

# **Lab notebook Week 2**

**Submitted by: Vishrut Sharma (OdinID: vishrut)**

## **Table of Contents**

<b>02.1: TCP, HTTP.....</b>	<b>2</b>
1. TCP #1 (netstat, lsof, nc).....	2
3. Throughput tests .....	6
5. Developer tools .....	7
6. Asynchronous HTTP requests.....	10
<b>02.2: DNS, Recap.....</b>	<b>12</b>
1. DNS #1 (dig) .....	12
2. Reverse DNS lookups.....	16
3. Host enumeration.....	17
4. DNS #2 (Geographic DNS).....	17
5. Network Recap Lab #3.....	20
6. Collect and analyze the network trace of a connection.....	21

## 02.1: TCP, HTTP

### 1. TCP #1 (netstat, lsof, nc)

1) Screenshot below contains the result from the command sudo netstat -lpt4

```
vboxuser@vishrut:~$ sudo netstat -lpt4
[sudo] password for vboxuser:
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:ipp          0.0.0.0:*
tcp      0      0 localhost:40147        0.0.0.0:*
vboxuser@vishrut:~$
```

2) The screenshot below contains the port numbers after examining /etc/services

```
vboxuser@vishrut:~$ sudo netstat -lpt4
[sudo] password for vboxuser:
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:ipp          0.0.0.0:*
tcp      0      0 localhost:40147        0.0.0.0:*
vboxuser@vishrut:~$ grep domain /etc/services
domain      53/tcp                      # Domain Name Server
domain      53/udp
domain-s    853/tcp                     # DNS over TLS [RFC7858]
domain-s    853/udp                     # DNS over DTLS [RFC8094]
vboxuser@vishrut:~$ grep ipp /etc/services
ipp        631/tcp                      # Internet Printing Protocol
vboxuser@vishrut:~$
```

The port that only has a number is running 716/containererd program. It is a daemon that manages the lifecycle of containers in a container runtime environment.

4) The screenshot below contains the result from running the netstat command on linux.cs.pdx.edu.

vishrut [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help Activities Terminal Apr 10 18:44 vboxuser@vishrut: ~

the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

Vishrut@vishrut:~\$ 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	172.56.151.24:62572	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	10.200.238.61:50210	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:52348	tanto.cs.pdx:postgresql	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	70.72.153.15:54540	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	c-67-161-106-103:49972	ESTABLISHED
tcp	0	0	localhost.localdo:52693	localhost.localdo:37765	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	172.30.7.159:59049	ESTABLISHED
tcp	0	0	localhost.localdo:52610	localhost.localdo:6016	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:52606	70.72.153.15:54546	TIME_WAIT
tcp	0	0	localhost.localdo:6018	localhost.localdo:44914	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	168.103.229.191.p:50130	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	172.30.30.189:62763	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:38924	tanto.cs.pdx:postgresql	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	72.20.10.100:59360	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	10.200.56.17:63358	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:52036	tanto.cs.pdx:postgresql	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	172.30.17.60:50577	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:50666	haopenldap.cat.pdx:ldaps	TIME_WAIT
tcp	0	0	ada.cs.pdx.edu:55788	71.75.153.15:54549	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	static-50-53-6-15:12663	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	50-39-190-193.bvt:64449	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	static-50-53-6-15:3153	ESTABLISHED
tcp	0	0	localhost.localdo:37765	localhost.localdo:52693	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	10.200.70.51:54549	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	64.251.242.170:61352	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	192.56.44.5:60871	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	10.200.97.172:56470	ESTABLISHED
tcp	0	0	localhost.localdo:47698	localhost.localdo:6017	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	71.75.153.15:53312	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	50-109-242-46:58393	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:55762	tanto.cs.pdx:postgresql	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	static-50-53-6-15:25108	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	c-71-193-198-157.hsd1.or.comcast.net:62616	ESTABLISHED
tcp	0	0	localhost.localdo:6817	localhost.localdo:47698	ESTABLISHED
tcp	0	0	localhost.localdo:6911	localhost.localdo:52698	ESTABLISHED
tcp	1	0	ada.cs.pdx.edu:40986	stlverfish.cat.pdx:10pp	CLOSE_WAIT
tcp	0	0	ada.cs.pdx.edu:ssh	10.200.73.165:1057	ESTABLISHED
tcp	0	0	ada.cs.pdx.edu:ssh	static-50-53-6-15:58268	ESTABLISHED

