

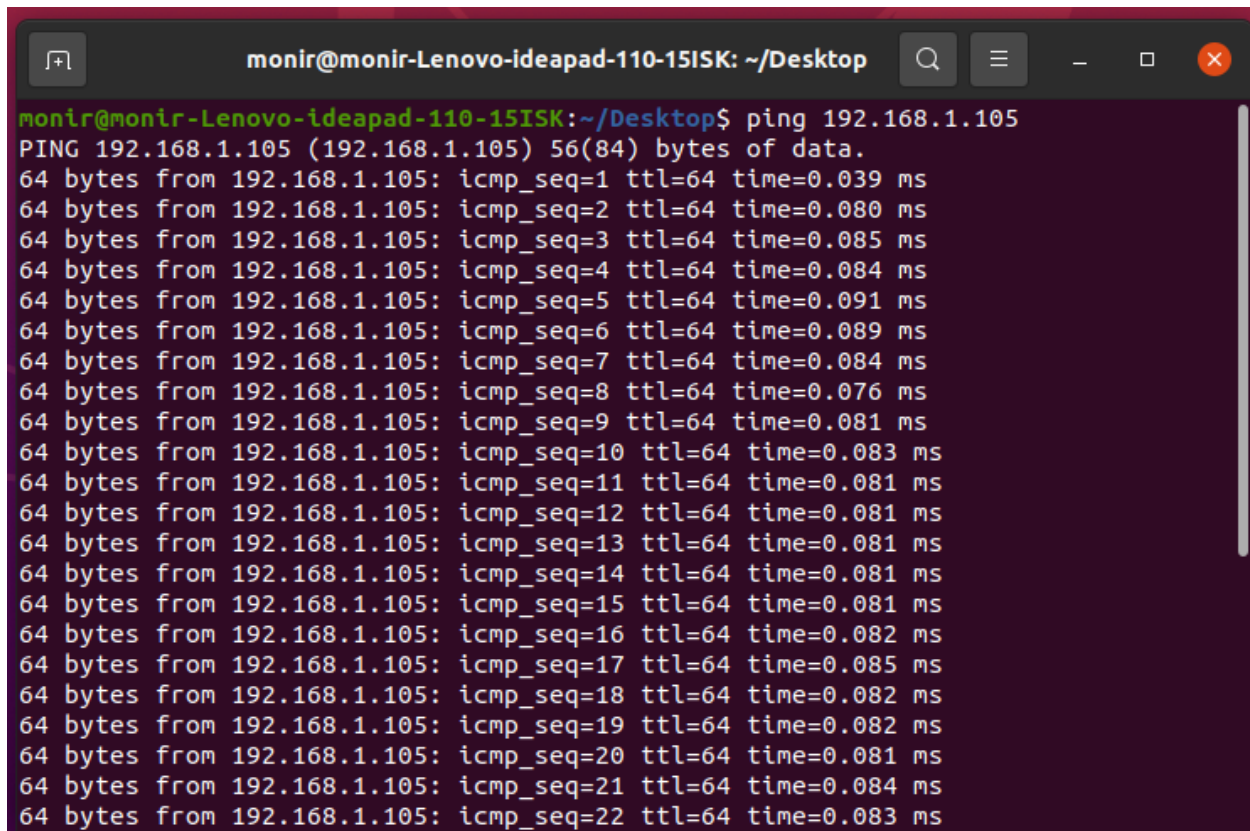
Name : Moniruzzaman

ID : IT-18007

Assignment No : 01

Assignment Name : Linux Commands

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.

