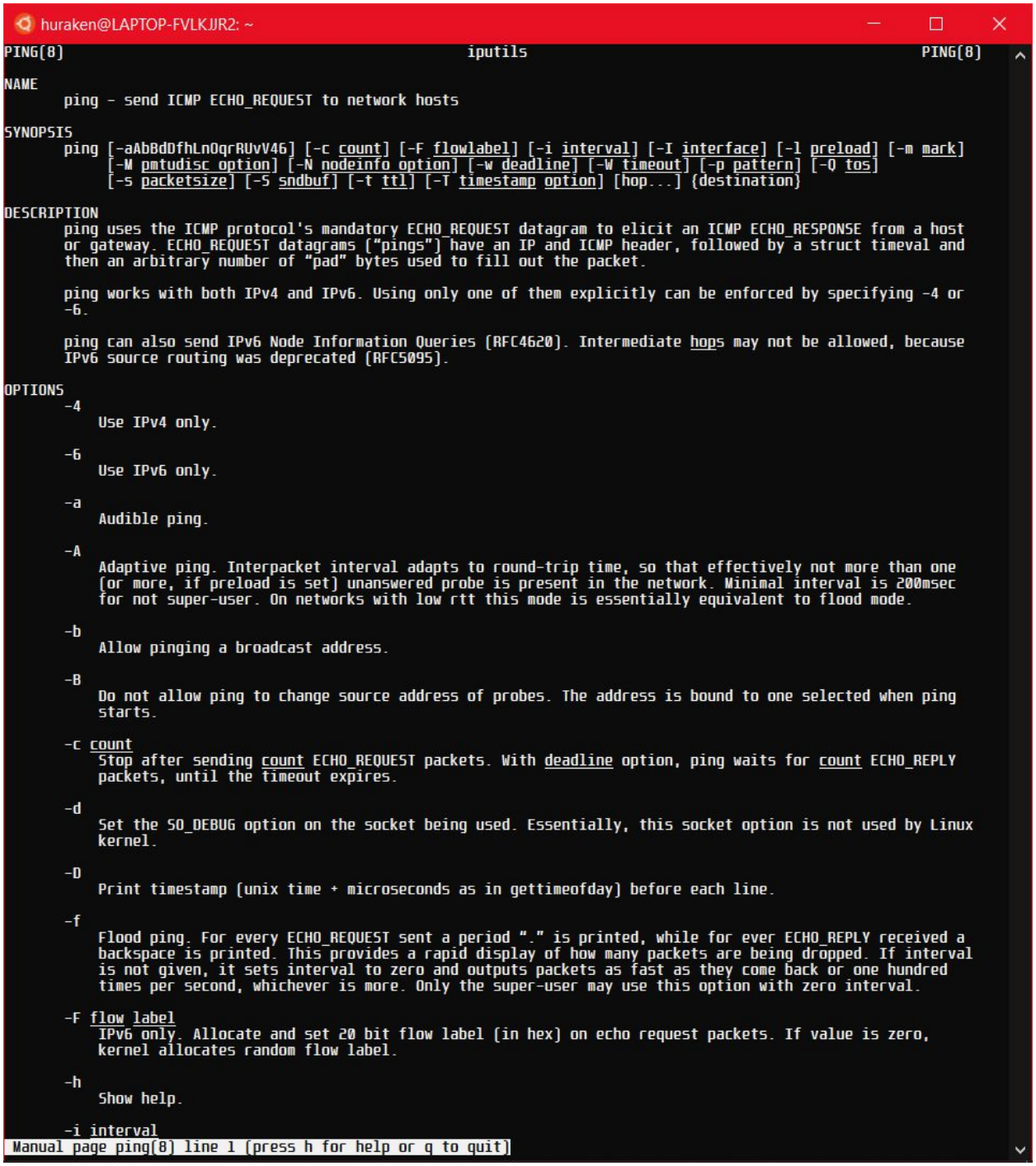
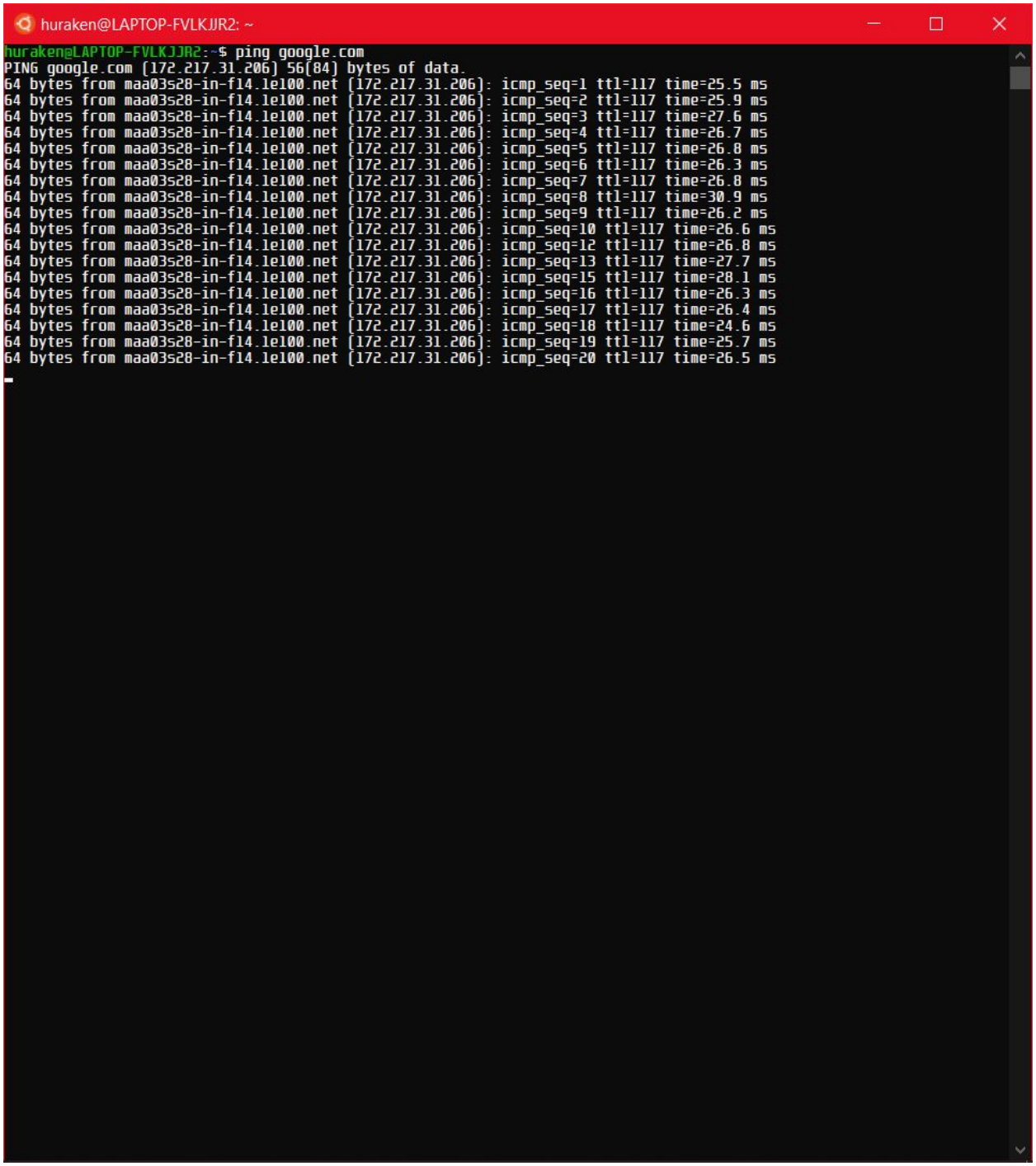
CS3093D | Networks Lab

Arjun Syam
B180031CS

1.ping :

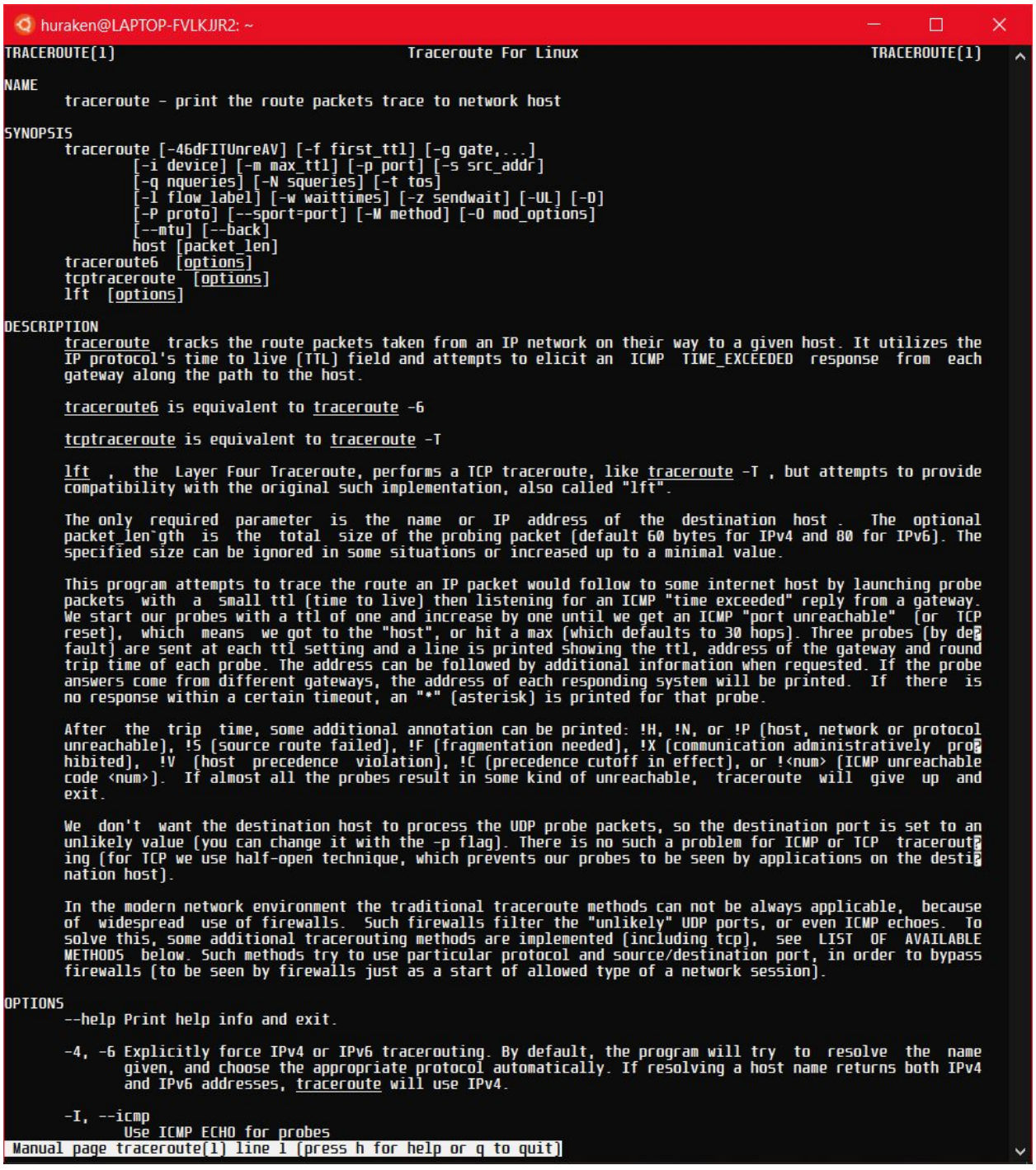
A Ping measures the time it takes for packets to be sent from the local host to a destination computer and back.

