

## Lab Notebook 2

Submitted By: Shrikrishna Bhat

### Contents

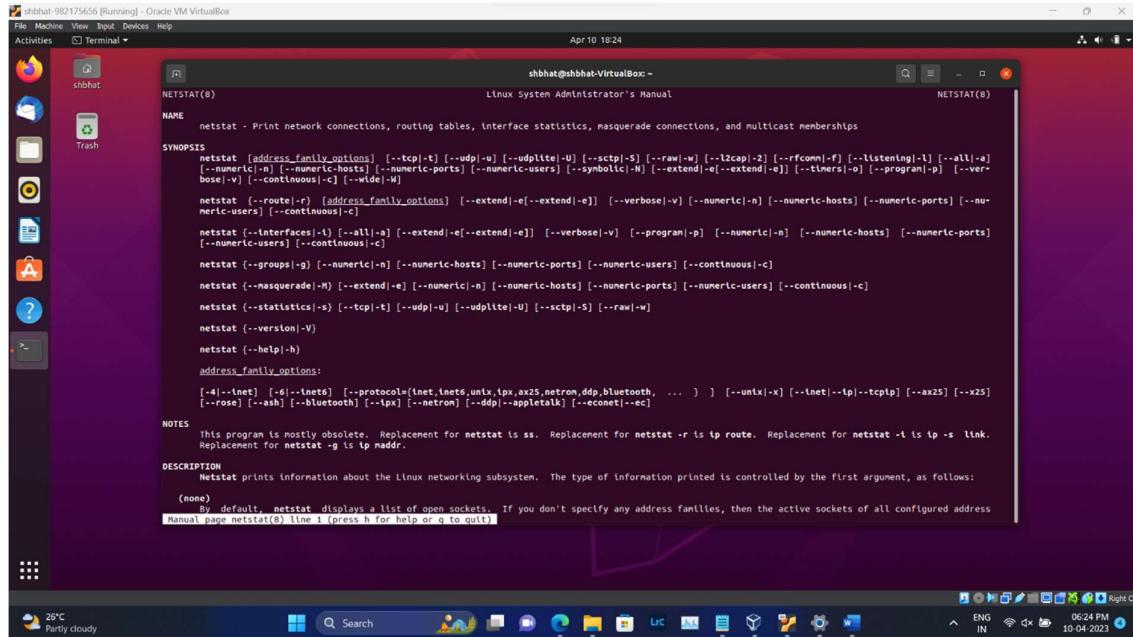
Section 1.....	2
TCP #1 .....	2
1.1 netstat.....	2
1.2 lsof.....	4
1.3 nc.....	5
TCP #2 .....	6
2.1 iperf.....	6
HTTP # 3.....	8
3.1 HTTP developer tools Part 1.....	8
3.2 HTTP developer tools Part 2.....	8
3.3 HTTP developer tools Part 3.....	10
3.4 Asynchronous HTTP requests.....	12
Section 2.....	14
DNS #1.....	14
1.1 dig .....	14
1.2 DNS iterative lookup .....	18
1.3 Reverse DNS Lookup .....	20
1.4 Hosts Enumeration .....	21
DNS #2.....	22
2.1 Geographic DNS.....	22
Network Recap Lab #3 .....	27
3.1 REVERSE DNS.....	27
3.2 ARP and Wireshark.....	29

## Section 1

### TCP #1

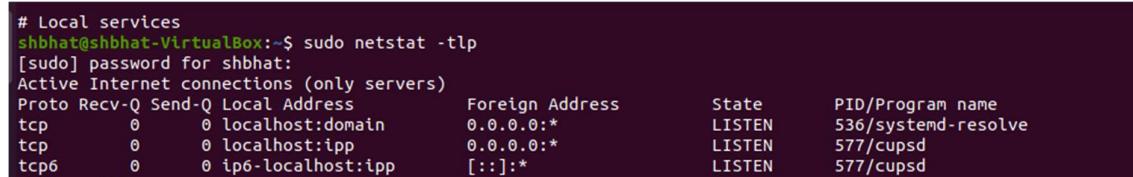
#### 1.1 netstat

##### 1.1.1 man netstat



A screenshot of a Linux desktop environment (Ubuntu) showing a terminal window with the netstat man page. The terminal window title is "NETSTAT(8)". The man page content includes sections for NAME, SYNOPSIS, NOTES, and DESCRIPTION. The NOTES section states: "This program is mostly obsolete. Replacement for netstat is ss. Replacement for netstat -r is ip route. Replacement for netstat -l is ip -s link." The DESCRIPTION section notes: "Netstat prints information about the Linux networking subsystem. The type of information printed is controlled by the first argument, as follows: (none) By default, netstat displays a list of open sockets. If you don't specify any address families, then the active sockets of all configured address families will be listed. netstat(8) line 1 (press h for help or q to quit)." The desktop background shows a purple abstract pattern, and the taskbar at the bottom shows various application icons.

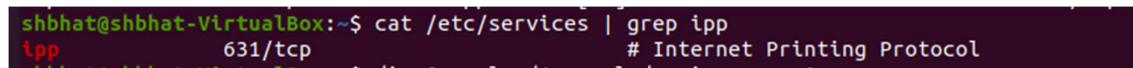
##### 1.1.2 Run the command using sudo and take a screenshot of the output to include in your lab notebook.



```
# Local services
shbhat@shbhat-VirtualBox:~$ sudo netstat -tlp
[sudo] password for shbhat:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp      0      0  localhost:domain        0.0.0.0:*             LISTEN     536/systemd-resolve
tcp      0      0  localhost:ipp          0.0.0.0:*             LISTEN     577/cupsd
tcp6     0      0  ip6-localhost:ipp       [::]:*              LISTEN     577/cupsd
```

##### 1.1.3 For port numbers that are named, examine /etc/services and find the port number that corresponds to it. Include this mapping in your lab notebook.

Answer: I got the port number as 631, which corresponds to ipp.



```
shbhat@shbhat-VirtualBox:~$ cat /etc/services | grep ipp
ipp          631/tcp          # Internet Printing Protocol
```

1.1.4 For ports that only have a number, what service might it be providing based on the name of the program that is being run?

Answer: I did not get any port numbers having only number but on reading about it I found out that it is used to run container services.

1.1.5 Run the netstat command again, but do not use sudo as this is a machine managed by CAT. Include a screenshot of the output.

```
shbhat@ada:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0  ada.cs.pdx.edu:ssh      172.36.151.24:2572  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      16.200.238.61:50219  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:4448     tanto.cs.pdx.postgresql:  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      70.219.13.10:5848    ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      c-07-101-106-103:49972  ESTABLISHED
tcp        0      0  localhost.localdo:52698   localhost.localdo:37705  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      172.36.77.159:59844   ESTABLISHED
tcp        0      0  localhost.localdo:52610   localhost.localdo:52610  ESTABLISHED
tcp        0      0  localhost.localdo:6918    localhost.localdo:44914  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      168.103.229.191:p50138  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      172.36.151.189:62671  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:22224   tanto.cs.pdx.postgresql:  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      223.126.256.35.bc19836  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      16.208.56.17:63358   ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:52036   tanto.cs.pdx.postgresql:  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      172.36.151.24:2572  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      71.237.152.53:5674    ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      staticc-50-53-6-15:12663  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      50-39-190-193.bvt:64449  ESTABLISHED
tcp        0      0  localhost.localdo:37705   staticc-50-53-6-15:12660  ESTABLISHED
tcp        0      0  localhost.localdo:37705   localhost.localdo:52698  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      16.200.215.175:53918  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      16.200.78.51:50457   ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      64.182.140.101:51552  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      192.56.44.5:68871    ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      16.208.97.172:5647   ESTABLISHED
tcp        0      0  localhost.localdo:47698   localhost.localdom:17  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      172.36.151.24:2572  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:55702   tanto.cs.pdx.postgresql:  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      staticc-50-53-6-15:25108  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      c-24-20-12-17.hsd1.comcast.net:62611  ESTABLISHED
tcp        0      0  localhost.localdo:6017   localhost.localdo:6017  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      c-71-191-198-157.53362  ESTABLISHED
tcp        0      0  localhost.localdom:6011  localhost.localdo:47268  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:35580   tanto.cs.pdx.postgresql:  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:35586   silverfire.cck.100.100.144.144:443  ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      10.0.73.15:51050   ESTABLISHED
tcp        0      0  ada.cs.pdx.edu:ssh      staticc-50-53-6-15:58268  ESTABLISHED
```

```
shbhat@ada:~$ netstat -an
File Machine View Input Devices Help
shbhat@shbhat-VirtualBox:~$ ssh-agent ssh-copy-id ssh-keyscan
shbhat@shbhat-VirtualBox:~$ ssh-add ssh-argve ssh-keygen
shbhat@shbhat-VirtualBox:~$ ssh linux.cs.pdx.edu
shbhat@linux.cs.pdx.edu's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-69-generic x86_64)

=====
This machine is for the exclusive use of those associated with
the Maseeh College of Engineering and Computer Science.

ALL ACTIVITY MAY BE RECORDED
=====
* CAT Support: https://cat.pdx.edu/
* Email: support@cat.pdx.edu
* Phone: 503-725-5420
* Chat: https://support.cat.pdx.edu
* Location: FAB 82-01

Last login: Thu Apr 13 19:41:14 2023 from c-71-193-198-157.hsd1.or.comcast.net
shbhat@ada:~$ netstat -lnp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
tcp        0      0  0.0.0.0:49311        0.0.0.0:*          LISTEN     -
tcp        0      0  0.127.0.0.1:25        0.0.0.0:*          LISTEN     -
tcp        0      0  0.127.0.0.1:631       0.0.0.0:*          LISTEN     -
tcp        0      0  0.127.0.0.1:6613      0.0.0.0:*          LISTEN     -
tcp        0      0  0.127.0.0.1:6612      0.0.0.0:*          LISTEN     -
tcp        0      0  0.127.0.0.1:6615      0.0.0.0:*          LISTEN     -
tcp        0      0  0.127.0.0.1:6611      0.0.0.0:*          LISTEN     -
tcp        0      0  0.127.0.0.1:6610      0.0.0.0:*          LISTEN     -
tcp        0      0  0.127.0.0.1:42711    0.0.0.0.*          LISTEN     -
tcp        0      0  0.0.0.0:22          0.0.0.0.*          LISTEN     -
tcp        0      0  0.0.0.0:111         0.0.0.0.*          LISTEN     -
tcp        0      0  0.127.0.0.53:53      0.0.0.0.*          LISTEN     -
tcp6       0      0  ::1:51701          ::*:*              LISTEN     -
tcp6       0      0  ::1::22            ::*:*              LISTEN     -
tcp6       0      0  ::1::113           ::*:*              LISTEN     -
tcp6       0      0  ::1::111           ::*:*              LISTEN     -
tcp6       0      0  ::1::6010          ::*:*              LISTEN     -
tcp6       0      0  ::1::6011          ::*:*              LISTEN     -
tcp6       0      0  ::1::6012          ::*:*              LISTEN     -
tcp6       0      0  ::1::6013          ::*:*              LISTEN     -
tcp6       0      0  ::1::6015          ::*:*              LISTEN     -
tcp6       0      0  ::1::631           ::*:*              LISTEN     -
tcp6       0      0  ::1::25            ::*:*              LISTEN     -
shbhat@ada:~$
```

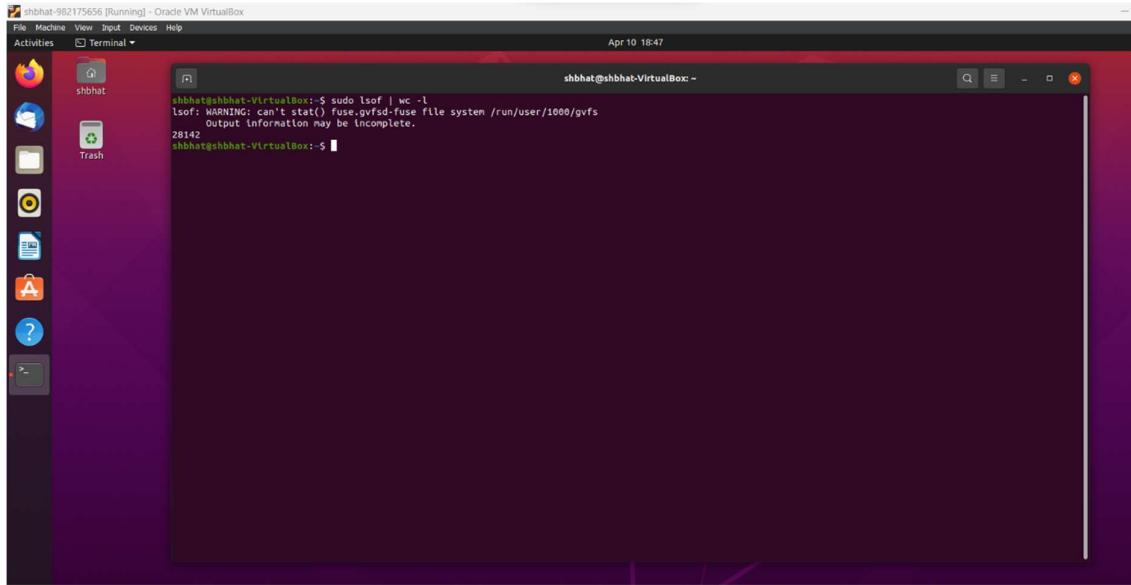
### 1.1.6 What services does this machine provide for external access?

Answer:

It depends on which port the services are being run, some may provide container service. Some may provide IPP service etc.