A screenshot of a Linux terminal window. The window title is 'monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop'. The prompt is 'monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop\$'. The command entered is 'ping 192.168.1.105'. The output shows a successful ping to 192.168.1.105 with 56(84) bytes of data. It lists 22 successful responses, each showing '64 bytes from 192.168.1.105: icmp_seq=X ttl=64 time=Y ms' where X ranges from 1 to 22 and Y ranges from 0.039 to 0.085 ms.

```
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ ping 192.168.1.105
PING 192.168.1.105 (192.168.1.105) 56(84) bytes of data:
64 bytes from 192.168.1.105: icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from 192.168.1.105: icmp_seq=2 ttl=64 time=0.080 ms
64 bytes from 192.168.1.105: icmp_seq=3 ttl=64 time=0.085 ms
64 bytes from 192.168.1.105: icmp_seq=4 ttl=64 time=0.084 ms
64 bytes from 192.168.1.105: icmp_seq=5 ttl=64 time=0.091 ms
64 bytes from 192.168.1.105: icmp_seq=6 ttl=64 time=0.089 ms
64 bytes from 192.168.1.105: icmp_seq=7 ttl=64 time=0.084 ms
64 bytes from 192.168.1.105: icmp_seq=8 ttl=64 time=0.076 ms
64 bytes from 192.168.1.105: icmp_seq=9 ttl=64 time=0.081 ms
64 bytes from 192.168.1.105: icmp_seq=10 ttl=64 time=0.083 ms
64 bytes from 192.168.1.105: icmp_seq=11 ttl=64 time=0.081 ms
64 bytes from 192.168.1.105: icmp_seq=12 ttl=64 time=0.081 ms
64 bytes from 192.168.1.105: icmp_seq=13 ttl=64 time=0.081 ms
64 bytes from 192.168.1.105: icmp_seq=14 ttl=64 time=0.081 ms
64 bytes from 192.168.1.105: icmp_seq=15 ttl=64 time=0.081 ms
64 bytes from 192.168.1.105: icmp_seq=16 ttl=64 time=0.082 ms
64 bytes from 192.168.1.105: icmp_seq=17 ttl=64 time=0.085 ms
64 bytes from 192.168.1.105: icmp_seq=18 ttl=64 time=0.082 ms
64 bytes from 192.168.1.105: icmp_seq=19 ttl=64 time=0.082 ms
64 bytes from 192.168.1.105: icmp_seq=20 ttl=64 time=0.081 ms
64 bytes from 192.168.1.105: icmp_seq=21 ttl=64 time=0.084 ms
64 bytes from 192.168.1.105: icmp_seq=22 ttl=64 time=0.083 ms
```