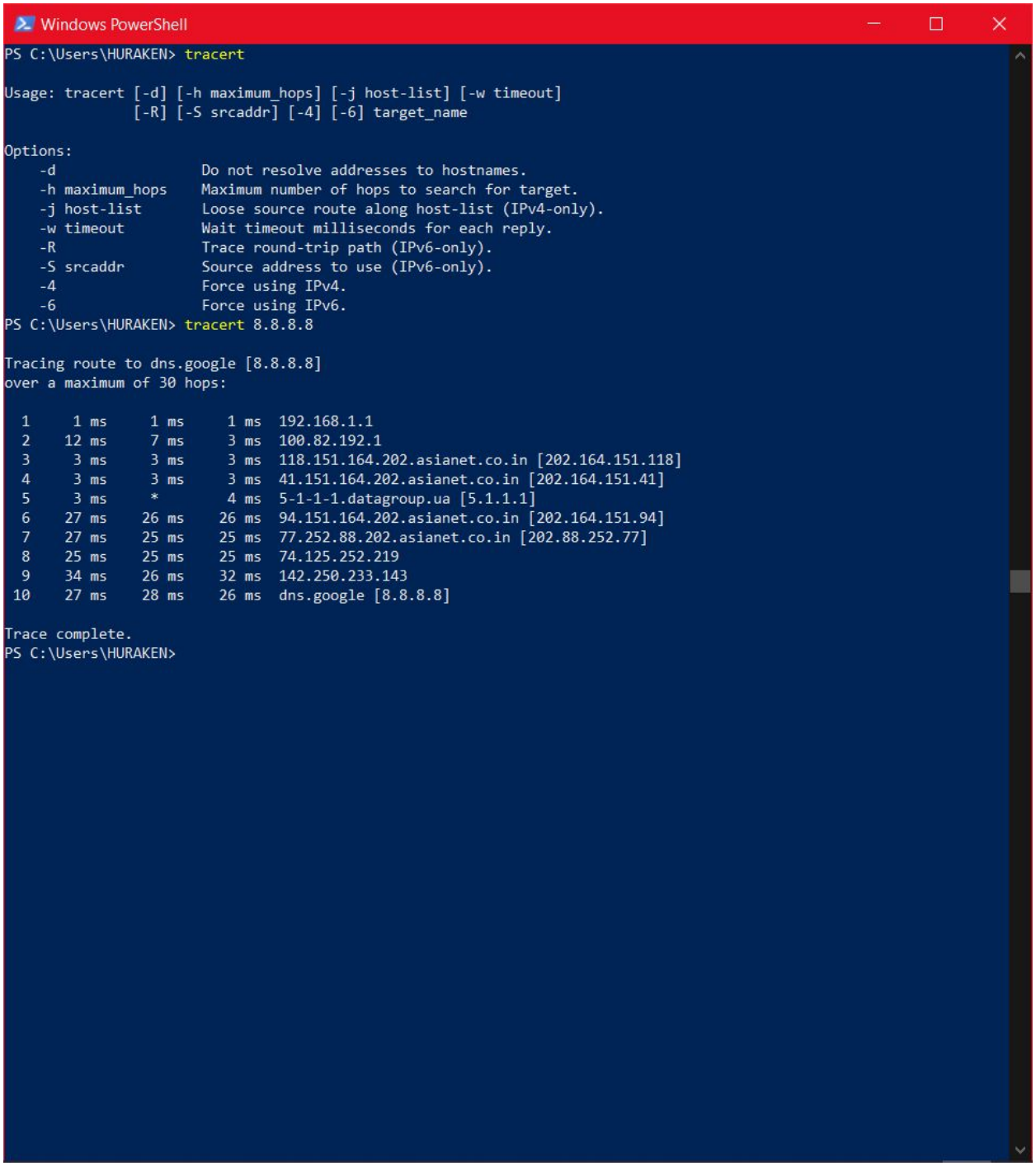



huraken@LAPTOP-FVLKJJR2: ~
huraken@LAPTOP-FVLKJJR2:~$ ping google.com
PING google.com (172.217.31.206) 56(84) bytes of data.
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=1 ttl=117 time=25.5 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=2 ttl=117 time=25.9 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=3 ttl=117 time=27.6 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=4 ttl=117 time=26.7 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=5 ttl=117 time=26.8 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=6 ttl=117 time=26.3 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=7 ttl=117 time=26.8 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=8 ttl=117 time=30.9 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=9 ttl=117 time=26.2 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=10 ttl=117 time=26.6 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=12 ttl=117 time=26.8 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=13 ttl=117 time=27.7 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=15 ttl=117 time=28.1 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=16 ttl=117 time=26.3 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=17 ttl=117 time=26.4 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=18 ttl=117 time=24.6 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=19 ttl=117 time=25.7 ms
64 bytes from maa03s28-in-f14.1e100.net (172.217.31.206): icmp_seq=20 ttl=117 time=26.5 ms

2. tracert/traceroute :

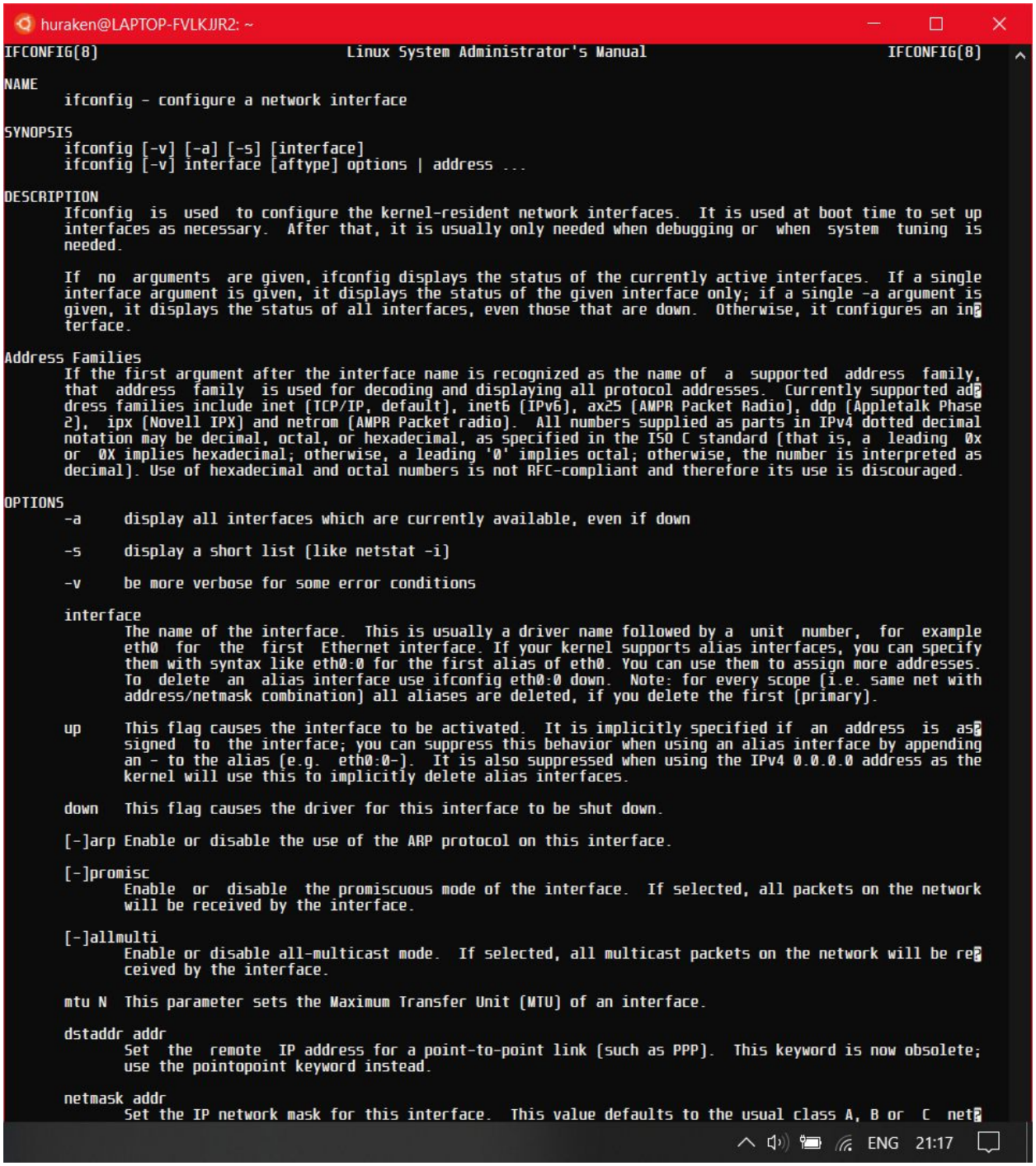
Computer network diagnostic commands for displaying possible routes (paths) and measuring transit delays of packets across an Internet Protocol (IP) network.