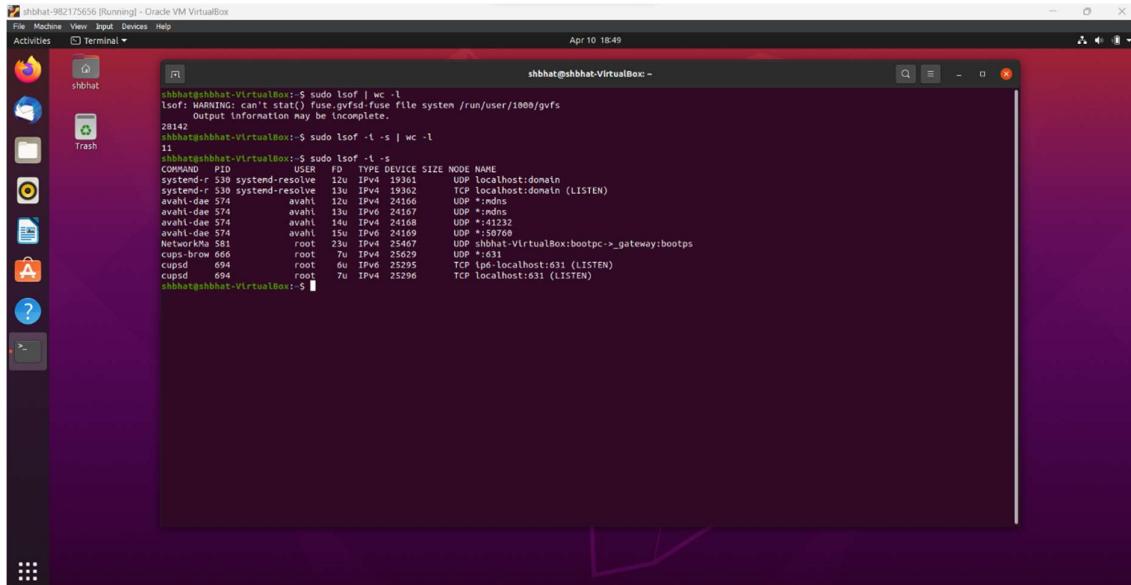
### 1.2 lsof

#### 1.2.1 sudo lsof | wc -l



```
shbhat@shbhat-VirtualBox:~$ sudo lsof | wc -l
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
          Output information may be incomplete.
28142
shbhat@shbhat-VirtualBox:~$
```

#### 1.2.2 Use the -i and the -s flag of lsof to generate a listing that is equivalent to the one generated with netstat previously and include it in your lab notebook



```
shbhat@shbhat-VirtualBox:~$ sudo lsof | wc -l
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
          Output information may be incomplete.
28142
shbhat@shbhat-VirtualBox:~$ sudo lsof -i -s | wc -l
11
shbhat@shbhat-VirtualBox:~$ sudo lsof -i -s
COMMAND PID   USER   FD   TYPE DEVICE SIZE NODE NAME
CupsAndP  520   root    1u  IPv4  19361      UDP localhost:domain
systemd-resolve  12u  IPv4  19361      UDP localhost:domain (LISTEN)
systemd-resolve  13u  IPv4  19362      TCP localhost:domain (LISTEN)
avahi-dae  574   avahi   12u  IPv4  24166      UDP *:mdns
avahi-dae  574   avahi   13u  IPv4  24167      UDP *:5353
avahi-dae  574   avahi   14u  IPv4  24168      UDP *:41232
avahi-dae  574   avahi   15u  IPv6  24169      UDP *:50769
NetworkM  581   root    23u  IPv4  25467      UDP shbhat-VirtualBox:bootpc->_gateway:bootps
cups-brow  666   root    7u  IPv4  25629      UDP *:631
CupsAndP  694   root    6u  IPv6  52359      TCP [::1]:631 (LISTEN)
cupsd    694   root    7u  IPv4  52296      TCP localhost:631 (LISTEN)
shbhat@shbhat-VirtualBox:~$
```

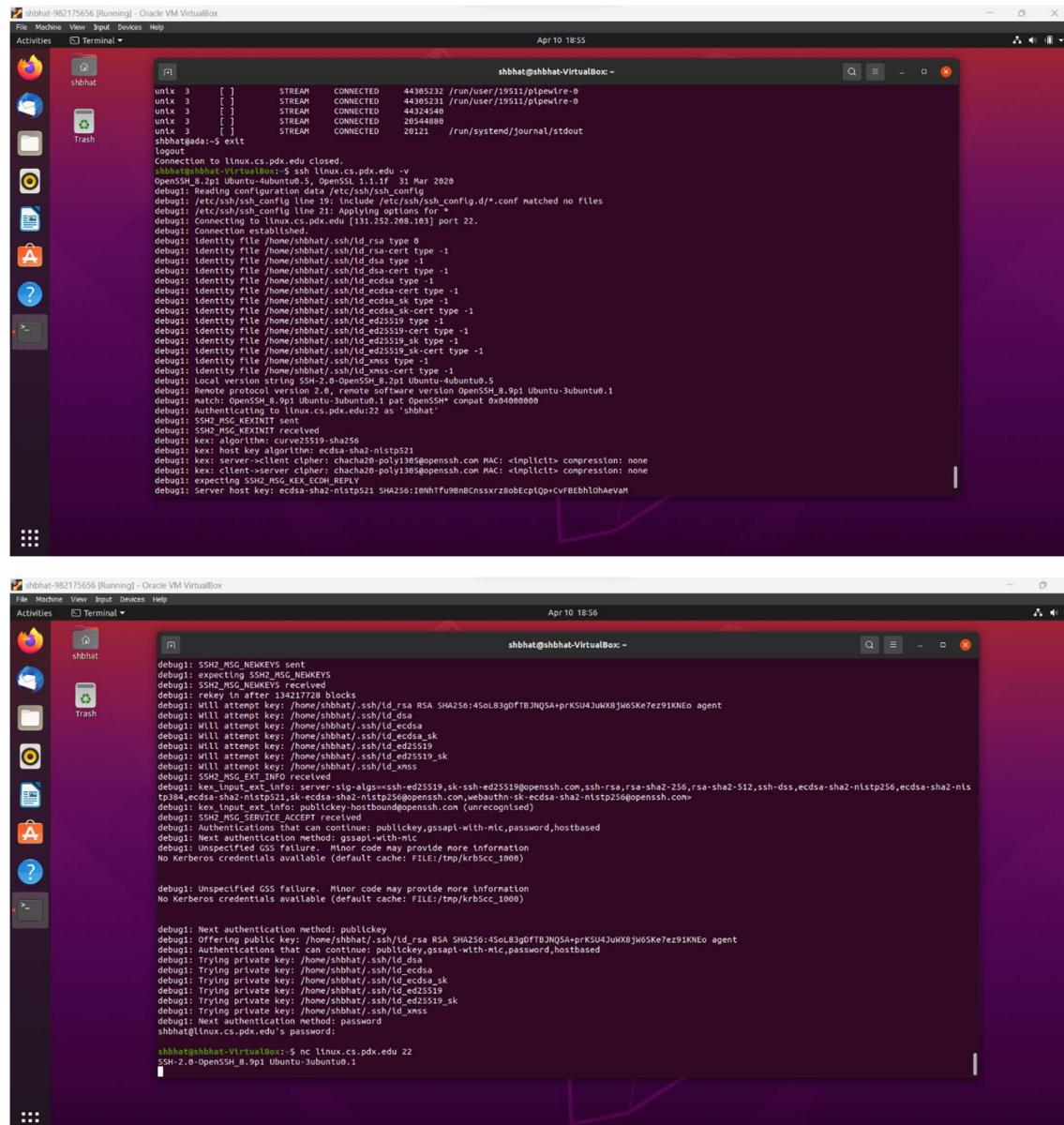
1.3 nc

1.3.1 Include for your lab notebook, the version of ssh that is being used. (Type Ctrl+c to exit)

Answer:

Port 22 is being used.

SSh version - SSH-2.0-OpenSSH\_8.9p1 is found.



```
shbhat@shbhat-VirtualBox:~
```

```
shbhat@shbhat:~$ nc linux.cs.pdx.edu 22
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
```

```
shbhat@shbhat-VirtualBox:~
```

```
shbhat@shbhat:~$ ssh -v
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Include /etc/ssh/ssh_config.d/*
debug1: Applying options for *
debug1: Connecting to linux.cs.pdx.edu [131.252.208.103] port 22.
debug1: Connection established.
debug1: identity file /home/shbhat/.ssh/id_rsa type 0
debug1: identity file /home/shbhat/.ssh/id_dsa type -1
debug1: identity file /home/shbhat/.ssh/id_ecdsa type -1
debug1: identity file /home/shbhat/.ssh/id_ecdsa-cert type -1
debug1: identity file /home/shbhat/.ssh/id_ed25519 type -1
debug1: identity file /home/shbhat/.ssh/id_ed25519-cert type -1
debug1: identity file /home/shbhat/.ssh/id_ed25519-sk type -1
debug1: identity file /home/shbhat/.ssh/id_ed25519-sk-cert type -1
debug1: identity file /home/shbhat/.ssh/id_x509 type -1
debug1: identity file /home/shbhat/.ssh/id_x509-cert type -1
debug1: remote protocol version 2.0, remote software version OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
debug1: match: OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 pat OpenSSH* compat 0x04000000
debug1: Authenticating to linux.cs.pdx.edu:22 as 'shbhat'
debug1: SSH2_MSG_KEXINIT received
debug1: Kex algorithm: curve25519-sha256
debug1: kex host key algorithm: ecdsa-sha2-nistp521
debug1: kex server key algorithm: ecdsa-sha2-nistp521
debug1: kex client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
shbhat@shbhat:~$
```

```
shbhat@shbhat-VirtualBox:~
```

```
shbhat@shbhat:~$ debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: host key algorithm: ecdsa-sha2-nistp521
debug1: rekey after 134217728 blocks
debug1: Will attempt key /home/shbhat/.ssh/id_rsa RSA SHA256:45oL83gDFTBjNQ5A+prKSU4JukX8jW65Ke7e91KNEo agent
debug1: Will attempt key /home/shbhat/.ssh/id_dsa DSA SHA256:zPwZGqfC9kV00yMnRzJLcOOGdIwQm
debug1: Will attempt key /home/shbhat/.ssh/id_ecdsa_sk ECDsa SHA256:zPwZGqfC9kV00yMnRzJLcOOGdIwQm
debug1: Will attempt key /home/shbhat/.ssh/id_ecdsa_sk-cert ECDsa-SHA256:zPwZGqfC9kV00yMnRzJLcOOGdIwQm
debug1: Will attempt key /home/shbhat/.ssh/id_ed25519 Ed25519 SHA256:45oL83gDFTBjNQ5A+prKSU4JukX8jW65Ke7e91KNEo agent
debug1: Will attempt key /home/shbhat/.ssh/id_ed25519-cert Ed25519-SHA256:45oL83gDFTBjNQ5A+prKSU4JukX8jW65Ke7e91KNEo agent
debug1: Will attempt key /home/shbhat/.ssh/id_x509 X509 SHA256:45oL83gDFTBjNQ5A+prKSU4JukX8jW65Ke7e91KNEo agent
debug1: Will attempt key /home/shbhat/.ssh/id_x509-cert X509-SHA256:45oL83gDFTBjNQ5A+prKSU4JukX8jW65Ke7e91KNEo agent
debug1: key_input_ext_info: server-sig-algs=ssh-ed25519,sk-ssh-ed25519@openssh.com,ssh-rsa,rsa-sha2-256,rsa-sha2-512,ssh-dss,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ecdsa-sha2-nistp256@openssh.com,webauthn-sk-ecdsa-sha2-nistp256@openssh.com
debug1: key_input_ext_info: pubkeykey/hostbound@openssh.com (unrecognized)
debug1: Authentication that can continue: publickey,gssapi-with-mic,password,hostbased
debug1: Next authentication method: gssapi-with-mic
debug1: Unspecified GSS failure. Minor code may provide more information
No Kerberos credentials available (default cache: FILE:/tmp/krb5cc_1000)

debug1: Next authentication method: publickey
debug1: Offering public key: /home/shbhat/.ssh/id_rsa RSA SHA256:45oL83gDFTBjNQ5A+prKSU4JukX8jW65Ke7e91KNEo agent
debug1: We have matching publickey key, can continue, offered publickey,gssapi-with-mic,password,hostbased
debug1: Trying private key: /home/shbhat/.ssh/id_dsa DSA
debug1: Trying private key: /home/shbhat/.ssh/id_ecdsa_sk ECDsa
debug1: Trying private key: /home/shbhat/.ssh/id_ecdsa_sk-cert ECDsa-SHA256:45oL83gDFTBjNQ5A+prKSU4JukX8jW65Ke7e91KNEo agent
debug1: Trying private key: /home/shbhat/.ssh/id_x509 X509
debug1: Trying private key: /home/shbhat/.ssh/id_x509-cert X509-SHA256:45oL83gDFTBjNQ5A+prKSU4JukX8jW65Ke7e91KNEo agent
debug1: Next authentication method: password
shbhat@linux.cs.pdx.edu's password:
```

```
shbhat@shbhat-VirtualBox:~$ nc linux.cs.pdx.edu 22
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
```

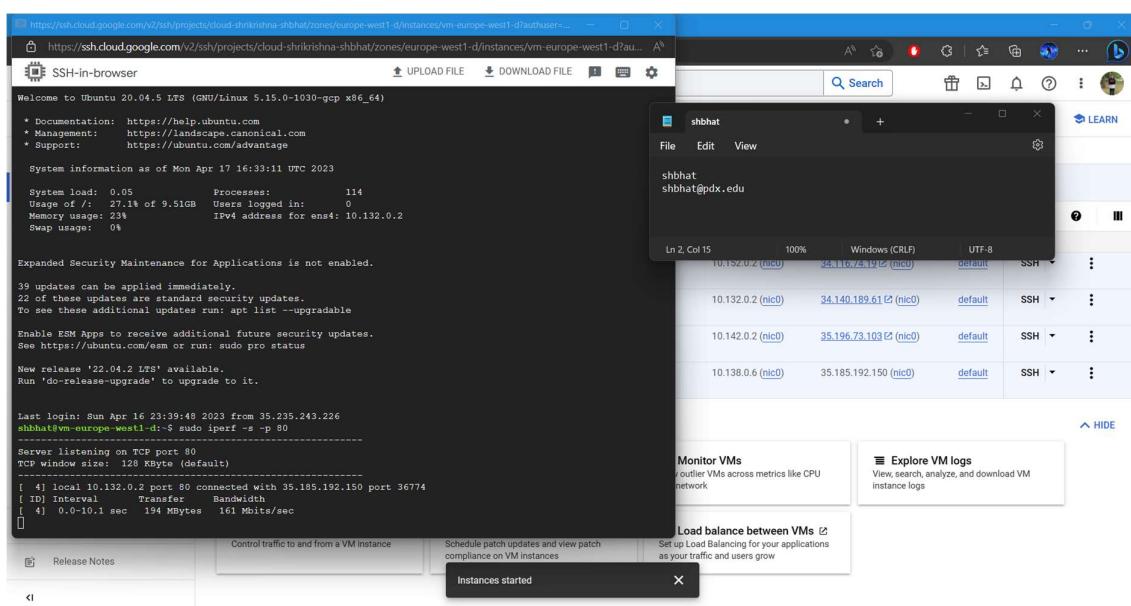
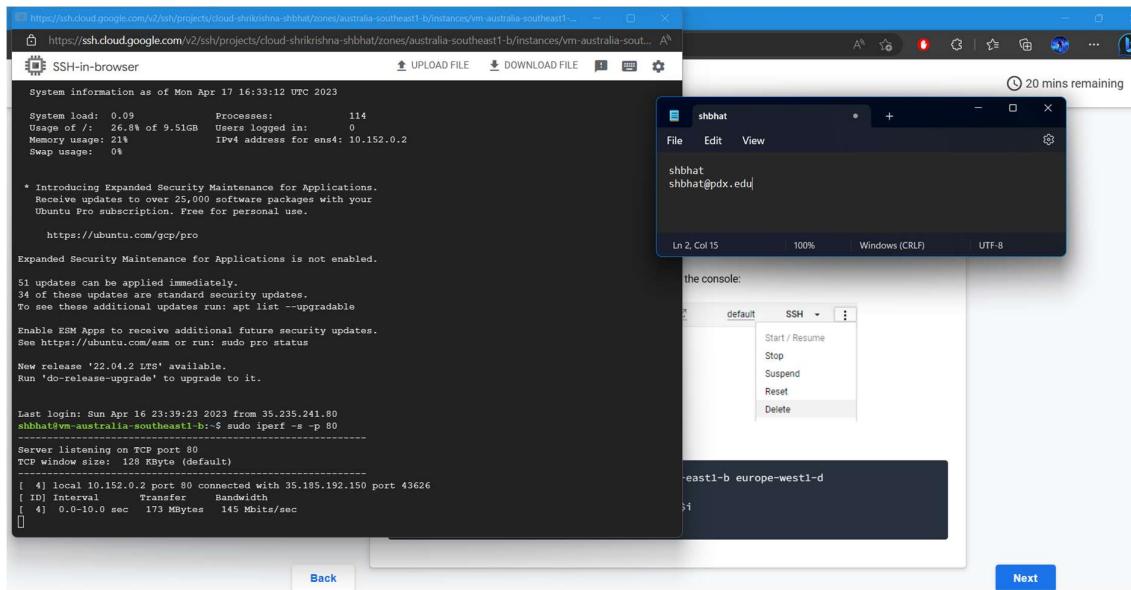
## TCP #2

### 2.1 iperf

#### 2.1.1 – Install iperf in all cloud instances.

Answer: Installed and checked it.