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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ curl --help
Usage: curl [options...] <url>
  --abstract-unix-socket <path> Connect via abstract Unix domain socket
  --alt-svc <file name> Enable alt-svc with this cache file
  --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
-C, --continue-at <offset> Resumed transfer offset
-b, --cookie <data|filename> Send cookies from string/file
-c, --cookie-jar <filename> Write cookies to <filename> after operation
  --create-dirs     Create necessary local directory hierarchy
  --crlf           Convert LF to CRLF in upload
  --crlfile <file>  Get a CRL list in PEM format from the given file
-d, --data <data>   HTTP POST data
  --data-ascii <data> HTTP POST ASCII data
  --data-binary <data> HTTP POST binary data
  --data-raw <data> HTTP POST data, '@' allowed
  --data-urlencode <data> HTTP POST data url encoded
  --delegation <LEVEL> GSS-API delegation permission
  --digest         Use HTTP Digest Authentication
-q, --disable      Disable .curlrc
```

HTTPEE: HTTPee – A Modern HTTP Client Similar to Curl and Wget commands. HTTPie (pronounced aitch-tee-tee-pie) is a cURL-like, modern, user-friendly, and cross-platform command line HTTP client written in Python. It is designed to make CLI interaction with web services easy and as user- friendly as possible.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ http
usage: http [--json] [--form] [--pretty {all,colors,format,none}]
        [--style STYLE] [--print WHAT] [--headers] [--body] [--verbose]
        [--all] [--history-print WHAT] [--stream] [--output FILE]
        [--download] [--continue]
        [--session SESSION_NAME_OR_PATH | --session-read-only SESSION_NAME_O
R_PATH]
        [--auth USER[:PASS]] [--auth-type {basic,digest}]
        [--proxy PROTOCOL:PROXY_URL] [--follow]
        [--max-redirects MAX_REDIRECTS] [--timeout SECONDS]
        [--check-status] [--verify VERIFY]
        [--ssl {ssl2.3,tls1,tls1.1,tls1.2}] [--cert CERT]
        [--cert-key CERT_KEY] [--ignore-stdin] [--help] [--version]
        [--traceback] [--default-scheme DEFAULT_SCHEME] [--debug]
        [METHOD] URL [REQUEST_ITEM [REQUEST_ITEM ...]]
http: error: the following arguments are required: URL

monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ wget --help
GNU Wget 1.20.3, 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

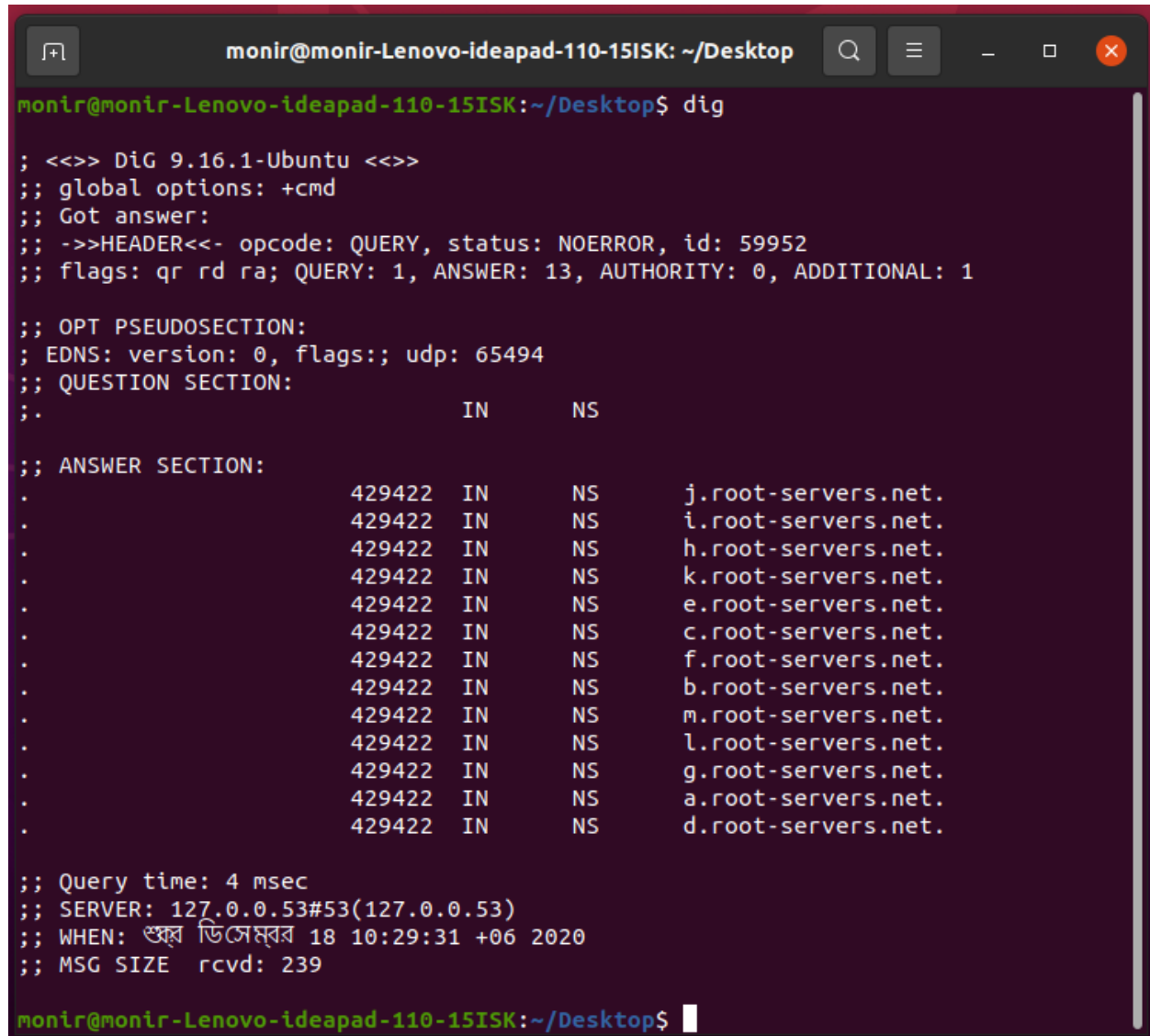
Logging and input file:
  -o, --output-file=FILE  log messages to FILE
  -a, --append-output=FILE append messages to FILE
  -d, --debug            print lots of debugging information
  -q, --quiet            quiet (no output)
  -v, --verbose          be verbose (this is the default)
  -nv, --no-verbose      turn off verbosity, without being quiet
  --report-speed=TYPE    output bandwidth as TYPE. TYPE can be bits
  -i, --input-file=FILE  download URLs found in local or external FILE
  -F, --force-html       treat input file as HTML
  -B, --base=URL         resolves HTML input-file links (-i -F)
                        relative to URL
  --config=FILE          specify config file to use
  --no-config            do not read any config file
  --rejected-log=FILE    log reasons for URL rejection to FILE

Download:
  -t, --tries=NUMBER     set number of retries to NUMBER (0 unlimited)
  --retry-connrefused    retry even if connection is refused
```

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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ tc
Usage: tc [ OPTIONS ] OBJECT { COMMAND | help }
       tc [-force] -batch filename
where  OBJECT := { qdisc | class | filter | chain |
                  action | monitor | exec }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[aw] |
                   -o[neline] | -j[son] | -p[retty] | -c[olor] |
                   -b[atch] [filename] | -n[etns] name | -N[umeric] |
                   -nm | -nam[es] | { -cf | -conf } path }
```

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.

A terminal window titled 'monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop' showing the output of the 'dig' command. The output includes header information, question section, answer section with 13 root servers, query time, server address, and timestamp.