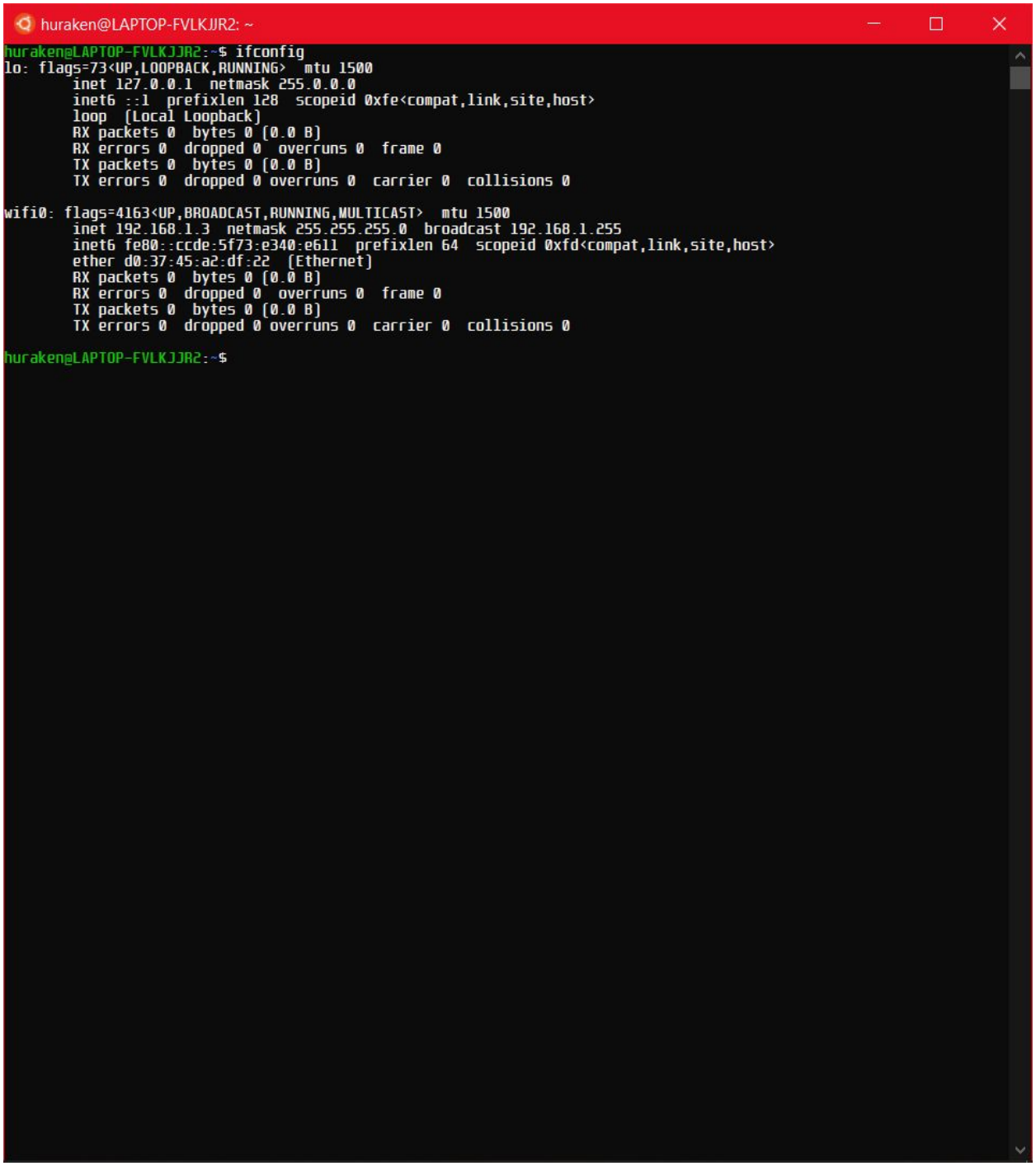




3.Ifconfig :