Last login: Wed Apr 12 17:31:58 2023 from c-71-193-198-157.hsd1.or.comcast.net  
vishrut@ada:~\$ netstat -tlnp  
(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.*	LISTEN	-
tcp	0	0	127.0.0.1:25	0.0.0.*	LISTEN	-
tcp	0	0	127.0.0.1:631	0.0.0.*	LISTEN	-
tcp	0	0	127.0.0.1:6013	0.0.0.*	LISTEN	-
tcp	0	0	127.0.0.1:6012	0.0.0.*	LISTEN	-
tcp	0	0	127.0.0.1:6015	0.0.0.*	LISTEN	-
tcp	0	0	127.0.0.1:6011	0.0.0.*	LISTEN	-
tcp	0	0	127.0.0.1:6010	0.0.0.*	LISTEN	-
tcp	0	0	127.0.0.1:42711	0.0.0.*	LISTEN	-
tcp	0	0	0.0.0.0:22	0.0.0.*	LISTEN	-
tcp	0	0	0.0.0.0:111	0.0.0.*	LISTEN	-
tcp	0	0	127.0.0.53:53	0.0.0.*	LISTEN	-
tcp6	0	0	:::51701	::*	LISTEN	-
tcp6	0	0	:::22	::*	LISTEN	-
tcp6	0	0	:::113	::*	LISTEN	-
tcp6	0	0	:::111	::*	LISTEN	-
tcp6	0	0	:::6010	::*	LISTEN	-
tcp6	0	0	:::6011	::*	LISTEN	-
tcp6	0	0	:::6012	::*	LISTEN	-
tcp6	0	0	:::6013	::*	LISTEN	-
tcp6	0	0	:::6015	::*	LISTEN	-
tcp6	0	0	:::631	::*	LISTEN	-
tcp6	0	0	:::25	::*	LISTEN	-

Odin ID vishrut

File Edit View Ln 1, Col 17 100% Windows (CRLF) UTF-8

vishrut@ada:~\$

5) The screenshot below shows all the services the machine provides for external access.

```
vboxuser@vishrut: ~
```

```
Last login: Sun Apr 16 14:59:39 2023 from c-71-193-198-157.hsd1.or.comcast.net
vishruti@ada1:~$ service --status-all
[ + ]  acpid
[ + ]  alsa-utils
[ - ]  anacron
[ + ]  apparmor
[ + ]  aptdaemon
[ + ]  autofs
[ - ]  avahi-daemon
[ + ]  bluetooth
[ - ]  console-setup.sh
[ + ]  cron
[ + ]  cups
[ + ]  cups-browsed
[ + ]  dbus
[ + ]  fallzban
[ - ]  fio
[ - ]  gdm3
[ - ]  gdm-common
[ - ]  hdlock.sh
[ + ]  irqbalance
[ + ]  kerneloops
[ - ]  keyboard-setup.sh
[ + ]  knod
[ - ]  lightdm
[ - ]  ligh
[ + ]  netfilter-persistent
[ + ]  networking
[ - ]  nfs-common
[ - ]  ntp
[ - ]  oidentd
[ - ]  openssh-inetd
[ - ]  openvswitch
[ - ]  plymouth
[ + ]  plymouth-log
[ + ]  postfix
[ + ]  procps
[ - ]  pulseaudio-enable-autospawn
[ + ]  rpd
[ - ]  rsync
[ - ]  saned
[ - ]  screen-cleanup
[ - ]  smartmontools
[ - ]  speech-dispatcher
[ - ]  spice-vdagent
[ + ]  ssh
```



```
Odin ID vishruti
```

```
File Edit View
```

```
Odin ID: vishruti
```

```
Ln 1, Col 17 | 100% | Windows (CRLF) | UTF-8
```