```
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ dig

;; <<>> DiG 9.16.1-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59952
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
.           429422 IN      NS      j.root-servers.net.
.           429422 IN      NS      i.root-servers.net.
.           429422 IN      NS      h.root-servers.net.
.           429422 IN      NS      k.root-servers.net.
.           429422 IN      NS      e.root-servers.net.
.           429422 IN      NS      c.root-servers.net.
.           429422 IN      NS      f.root-servers.net.
.           429422 IN      NS      b.root-servers.net.
.           429422 IN      NS      m.root-servers.net.
.           429422 IN      NS      l.root-servers.net.
.           429422 IN      NS      g.root-servers.net.
.           429422 IN      NS      a.root-servers.net.
.           429422 IN      NS      d.root-servers.net.

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: শুক্র ডিসেম্বর 18 10:29:31 +06 2020
;; MSG SIZE rcvd: 239

monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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 humanreadable format.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-I                      query whois.iana.org and follow its referral
-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
-r                      turn off recursive look-ups for contact information
-R                      force to show local copy of the domain object even
                        if it contains referral
-a                      also search all the mirrored databases
-s SOURCE[,SOURCE]...  search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST   find updates from SOURCE from serial FIRST to LAST
-t TYPE                request template for object of TYPE
-v TYPE                request verbose template for object of TYPE
-q [version|sources|types] query specified server info
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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.


```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ ssh
usage: ssh [-46AaCfGgKkMMNqsTtVvXxYy] [-B bind_interface]
          [-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]] destination [command]
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ scp
usage: scp [-346BCpqrTv] [-c cipher] [-F ssh_config] [-i identity_file]
          [-J destination] [-l limit] [-o ssh_option] [-P port]
          [-S program] source ... target
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ rsync
rsync version 3.1.3 protocol version 31
Copyright (C) 1996-2018 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
```