To configure kernel-resident network interface

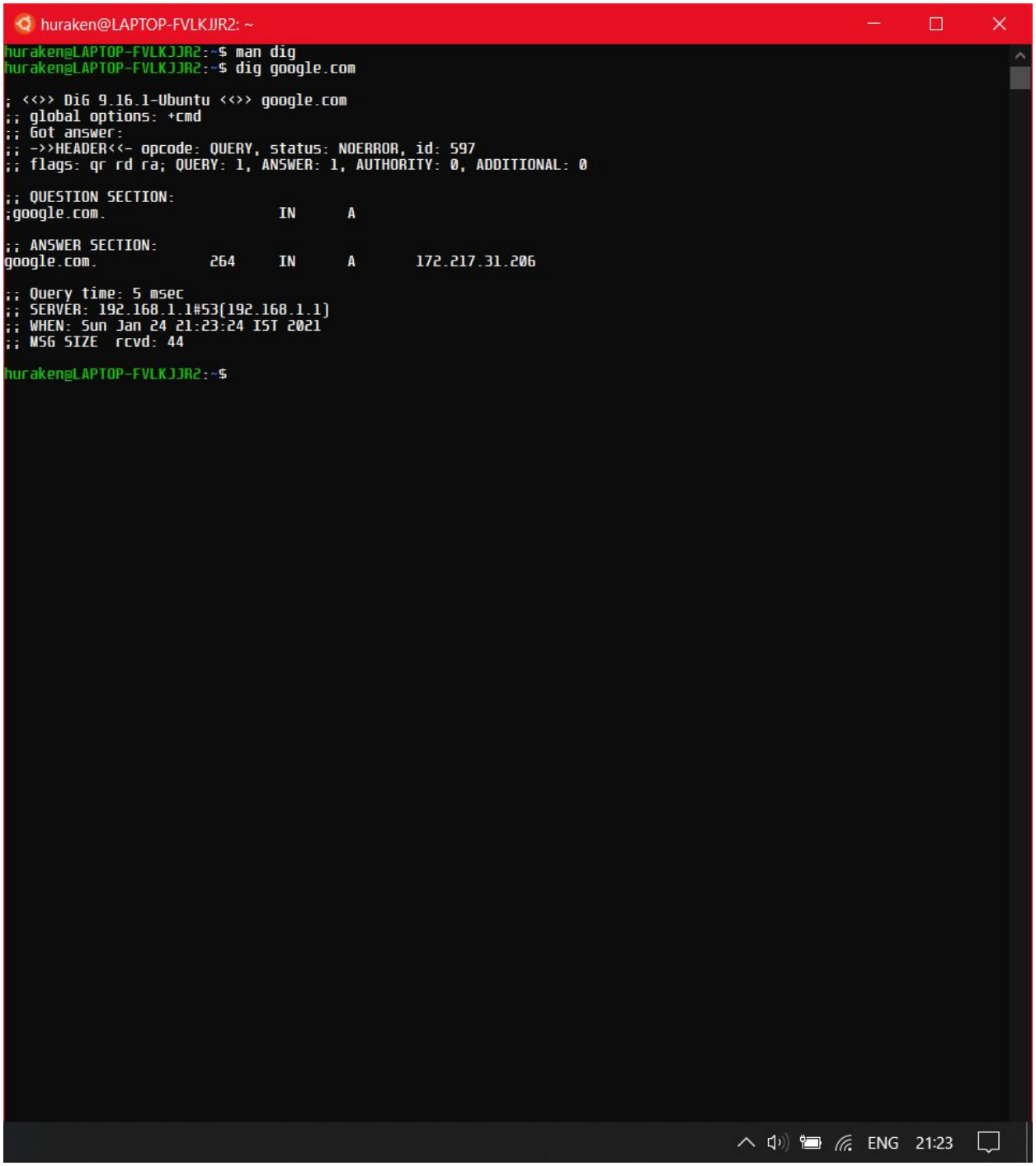

huraken@LAPTOP-FVLKJJR2: ~
IFCONFIG(8) Linux System Administrator's Manual IFCONFIG(8)
NAME
ifconfig - configure a network interface
SYNOPSIS
ifconfig [-v] [-a] [-s] [interface]
ifconfig [-v] interface [aftype] options | address ...
DESCRIPTION
Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed.
If no arguments are given, ifconfig displays the status of the currently active interfaces. If a single interface argument is given, it displays the status of the given interface only; if a single -a argument is given, it displays the status of all interfaces, even those that are down. Otherwise, it configures an interface.
Address Families
If the first argument after the interface name is recognized as the name of a supported address family, that address family is used for decoding and displaying all protocol addresses. Currently supported address families include inet (TCP/IP, default), inet6 (IPv6), ax25 (AMPR Packet Radio), ddp (Appletalk Phase 2), ipx (Novell IPX) and netrom (AMPR Packet radio). All numbers supplied as parts in IPv4 dotted decimal notation may be decimal, octal, or hexadecimal, as specified in the ISO C standard (that is, a leading 0x or 0X implies hexadecimal; otherwise, a leading '0' implies octal; otherwise, the number is interpreted as decimal). Use of hexadecimal and octal numbers is not RFC-compliant and therefore its use is discouraged.
OPTIONS
-a display all interfaces which are currently available, even if down
-s display a short list (like netstat -i)
-v be more verbose for some error conditions
interface
The name of the interface. This is usually a driver name followed by a unit number, for example eth0 for the first Ethernet interface. If your kernel supports alias interfaces, you can specify them with syntax like eth0:0 for the first alias of eth0. You can use them to assign more addresses. To delete an alias interface use ifconfig eth0:0 down. Note: for every scope (i.e. same net with address/netmask combination) all aliases are deleted, if you delete the first (primary).
up This flag causes the interface to be activated. It is implicitly specified if an address is assigned to the interface; you can suppress this behavior when using an alias interface by appending an - to the alias (e.g. eth0:0-). It is also suppressed when using the IPv4 0.0.0.0 address as the kernel will use this to implicitly delete alias interfaces.
down This flag causes the driver for this interface to be shut down.
[-]arp Enable or disable the use of the ARP protocol on this interface.
[-]promisc
Enable or disable the promiscuous mode of the interface. If selected, all packets on the network will be received by the interface.
[-]allmulti
Enable or disable all-multicast mode. If selected, all multicast packets on the network will be received by the interface.
mtu N This parameter sets the Maximum Transfer Unit (MTU) of an interface.
dstaddr addr
Set the remote IP address for a point-to-point link (such as PPP). This keyword is now obsolete; use the pointopoint keyword instead.
netmask addr
Set the IP network mask for this interface. This value defaults to the usual class A, B or C net
ENG 21:17



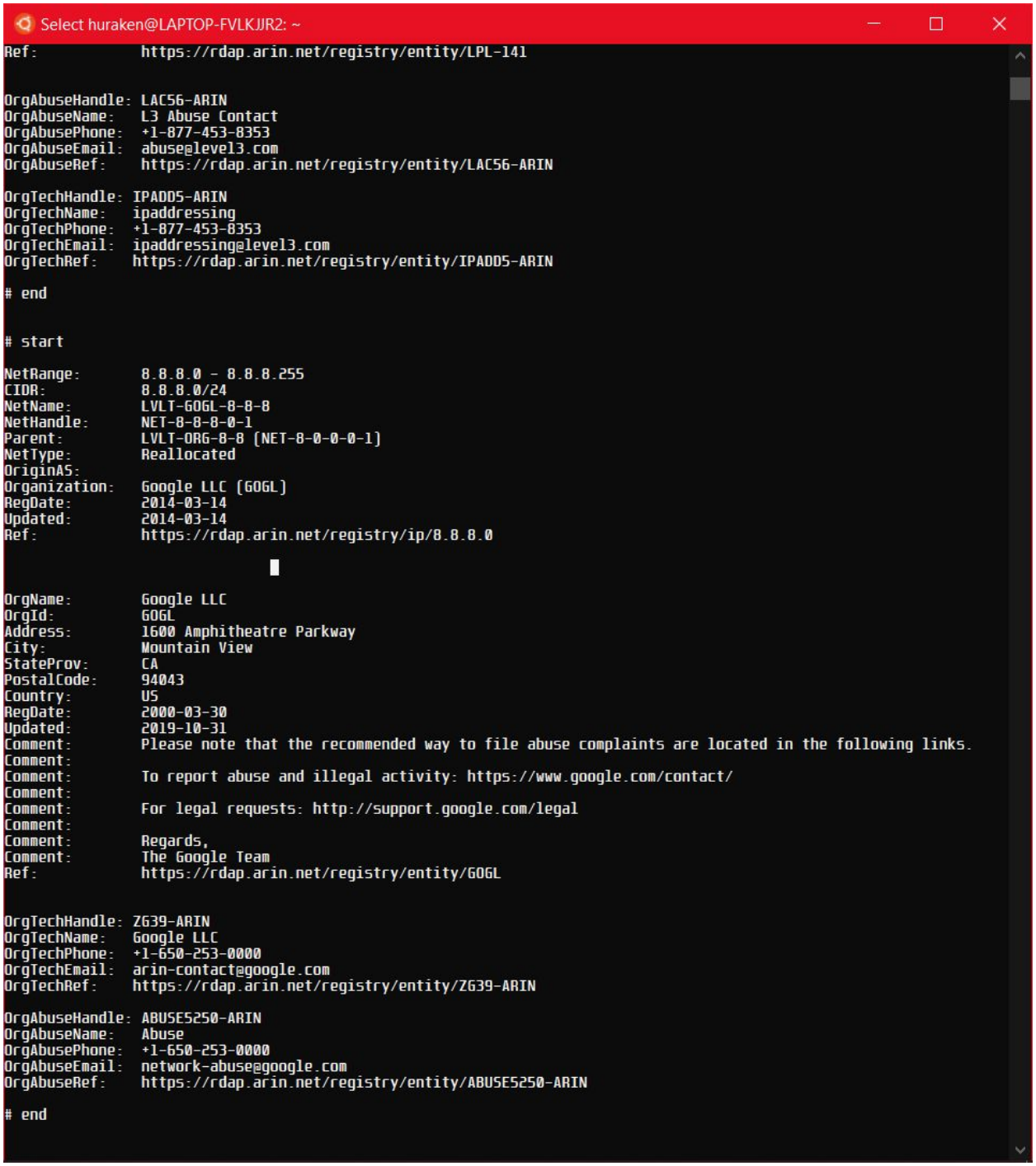
4. Dig :

Used to display the DNS lookups and displays the answers from the name server that was queried