2.1.2 Show a screenshot of the measured bandwidth available between your us-west1-b VM and each of the other Compute Engine VMs. Explain the relative differences (or lack thereof) in your results.



```

https://ssh.cloud.google.com/v2/ssh/projects/cloud-shrkrishna-shbhat/zones/us-east1-b/instances/vm-us-east1-b?authuser=1&... A
https://ssh.cloud.google.com/v2/ssh/projects/cloud-shrkrishna-shbhat/zones/us-east1-b/instances/vm-us-east1-b?authuser=1&...
SSH-in-browser UPLOAD FILE DOWNLOAD FILE
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Mon Apr 17 16:33:08 UTC 2023
System load: 0.09 Processes: 116
Usage of /: 26.8% of 9.51GB Users logged in: 0
Memory usage: 21% IPv4 address for ens4: 10.142.0.2
Swap usage: 0%
Expanded Security Maintenance for Applications is not enabled.
51 updates can be applied immediately.
34 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Apr 16 23:39:30 2023 from 35.235.240.64
shbhat@vm-us-east1-b:~$ sudo iperf -s -p 80
-----
Server listening on TCP port 80
TCP window size: 128 KByte (default)
[ 4] local 10.142.0.2 port 80 connected with 35.185.192.150 port 54118
[ 5] local 10.142.0.2 port 80 connected with 179.43.177.243 port 49866 (peer 14384.3338.21875-rc)
[ ID] Interval Transfer Bandwidth
[ 4] 0.0-0.10 sec 407 MBbytes 341 Mbit/s/sec
[ 5] 0.0-0.10 sec 67.0 Bytes 53.6 bits/sec
[ ] 
shbhat@vm-us-east1-b:~$ 
Control traffic to and from a VM instance
Schedule patch updates and view patch compliance on VM instances
Instances started X

```

```

https://ssh.cloud.google.com/v2/ssh/projects/cloud-shrkrishna-shbhat/zones/us-west1-b/instances/vm-us-west1-b?authuser=1... A
https://ssh.cloud.google.com/v2/ssh/projects/cloud-shrkrishna-shbhat/zones/us-west1-b/instances/vm-us-west1-b?authuser=1...
SSH-in-browser UPLOAD FILE DOWNLOAD FILE
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Mon Apr 17 16:33:08 UTC 2023
System load: 0.09 Processes: 116
Usage of /: 26.8% of 9.51GB Users logged in: 0
Memory usage: 21% IPv4 address for ens4: 10.142.0.2
Swap usage: 0%
Expanded Security Maintenance for Applications is not enabled.
51 updates can be applied immediately.
34 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Apr 16 23:39:35 2023 from 35.235.244.1
shbhat@vm-us-west1-b:~$ sudo iperf -c 34.116.74.19 -p 80
-----
Client connecting to 34.116.74.19, TCP port 80
TCP window size: 85.0 KByte (default)
[ 3] local 10.138.0.6 port 43624 connected with 34.116.74.19 port 80
[ ID] Interval Transfer Bandwidth
[ 3] 0.0-0.1 sec 173 MBbytes 145 Mbit/s/sec
shbhat@vm-us-west1-b:~$ sudo iperf -c 34.140.189.61 -p 80
-----
Client connecting to 34.140.189.61, TCP port 80
TCP window size: 85.0 KByte (default)
[ 3] local 10.138.0.6 port 36774 connected with 34.140.189.61 port 80
[ ID] Interval Transfer Bandwidth
[ 3] 0.0-0.1 sec 194 MBbytes 161 Mbit/s/sec
shbhat@vm-us-west1-b:~$ sudo iperf -c 35.196.73.103 -p 80
-----
Client connecting to 35.196.73.103, TCP port 80
TCP window size: 85.0 KByte (default)
[ 3] local 10.138.0.6 port 54118 connected with 35.196.73.103 port 80
[ ID] Interval Transfer Bandwidth
[ 3] 0.0-0.1 sec 107 MBbytes 341 Mbit/s/sec
shbhat@vm-us-west1-b:~$ 
Control traffic to and from a VM instance
Schedule patch updates and view patch compliance on VM instances
Instances started X

```

Why relative differences?

Answer:

There are various causes for differences in bandwidth, it might be due to distance since it might have to fetch from nearby server or distant server. It might also be due to congestion of packets. It might also be due to the quality of the network connection. Networks with higher latency or packet loss rates can result in reduced bandwidth or less consistent bandwidth measurements. It might also be due to not choosing the optimal routing path which can cause more traffic and there might be reduced bandwidth.

## HTTP # 3

### 3.1 HTTP developer tools Part 1

#### 3.1.1 What is the URL being requested?

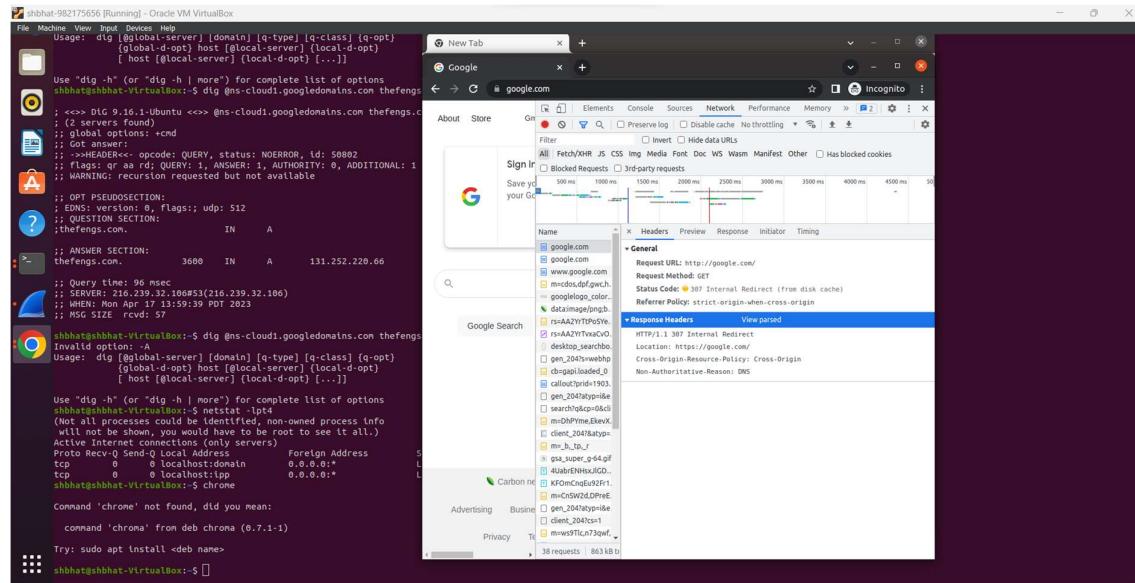
Answer: URL being requested is: <http://google.com/>

#### 3.1.2 What is the HTTP status code in the response and what does it mean?

Answer: Status code 307 Internal Redirect

#### 3.1.3 Look up the status code. Show the associated HTTP response header that is sent in conjunction with this status code for the request.

Answer:



### 3.2 HTTP developer tools Part 2

#### 3.2.1 What is the URL being requested? Is it using HTTP or HTTPS?

Answer: HTTPS

#### 3.2.2 What are the Host: (HTTP 1.1) or: authority: (HTTP 2.0) headers sent by the browser? What is the User-Agent: HTTP header that is sent?

Answer: User agent is mozilla/5.0

Authority: google.com

```

shbhat@shbhat-VirtualBox:~$ dig ns-cloud1.googledomains.com thefengs
...
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 512
; QUESTION SECTION:
;thefengs.com. IN A
...
; ANSWER SECTION:
thefengs.com. 3600 IN A 131.252.220.66
...
shbhat@shbhat-VirtualBox:~$ dig ns-cloud1.googledomains.com thefengs
Invalid option: -A
Usage: dig [[@global-server] | [domain] [q-type] [q-class] [q-opt]
          {[@global-d-opt] host [@local-server] [local-d-opt]
          [ host [@local-server] [local-d-opt] [...]}]
...
shbhat@shbhat-VirtualBox:~$ netstat -lpt4
(Not all processes could be identified, non-owned process info
will not be shown, you may need root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp      0      0 localhost:domain          0.0.0.0:*
tcp      0      0 localhost:tcp            0.0.0.0:*
...
shbhat@shbhat-VirtualBox:~$ chrome
Command 'chrome' not found, did you mean:
  command 'chroma' from deb chroma (0.7.1-1)
Try: sudo apt install <deb name>
shbhat@shbhat-VirtualBox:~$ 

```

The Network tab in the developer tools shows a request to `google.com`. The Headers section includes:

- `Host: google.com`
- `Accept: */*`
- `Accept-Encoding: gzip, deflate, br`
- `Accept-Language: en-US,en;q=0.9`
- `Sec-CH-UA: "Chromium";v="112", "Google Chrome";v="112", "Not:A-Brand";v="99"`
- `Sec-CH-UA-Arch: "x86"`
- `Sec-CH-UA-Bitwidth: "64"`
- `Sec-CH-UA-Full-Version-List: "Chromium";v="112.0.5615.49", "Google Chrome";v="112.0.5615.49", "Not:A-Brand";v="99.0.0.0"`
- `Sec-CH-UA-Mobile: "0"`
- `Sec-CH-UA-Model: "`
- `Sec-CH-UA-Platform: "Linux"`
- `Sec-CH-UA-Platform-Version: "5.15.0"`
- `Sec-CH-UA-Wow64: 70`

```

shbhat@shbhat-VirtualBox:~$ dig ns-cloud1.googledomains.com thefengs
...
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 512
; QUESTION SECTION:
;thefengs.com. IN A
...
; ANSWER SECTION:
thefengs.com. 3600 IN A 131.252.220.66
...
shbhat@shbhat-VirtualBox:~$ dig ns-cloud1.googledomains.com thefengs
Invalid option: -A
Usage: dig [[@global-server] | [domain] [q-type] [q-class] [q-opt]
          {[@global-d-opt] host [@local-server] [local-d-opt]
          [ host [@local-server] [local-d-opt] [...]}]
...
shbhat@shbhat-VirtualBox:~$ netstat -lpt4
(Not all processes could be identified, non-owned process info
will not be shown, you may need root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp      0      0 localhost:domain          0.0.0.0:*
tcp      0      0 localhost:tcp            0.0.0.0:*
...
shbhat@shbhat-VirtualBox:~$ chrome
Command 'chrome' not found, did you mean:
  command 'chroma' from deb chroma (0.7.1-1)
Try: sudo apt install <deb name>
shbhat@shbhat-VirtualBox:~$ 

```

The Network tab in the developer tools shows a request to `google.com`. The Headers section includes:

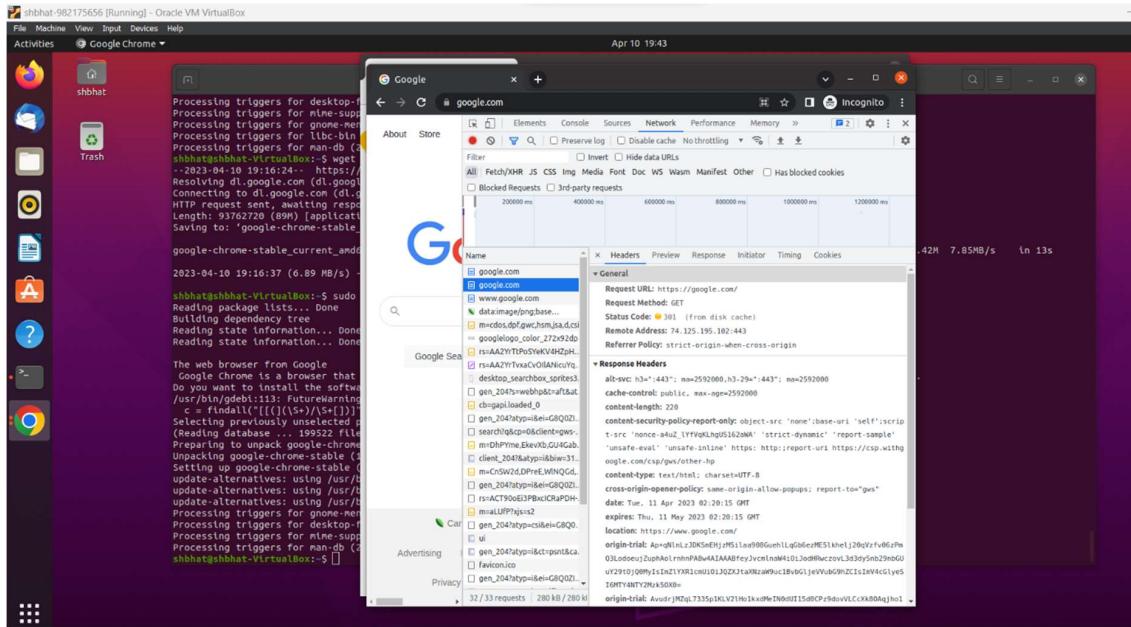
- `Host: google.com`
- `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8`
- `Accept-Encoding: gzip, deflate, br`
- `Accept-Language: en-US,en;q=0.9`
- `Sec-CH-UA: "Chromium";v="112", "Google Chrome";v="112", "Not:A-Brand";v="99"`
- `Sec-CH-UA-Arch: "x86"`
- `Sec-CH-UA-Bitwidth: "64"`
- `Sec-CH-UA-Full-Version-List: "Chromium";v="112.0.5615.49", "Google Chrome";v="112.0.5615.49", "Not:A-Brand";v="99.0.0.0"`
- `Sec-CH-UA-Mobile: "0"`
- `Sec-CH-UA-Model: "`
- `Sec-CH-UA-Platform: "Linux"`
- `Sec-CH-UA-Platform-Version: "5.15.0"`
- `Sec-CH-UA-Wow64: 70`

3.2.3 What is the HTTP status code in the response and what does it mean? Is it different from the first status code? If so, what is the semantic difference?