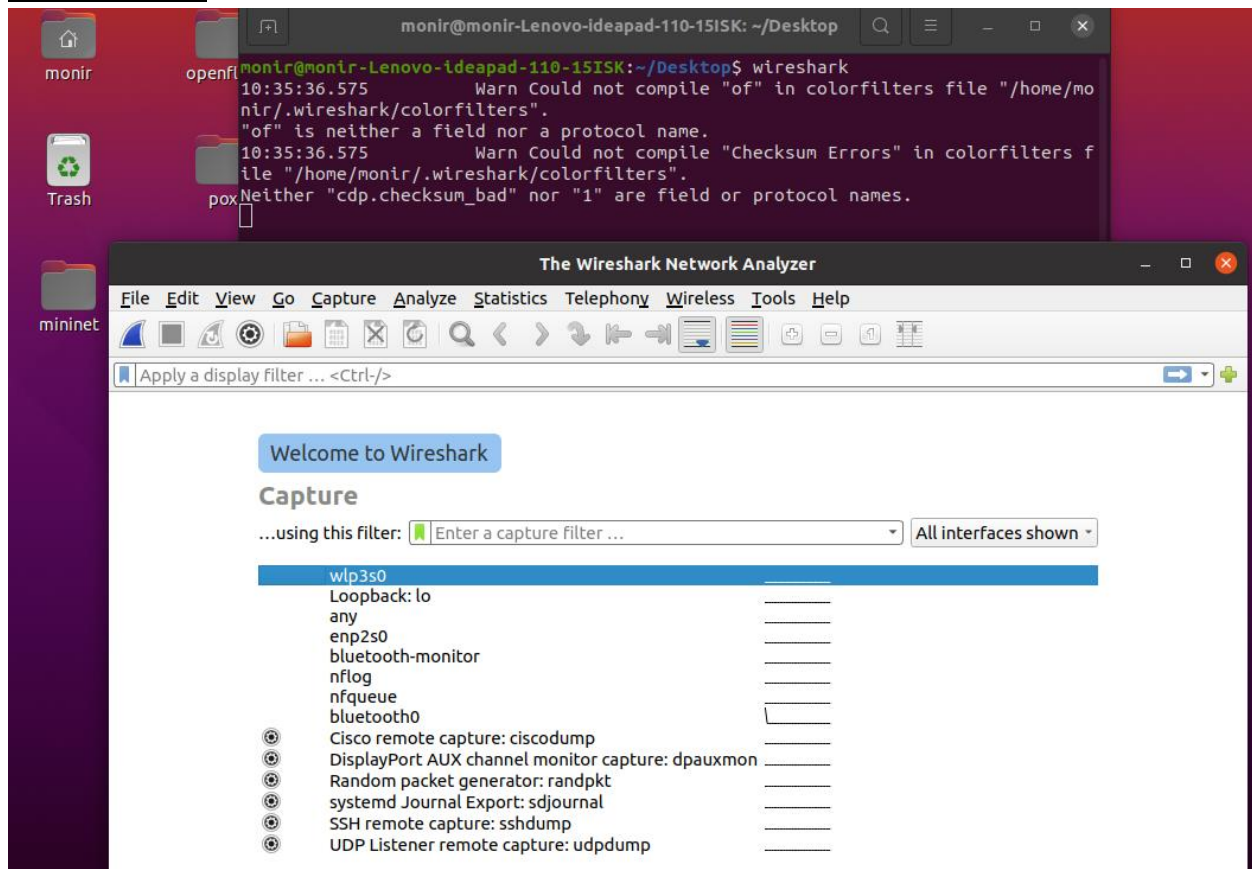
NGREP: **ngrep (network grep)** is a network packet analyzer written by Jordan Ritter. It has a command-line interface, and relies upon the pcap library and the ... it works in many UNIX-like operating systems: Linux, Solaris, illumos, BSD, AIX.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ ngrep
wlp3s0: You don't have permission to capture on that device (socket: Operation not permitted): Operation not permitted
exit
0 received, 0 matched
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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.


```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ tcpdump
tcpdump: wlp3s0: You don't have permission to capture on that device
(socket: Operation not permitted)
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

WIRESHARK:



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

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ ifconfig
enp2s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether fc:45:96:91:48:9f 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 530 bytes 49902 (49.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 530 bytes 49902 (49.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.105 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::e299:4352:6212:69e9 prefixlen 64 scopeid 0x20<link>
    ether c8:3d:d4:9c:0c:c5 txqueuelen 1000 (Ethernet)
    RX packets 16752 bytes 23205485 (23.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12745 bytes 1798021 (1.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

ROUTE: **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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ 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
192.168.1.0    0.0.0.0         255.255.255.0   U     600    0      0 wlp3s0