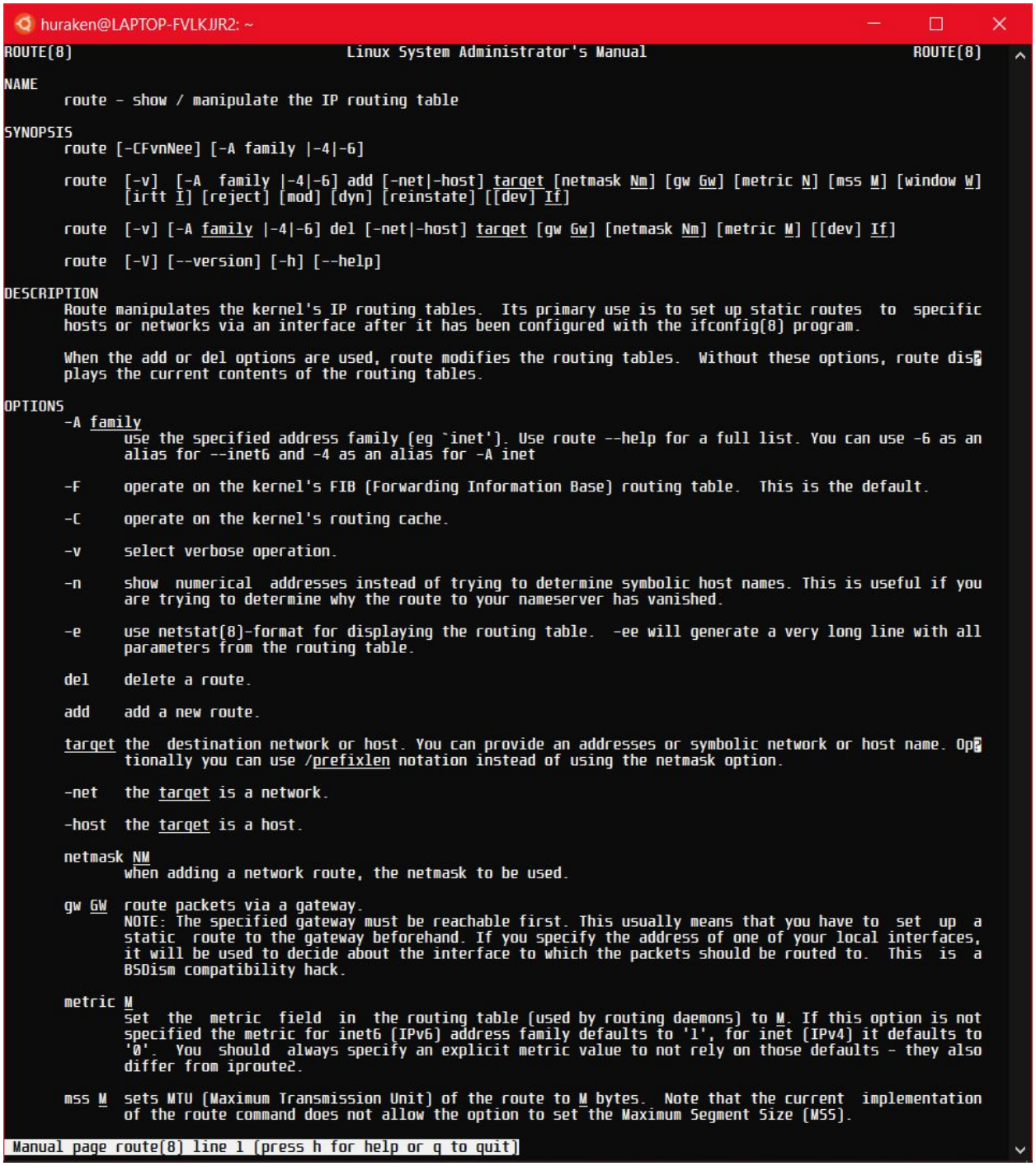

huraken@LAPTOP-FVLKJJR2: ~
DIG(1) BIND9 DIG(1)
NAME
dig - DNS lookup utility
SYNOPSIS
dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-m] [-p port#] [-q name] [-t type] [-v]
[-x addr] [-y [hmac:]name:key] [[-4] | [-6]] [name] [type] [class] [queryopt...]
dig [-h]
dig [global-queryopt...] [query...]
DESCRIPTION
dig is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers
that are returned from the name server(s) that were queried. Most DNS administrators use dig to
troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools
tend to have less functionality than dig.
Although dig is normally used with command-line arguments, it also has a batch mode of operation for
reading lookup requests from a file. A brief summary of its command-line arguments and options is printed
when the -h option is given. Unlike earlier versions, the BIND 9 implementation of dig allows multiple
lookups to be issued from the command line.
Unless it is told to query a specific name server, dig will try each of the servers listed in
/etc/resolv.conf. If no usable server addresses are found, dig will send the query to the local host.
When no command line arguments or options are given, dig will perform an NS query for "." (the root).
It is possible to set per-user defaults for dig via ${HOME}/.digrc. This file is read and any options in it
are applied before the command line arguments. The -r option disables this feature, for scripts that need
predictable behaviour.
The IN and CH class names overlap with the IN and CH top level domain names. Either use the -t and -c
options to specify the type and class, use the -q the specify the domain name, or use "IN." and "CH." when
looking up these top level domains.
SIMPLE USAGE
A typical invocation of dig looks like:
dig @server name type
where:
server
is the name or IP address of the name server to query. This can be an IPv4 address in dotted-decimal
notation or an IPv6 address in colon-delimited notation. When the supplied server argument is a
hostname, dig resolves that name before querying that name server.
If no server argument is provided, dig consults /etc/resolv.conf; if an address is found there, it
queries the name server at that address. If either of the -4 or -6 options are in use, then only
addresses for the corresponding transport will be tried. If no usable addresses are found, dig will
send the query to the local host. The reply from the name server that responds is displayed.
name
is the name of the resource record that is to be looked up.
type
indicates what type of query is required - ANY, A, MX, SIG, etc. type can be any valid query type. If
no type argument is supplied, dig will perform a lookup for an A record.
OPTIONS
-4
Use IPv4 only.
-6
Use IPv6 only.
ENG 21:20

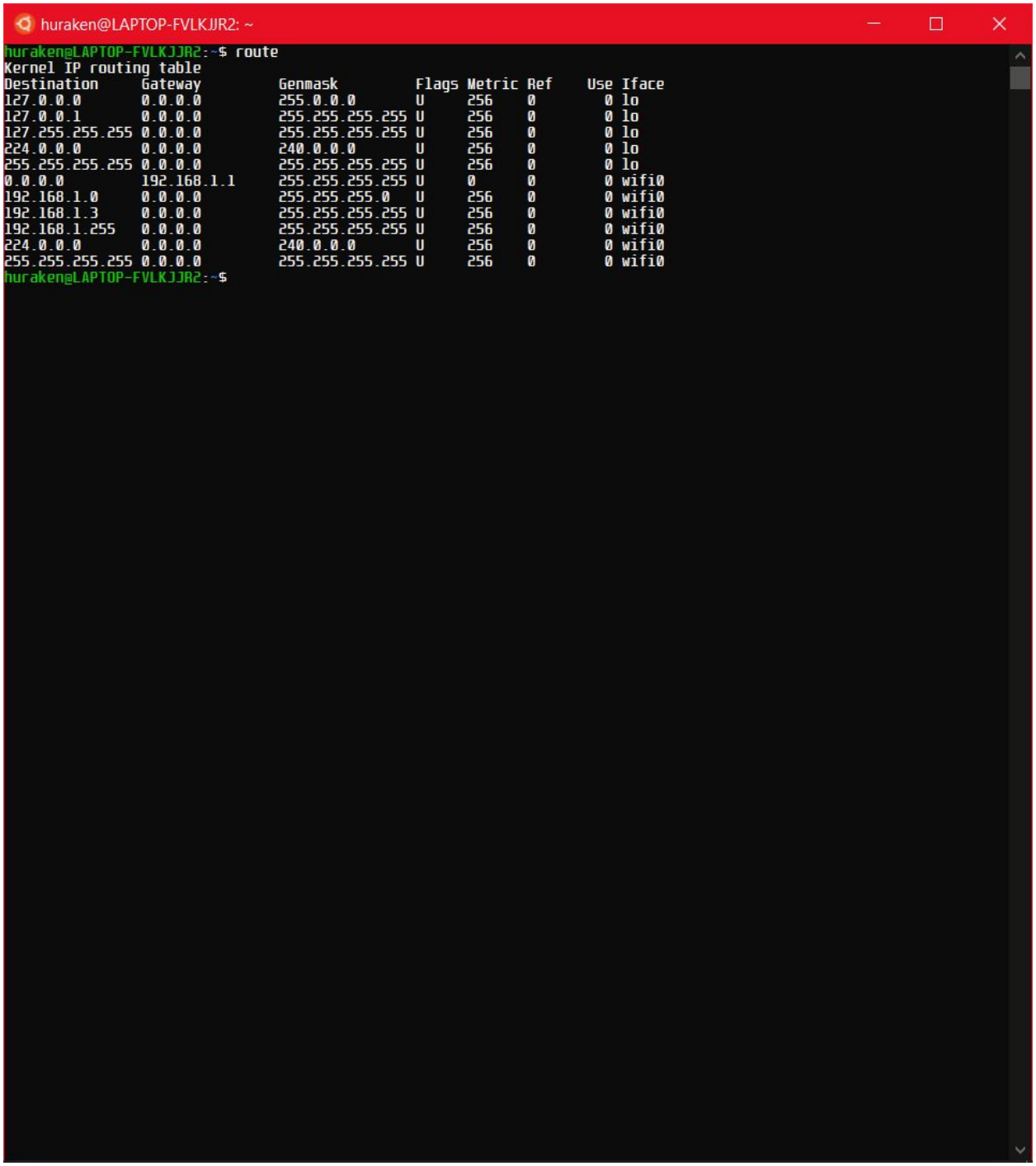


5. Whois
Cmd : whois 8.8.8.8
To get info regarding a specific IP address

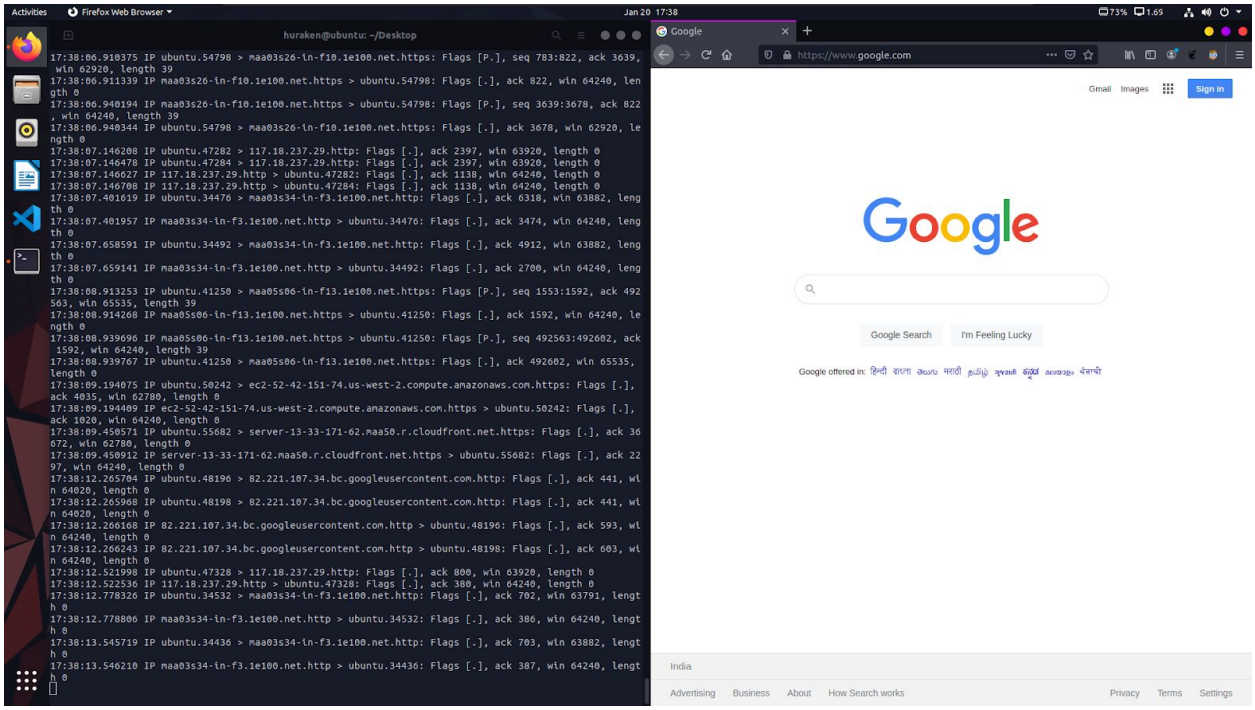

Select huraken@LAPTOP-FVLKJJR2: ~
Ref: https://rdap.arin.net/registry/entity/LPL-141
OrgAbuseHandle: LAC56-ARIN
OrgAbuseName: L3 Abuse Contact
OrgAbusePhone: +1-877-453-8353
OrgAbuseEmail: abuse@level3.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/LAC56-ARIN
OrgTechHandle: IPADD5-ARIN
OrgTechName: ipaddressing
OrgTechPhone: +1-877-453-8353
OrgTechEmail: ipaddressing@level3.com
OrgTechRef: https://rdap.arin.net/registry/entity/IPADD5-ARIN
end
start
NetRange: 8.8.8.0 - 8.8.8.255
CIDR: 8.8.8.0/24
NetName: LVLT-GOGL-8-8-8
NetHandle: NET-8-8-8-0-1
Parent: LVLT-ORG-8-8 (NET-8-0-0-0-1)
NetType: Reallocated
OriginAS:
Organization: Google LLC (GOGL)
RegDate: 2014-03-14
Updated: 2014-03-14
Ref: https://rdap.arin.net/registry/ip/8.8.8.0
OrgName: Google LLC
OrgId: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2000-03-30
Updated: 2019-10-31
Comment: Please note that the recommended way to file abuse complaints are located in the following links.
Comment:
Comment: To report abuse and illegal activity: https://www.google.com/contact/
Comment:
Comment: For legal requests: http://support.google.com/legal
Comment:
Comment: Regards,
Comment: The Google Team
Ref: https://rdap.arin.net/registry/entity/GOGL
OrgTechHandle: ZG39-ARIN
OrgTechName: Google LLC
OrgTechPhone: +1-650-253-0000
OrgTechEmail: arin-contact@google.com
OrgTechRef: https://rdap.arin.net/registry/entity/ZG39-ARIN
OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-650-253-0000
OrgAbuseEmail: network-abuse@google.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE5250-ARIN
end