Answer: 301, it is different from first status code.

301 redirect is a permanent redirect, while a 307 redirect is a temporary redirect. If you are permanently moving a page to a new location, use a 301 redirect. If you are temporarily moving a page to a new location, use a 307 redirect.

3.2.4 Show the associated HTTP response header that is sent in conjunction with this status code for the request.



### 3.3 HTTP developer tools Part 3

#### 3.3.1 What is the URL being requested? Is it using HTTP or HTTPS?

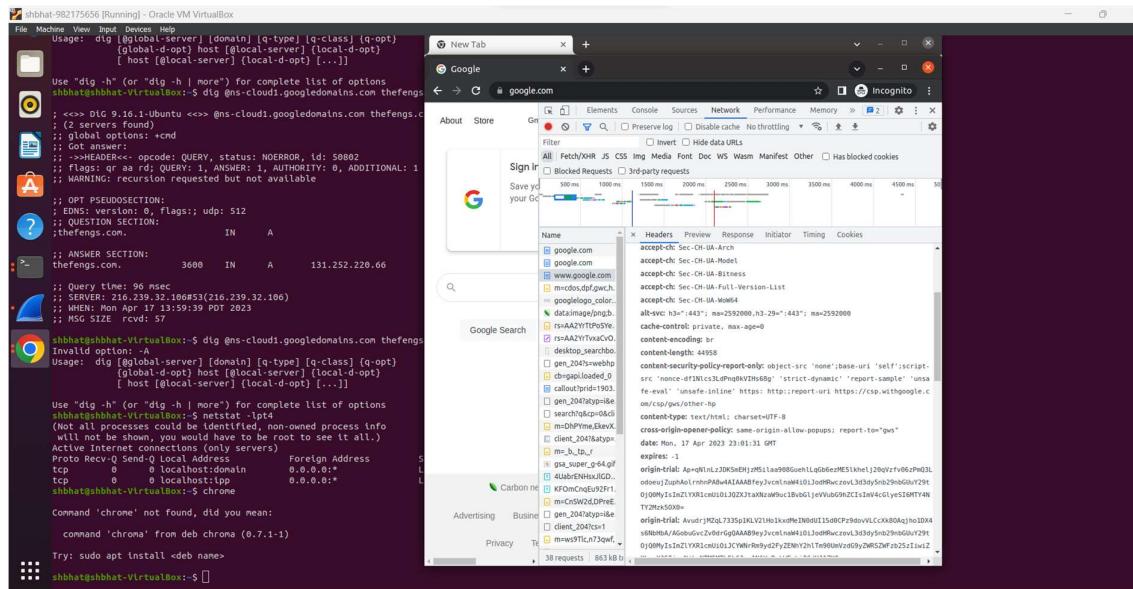
Answer: <https://google.com>, it is using HTTPS.

#### 3.3.2 What is the HTTP status code in the response?

Answer: Status code 200

#### 3.3.3 Look for an alt-svc: HTTP response header. Does the server believe the client can use HTTP3/QUIC?

Answer: On looking at the alt-svc, we can see that server believes that client can use HTTP3 since we can see the value h3 there.



3.3.4 Examine the HTTP response headers for cookies. Show the cookies that are set and which ones specify that no SameSite restrictions are in place. What does the setting indicate about the cookies that are set?

Answer:

On examining the cookies we can see that there are two values ‘lax’ and ‘none’.

Lax - Means that the cookie is not sent on cross-site requests, such as on requests to load images or frames, but is sent when a user is navigating to the origin site from an external site (for example, when following a link). This is the default behaviour if the SameSite attribute is not specified.

None - means that the browser sends the cookie with both cross-site and same-site requests. The Secure attribute must also be set when setting this value, like so SameSite=None; Secure. If Secure is missing an error will be logged.

Source : [Set-Cookie - HTTP | MDN \(mozilla.org\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)

```

shbhui1-902175656 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Usage: dig {global-server} {domain} {q-type} {q-class} {q-opt}
        {global-d-opt} host {@local-server} {local-d-opt}
        [ host {@local-server} {local-d-opt} [...]
]

Use "dig -h" (or "dig -h | more") for complete list of options
shbhui1-902175656 [Running] - Oracle VM VirtualBox
; <>> DIG 9.16.1-Ubuntu <>> @ns-cloudi.googledomains.com thefengs.
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 50802
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 512
;; QUESTION SECTION:
;thefengs.com. IN A
;; ANSWER SECTION:
thefengs.com. 3600 IN A 131.252.220.06
;; Query time: 96 msec
;; SERVER: 216.239.32.106#53(216.239.32.106)
;; WHEN: Mon Apr 17 13:59:39 PDT 2023
;; MSG SIZE rcvd: 57

shbhui1-902175656 [Running] - Oracle VM VirtualBox
$ dig @ns-cloudi.googledomains.com thefengs.
Invalid option: -A
Usage: dig {global-server} {domain} {q-type} {q-class} {q-opt}
        {global-d-opt} host {@local-server} {local-d-opt}
        [ host {@local-server} {local-d-opt} [...]
]

Use "dig -h" (or "dig -h | more") for complete list of options
shbhui1-902175656 [Running] - Oracle VM VirtualBox
$ netstat -lpt4
(Not all processes could be identified, non-owned process info
 will not be shown, you may have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address      State       PID/Program name
tcp      0      0  localhost:domain          0.0.0.0:*
          0      0  localhost:tip             0.0.0.0:*
shbhui1-902175656 [Running] - Oracle VM VirtualBox
$ chrome

Command 'chrome' not found, did you mean:
  command 'chrome' from deb chrome (0.7.1-1)

Try: sudo apt install <deb name>
shbhui1-902175656 [Running] - Oracle VM VirtualBox

```

### 3.4 Asynchronous HTTP requests

3.4.1 Show the requests and responses in the listing. Click on the last request sent, then click on the response to see that its payload has returned the data that is then rendered on the search page similar to what is shown below for “rabbid”.

```

shbhui1-902175656 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Usage: dig {global-server} {domain} {q-type} {q-class} {q-opt}
        {global-d-opt} host {@local-server} {local-d-opt}
        [ host {@local-server} {local-d-opt} [...]
]

Use "dig -h" (or "dig -h | more") for complete list of options
shbhui1-902175656 [Running] - Oracle VM VirtualBox
; <>> DIG 9.16.1-Ubuntu <>> @ns-cloudi.googledomains.com thefengs.
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 50802
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 512
;; QUESTION SECTION:
;thefengs.com. IN A
;; ANSWER SECTION:
thefengs.com. 3600 IN A 131.252.220.06
;; Query time: 96 msec
;; SERVER: 216.239.32.106#53(216.239.32.106)
;; WHEN: Mon Apr 17 13:59:39 PDT 2023
;; MSG SIZE rcvd: 57

shbhui1-902175656 [Running] - Oracle VM VirtualBox
$ dig @ns-cloudi.googledomains.com thefengs.
Invalid option: -A
Usage: dig {global-server} {domain} {q-type} {q-class} {q-opt}
        {global-d-opt} host {@local-server} {local-d-opt}
        [ host {@local-server} {local-d-opt} [...]
]

Use "dig -h" (or "dig -h | more") for complete list of options
shbhui1-902175656 [Running] - Oracle VM VirtualBox
$ netstat -lpt4
(Not all processes could be identified, non-owned process info
 will not be shown, you may have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address      State       PID/Program name
tcp      0      0  localhost:domain          0.0.0.0:*
          0      0  localhost:tip             0.0.0.0:*
shbhui1-902175656 [Running] - Oracle VM VirtualBox
$ chrome

Command 'chrome' not found, did you mean:
  command 'chrome' from deb chrome (0.7.1-1)

Try: sudo apt install <deb name>
shbhui1-902175656 [Running] - Oracle VM VirtualBox

```

```

shbhat@shbhat-VirtualBox:~$ dig @ns-cloud1.googledomains.com thefengs.com
...
; Use "dig -h" (or "dig -h more") for complete list of options
shbhat@shbhat-VirtualBox:~$ dig @ns-cloud1.googledomains.com thefengs.com
...
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp; pld: 512
;; QUESTION SECTION:
;thefengs.com. IN A
...
;; ANSWER SECTION:
thefengs.com. 3600 IN A 131.252.220.66
...
; Use "dig -h" (or "dig -h more") for complete list of options
shbhat@shbhat-VirtualBox:~$ netstat -an
...
Proto Recv-Q Send-Q Local Address Foreign Address S
tcp 0 0 localhost:domain 0.0.0.0:*
tcp 0 0 localhost:ipp 0.0.0.0:*
...
shbhat@shbhat-VirtualBox:~$ chrome
...
Command 'chroma' not found, did you mean:
  command 'chroma' from deb chroma (0.7.1-1)
...
Try: sudo apt install <deb name>
shbhat@shbhat-VirtualBox:~$ 

```

Google Chrome Network tab showing request headers for Google.com:

- Request Headers:
  - Host: www.google.com
  - method: GET
  - path: /complete/search/>PortlandStateUniversity
  - scheme: https
- Accept: \*/\*
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US,en;q=0.9
- Cookie: IP\_JAN-2023-04-17-23=AEC-AUEFuzeCavdFYPGVxaTixIPHs5v4lrxQBjKwosjySRP04cX30TUNE-ND51nVpJNvTPSKMhBLQkx1z7m3B7ps0M6Mrjz8C9h0sR2tHMDU17cf8jyJee57A...; \_ga=GA1.2.168177249205656p1v1[...]; \_gaq=GA1.2.168177249205656p1v1[...]; \_gat=1; \_gid=GA1.2.168177249205656p1v1[...]
- Sec-Chua: "Chronium";v="132", "Google Chrome";v="132", "Not-A-Brand";v="99"
- Sec-Chua-Arch: "x86"
- Sec-Chua-Bitsize: "64"
- Sec-Chua-Full-Version-Bit: "112.0.5615.49"
- Sec-Chua-Full-Version-Bit: "Chronium";v="112.0.5615.49", "Google Chrome";v="112.0.5615.49", "Not-A-Brand";v="99,0,0,0"
- Sec-Chua-Mobile: "70"
- Sec-Chua-Model: "--"
- Sec-Chua-Platform: "Linux"
- Sec-Chua-Platform-Version: "5.15.0"

```

shbhat@shbhat-VirtualBox:~$ wget https://dl.google.com/linux/direct/stable_current_amd64.deb
...
shbhat@shbhat-VirtualBox:~$ sudo gdebi google-chrome-stable_current_amd64.deb
Reading package lists... done
Building dependency tree
Reading state information... Done
Reading state information... Done
Reading state information... Done
The web browser from Google
Google Chrome is a browser that combines a minimal design
Do you want to install the software package? [Y/n]:y
/usr/bin/gdebi:113: FutureWarning: Possible nested set at position 1. This will be removed in a future version of Python.
  c = set([x for x in s if x != {}]) + msg[0].tower('
Selecting previously unselected package google-chrome-stable.
Preparing to unpack google-chrome-stable_current_amd64.deb ...
Unpacking google-chrome-stable (1:112.0.5615.49-1) ...
update-alternatives: using /usr/bin/google-chrome-stable to update alternatives: using /usr/bin/google-chrome-stable to update alternatives: using /usr/bin/google-chrome-stable to prepare alternatives for /usr/bin/google-chrome-stable ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
shbhat@shbhat-VirtualBox:~$ 

```

Google Chrome Network tab showing request headers for Google.com:

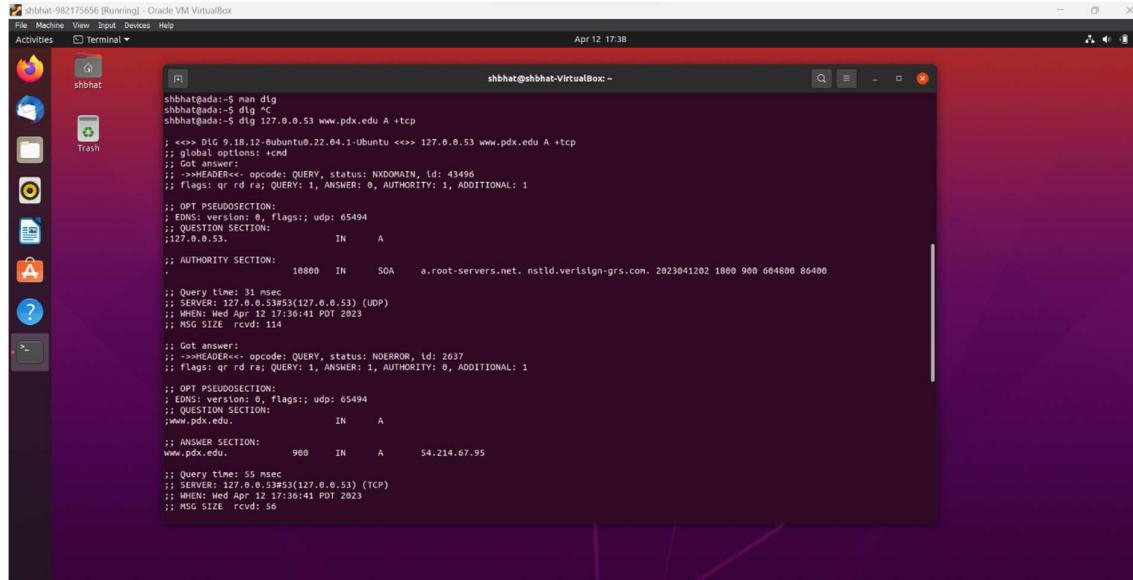
- Request Headers:
  - Host: www.google.com
  - method: GET
  - path: /complete/search/>PortlandStateUniversity
  - scheme: https
- Accept: \*/\*
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US,en;q=0.9
- Cookie: IP\_JAN-2023-04-17-23=AEC-AUEFuzeCavdFYPGVxaTixIPHs5v4lrxQBjKwosjySRP04cX30TUNE-ND51nVpJNvTPSKMhBLQkx1z7m3B7ps0M6Mrjz8C9h0sR2tHMDU17cf8jyJee57A...; \_ga=GA1.2.168177249205656p1v1[...]; \_gaq=GA1.2.168177249205656p1v1[...]; \_gat=1; \_gid=GA1.2.168177249205656p1v1[...]
- Sec-Chua: "Chronium";v="132", "Google Chrome";v="132", "Not-A-Brand";v="99"
- Sec-Chua-Arch: "x86"
- Sec-Chua-Bitsize: "64"
- Sec-Chua-Full-Version-Bit: "112.0.5615.49"
- Sec-Chua-Full-Version-Bit: "Chronium";v="112.0.5615.49", "Google Chrome";v="112.0.5615.49", "Not-A-Brand";v="99,0,0,0"
- Sec-Chua-Mobile: "70"
- Sec-Chua-Model: "--"
- Sec-Chua-Platform: "Linux"
- Sec-Chua-Platform-Version: "5.15.0"

