
MITMPROXY: The "*mitmproxy"* is a set of tools that provide an interactive, SSL/TLS-capable intercepting proxy for HTTP/1, HTTP/2, and WebSockets.



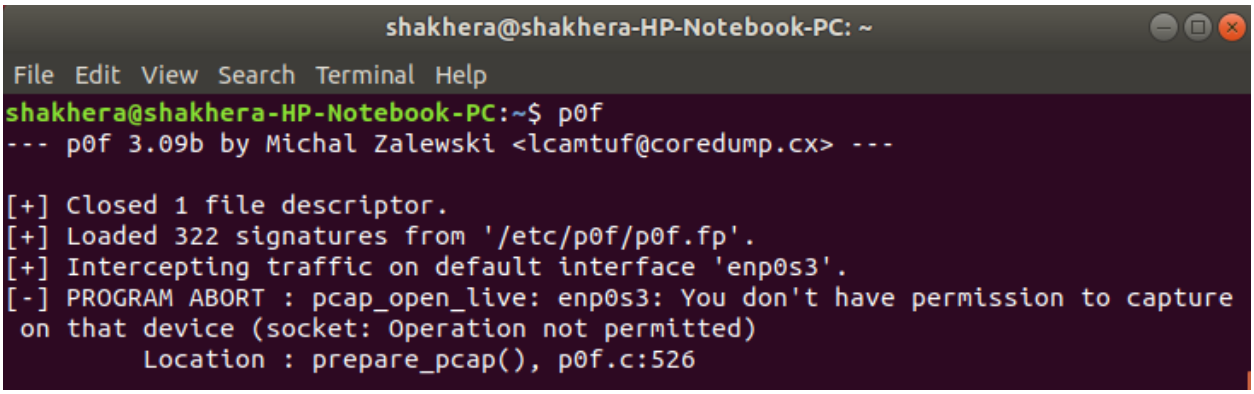
NMAP: Linux "*nmap*" is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators.



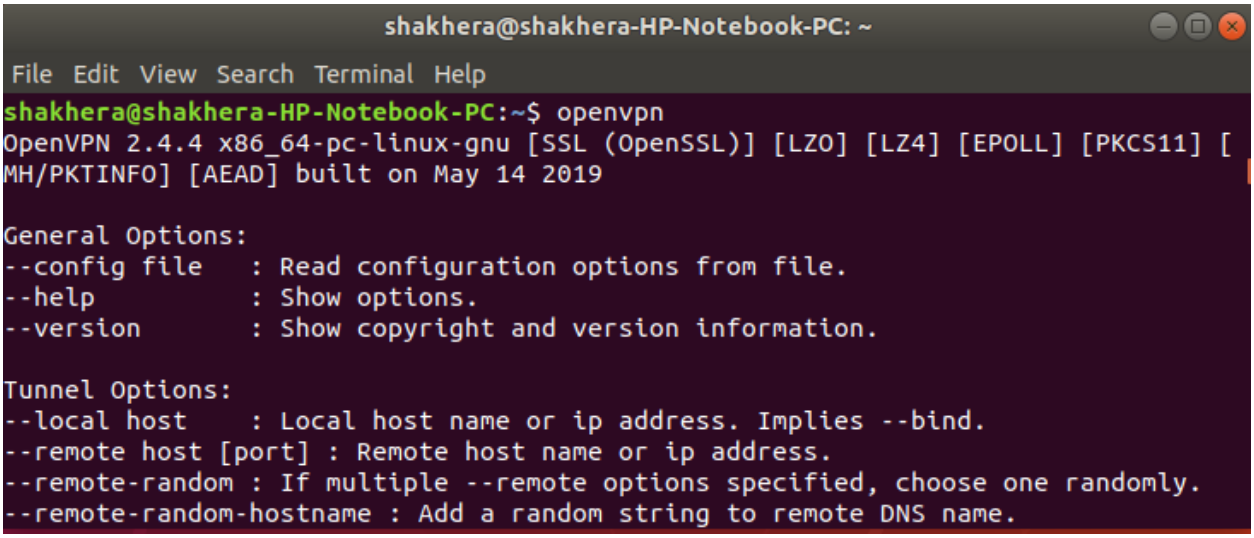
ZENMAP: Linux *"zenmap"* command is a graphical user interface developed for "nmap", a tool that we use on the command line terminal for scanning ports and networks.