6. Route : to manipulate IP routing tables



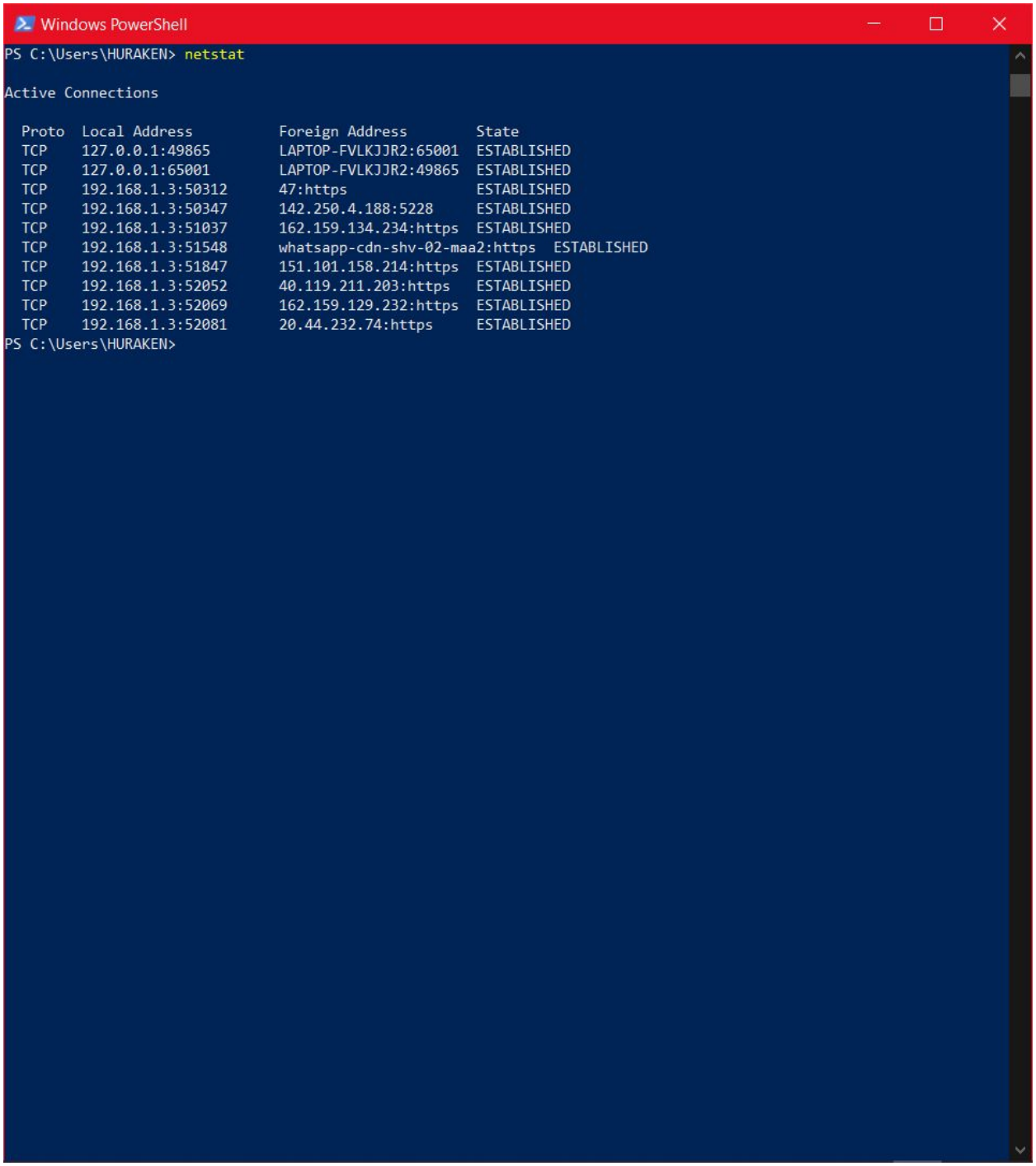

huraken@LAPTOP-FVLKJJR2: ~
huraken@LAPTOP-FVLKJJR2:~$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
127.0.0.0 0.0.0.0 255.0.0.0 U 256 0 0 lo
127.0.0.1 0.0.0.0 255.255.255.255 U 256 0 0 lo
127.255.255.255 0.0.0.0 255.255.255.255 U 256 0 0 lo
224.0.0.0 0.0.0.0 240.0.0.0 U 256 0 0 lo
255.255.255.255 0.0.0.0 255.255.255.255 U 256 0 0 lo
0.0.0.0 192.168.1.1 255.255.255.255 U 0 0 0 wifi0
192.168.1.0 0.0.0.0 255.255.255.0 U 256 0 0 wifi0
192.168.1.3 0.0.0.0 255.255.255.255 U 256 0 0 wifi0
192.168.1.255 0.0.0.0 255.255.255.255 U 256 0 0 wifi0
224.0.0.0 0.0.0.0 240.0.0.0 U 256 0 0 wifi0
255.255.255.255 0.0.0.0 255.255.255.255 U 256 0 0 wifi0
huraken@LAPTOP-FVLKJJR2:~$

7. Tcpdump : displays the contents of the packets on a network interface


Activities
Firefox Web Browser
Jan 20 17:38
huraken@ubuntu: ~/Desktop
17:38:06.910375 IP ubuntu.54798 > maa03s26-in-f10.1e100.net.https: Flags [P.], seq 783:822, ack 3639, win 62920, length 39
17:38:06.911339 IP maa03s26-in-f10.1e100.net.https > ubuntu.54798: Flags [.], ack 822, win 64240, length 0
17:38:06.940194 IP maa03s26-in-f10.1e100.net.https > ubuntu.54798: Flags [P.], seq 3639:3678, ack 822, win 64240, length 39
17:38:06.940344 IP ubuntu.54798 > maa03s26-in-f10.1e100.net.https: Flags [.], ack 3678, win 62920, length 0
17:38:07.146208 IP ubuntu.47282 > 117.18.237.29.http: Flags [.], ack 2397, win 63920, length 0
17:38:07.146478 IP ubuntu.47284 > 117.18.237.29.http: Flags [.], ack 2397, win 63920, length 0
17:38:07.146627 IP 117.18.237.29.http > ubuntu.47282: Flags [.], ack 1138, win 64240, length 0
17:38:07.146708 IP 117.18.237.29.http > ubuntu.47284: Flags [.], ack 1138, win 64240, length 0
17:38:07.401619 IP ubuntu.34476 > maa03s34-in-f3.1e100.net.http: Flags [.], ack 6318, win 63882, length 0
17:38:07.401957 IP maa03s34-in-f3.1e100.net.http > ubuntu.34476: Flags [.], ack 3474, win 64240, length 0
17:38:07.658591 IP ubuntu.34492 > maa03s34-in-f3.1e100.net.http: Flags [.], ack 4912, win 63882, length 0
17:38:07.659141 IP maa03s34-in-f3.1e100.net.http > ubuntu.34492: Flags [.], ack 2700, win 64240, length 0
17:38:08.913253 IP ubuntu.41250 > maa05s06-in-f13.1e100.net.https: Flags [P.], seq 1553:1592, ack 492563, win 65535, length 39
17:38:08.914268 IP maa05s06-in-f13.1e100.net.https > ubuntu.41250: Flags [.], ack 1592, win 64240, length 0
17:38:08.939696 IP maa05s06-in-f13.1e100.net.https > ubuntu.41250: Flags [P.], seq 492563:492602, ack 1592, win 64240, length 39
17:38:08.939767 IP ubuntu.41250 > maa05s06-in-f13.1e100.net.https: Flags [.], ack 492602, win 65535, length 0
17:38:09.194075 IP ubuntu.50242 > ec2-52-42-151-74.us-west-2.compute.amazonaws.com.https: Flags [.], ack 4035, win 62780, length 0
17:38:09.194409 IP ec2-52-42-151-74.us-west-2.compute.amazonaws.com.https > ubuntu.50242: Flags [.], ack 1020, win 64240, length 0
17:38:09.450571 IP ubuntu.55682 > server-13-33-171-62.maa50.r.cloudfront.net.https: Flags [.], ack 3672, win 62780, length 0
17:38:09.450912 IP server-13-33-171-62.maa50.r.cloudfront.net.https > ubuntu.55682: Flags [.], ack 2297, win 64240, length 0
17:38:12.265704 IP ubuntu.48196 > 82.221.107.34.bc.googleusercontent.com.http: Flags [.], ack 441, win 64020, length 0
17:38:12.265968 IP ubuntu.48198 > 82.221.107.34.bc.googleusercontent.com.http: Flags [.], ack 441, win 64020, length 0
17:38:12.266168 IP 82.221.107.34.bc.googleusercontent.com.http > ubuntu.48196: Flags [.], ack 593, win 64240, length 0
17:38:12.266243 IP 82.221.107.34.bc.googleusercontent.com.http > ubuntu.48198: Flags [.], ack 603, win 64240, length 0
17:38:12.521998 IP ubuntu.47328 > 117.18.237.29.http: Flags [.], ack 800, win 63920, length 0
17:38:12.522536 IP 117.18.237.29.http > ubuntu.47328: Flags [.], ack 380, win 64240, length 0
17:38:12.778326 IP ubuntu.34532 > maa03s34-in-f3.1e100.net.http: Flags [.], ack 702, win 63791, length 0
17:38:12.778806 IP maa03s34-in-f3.1e100.net.http > ubuntu.34532: Flags [.], ack 386, win 64240, length 0
17:38:13.545719 IP ubuntu.34436 > maa03s34-in-f3.1e100.net.http: Flags [.], ack 703, win 63882, length 0
17:38:13.546210 IP maa03s34-in-f3.1e100.net.http > ubuntu.34436: Flags [.], ack 387, win 64240, length 0
Google
https://www.google.com
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Google offered in:
India
Advertising
Business
About
How Search works
Privacy
Terms
Settings