6) The screenshot below contains the result from running the lsof command on the Ubuntu VM. The number of open descriptors were 31045.

```
vishrut@vishrut:~$ netstat -an | grep :25
tcp6       0      0 127.0.0.1:25          0.0.0.0:*           LISTEN      -
tcp6       0      0 127.0.0.1:33          0.0.0.0:*           LISTEN      -
tcp6       0      0 127.0.0.1:5813        0.0.0.0:*           LISTEN      -
tcp6       0      0 127.0.0.1:69812       0.0.0.0:*           LISTEN      -
tcp6       0      0 127.0.0.1:69815       0.0.0.0:*           LISTEN      -
tcp6       0      0 127.0.0.1:69816       0.0.0.0:*           LISTEN      -
tcp6       0      0 127.0.0.1:69819       0.0.0.0:*           LISTEN      -
tcp6       0      0 127.0.0.1:69820       0.0.0.0:*           LISTEN      -
tcp6       0      0 127.0.0.1:69825       0.0.0.0:*           LISTEN      -
tcp6       0      0 127.0.0.1:69826       0.0.0.0:*           LISTEN      -
tcp6       0      0 127.0.0.1:37705       0.0.0.0.*          LISTEN      -
tcp6       0      0 0.0.0.0:22          0.0.0.0.*          LISTEN      -
tcp6       0      0 0.0.0.0:111         0.0.0.0.*          LISTEN      -
tcp6       0      0 0.0.0.0:53/53       0.0.0.0.*          LISTEN      -
tcp6       0  ::1:51701  ::*              LISTEN      -
tcp6       0  ::1::22   ::*              LISTEN      -
tcp6       0  ::1::113  ::*              LISTEN      -
tcp6       0  ::1::116  ::*              LISTEN      -
tcp6       0  ::1::6016  ::*             LISTEN      -
tcp6       0  ::1::6017  ::*             LISTEN      -
tcp6       0  ::1::6018  ::*             LISTEN      -
tcp6       0  ::1::6019  ::*             LISTEN      -
tcp6       0  ::1::6023  ::*             LISTEN      -
tcp6       0  ::1::6025  ::*             LISTEN      -
tcp6       0  ::1::6026  ::*             LISTEN      -
tcp6       0  ::1::6010  ::*             LISTEN      -
tcp6       0  ::1::6011  ::*             LISTEN      -
tcp6       0  ::1::6012  ::*             LISTEN      -
tcp6       0  ::1::6013  ::*             LISTEN      -
tcp6       0  ::1::6014  ::*             LISTEN      -
tcp6       0  ::1::6015  ::*             LISTEN      -
tcp6       0  ::1::6031  ::*             LISTEN      -
tcp6       0  ::1::25   ::*             LISTEN      -
vishrut@vishrut:~$ ext
logout
Connection to linux.cs.pdx.edu closed.
vboxuser@vishrut:~$ sudo lsdf | wc -l
[sudo] password for vboxuser:
lsdf: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
        Output information may be incomplete.
31045
vboxuser@vishrut:~$ `c
vboxuser@v: Start :-$
```

The screenshot below contains the result from running the lsof command but with the -i and the -s flag included. The result was 12.

7) The 2 screenshots below contains the result from netcat command. The first screenshot shows us which port is being used to connect to `linux.cs.pdx.edu`.