P0F: The "*p0f*" is a passive TCP/IP stack fingerprinting tool. P0f can attempt to identify the system running on machines that sent 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 analyzing other aspects of the remote system.

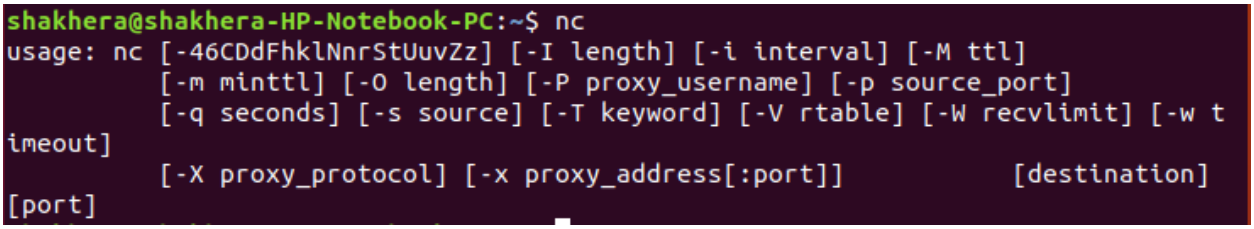


OPENVPN: Linux "*openvpn*" command is open source *openvpn* CLI program. The open source project client program can also connect to the access server

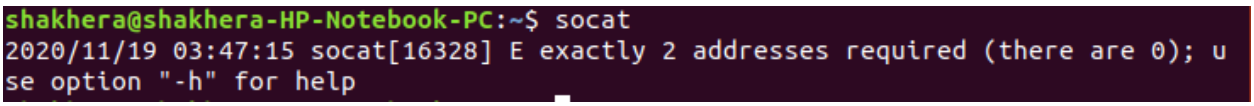


WIREGUARD:

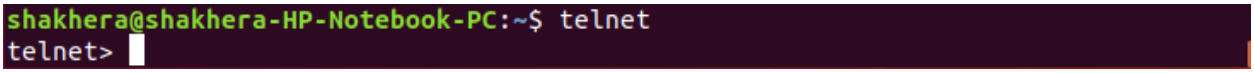
NC: Linux "*nc*" command runs netcat, a utility for sending raw data over a network connection.



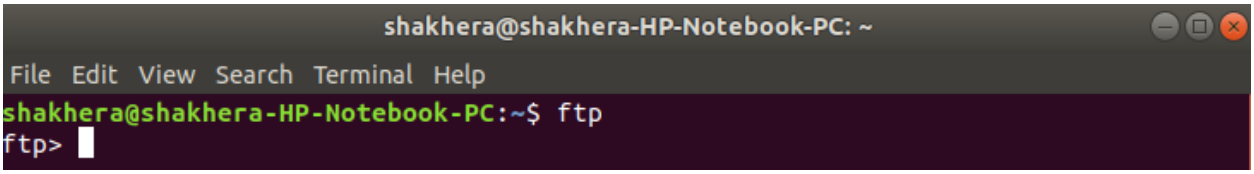
SOCAT: Linux "*socat*" is a command line based utility that establishes two bidirectional byte streams and transfers data between them.