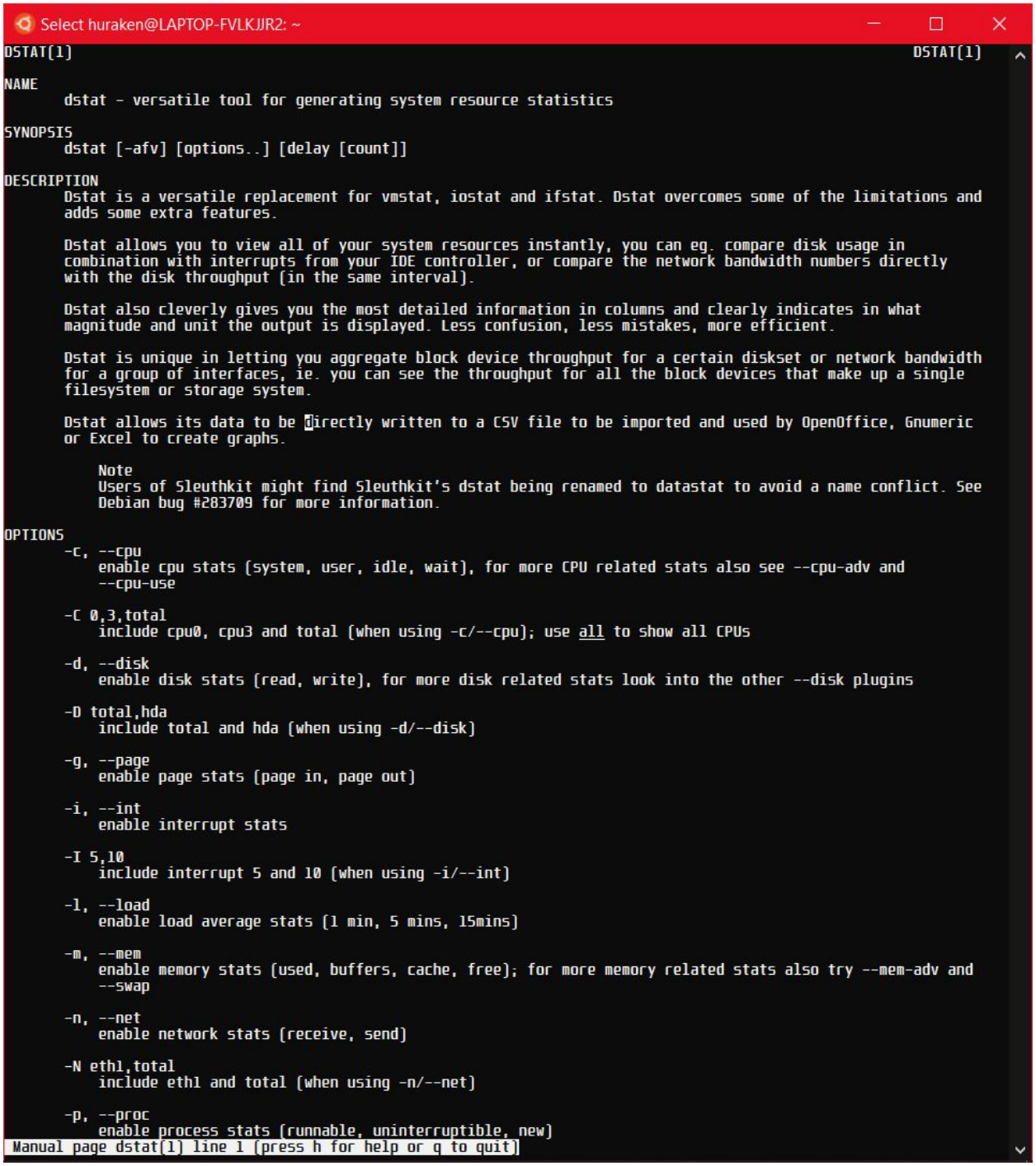
8. Netstat

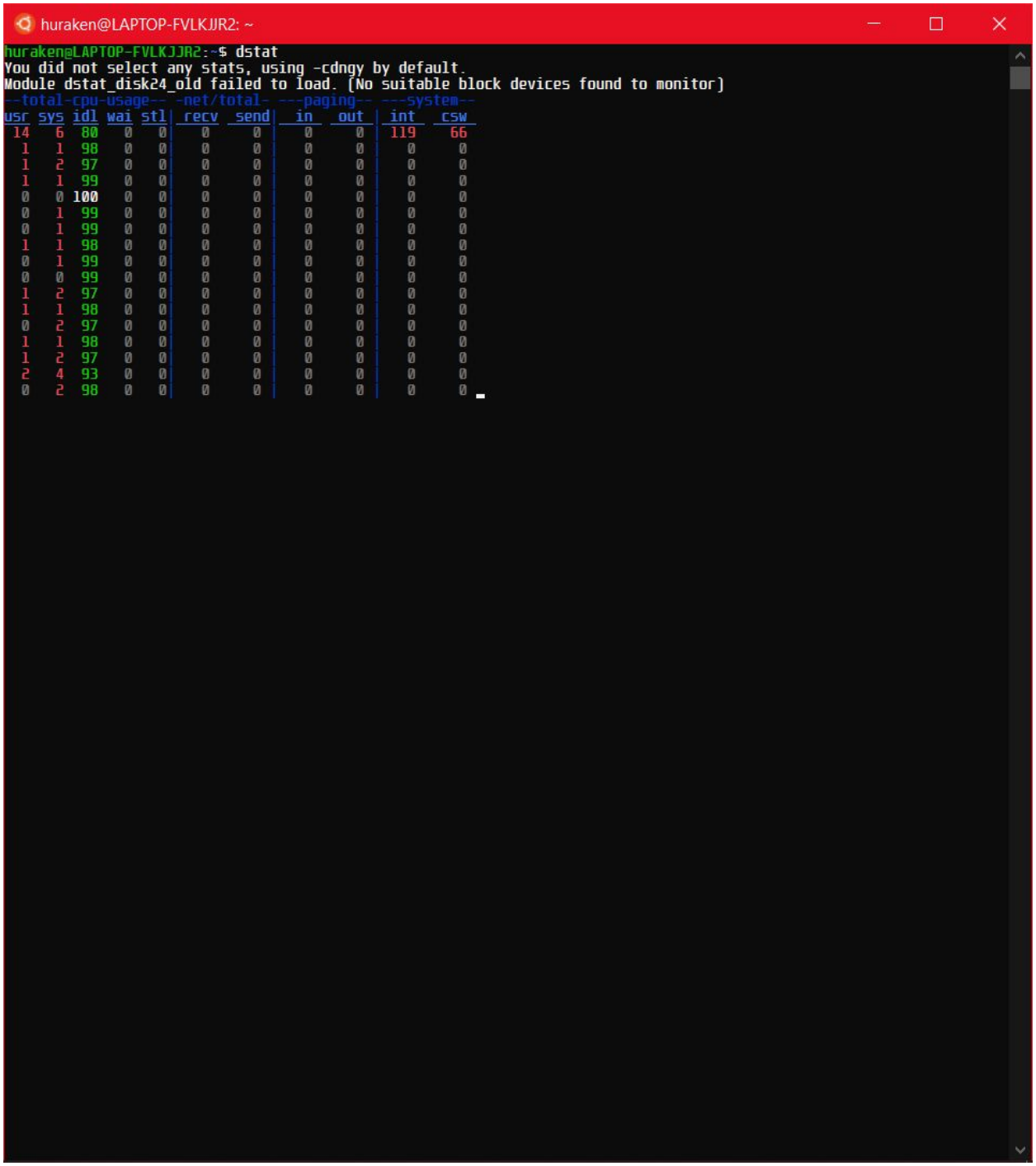
The network statistics (**netstat**) command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and usage statistics are common uses for this command.