## Section 2

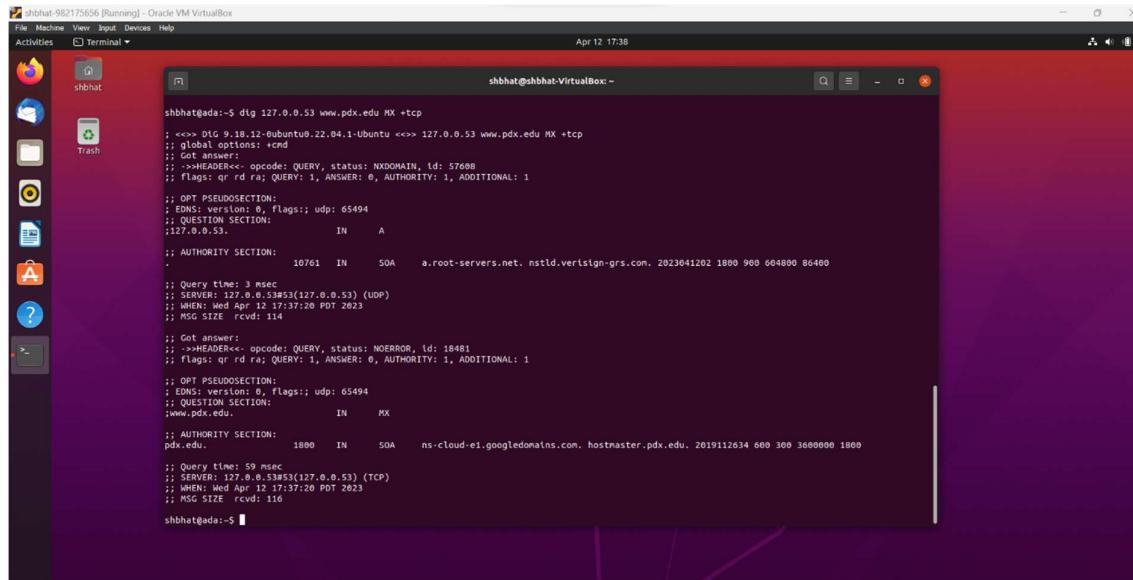
### DNS #1

#### 1.1 dig

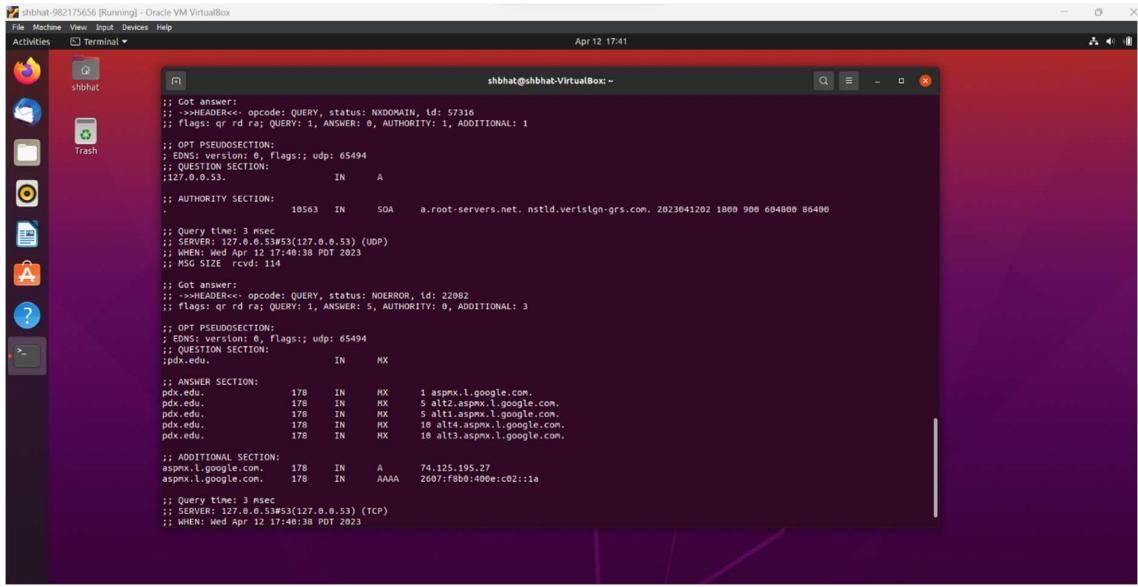
1.1.1 Use dig to query the PSU's local DNS server at 131.252.208.53 for the A record of www.pdx.edu using TCP. Then, use dig to do the same for the MX record of pdx.edu. What do the ANSWER sections explain about where PSU's web/mail services are run from?



```
shbhat@ada:~$ man dig
shbhat@ada:~$ dig
shbhat@ada:~$ dig 127.0.0.53 www.pdx.edu A +tcp
; <>> DLG 9.18.12-0ubuntu22.04.1-Ubuntu <>> 127.0.0.53 www.pdx.edu A +tcp
; global options: +cd
; Got answer:
; >>>HEADER<< opcode: QUERY, status: NXDOMAIN, id: 43496
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;www.pdx.edu.           IN      A
;
; AUTHORITY SECTION:
;ns.          10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023041202 1800 900 604800 86400
;
; Got answer:
; >>>HEADER<< opcode: QUERY, status: NOERROR, id: 2637
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;www.pdx.edu.           IN      A
;
; ANSWER SECTION:
;www.pdx.edu.         900    IN      A       54.214.67.95
;
; Query time: 55 msec
; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
; WHEN: Wed Apr 12 17:36:41 PDT 2023
; MSG SIZE rcvd: 56
```



```
shbhat@ada:~$ dig 127.0.0.53 www.pdx.edu MX +tcp
; <>> DLG 9.18.12-0ubuntu22.04.1-Ubuntu <>> 127.0.0.53 www.pdx.edu MX +tcp
; global options: +cd
; Got answer:
; >>>HEADER<< opcode: QUERY, status: NXDOMAIN, id: 57608
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;www.pdx.edu.           IN      MX
;
; AUTHORITY SECTION:
;ns.          10761   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023041202 1800 900 604800 86400
;
; Got answer:
; >>>HEADER<< opcode: QUERY, status: NOERROR, id: 18481
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;www.pdx.edu.           IN      MX
;
; AUTHORITY SECTION:
;pdx.edu.            1800    IN      SOA     ns-cloud-e1.googledomains.com. hostmaster.pdx.edu. 2019112634 600 300 3600000 1800
;
; Query time: 55 msec
; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
; WHEN: Wed Apr 12 17:37:20 PDT 2023
; MSG SIZE rcvd: 116
shbhat@ada:~$
```



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "shbhat@shbhat-VirtualBox: ~". The content of the terminal shows the output of a DNS query. The output includes several sections: a question section for "www.pdx.edu.", an authority section for "a.root-servers.net", and multiple additional sections for "pdx.edu." pointing to various Google IP addresses. The terminal window is part of a desktop interface with a purple background, icons for a browser, file manager, and terminal, and a system tray.

```

shbhat@shbhat-VirtualBox: ~
File Machine View Input Devices Help
Activities Terminal Apr 12 17:41
shbhat
shbhat@shbhat-VirtualBox: ~
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 57316
;; flags qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT_PSEUDOSECTION:
; EDNS: version: 0, Flags: udp: 65494
;; QUESTION SECTION:
;@27.0.0.53.          IN      A
;; AUTHORITY SECTION:
.
10563 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023041202 1800 900 604800 86400
;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 17:40:38 PDT 2023
;; MSG SIZE rcvd: 114
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 22082
;; flags qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 3
;; OPT_PSEUDOSECTION:
; EDNS: version: 0, Flags: udp: 65494
;; QUESTION SECTION:
;pdx.edu.           IN      MX
;; ANSWER SECTION:
pdx.edu.        178    IN      MX    1 aspmx.l.google.com.
pdx.edu.        178    IN      MX    5 alt2.aspmx.l.google.com.
pdx.edu.        178    IN      MX    5 alt1.aspmx.l.google.com.
pdx.edu.        178    IN      MX    10 alt4.aspmx.l.google.com.
pdx.edu.        178    IN      MX    10 alt3.aspmx.l.google.com.
;; ADDITIONAL SECTION:
aspmx.l.google.com. 178    IN      A     74.125.195.27
aspmx.l.google.com. 178    IN      AAAA   2607:f8b0:400e:c02::1a
;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
;; WHEN: Wed Apr 12 17:40:38 PDT 2023

```

The ANSWER section of the first query should provide an IP address, which is where the web server for www.pdx.edu is hosted. The ANSWER section of the second query should provide one or more mail server names, along with their priority values, which are used for handling email traffic for pdx.edu.

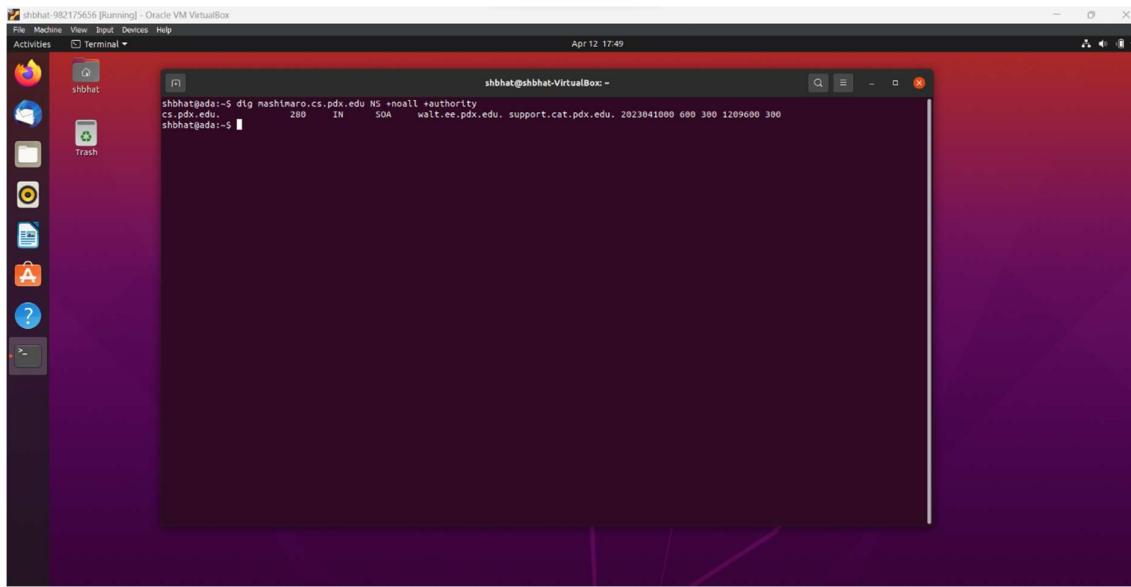
#### 54.214.67.95 – Web services are hosted

**;; ANSWER SECTION:**

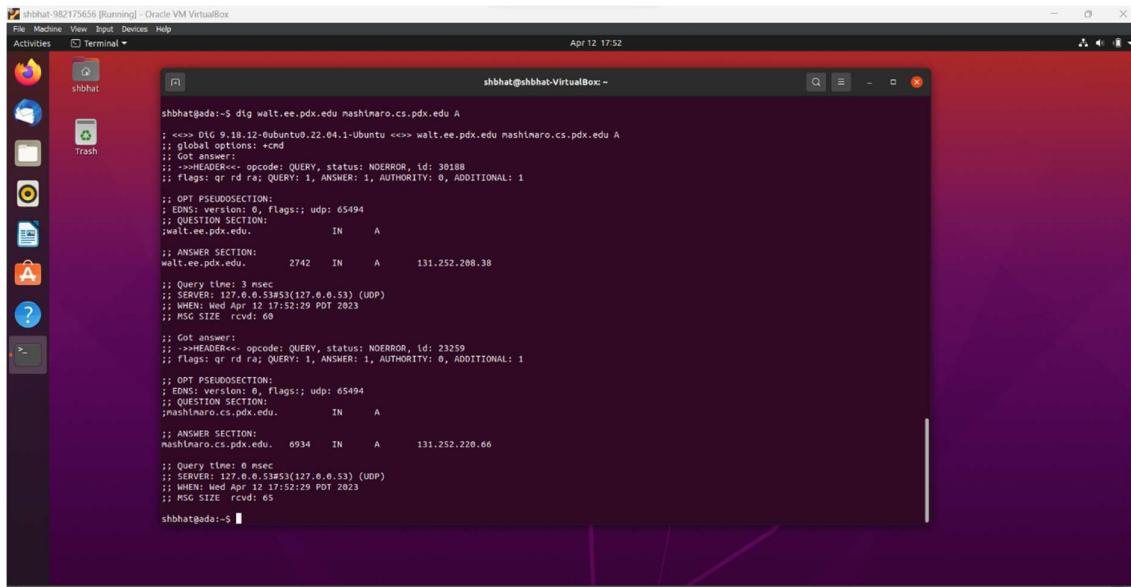
pdx.edu.	178	IN	MX	1 aspmx.l.google.com.
pdx.edu.	178	IN	MX	5 alt2.aspmx.l.google.com.
pdx.edu.	178	IN	MX	5 alt1.aspmx.l.google.com.
pdx.edu.	178	IN	MX	10 alt4.aspmx.l.google.com.
pdx.edu.	178	IN	MX	10 alt3.aspmx.l.google.com.

Mail services are hosted

1.1.2 Find the authoritative server (NS record type, AUTHORITY section response) for mashimaro.cs.pdx.edu and then query that server for the A record of mashimaro.cs.pdx.edu. Show both.