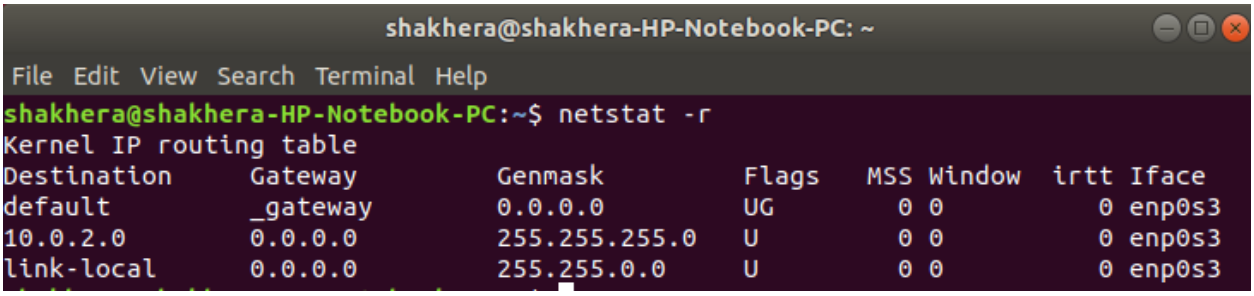
TELNET: Linux "*telnet*" command is used to create a remote connection with a system over a TCP/IP network. It allows us to administrate other systems by the terminal. We can run a program to conduct administration.



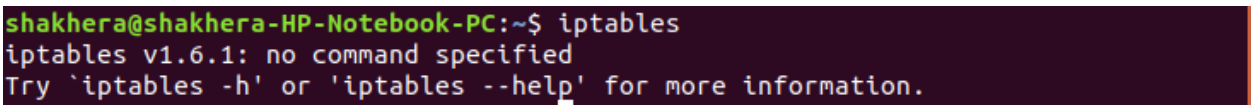
FTP/SFTP: Linux *"ftp"* command is a standard network protocol used to transfer files to and from a remote network. FTP client to connect to the remote server and download or upload files.



NETSTAT/SS/LSOF/FUSER: Linux **"***netstat*" command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.

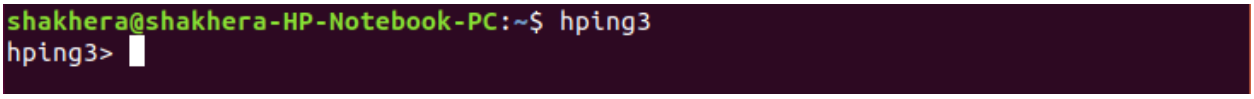


IPTABLES: Linux **"***iptables"* is a command line interface used to set up and maintain tables for the Netfilter firewall for IPv4, included in the Linux kernel. The firewall matches packets with rules defined in these tables and then takes the specified action on a possible match.



NFTABLES:

HPING3: Linux **"***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.



TRACEROUTE/MTR: Linux "traceroute" command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes.

```
shakhera@shakhera-HP-Notebook-PC:~$ traceroute --help
Usage: traceroute [OPTION...] HOST
Print the route packets trace to network host.

  -f, --first-hop=NUM        set initial hop distance, i.e., time-to-live
  -g, --gateways=GATES       list of gateways for loose source routing
  -I, --icmp                 use ICMP ECHO as probe
  -m, --max-hop=NUM          set maximal hop count (default: 64)
  -M, --type=METHOD          use METHOD (`icmp' or `udp') for traceroute
                             operations, defaulting to `udp'
  -p, --port=PORT            use destination PORT port (default: 33434)
  -q, --tries=NUM            send NUM probe packets per hop (default: 3)
      --resolve-hostnames    resolve hostnames
  -t, --tos=NUM              set type of service (TOS) to NUM
  -w, --wait=NUM             wait NUM seconds for response (default: 3)
  -?, --help                 give this help list
      --usage                give a short usage message
  -V, --version              print program version

Mandatory or optional arguments to long options are also mandatory or optional
for any corresponding short options.
```

ETHTOOL: Linux "*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.

```
shakhera@shakhera-HP-Notebook-PC:~$ ethtool
ethtool: bad command line argument(s)
For more information run ethtool -h
```