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

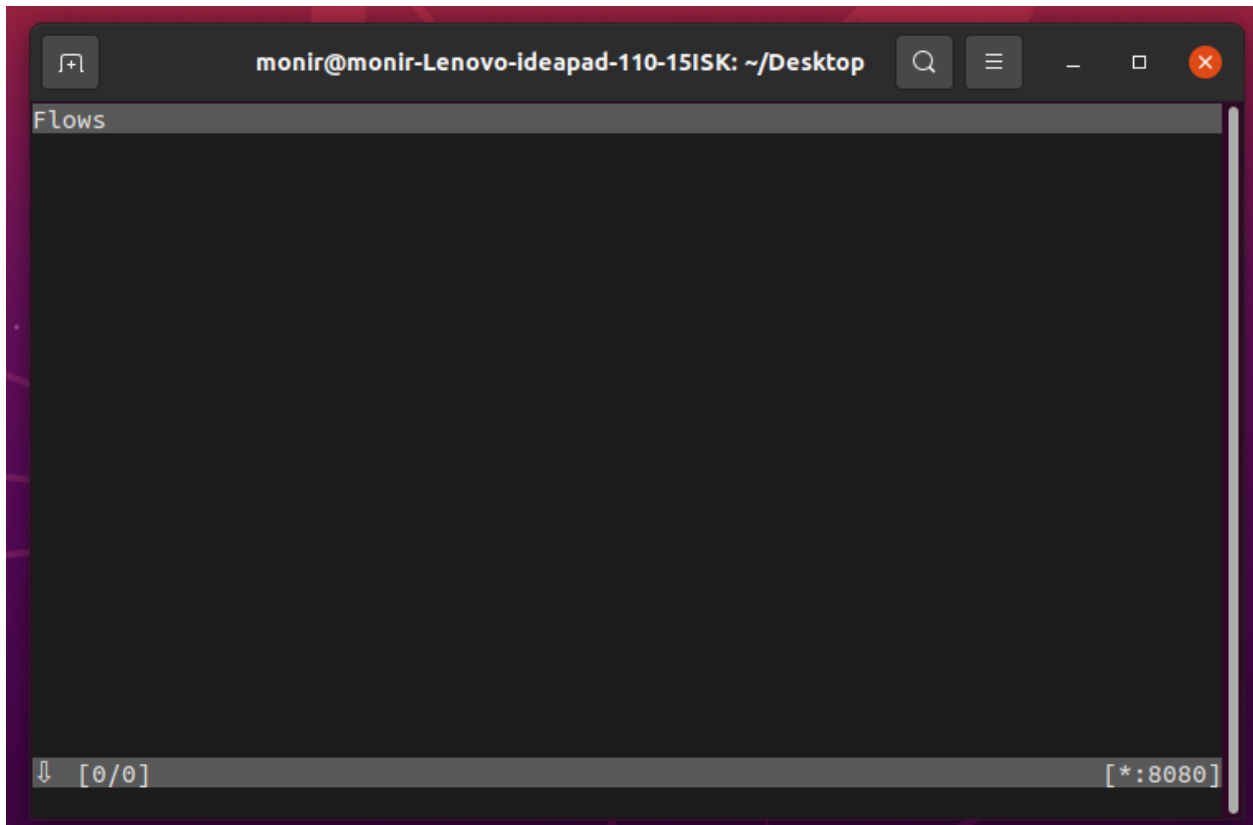
IP: The **ip** command is a Linux net-tool for system and network administrators. **IP** stands for Internet Protocol and as the name suggests, the tool is used for configuring network interfaces. Older Linux distributions used the **ifconfig** command, which operates similarly.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | address | addlabel | route | rule | neigh | ntable |
                  tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm
                  |
                  netns | l2tp | fou | macsec | tcp_metrics | token | netconf |
                  ila |
                  vrf | sr | nexthop }
OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
             -h[uman-readable] | -iec | -j[son] | -p[retty] |
             -f[amily] { inet | inet6 | mpls | bridge | link } |
             -4 | -6 | -I | -D | -M | -B | -O |
             -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
             -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename]
             |
             -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
             -c[olor]}
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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).

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
_gateway         ether    c8:e7:d8:92:ef:b8  C             wlp3s
0
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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.



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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ nmap
Nmap 7.91 ( 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
  --exclude-file <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
```