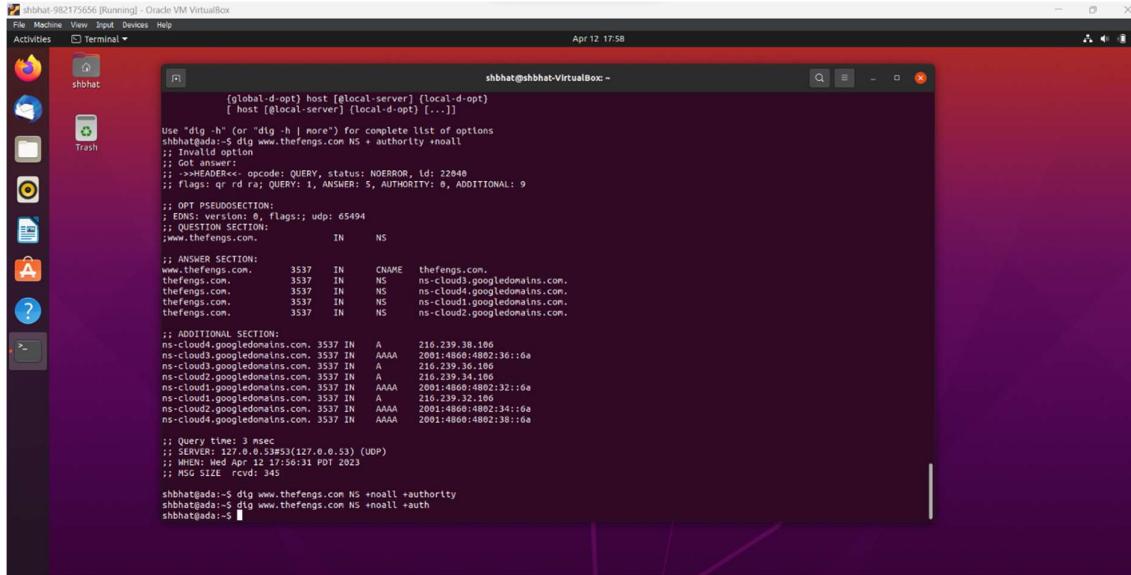


```
shbhat@shbhat-VirtualBox:~$ dig mashimaro.cs.pdx.edu NS +noall +authority
; <>> OIG 9.18.12-ubuntu0.22.04.1-Ubuntu <>> walt.ee.pdx.edu mashimaro.cs.pdx.edu A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 30188
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;mashimaro.cs.pdx.edu.           IN      A
;
;; ANSWER SECTION:
walt.ee.pdx.edu.    2742   IN      A      131.252.208.38
;
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 23259
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;mashimaro.cs.pdx.edu.           IN      A
;
;; ANSWER SECTION:
mashimaro.cs.pdx.edu. 6934   IN      A      131.252.220.66
;
;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 17:52:29 PDT 2023
;; MSG SIZE rcvd: 63
```



```
shbhat@shbhat-VirtualBox:~$ dig walt.ee.pdx.edu mashimaro.cs.pdx.edu A
; <>> OIG 9.18.12-ubuntu0.22.04.1-Ubuntu <>> walt.ee.pdx.edu mashimaro.cs.pdx.edu A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 30188
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;mashimaro.cs.pdx.edu.           IN      A
;
;; ANSWER SECTION:
walt.ee.pdx.edu.    2742   IN      A      131.252.208.38
;
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 23259
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;mashimaro.cs.pdx.edu.           IN      A
;
;; ANSWER SECTION:
mashimaro.cs.pdx.edu. 6934   IN      A      131.252.220.66
;
;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 17:52:29 PDT 2023
;; MSG SIZE rcvd: 63
```

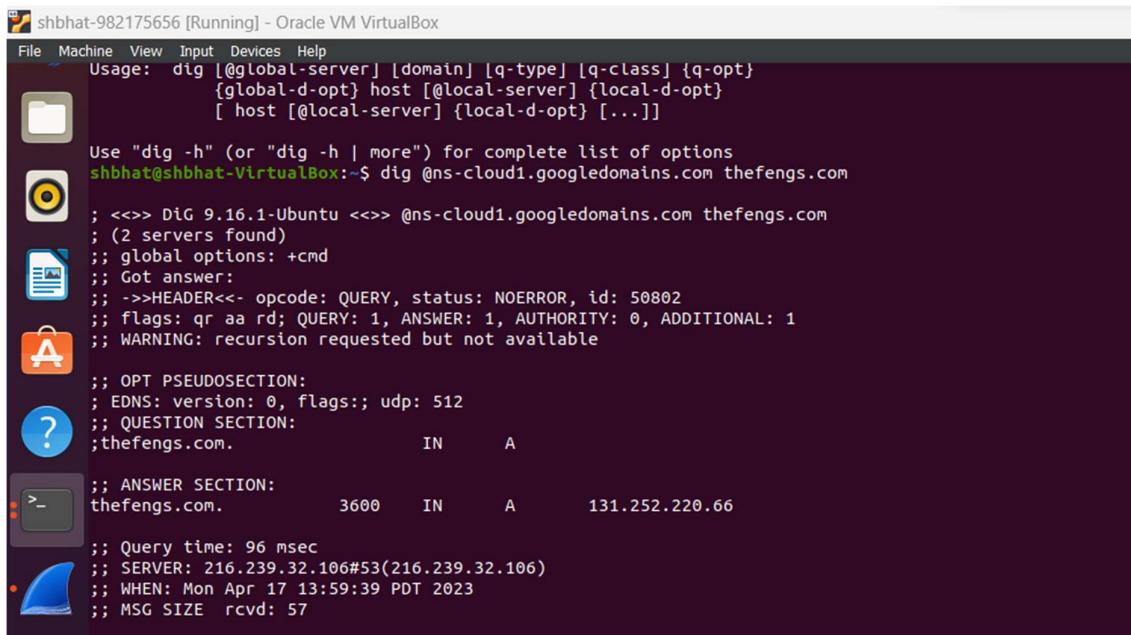
### 1.1.3 Find the authoritative server for thefengs.com and then query that server for the A record of thefengs.com.



```
shbhat@shbhat-VirtualBox ~
(shbhat@shbhat-VirtualBox) host [local-server] {local-d-opt}
[ host [local-server] {local-d-opt} [...]
{global-d-opt} host [local-server] {local-d-opt}
[ host [local-server] {local-d-opt} [...]
Use "dig -h" (or "dig -h | more") for complete list of options
shbhat@shbhat:~$ dig www.thefengs.com NS +authority +noall
;; Invalid option
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.thefengs.com.           IN      NS
;; ANSWER SECTION:
www.thefengs.com.      3537    IN      CNAME   thefengs.com.
thefengs.com.          3537    IN      NS      ns-cloud3.googledomains.com.
thefengs.com.          3537    IN      NS      ns-cloud1.googledomains.com.
thefengs.com.          3537    IN      NS      ns-cloud1.googledomains.com.
thefengs.com.          3537    IN      NS      ns-cloud2.googledomains.com.

;; ADDITIONAL SECTION:
ns-cloud3.googledomains.com. 3537 IN  A      216.239.38.106
ns-cloud3.googledomains.com. 3537 IN  AAAA  2001:4800:4802:36::6a
ns-cloud3.googledomains.com. 3537 IN  A      216.239.36.106
ns-cloud3.googledomains.com. 3537 IN  AAAA  2001:4800:4802:36::6a
ns-cloud1.googledomains.com. 3537 IN  A      216.239.32.106
ns-cloud1.googledomains.com. 3537 IN  AAAA  2001:4800:4802:32::6a
ns-cloud1.googledomains.com. 3537 IN  A      216.239.32.106
ns-cloud1.googledomains.com. 3537 IN  AAAA  2001:4800:4802:34::6a
ns-cloud1.googledomains.com. 3537 IN  AAAA  2001:4800:4802:38::6a

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 17:56:31 PDT 2023
;; MSG SIZE rcvd: 345
shbhat@shbhat:~$ dig www.thefengs.com NS +noall +authority
shbhat@shbhat:~$ dig www.thefengs.com NS +noall +auth
shbhat@shbhat:~$
```



```
File Machine View Input Devices Help
Usage: dig [@global-server] [domain] [q-type] [q-class] {q-opt}
{global-d-opt} host [@local-server] {local-d-opt}
[ host [@local-server] {local-d-opt} [...]
Use "dig -h" (or "dig -h | more") for complete list of options
shbhat@shbhat-VirtualBox:~$ dig @ns-cloud1.googledomains.com thefengs.com
; <>> DiG 9.16.1-Ubuntu <>> @ns-cloud1.googledomains.com thefengs.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50802
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;thefengs.com.           IN      A
;; ANSWER SECTION:
thefengs.com.      3600    IN      A      131.252.220.66

;; Query time: 96 msec
;; SERVER: 216.239.32.106#53(216.239.32.106)
;; WHEN: Mon Apr 17 13:59:39 PDT 2023
;; MSG SIZE rcvd: 57
```

### 1.1.4 When a web request hits port 80 of 131.252.220.66, how does the server know which site to serve from? (i.e. what protocol header)

Answer:

When a web request hits port 80 of an IP address, the server relies on the HTTP protocol header to determine which site to serve from. The HTTP protocol header is a part of the HTTP request that a client sends to a server when making an HTTP request. This header

contains several fields, including the "Host" field, which specifies the domain name of the website being requested.

For example, if a client sends an HTTP request to 131.252.220.66 with the following header:

## GET / HTTP/1.1

Host: example.com

The server at 131.252.220.66 will check the "Host" field in the HTTP header to determine which site the request is intended for. In this case, the server will recognize that the request is intended for the "example.com" website and will serve the appropriate content.

If the "Host" field is missing or contains an unrecognized domain name, the server will typically serve a default website or return an error message.

## 1.2 DNS iterative lookup

1.2.1 Include the results of each query for your lab notebook.

```
shbhat@shbhat-VirtualBox:~$ dig @192.5.5.241 www.amazon.co.uk NS +norecurse +tcp A
;; Warning, extra type option
;: SERVER: 192.5.5.241#53(192.5.5.241) (TCP)
;: WHEN: Wed Apr 12 18:26:53 PDT 2023
;: MSG SIZE rcvd: 549
shbhat@shbhat:~$ dig @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
;; Warning, extra type option
;: SERVER: 192.5.5.241#53(192.5.5.241) (TCP)
;: WHEN: Wed Apr 12 18:26:53 PDT 2023
;: MSG SIZE rcvd: 549
shbhat@shbhat:~$ dig @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65535
;; QUESTION SECTION:
;www.amazon.co.uk. IN A
;; AUTHORITY SECTION:
uk. 172800 IN NS nsa.nic.uk.
uk. 172800 IN NS nsb.nic.uk.
uk. 172800 IN NS nsc.nic.uk.
uk. 172800 IN NS nsd.nic.uk.
uk. 172800 IN NS dns1.nic.uk.
uk. 172800 IN NS dns2.nic.uk.
uk. 172800 IN NS dns3.nic.uk.
uk. 172800 IN NS dns4.nic.uk.
;; ADDITIONAL SECTION:
nsa.nic.uk. 172800 IN A 156.154.100.3
nsa.nic.uk. 172800 IN AAAA 2a01:502:2ed9::3
nsb.nic.uk. 172800 IN A 156.154.101.3
nsb.nic.uk. 172800 IN AAAA 2a01:502:2ed9::3
nsc.nic.uk. 172800 IN A 156.154.102.3
nsc.nic.uk. 172800 IN AAAA 2a01:502:100c::3
nsd.nic.uk. 172800 IN A 156.154.103.3
nsd.nic.uk. 172800 IN AAAA 2a01:a1:1010::3
dns1.nic.uk. 172800 IN A 213.248.216.1
dns1.nic.uk. 172800 IN AAAA 2a01:502:2ed9::1
dns2.nic.uk. 172800 IN A 103.49.86.1
dns2.nic.uk. 172800 IN AAAA 2a01:f6b8:49e0::1
dns3.nic.uk. 172800 IN A 213.248.226.1
dns3.nic.uk. 172800 IN AAAA 2a01:f6b8:49e0::1
```

```
shbhat@shbhat-VirtualBox:~$ dig @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
;; Query time: 3 msec
;; SERVER: 192.5.5.241#53(192.5.5.241) (TCP)
;; WHEN: Wed Apr 12 18:26:53 PDT 2023
;; MSG SIZE rcvd: 549
shbhat@shbhat:~$ dig @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
;; Warning, extra type option
;: SERVER: 192.5.5.241#53(192.5.5.241) (TCP)
;: WHEN: Wed Apr 12 18:26:53 PDT 2023
;: MSG SIZE rcvd: 549
shbhat@shbhat:~$ dig @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; COOKIE: 1561545084c1010900064375ab269ea47d227565093 (good)
;; QUESTION SECTION:
;www.amazon.co.uk. IN A
;; AUTHORITY SECTION:
amazon.co.uk. 172800 IN NS ns1.p31.dynect.net.
amazon.co.uk. 172800 IN NS pdns3.ultradsns.info.
amazon.co.uk. 172800 IN NS pdns3.ultradsns.org.
amazon.co.uk. 172800 IN NS pdns1.ultradsns.net.
amazon.co.uk. 172800 IN NS pdns4.ultradsns.org.
amazon.co.uk. 172800 IN NS ns1.p31.dynect.net.
amazon.co.uk. 172800 IN NS ns4.p31.dynect.net.
amazon.co.uk. 172800 IN NS pdns2.ultradsns.net.
amazon.co.uk. 172800 IN NS pdns0.ultradsns.co.uk.
;; Query time: 19 msec
;; SERVER: 156.154.100.3#53(nsa.nic.uk) (TCP)
;; WHEN: Wed Apr 12 18:28:18 PDT 2023
;; MSG SIZE rcvd: 336
shbhat@shbhat:~$
```

```

shbhat@shbhat-VirtualBox: ~
dig @ns1.p31.dynect.net www.amazon.co.uk NS +noredirect +tcp A
; Query time: 19 msec
; SERVER: 156.154.106.3#53(ns1.p31.dynect.net) (TCP)
; WHEN: Wed Apr 12 18:28:18 PDT 2023
; MSG SIZE rcvd: 338
shbhat@ada:~$ dig @ns1.p31.dynect.net www.amazon.co.uk NS +noredirect +tcp A
; Warning, extra type option
; <>> DLG 9.18.12.0ubuntu0.22.04.1-Ubuntu <>> @ns1.p31.dynect.net www.amazon.co.uk NS +noredirect +tcp A
; (1 server found)
; global options: +cmd
; Got answer:
; flags: qr aa; opcode: QUERY, status: NOERROR, id: 19957
; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: ud; cookie: 2abed04ad3af5cisc96d9364375b068e1a44f0b27f6fd5 (good)
; QUESTION SECTION:
;www.amazon.co.uk. IN A
; ANSWER SECTION:
www.amazon.co.uk. 1800 IN CNAME tp.bfdc3ca1-frontier.amazon.co.uk.
; AUTHORITY SECTION:
bfdc3ca1-frontier.amazon.co.uk. 900 IN NS ns-248.awsdns-31.com.
bfdc3ca1-frontier.amazon.co.uk. 900 IN NS ns-1624.awsdns-11.co.uk.
bfdc3ca1-frontier.amazon.co.uk. 900 IN NS ns-1078.awsdns-06.org.
bfdc3ca1-frontier.amazon.co.uk. 900 IN NS ns-853.awsdns-42.net.

; Query time: 19 msec
; SERVER: 108.59.163.31#53(ns1.p31.dynect.net) (TCP)
; WHEN: Wed Apr 12 18:29:42 PDT 2023
; MSG SIZE rcvd: 261
shbhat@ada:~$
```

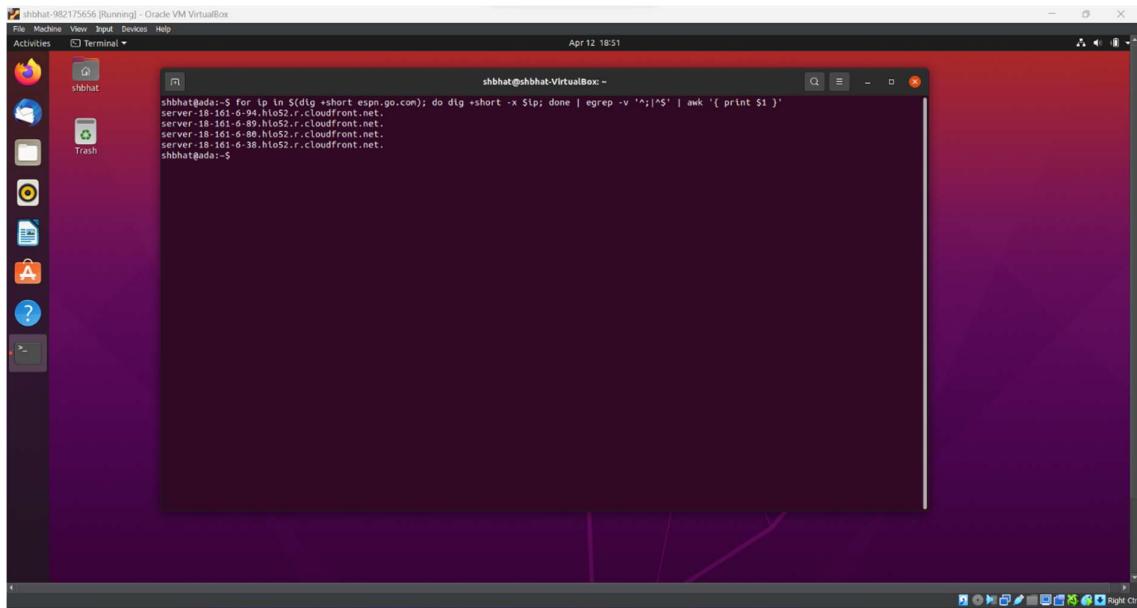
### 1.3 Reverse DNS Lookup

1.3.1 Use a single command line with commands dig, egrep, and awk, to list all IPv4 addresses that espn.go.com points to.

```

shbhat@shbhat-VirtualBox: ~
dig +short espn.go.com | egrep '^([0-9]+\.(0-9]+\.(0-9]+\.(0-9)+$' | awk '{ print $1 }'
18.161.6.34
18.161.6.38
18.161.6.80
18.161.6.89
shbhat@ada:~$
```

1.3.2 Take that list and create a single for loop in the shell that iterates over the list and performs a reverse lookup of each IP address to find each address's associated DNS name. As with the previous step, pipe the output of the for loop to egrep and awk so that the output consists only of the DNS names.