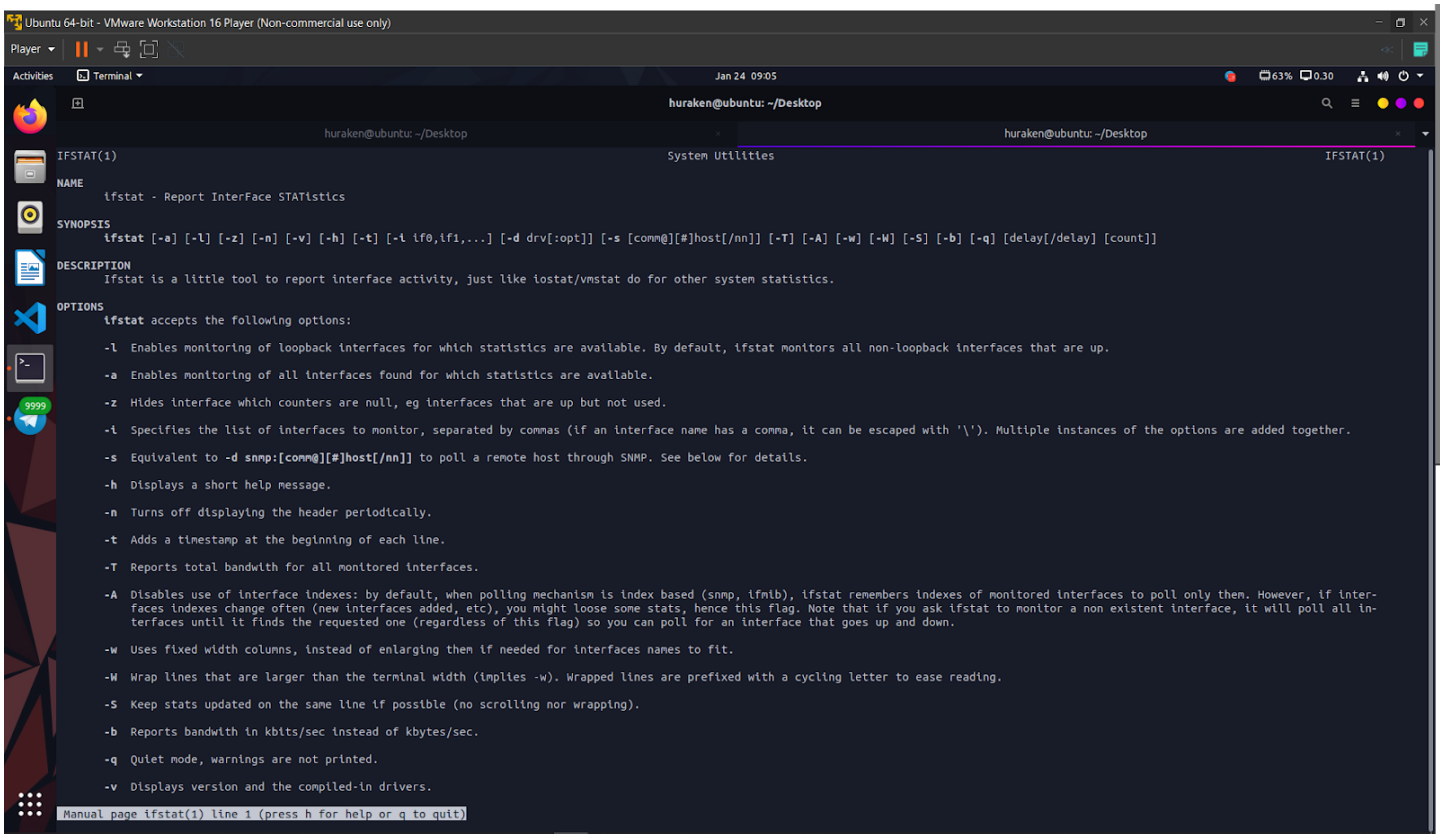
9.Dstat :

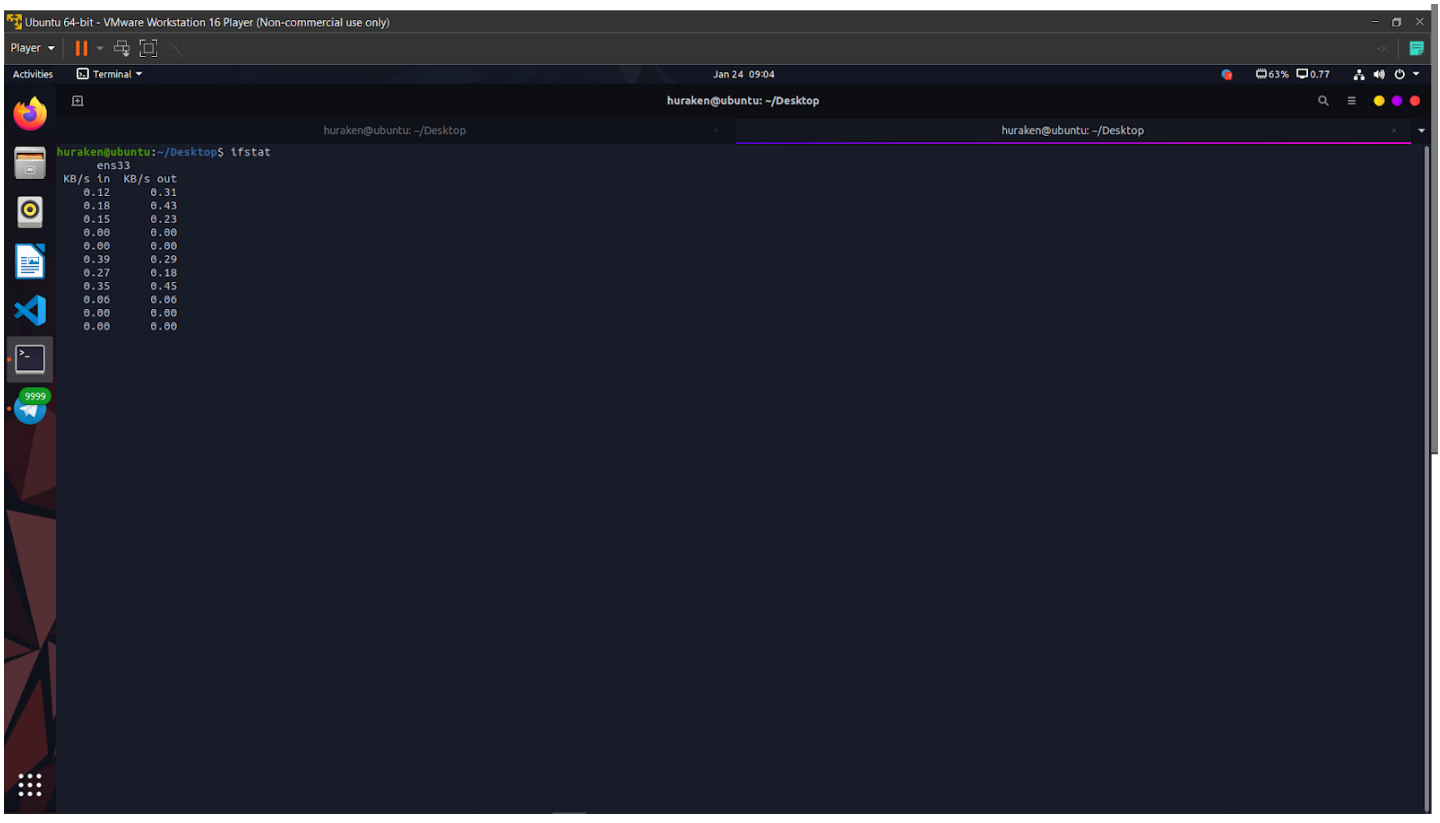
To view all your system resources instantly





10. Ifstat: to show interface activity


Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
Jan 24 09:05
63% 0.30
huraken@ubuntu: ~/Desktop
huraken@ubuntu: ~/Desktop
huraken@ubuntu: ~/Desktop
IFSTAT(1) System Utilities IFSTAT(1)
NAME
ifstat - Report InterFace STATistics
SYNOPSIS
ifstat [-a] [-l] [-z] [-n] [-v] [-h] [-t] [-i if0,if1,...] [-d drv[:opt]] [-s [comm@][#]host[/nn]] [-T] [-A] [-w] [-W] [-S] [-b] [-q] [delay[/delay] [count]]
DESCRIPTION
Ifstat is a little tool to report interface activity, just like iostat/vmstat do for other system statistics.
OPTIONS
ifstat accepts the following options:
-l Enables monitoring of loopback interfaces for which statistics are available. By default, ifstat monitors all non-loopback interfaces that are up.
-a Enables monitoring of all interfaces found for which statistics are available.
-z Hides interface which counters are null, eg interfaces that are up but not used.
-i Specifies the list of interfaces to monitor, separated by commas (if an interface name has a comma, it can be escaped with '\'). Multiple instances of the options are added together.
-s Equivalent to -d snmp:[comm@][#]host[/nn] to poll a remote host through SNMP. See below for details.
-h Displays a short help message.
-n Turns off displaying the header periodically.
-t Adds a timestamp at the beginning of each line.
-T Reports total bandwith for all monitored interfaces.
-A Disables use of interface indexes: by default, when polling mechanism is index based (snmp, ifmib), ifstat remembers indexes of monitored interfaces to poll only them. However, if interfaces indexes change often (new interfaces added, etc), you might loose some stats, hence this flag. Note that if you ask ifstat to monitor a non existent interface, it will poll all interfaces until it finds the requested one (regardless of this flag) so you can poll for an interface that goes up and down.
-w Uses fixed width columns, instead of enlarging them if needed for interfaces names to fit.
-W Wrap lines that are larger than the terminal width (implies -w). Wrapped lines are prefixed with a cycling letter to ease reading.
-S Keep stats updated on the same line if possible (no scrolling nor wrapping).
-b Reports bandwith in kbits/sec instead of kbytes/sec.
-q Quiet mode, warnings are not printed.
-v Displays version and the compiled-in drivers.
Manual page ifstat(1) line 1 (press h for help or q to quit)


Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
Jan 24 09:04
63% 0.77
huraken@ubuntu: ~/Desktop
huraken@ubuntu: ~/Desktop
huraken@ubuntu: ~/Desktop
huraken@ubuntu:~/Desktop$ ifstat
ens33
KB/s in KB/s out
0.12 0.31
0.18 0.43
0.15 0.23
0.00 0.00
0.00 0.00
0.39 0.29
0.27 0.18
0.35 0.45
0.06 0.06
0.00 0.00
0.00 0.00

11. Wget used to retrieve files using HTTP, HTTPS, FTP, FTPS