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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ 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

monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

OPENVPN:

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ openvpn
OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [
MH/PKTINFO] [AEAD] built on Sep  5 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.
                    p = udp (default), tcp-server, or tcp-client
--proto-force p    : only consider protocol p in list of connection profiles.
                    p = udp6, tcp6-server, or tcp6-client (ipv6)
--connect-retry n [m] : For client, number of seconds to wait between
                    connection retries (default=5). On repeated retries
                    the wait time is exponentially increased to a maximum of m
                    (default=300).
--connect-retry-max n : Maximum connection attempt retries, default infinite.
```

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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ 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]
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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


```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ socat
2020/12/18 10:46:55 socat[8211] E exactly 2 addresses required (there are 0); use option "-h" for help
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

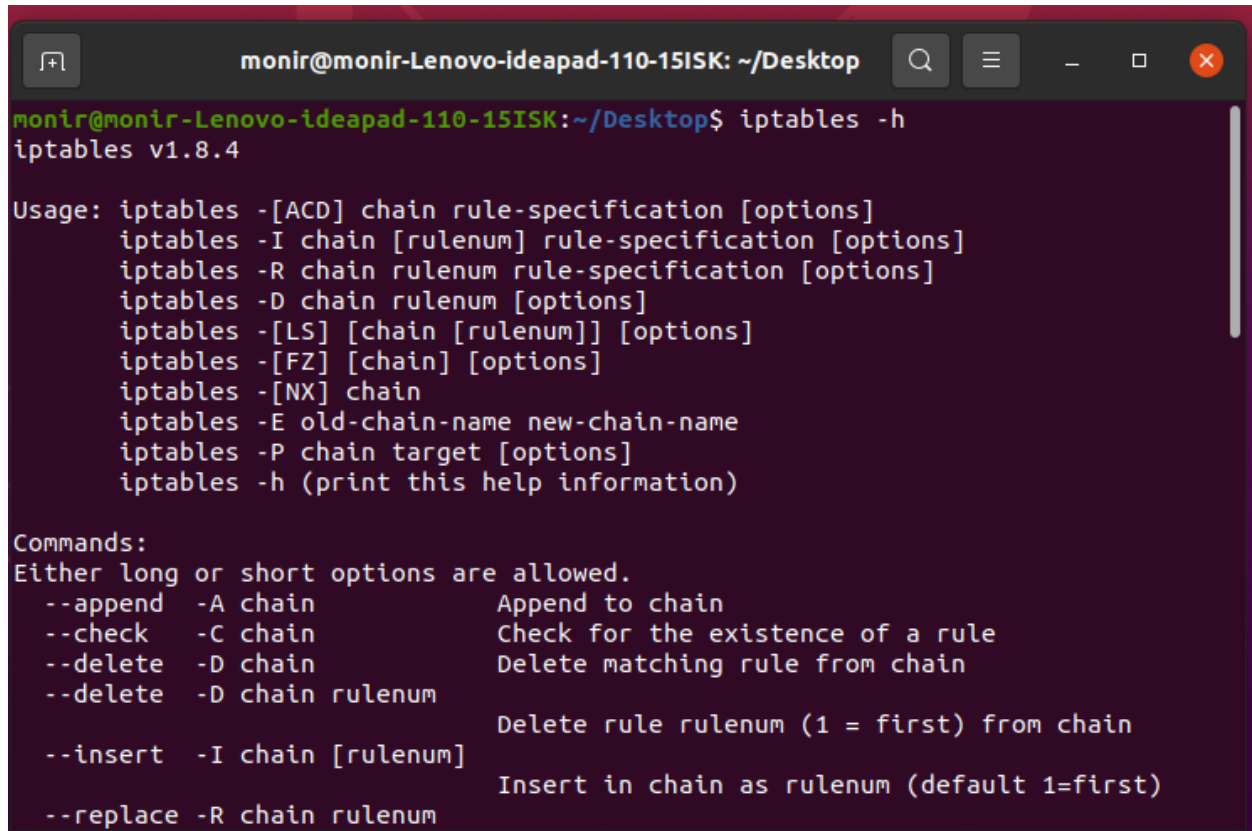
TELNET: In Linux, the **telnet** command is used to create a remote connection with a system over a TCP/IP network. It allows us to administrate other systems by the terminal. We can run a program to conduct administration. It uses a **TELNET** protocol. **FTP/SFTP:** **FTP (File Transfer Protocol)** 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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ telnet
telnet>
```

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** .

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ 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
192.168.1.0      0.0.0.0        255.255.255.0   U         0  0        0 wlp3s0
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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.

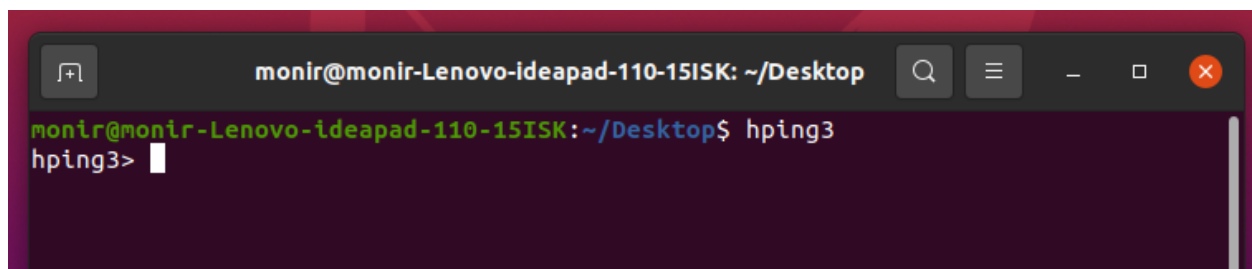


```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ iptables -h
iptables v1.8.4

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
       iptables -R chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       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)

Commands:
Either long or short options are allowed.
--append -A chain          Append to chain
--check  -C chain          Check for the existence of a rule
--delete -D chain          Delete matching rule from chain
--delete -D chain rulenum  Delete rule rulenum (1 = first) from chain
--insert -I chain [rulenum] Insert in chain as rulenum (default 1=first)
--replace -R chain rulenum
```

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.