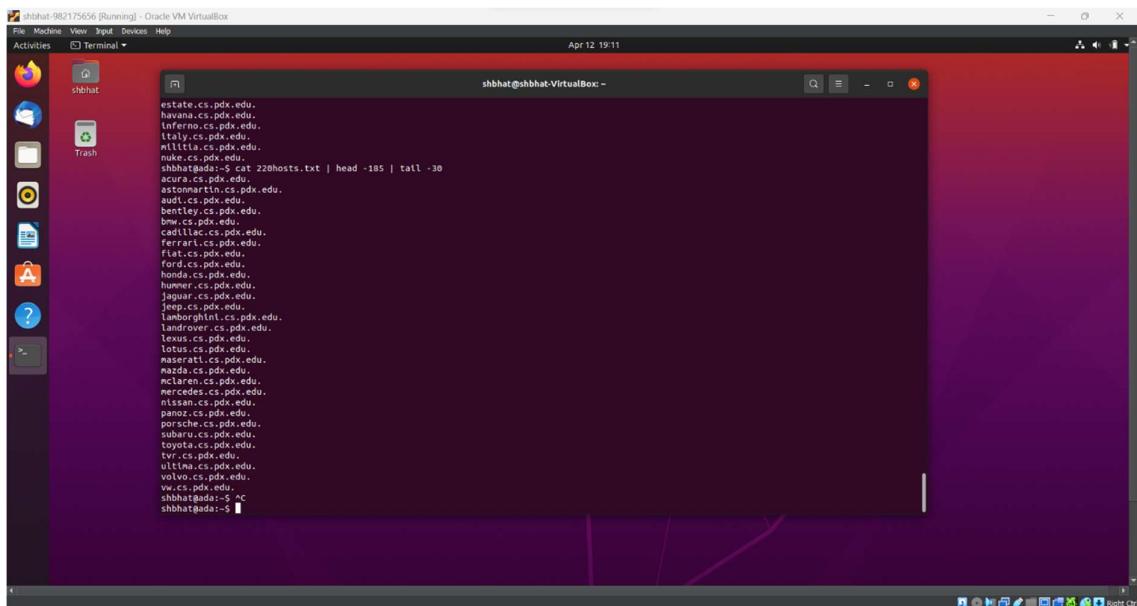


## 1.4 Hosts Enumeration

### 1.4.1 Show the results in your lab notebook.

Answer:

```
cat 220hosts.txt | head -185 | tail -30
```



## DNS #2

### 2.1 Geographic DNS

#### 2.1.1 What geographic locations do ipinfo.io and DB-IP return?

The screenshot shows two separate sessions of a web browser, each displaying four geolocation results from different sources. The top session is for IP address 131.252.208.53 and the bottom session is for 198.82.247.66. Each session contains four cards: IP2Location, ipinfo.io, DB-IP, and iPregistry.co. The results are identical for both IP addresses.

**Geolocation data from IP2Location (Product: DB6, 2023-4-1)**

IP ADDRESS: 131.252.208.53	ISP: Portland State University
COUNTRY: United States	ORGANIZATION: Not available
REGION: Oregon	LATITUDE: 45.5213
CITY: Portland	LONGITUDE: -122.6859

**Geolocation data from ipinfo.io (Product: API, real-time)**

IP ADDRESS: 131.252.208.53	ISP: Portland State University
COUNTRY: United States	ORGANIZATION: Portland State University (pdx.edu)
REGION: Oregon	LATITUDE: 45.5234
CITY: Portland	LONGITUDE: -122.6762

**Geolocation data from DB-IP (Product: API, real-time)**

IP ADDRESS: 131.252.208.53	ISP: Portland State University
COUNTRY: United States	ORGANIZATION: Portland State University
REGION: Oregon	LATITUDE: 45.584
CITY: Portland (North Portland)	LONGITUDE: -122.728

**Geolocation data from iPregistry.co (Product: API, real-time)**

IP ADDRESS: 131.252.208.53	ISP: Portland State University
COUNTRY: United States	ORGANIZATION: Portland State University
REGION: Oregon	LATITUDE: 45.584
CITY: Portland (North Portland)	LONGITUDE: -122.728

**Geolocation data from IP2Location (Product: DB6, 2023-4-1)**

IP ADDRESS: 198.82.247.66	ISP: Virginia Polytechnic Institute and State Univ.
COUNTRY: United States	ORGANIZATION: Not available
REGION: Virginia	LATITUDE: 37.2557
CITY: Blacksburg	LONGITUDE: -80.4315

**Geolocation data from ipinfo.io (Product: API, real-time)**

IP ADDRESS: 198.82.247.66	ISP: Virginia Polytechnic Institute and State Univ.
COUNTRY: United States	ORGANIZATION: Virginia Polytechnic Institute and State Univ. (vt.edu)
REGION: Virginia	LATITUDE: 37.2296
CITY: Blacksburg	LONGITUDE: -80.4139

**Geolocation data from DB-IP (Product: API, real-time)**

IP ADDRESS: 198.82.247.66	ISP: Virginia Polytechnic Institute and State Univ.
COUNTRY: United States	ORGANIZATION: Virginia Polytechnic Institute and State Univ.
REGION: Virginia	LATITUDE: 37.2037
CITY: Blacksburg (Farmview - Ramble)	LONGITUDE: -80.4143

#### 2.1.2 Record one address for www.google.com from each result for your lab notebook.

Answer:

Web server: 142.251.33.100

The image shows two side-by-side terminal windows running on an Ubuntu 22.04 desktop environment within Oracle VM VirtualBox. Both windows have a red header bar with the title "shbhat@shbhat-VirtualBox:~".

**Terminal Window 1 (Left):**

```
shbhat@ada:~$ dig www.google.com @131.252.208.53
; <>> DIG 9.18.12-0ubuntu0.22.04.1-Ubuntu <>> www.google.com @131.252.208.53
; global options: +cmd
; Got answer:
; >>>HEADER<- opcode: QUERY, status: NOERROR, id: 5258
; Flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
; COOKIE: 0027bd95c257aa90100000643767ad551039b3e41cebfff (good)
; QUESTION SECTION:
;www.google.com.           IN      A
;
;ANSWER SECTION:
www.google.com.      218     IN      A      142.251.33.100
;
; Query time: 0 msec
; SERVER: 131.252.208.53#(131.252.208.53) (UDP)
; WHEN: Wed Apr 12 19:23:34 PDT 2023
; MSG SIZE rcvd: 87
shbhat@ada:~$
```

**Terminal Window 2 (Right):**

```
shbhat@shbhat-VirtualBox:~$ dig www.google.com @198.82.247.66
; <>> DIG 9.18.12-0ubuntu0.22.04.1-Ubuntu <>> www.google.com @198.82.247.66
; global options: +cmd
; Got answer:
; >>>HEADER<- opcode: QUERY, status: NOERROR, id: 2241
; Flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; COOKIE: c441978698fb3a35035755a643767d24be37b3ec8f4cc09 (good)
; QUESTION SECTION:
;www.google.com.           IN      A
;
;ANSWER SECTION:
www.google.com.      34     IN      A      172.253.62.99
www.google.com.      34     IN      A      172.253.62.147
www.google.com.      34     IN      A      172.253.62.103
www.google.com.      34     IN      A      172.253.62.105
www.google.com.      34     IN      A      172.253.62.164
www.google.com.      34     IN      A      172.253.62.106
;
; Query time: 67 msec
; SERVER: 198.82.247.66#53(198.82.247.66) (UDP)
; WHEN: Wed Apr 12 19:24:18 PDT 2023
; MSG SIZE rcvd: 107
shbhat@shbhat:~$
```

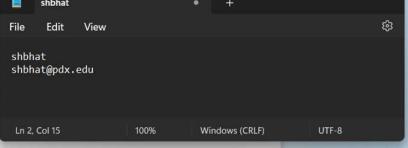
The desktop environment includes a dock with icons for various applications like a browser, file manager, and system tools. The bottom right corner shows system status: 27°C, Mostly sunny, ENG IN, 07:24 PM, 12-04-2023.

2.1.3 What is the geographic distance between each DNS server and the IP address it resolves for [www.google.com](http://www.google.com)?

Answer:

DNS Servers:

- 172.253.62.105 -> 2016 n mi, 3734 km
- 172.253.62.103 -> 2016 n mi, 3734 km
- 172.253.62.147 -> 611 n mi, 1132 km
- 172.253.62.104 -> 2016 n mi, 3734 km
- 172.253.62.106 -> 2016 n mi, 3734 km
- 172.253.62.99 -> 2016 n mi, 3734 km



A screenshot of a Microsoft Edge browser window. The address bar shows <https://www.nhc.noaa.gov/grcalc.shtml>. The page is titled "Latitude/Longitude Distance Calculator". It has input fields for two locations: Latitude 1 (47.6062 N) and Longitude 1 (122.3321 W), and Latitude 2 (38.8951 N) and Longitude 2 (77.0364 W). Below these, a "Distance" field is set to 2016 n mi. A "Compute" button is visible. At the bottom, there's a note about the Great Circle Calculator and a link to more information. A Windows Command Prompt window is overlaid on the browser, showing the command "shbhat" and its email address "shbhat@pdx.edu".

02.2: DNS, Recap | IP Address Lookup | Geolocation | IP Address Lookup | Geolocation | Latitude/Longitude Distance | dig: server, flag, options | WhatsApp

ANALYSES & FORECASTS • DATA & TOOLS • EDUCATIONAL RESOURCES • ARCHIVES • ABOUT • SEARCH •

## Latitude/Longitude Distance Calculator

Enter latitude and longitude of two points, select the desired units: nautical miles (in mi), statute miles (in miles), kilometers (in km) or meters (in m). Latitudes and longitudes may be entered in any of three different formats: decimal degrees (DD.DD), degrees and decimal minutes (DD MM.MM), or degrees, minutes and decimal seconds (DD MM.SS.SS).

**Important Note:** The distance calculator on this page is provided for informational purposes only. The calculations are approximate in nature and may differ a little from the distances as given in the official forecasts and advisories.

[Click here to find your latitude/longitude](#)

**Input Location Points**

Latitude 1	Longitude 1		
47.6062	N	122.3321	W

Latitude 2	Longitude 2		
38.8951	N	77.0364	W

**Distance**  
(rounded to the nearest whole unit)

3734	km
------	----

**Compute** **Reset**

adapted from the Great Circle Calculator  
written by Ed Williams  
(used with permission)

More information on Great Circle navigation can be found [here](#).

**Quick Links and Additional Resources**

**TROPICAL CYCLONE FORECASTS**  
Tropical Cyclone Advisories  
Tropical Cyclone Outlook

**SOCIAL MEDIA**  
NHC on Facebook  
Twitter

**RESEARCH AND DEVELOPMENT**  
NOAA Hurricane Research Division  
Hurricane Forecast Model

**NWS FORECAST OFFICES**  
Weather Prediction Center  
Storm Prediction Center  
Ocean Prediction Center

Ln 2, Col 15      100%      Windows (CRLF)      UTF-8

02.2: DNS, Recap | IP Address Lookup | Geolocation | IP Address Lookup | Geolocation | Latitude/Longitude Distance | dig: server, flag, options | WhatsApp

Home Mobile Site Text Version RSS Local Forecast Enter City, State or ZIP code

## NATIONAL HURRICANE CENTER and CENTRAL PACIFIC HURRICANE CENTER

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

ANALYSES & FORECASTS • DATA & TOOLS • EDUCATIONAL RESOURCES •

## Latitude/Longitude Distance Calculator

Enter latitude and longitude of two points, select the desired units: nautical miles (in mi), statute miles (in miles), kilometers (in km) or meters (in m). Latitudes and longitudes may be entered in any of three different formats: decimal degrees (DD.DD), degrees and decimal minutes (DD MM.MM), or degrees, minutes and decimal seconds (DD MM.SS.SS).

**Important Note:** The distance calculator on this page is provided for informational purposes only. The calculations are approximate in nature and may differ a little from the distances as given in the official forecasts and advisories.

[Click here to find your latitude/longitude](#)

**Input Location Points**

Latitude 1	Longitude 1		
47.6062	N	122.3321	W

Latitude 2	Longitude 2		
37.422	N	122.084	W

**Distance**  
(rounded to the nearest whole unit)

1132	km
------	----

**Compute** **Reset**

adapted from the Great Circle Calculator  
written by Ed Williams  
(used with permission)

More information on Great Circle navigation can be found [here](#).