The 2<sup>nd</sup> screenshot shows the SSH version being used to connect to `linux.cs.pdx.edu`.

```
File Machine View Input Devices Help
Activities Terminal -> vboxuser@vishruth: ~
vboxuser@vishruth: ~
systemd-r 531 systemd-resolve 12u IPv4 21077      UDP localhost:domain
systemd-dæ 531 systemd-resolve 13u IPv4 21078      TCP localhost:domain (LISTEN)
avahi-dæ 574 avahi 12u IPv4 23451      UDP *:mdns
avahi-dæ 574 avahi 13u IPv6 23452      UDP *:mdns
avahi-dæ 574 avahi 14u IPv6 23453      UDP *:mdns
avahi-dæ 574 avahi 15u IPv6 23454      UDP *:mdns
cupsd 576 root 6u IPv6 24657      TCP ipo-localhost:ipp (LISTEN)
cupsd 576 root 7u IPv6 24658      TCP localhost:ipp (LISTEN)
Networkk 578 root 23u IPv4 55592      UDP vishruth:bootpc->.gateway:bootps
cups-brow 666 root 7u IPv4 24985      UDP *:631
cups-brow 666 root 14u IPv4 28294      TCP localhost:44255 (LISTEN)
vboxuser@vishruth: ~$ sudo lsof -l -s | wc -l
12
vboxuser@vishruth: ~$ man nc
vboxuser@vishruth: ~$ nc vishruth@linux.cs.pdx.edu
nc: missing port number
vboxuser@vishruth: ~$ nc vishruth@linux.cs.pdx.edu -v
OpenSSH_8.2p1 Ubuntu-4ubuntu0.5, OpenSSH 1.1.1f 31 Mar 2020
debug1: Reading configuration data /etc/ssh/sshd_config
debug1: /etc/ssh/sshd_config line 1: inclu 1: /etc/ssh/ssh_config.d/* conf matched no files
debug1: /etc/ssh/sshd_config line 21: Analyzing options for *
debug1: Connecting to linux.cs.pdx.edu [131.252.208.103] port 22.
debug1: Connection established.
debug1: identity file /home/vboxuser/.ssh/ld_rsa type 0
debug1: identity file /home/vboxuser/.ssh/ld_rsa type -1
debug1: identity file /home/vboxuser/.ssh/ld_dsa type -1
debug1: identity file /home/vboxuser/.ssh/ld_ecdsa type -1
debug1: identity file /home/vboxuser/.ssh/ld_ecdsa-cert type -1
debug1: identity file /home/vboxuser/.ssh/ld_ecdh type -1
debug1: identity file /home/vboxuser/.ssh/ld_ecdh-cert type -1
debug1: identity file /home/vboxuser/.ssh/ld_ed25519 type -1
debug1: identity file /home/vboxuser/.ssh/ld_ed25519-cert type -1
debug1: identity file /home/vboxuser/.ssh/ld_ed25519_sk type -1
debug1: identity file /home/vboxuser/.ssh/ld_ed25519_sk-cert type -1
debug1: identity file /home/vboxuser/.ssh/ld_x509 type -1
debug1: identity file /home/vboxuser/.ssh/ld_x509-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
debug1: Remote program version 2.0, remote software version OpenSSH_8.0p1 Ubuntu-3ubuntu0.1
debug1: rekey after 4096 bytes, 60 seconds
debug1: Authentication to linux.cs.pdx.edu:22 as 'vishruth'
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: ciphers:ecc25519-sha256
debug1: kex: host key algorithm: ecdsa-sha2-nistp256
debug1: kex: server-client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client-server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: expecting SSH2_MSG_ECDH_REPLY
```

### 3. Throughput tests

- 1) The screenshot below shows the measured bandwidth available between us-west1-b (right image) and australia-southeast1-b (left image).



The screenshot shows two terminal windows side-by-side. Both windows have a title bar 'Odin ID v1' and a header bar with 'File', 'Edit', 'View', and a gear icon.

**Left Terminal:**

- Title: Odin ID v1
- Content:
  - SSH-in-browser
  - SSH-in-browser
  - 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
  - Last login: Tue Apr 11 02:02:00 2023 from 35.235.241.96
  - vishrut@us-**australia-southeast1:b**:~\$ sudo iperf -s -p 80
  - Server listening on TCP port 80
  - TCP window size: 128 KByte (default)
  - [ 4 ] local 10.152.0.2 port 80 connected with 35.203.129.238 port 45556
  - [ 1D] Interval Transfer Bandwidth
  - [ 4 ] 0.0-10.1 sec 170 MBytes 141 Mbit/sec

**Right Terminal:**

- Title: Odin ID v1
- Content:
  - SSH-in-browser
  - SSH-in-browser
  - 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
  - Last login: Tue Apr 11 02:05:41 2023 from 35.235.241.66
  - vishrut@us-**west1-b**:~\$ iperf -c 35.189.43.237 -p 80
  - Client connecting to 35.189.43.237, TCP port 80
  - TCP window size: 85.0 KByte (default)
  - [ 3 ] local 10.138.0.6 port 45556 connected with 35.189.43.237 port 80
  - [ 1D] Interval Transfer Bandwidth
  - [ 3 ] 0.0-10.1 sec 170 MBytes 141 Mbit/sec

- 2) The screenshot below shows the measured bandwidth available between us-west1-b (right image) and europe-west1-d (left image).