IW/IWCONFIG: Linux *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. *iwconfig* may also be used to display the parameters, and the wireless statistics which are extracted from */proc/net/wireless*.

```
shakhera@shakhera-HP-Notebook-PC:~$ iwconfig
enp0s3    no wireless extensions.

lo        no wireless extensions.

s1        no wireless extensions.

ovs-system  no wireless extensions.
```

SYSCTL: Linux *"sysctl"* command is used to modify kernel parameters at runtime. The parameters available are those listed under /proc/sys/.

```
shakhera@shakhera-HP-Notebook-PC:~$ 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
      --system         read values from all system directories
  -r, --pattern <expression>
```

OPENSSL: The *"openssl"* is a cryptography software library or toolkit that makes communication over computer networks more secure. The *openssl* program is a command-line tool for using the various cryptography functions of *openssl*'s crypto library from the shell. It is generally used for Transport Layer Security(TSL) or Secure Socket Layer(SSL) protocols.

```
shakhera@shakhera-HP-Notebook-PC:~$ openssl
OpenSSL> quit
shakhera@shakhera-HP-Notebook-PC:~$
```

STUNNEL: The "*stunnel"* program is designed to work as *SSL* encryption wrapper between remote clients and local (*inetd*-startable) or remote servers. The concept is that having non-SSL aware daemons running on your system you can easily set them up to communicate with clients over secure SSL channels.

```
shakhera@shakhera-HP-Notebook-PC:~$ stunnel
[ ] 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)
```

IPTRAF/NETHOGS/IFTOP/NTOP: Linux **"***iftop"* command is a network analyzing tool used by system administrators to view the bandwidth related stats. It shows a quick overview of the networking activities on an interface. It stands from Interface TOP and the top is derived from op command in Linux. It even acts as a diagnostics to diagnose which program is causing the problem to the network.

```
shakhera@shakhera-HP-Notebook-PC:~$ iftop
interface: enp0s3
IP address is: 10.0.2.15
MAC address is: 08:00:27:25:23:01
pcap_open_live(enp0s3): enp0s3: You don't have permission to capture on that dev
ice (socket: Operation not permitted)
```

AB/NLOAD/IPERF: Linux **"***nload"* is a Linux command-line tool used to monitor network traffic and bandwidth usage in real time, using insightful graphs and traffic statistics.

```
shakhera@shakhera-HP-Notebook-PC: ~
File  Edit  View  Search  Terminal  Help
Device enp0s3 [10.0.2.15] (1/4):
================================================================================
Incoming:


                                                  Curr: 0.00 Bit/s
                                                  Avg: 48.00 Bit/s
                                                  Min: 0.00 Bit/s
                                                  Max: 888.00 Bit/s
                                                  Ttl: 54.12 MByte
Outgoing:


                                                  Curr: 0.00 Bit/s
                                                  Avg: 176.00 Bit/s
                                                  Min: 0.00 Bit/s
                                                  Max: 1.98 kBit/s
                                                  Ttl: 1.27 MByte
```

PYTHON-M:

```
shakhera@shakhera-HP-Notebook-PC:~$ python3m
Python 3.6.9 (default, Jul 17 2020, 12:50:27)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

IPCALC: The *"ipcalc"* provides a simple way to calculate IP information for a host. The various options specify what information *ipcalc* should display on standard out. Multiple options may be specified. An IP address to operate on must always be specified. Most operations also require a netmask or a CIDR prefix as well.

```
shakhera@shakhera-HP-Notebook-PC:~$ 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.
```

NSENTER: The "*nsenter"* command executes program in the namespace(s) that are specified in the command-line options.

```
shakhera@shakhera-HP-Notebook-PC:~$ nsenter
shakhera@shakhera-HP-Notebook-PC:~$
```

Discussion: Every computer in connected to some other computer through a network whether internally or externally to exchange some information. This network can be small as some computers connected in your home or office, or can be large or complicated as in large University or the entire Internet. Maintaining a system's network we use some task. This task include configuration and troubleshooting commands, that some command run above.So, we can say that, from assignment, we learn about Linux Networking commands.