Ln 2, Col 15      100%      Windows (CRLF)      UTF-8

## 2.1.4 Traceroute - Do the routes reveal any information on the accuracy of the geographic locations given? (Answer might be no)

```

Windows PowerShell
shbhat@ada:~$ traceroute 131.252.288.53
traceroute to 131.252.288.53 (131.252.288.53), 30 hops max, 60 byte packets
1 r0ns.cat.pdx.edu (131.252.288.53) 1.165 ms 1.051 ms 0.997 ms
shbhat@ada:~$ traceroute 198.82.247.66
traceroute to 198.82.247.66 (198.82.247.66), 30 hops max, 60 byte packets
1 radiant.seas.pdx.edu (131.252.288.212) 2.258 ms 2.224 ms 2.305 ms
2 CORE1.net.pdx.edu (131.252.5.142) 0.994 ms 0.874 ms 0.822 ms
3 131.252.5.213 (131.252.5.213) 1.048 ms 0.997 ms 0.893 ms
4 port-psu-pe-01.net.linkoregon.org (199.98.165.177.48) 0.735 ms 0.686 ms 0.636 ms
5 eugn-oh-vpn-01.net.linkoregon.org (207.98.126.3) 10.362 ms 10.295 ms 10.287 ms
6 bois-gtwy-pe-01.net.linkoregon.org (207.98.126.135) 16.334 ms 10.173 ms 10.125 ms
7 bois-gtwy-pe-01-loren.net.linkoregon.org (163.253.5.65) 18.059 ms 9.993 ms 9.993 ms
8 hundredrudge-0-0-0-0.4079.core1.bois.net.internet2.edu (163.253.5.64) 11.195 ms 11.085 ms 11.016 ms
9 fourhundredrudge-0-0-0-0.4079.core2.salt.net.internet2.edu (163.253.1.249) 65.928 ms 65.699 ms 65.524 ms
10 fourhundredrudge-0-0-0-0.4079.core1.salt.net.internet2.edu (163.253.1.30) 64.413 ms fourhundredrudge-0-0-0-0.4079.core2.salt.net.internet2.edu (163.253.1.3)
2) 65.105 ms 65.052 ms
11 fourhundredrudge-0-0-0-0.4079.core1.denv.net.internet2.edu (163.253.1.170) 65.874 ms 65.856 ms fourhundredrudge-0-0-0-0.4079.core2.kans.net.internet2.edu (163.253.1.251) 64.666 ms
12 fourhundredrudge-0-0-0-0.4079.core1.kans.net.internet2.edu (163.253.1.243) 64.349 ms 64.358 ms 64.288 ms
13 fourhundredrudge-0-0-0-0.4079.core2.chic.net.internet2.edu (163.253.1.240) 66.514 ms 66.505 ms fourhundredrudge-0-0-0-0.4079.core2.chic.net.internet2.edu (163.253.1.97) 66.416 ms
14 fourhundredrudge-0-0-0-0.4079.core2.eqch.net.internet2.edu (163.253.2.19) 65.010 ms 65.036 ms 64.932 ms
15 fourhundredrudge-0-0-0-0.4079.core2.clev.net.internet2.edu (163.253.2.16) 66.487 ms 66.414 ms 64.777 ms
16 fourhundredrudge-0-0-0-0.4079.core2.ashb.net.internet2.edu (163.253.1.138) 65.437 ms 65.379 ms 65.313 ms
17 192.175.14 (192.175.14) 63.457 ms 63.403 ms 63.340 ms
18 vtacs-1.msap.cns.vt.edu (192.70.187.18) 114.241 ms 114.266 ms 114.204 ms
19 hill-border.xe-5-0-2.0.cns.vt.edu (128.173.0.194) 112.822 ms 112.757 ms 112.614 ms
20 128.173.0.210 (128.173.0.210) 114.096 ms 114.041 ms 113.971 ms
21 * cas-core.lo6.2000.cns.vt.edu (198.82.1.143) 115.274 ms 115.189 ms
22 jeru.cns.vt.edu (198.82.247.66) 68.950 ms 68.886 ms 68.881 ms
shbhat@ada:~$
```

Yes they do reveal the location details, For first 2 IP addresses, we got the traceroute and it describes the accuracy of location.

When traceroute is done to 2 of the google servers it times out after reaching some point, but when we do traceroute to main webserver of google it points to a location in Seattle.

```

Windows PowerShell
shbhat@ada:~$ traceroute 172.253.62.105
traceroute to 172.253.62.105 (172.253.62.105), 30 hops max, 60 byte packets
1 r0ns.cat.pdx.edu (131.252.288.212) 1.143 ms 1.235 ms 1.340 ms
2 CORE1.net.pdx.edu (131.252.5.142) 0.986 ms 0.968 ms 0.959 ms
3 131.252.5.213 (131.252.5.213) 0.892 ms 0.879 ms 0.900 ms
4 google.maxx.net (198.32.195.34) 24.202 ms 24.142 ms 24.099 ms
5 188.170.248.139 (188.170.248.139) 11.386 ms 11.255 ms 11.203 ms
6 192.250.230.197 (192.250.230.197) 13.333 ms 13.298 ms 13.256 ms
7 192.250.230.197 (192.250.230.197) 13.333 ms 13.298 ms 13.256 ms
8 192.250.230.197 (192.250.230.197) 13.333 ms 13.298 ms 13.256 ms
9 192.250.230.197 (192.250.230.197) 13.333 ms 13.298 ms 13.256 ms
10 192.250.230.197 (192.250.230.197) 13.333 ms 13.298 ms 13.256 ms
11 192.250.230.197 (192.250.230.197) 13.333 ms 13.298 ms 13.256 ms
12 192.250.230.197 (192.250.230.197) 13.333 ms 13.298 ms 13.256 ms
13 * *
14 * *
15 * *
16 * *
17 * *
18 * *
19 * *
20 * *
21 bc-in-f105.le100.net (172.253.62.105) 65.305 ms 65.263 ms *
shbhat@ada:~$ traceroute 172.253.62.105
traceroute to 172.253.62.105 (172.253.62.105), 30 hops max, 60 byte packets
1 radiant.seas.pdx.edu (131.252.288.212) 1.109 ms 4.155 ms 4.111 ms
2 CORE1.net.pdx.edu (131.252.5.142) 0.998 ms 0.816 ms 0.761 ms
3 131.252.5.213 (131.252.5.213) 0.892 ms 0.879 ms 0.893 ms
4 google.maxx.net (198.32.195.34) 42.023 ms 41.958 ms 42.093 ms
5 74.125.243.179 (74.125.243.179) 6.120 ms 108.178.245.188 (108.178.245.188) 5.135 ms 108.178.245.118 (108.178.245.118) 4.814 ms
6 172.253.76.192 (172.253.76.192) 13.770 ms 12.348 ms 216.239.57.194 (216.239.57.194) 12.068 ms
7 172.253.76.192 (172.253.76.192) 13.770 ms 12.348 ms 192.250.230.197 (192.250.230.197) 12.068 ms
8 * 192.251.64.2 (192.251.64.2) 64.901 ms
9 *
10 192.250.209.206 (192.250.209.206) 66.642 ms 192.251.240.161 (192.251.240.161) 66.280 ms 192.251.240.199 (192.251.240.199) 65.390 ms
11 70.125.37.153 (70.125.37.153) 65.392 ms 172.253.68.81 (172.253.68.81) 66.373 ms 192.251.245.183 (192.251.245.183) 66.455 ms
12 * *
13 * *
14 * *
15 * *
16 * *
17 * *
18 * *
19 * *
20 * *
21 bc-in-f103.le100.net (172.253.62.105) 65.607 ms 65.599 ms 65.153 ms
shbhat@ada:~$ traceroute 192.251.33.100
traceroute to 192.251.33.100 (192.251.33.100), 30 hops max, 60 byte packets
1 radiant.seas.pdx.edu (131.252.288.212) 1.109 ms 4.155 ms 4.111 ms
2 CORE1.net.pdx.edu (131.252.5.142) 0.998 ms 0.879 ms 0.733 ms
3 131.252.5.213 (131.252.5.213) 1.058 ms 1.008 ms 0.939 ms
4 google.maxx.net (198.32.195.34) 30.131 ms 34.066 ms 34.087 ms
5 74.125.243.179 (74.125.243.179) 10.197 ms 12.125.243.193 (12.125.243.193) 9.015 ms 4.132 ms
6 192.251.50.177 (192.251.50.177) 4.222 ms 3.985 ms 192.251.50.175 (192.251.50.175) 4.536 ms
7 sea3910-in-f11.le100.net (192.251.33.100) 9.966 ms 4.799 ms 4.734 ms
shbhat@ada:~$
```

## Network Recap Lab #3

### 3.1 REVERSE DNS

3.1.1 Perform a reverse DNS lookup on the DNS server to find its name.

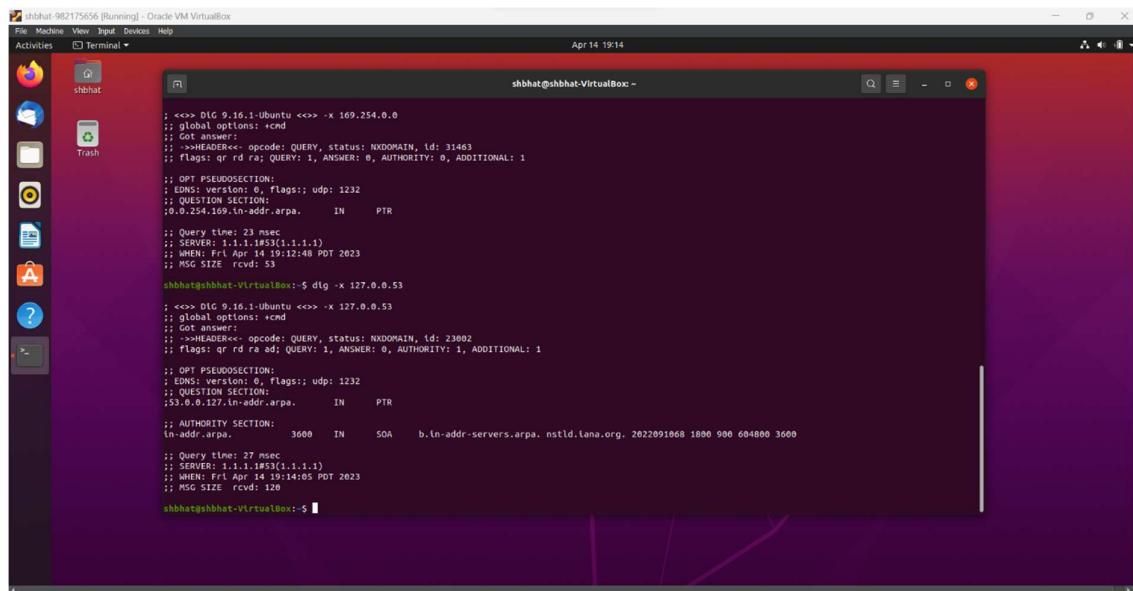
Include it in your lab notebook.

## Answer:

```
shbhat@shbhat-VirtualBox: ~$ ifconfig
ensps3: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
                fe80::fe0:2fffe%ensps3 brd fe80::ff:fe0:2fffe linklayer
        ether 00:0c:27:32:9c:2c txqueuelen 1000 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 172 bytes 22692 (22.6 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                loop brd 127.0.0.1 linklayer
        ether 00:00:00:00:00:00 txqueuelen 1000 (Localhost Networkback)
        RX packets 156 bytes 13278 (13.2 kB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 156 bytes 13278 (13.2 kB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

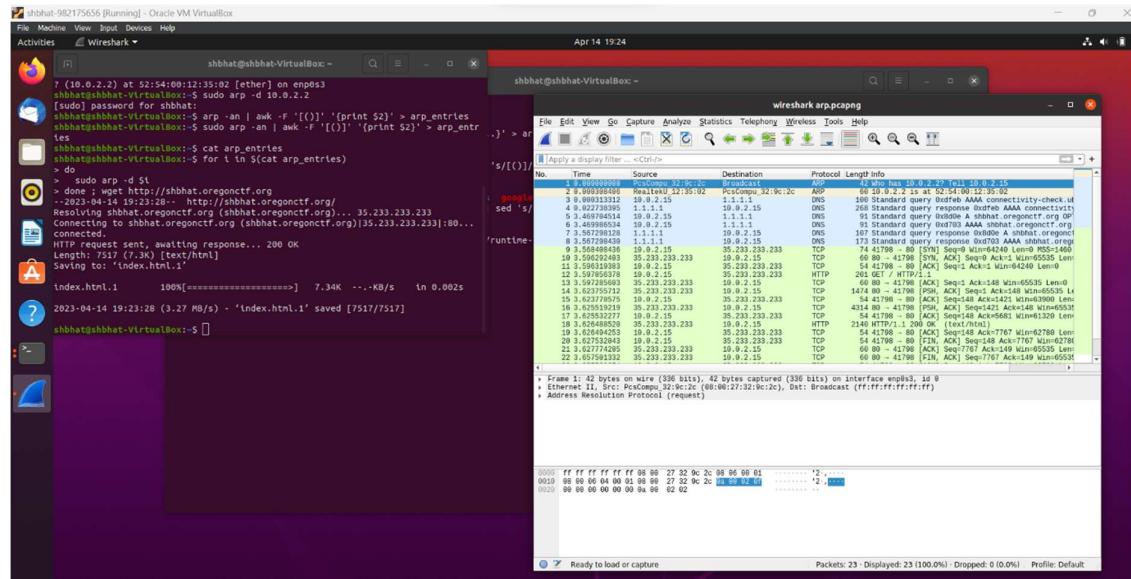
shbhat@shbhat-VirtualBox: ~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask        Flags   MSS Window irtt Iface
0.0.0.0         10.0.2.2      0.0.0.0       UG        0          0 enps3
10.0.2.0        0.0.0.0       255.255.255.0 U        0          0 enps3
109.254.0.0     0.0.0.0       255.255.0.0   U        0          0 enp0s3
shbhat@shbhat-VirtualBox: ~$
```



```
; <>>. DLG 9.16.1-Ubuntu <>> -x 169.254.0.0
; global options: +cmd
; Got answer:
; >>>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 31463
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; QUESTION SECTION:
;_0.0.254.169.in-addr.arpa. IN PTR
; Query time: 23 msec
; SERVER: 1.1.1.1#53(1.1.1.1)
; WHEN: Fri Apr 14 19:12:48 PDT 2023
; MSG SIZE rcvd: 53
shbhat@shbhat-VirtualBox:~$ dig -x 127.0.0.53
; <>>. DLG 9.16.1-Ubuntu <>> -x 127.0.0.53
; global options: +cmd
; Got answer:
; >>>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 23802
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; QUESTION SECTION:
;_53.0.0.127.in-addr.arpa. IN PTR
; AUTHORITY SECTION:
;_in-addr.arpa. 3600 IN SOA b.in-addr-servers.arpa. ns.tld.lana.org. 2022091068 1800 900 604800 3600
; Query time: 27 msec
; SERVER: 1.1.1.1#53(1.1.1.1)
; WHEN: Fri Apr 14 19:14:05 PDT 2023
; MSG SIZE rcvd: 328
shbhat@shbhat-VirtualBox:~$
```

### 3.2 ARP and Wireshark

3.2.1 Take a screenshot of the trace within Wireshark and include an annotation of the packets in the trace to explain the purpose of each of the packets being exchanged.



### 3.2.2 How many DNS requests are made?

Answer:

3 DNS requests are made and 3 DNS responses.

### 3.2.3 How many TCP connections does the browser initiate simultaneously to the site?

Answer:

Total 14 TCP requests and if we divide it by 2 we will get 7 which is the request initiated simultaneously to the site.

### 3.3.4 How many HTTP GET requests are there for embedded objects?

Answer:

1 HTTP Get