```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ hping3
hping3> 
```

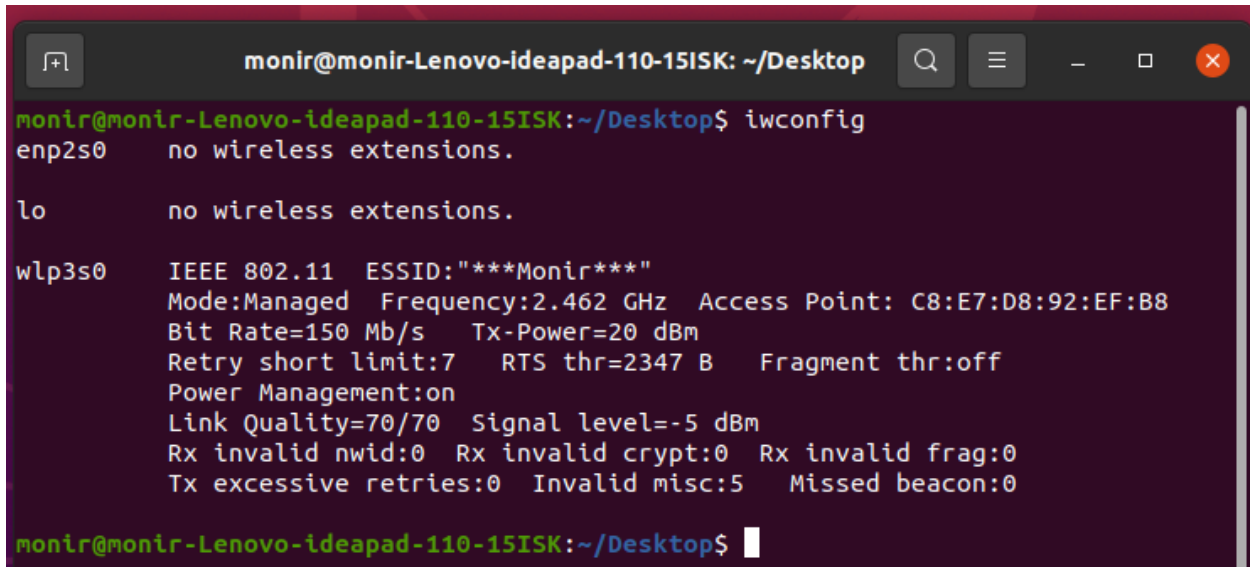
TRACEROUTE/MTR: **traceroute** command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ traceroute --usage
Usage: traceroute [-I?V] [-f NUM] [-g GATES] [-m NUM] [-M METHOD] [-p PORT]
      [-q NUM] [-t NUM] [-w NUM] [--first-hop=NUM] [--gateways=GATES]
      [--icmp] [--max-hop=NUM] [--type=METHOD] [--port=PORT]
      [--tries=NUM] [--resolve-hostnames] [--tos=NUM] [--wait=NUM]
      [--help] [--usage] [--version] HOST
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ ethtool -h
ethtool version 5.4
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|f|d... ]
        [ sopass %x:%x:%x:%x:%x:%x ]
        [ msglvl %d | msglvl type on|off ... ]
    ethtool -a|--show-pause DEVNAME Show pause options
    ethtool -A|--pause DEVNAME        Set pause options
        [ autoneg on|off ]
        [ rx on|off ]
        [ tx on|off ]
    ethtool -c|--show-coalesce DEVNAME Show coalesce options
    ethtool -C|--coalesce DEVNAME    Set coalesce options
        [ adaptive-rx 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.

A terminal window titled 'monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop' with standard window controls. The terminal shows the command 'iwconfig' being executed. The output lists three network interfaces: 'enp2s0' and 'lo' both show 'no wireless extensions.', while 'wlp3s0' shows detailed IEEE 802.11 configuration including ESSID, mode, frequency, access point MAC, bit rate, power, retry limits, RTS threshold, fragment threshold, power management, link quality, signal level, and various error statistics.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop$ iwconfig
enp2s0    no wireless extensions.

lo        no wireless extensions.

wlp3s0    IEEE 802.11  ESSID:"***Monir***"
          Mode:Managed  Frequency:2.462 GHz  Access Point: C8:E7:D8:92:EF:B8
          Bit Rate=150 Mb/s   Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:on
          Link Quality=70/70   Signal level=-5 dBm
          Rx invalid nwid:0    Rx invalid crypt:0   Rx invalid frag:0
          Tx excessive retries:0 Invalid misc:5   Missed beacon:0

monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop$
```

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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ 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 the given variable(s)
  -p, --load[=<file>]    read values from file
  -f                        alias of -p
      --system            read values from all system directories
  -r, --pattern <expression>
                          select setting that match expression
  -q, --quiet            do not echo variable set
  -w, --write            enable writing a value to variable
  -o                        does nothing
  -x                        does nothing
  -d                        alias of -h

  -h, --help            display this help and exit
  -V, --version        output version information and exit

For more details see sysctl(8).
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ 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.

```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ stunnel
[ ] Clients allowed=500
[.] stunnel 5.56 on x86_64-pc-linux-gnu platform
[.] Compiled with OpenSSL 1.1.1c 28 May 2019
[.] Running with OpenSSL 1.1.1f 31 Mar 2020
[.] Threading:PTHREAD Sockets:POLL,IPv6,SYSTEMD TLS:ENGINE,FIPS,OCSP,PSK,SNI Auth:LIBWRAP
[ ] errno: (*__errno_location ())
[!] Invalid configuration file name "/etc/stunnel/stunnel.conf"
[!] realpath: No such file or directory (2)
[ ] Deallocating section defaults
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$
```

IPCALC:


```
monir@monir-Lenovo-ideapad-110-15ISK: ~/Desktop
monir@monir-Lenovo-ideapad-110-15ISK:~/Desktop$ 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
ipcalc 192.168.0.1 255.255.128.0 255.255.192.0
ipcalc 192.168.0.1 0.0.63.255

ipcalc <ADDRESS1> - <ADDRESS2>  deaggregate address range

ipcalc <ADDRESS>/<NETMASK> --s a b c
                                split network to subnets
                                where a b c fits in.

! New HTML support not yet finished.

ipcalc 0.41
```