The screenshot shows two separate terminal windows, both titled "SSH-in-browser". The left window displays a command-line interface with several log entries, including updates from "apt list --upgradable" and status from "sudo pro status". The right window shows a similar interface with log entries related to network connections and bandwidth usage.

```
https://ssh.cloud.google.com/v2/ssh/projects/cloud-sharma-vishruti/zones/eu-central1-a/instances/vm-us-west1-b

Added security | https://ssh.cloud.google.com/v2/ssh/projects/cloud-sharma-vishruti/zones/eu-central1-a/instances/vm-us-west1-b... A

SSH-in-browser UPLOAD FILE DOWNLOAD FILE G

File Edit View
Odin ID: vishruti| ln 1. Col 17 | 100% Windows (CRLF) UTF-8

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

Last login: Tue Apr 11 02:03:31 2023 from 35.235.243.224
vishruti@vm-europe-west1-d:~$ sudo iperf -s -p 80
-----
Server listening on TCP port 80
TCP window size: 128 KByte (default)

[ 4] local 10.13.0.2 port 80 connected with 35.203.129.238 port 59108
[ ID] Interval Transfer Bandwidth
[ 4] 0.0-10.1 sec 190 MBytes 158 Mbits/sec

-----
```

```
https://ssh.cloud.google.com/v2/ssh/projects/cloud-sharma-vishruti/zones/us-west1-b/instances/vm-us-west1-b... A

Added security | https://ssh.cloud.google.com/v2/ssh/projects/cloud-sharma-vishruti/zones/us-west1-b/instances/vm-us-west1-b... A

SSH-in-browser UPLOAD FILE DOWNLOAD FILE G

File Edit View
Odin ID: vishruti| ln 1. Col 17 | 100% Windows (CRLF) UTF-8

Last login: Tue Apr 11 02:05:41 2023 from 35.235.241.66
vishruti@vm-us-west1-b:~$ iperf -c 35.189.43.237 -p 80
-----
Client connecting to 35.189.43.237, TCP port 80
TCP window size: 85.0 KByte (default)

[ 3] local 10.138.0.6 port 45556 connected with 35.189.43.237 port 80
[ ID] Interval Transfer Bandwidth
[ 3] 0.0-10.1 sec 170 MBytes 141 Mbits/sec
vishruti@vm-us-west1-b:~$ iperf -c 34.78.94.195 -p 80
-----
Client connecting to 34.78.94.195, TCP port 80
TCP window size: 85.0 KByte (default)

[ 3] local 10.138.0.6 port 59108 connected with 34.78.94.195 port 80
[ ID] Interval Transfer Bandwidth
[ 3] 0.0-10.1 sec 190 MBytes 158 Mbits/sec
vishruti@vm-us-west1-b:~$ [ ]
```

- 3) The screenshot below shows the measured bandwidth available between us-west1-b (right image) and us-east1-b (left image).

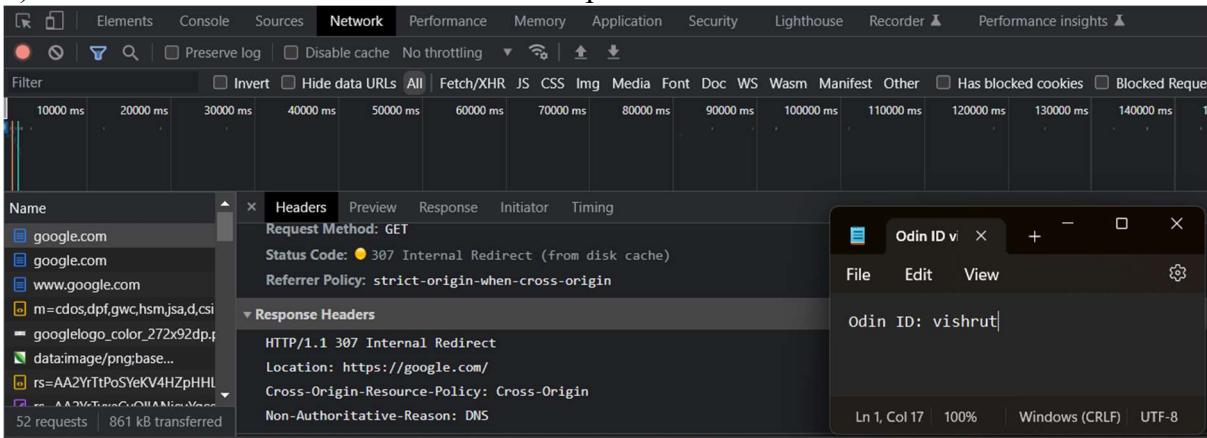
The screenshot displays two terminal windows side-by-side. The left window, titled 'SSH-in-browser', shows iperf test results from a VM in us-east1-b to a VM in us-west1-b. The right window, also titled 'SSH-in-browser', shows iperf test results from a VM in us-west1-b to a VM in us-east1-b. Both tests use TCP port 80 with a TCB Window size of 85.0 KByte (default). The bandwidth values are as follows:

Test Direction	Client IP	Server IP	Bandwidth
us-east1-b to us-west1-b	10.138.0.6	34.148.238.90	141 Mbit/sec
us-west1-b to us-east1-b	10.138.0.6	34.78.94.195	158 Mbit/sec
us-west1-b to us-west1-b	10.138.0.6	34.148.238.90	93.5 Mbit/sec
us-east1-b to us-east1-b	10.138.0.6	34.148.238.90	112 Mbit/sec

There is a relative difference between the bandwidths between us-west1-b and all the other VMs. Surprisingly the lowest bandwidth (93.5 Mbit/sec) was between us-west1-b and us-east1-b. This might be because of internet traffic and network congestion. The bandwidth between us-west1-b and australia-southeast1-b was 141 Mbit/sec and the highest bandwidth was between us-west1-b and europe-west1-d (158 Mbit/sec).

## 5. Developer tools

- 1) URL being requested is <http://google.com/>
- 2) The Status code is 307: ‘HTTP 307 Temporary Redirect’ response code indicates that the resource requested has been temporarily moved to the URL given by the Location headers.
- 3) The screenshot below shows the HTTP response header.



- 4) URL being requested is <https://google.com/>. It uses HTTPS.

5) The 2 screenshots below show the authority header and the user-agent field.

The image contains two vertically stacked screenshots of the Chrome DevTools Network tab. Both screenshots show a list of requests for 'google.com' and its sub-resources. A context menu is open over one of the requests, specifically for the 'google.com' entry in the list. The menu is titled 'Odin ID vi:' and contains options for File, Edit, and View. In the first screenshot, the 'View' option is selected, displaying the value 'Odin ID: vishrut'. In the second screenshot, the 'Edit' option is selected, also displaying 'Odin ID: vishrut'. Below the menu, the browser's status bar shows 'Ln 1, Col 17 100% Windows (CRLF) UTF-8'. The Network tab has various filters and performance metrics at the top, and a detailed view of the selected request's headers (Request Headers) is shown in the main pane.

6) The Status code is 301: ‘HTTP status code 301’ indicates a permanent redirect, meaning that the requested resource has moved permanently to a new URL. And ‘HTTP 307 Temporary Redirect’ response code indicates that the resource requested has been temporarily moved to the URL given by the Location headers.

7) The screenshot below shows the associated HTTP response header that is sent in conjunction with this status code for the request.

The screenshot shows the Network tab in the Chrome DevTools. A request to `https://google.com/` is selected. The Headers section shows the following response headers:

```
Request URL: https://google.com/
Request Method: GET
Status Code: 301
Remote Address: [2607:f8b0:400a:80e::200e]:443
Referer Policy: strict-origin-when-cross-origin

Response Headers
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
cache-control: public, max-age=2592000
content-length: 220
content-security-policy-report-only: object-src 'none';base-uri 'self';script-src 'nonce-TNlqXlltHffyAuxGhMAQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http;;report-uri https://csp.withgoogle.com/csp/gws/other-hp
content-type: text/html; charset=UTF-8
cross-origin-opener-policy: same-origin-allow-popups; report-to="gws"
date: Mon, 17 Apr 2023 23:24:06 GMT
expires: Wed, 17 May 2023 23:24:06 GMT
location: https://www.google.com/
origin-trial: Ap+qInLzIDK5mEHjM51la98Gueh1lqGb6ezME51khe1j2BqVzfV06zPwQ3lodoueu3UphAo1rnhnPAw4AIAAA8feyJvcmlna41011odRwczovL3d3dy5nb29nbGluY29tDjQ9MyIsImZ1YX81cmI1O1JQ/XtaXnzab9uc1BvbG1jeVuVub...
```

8) URL being requested is <https://www.google.com/>. It is using HTTPS.

9) The status code is 200.

10) The screenshot below shows the alt-svc section in the response header. The client can use HTTP3/QUIC based on the h3-29 tag in alt-svc.

The screenshot shows the Network tab in the Chrome DevTools. A request to `https://google.com/` is selected. The Headers section shows the following response headers:

```
accept-ch: Sec-CH-UA-Platform
accept-ch: Sec-CH-UA-Platform-Version
accept-ch: Sec-CH-UA-Full-Version
accept-ch: Sec-CH-UA-Arch
accept-ch: Sec-CH-UA-Model
accept-ch: Sec-CH-UA-Bitness
accept-ch: Sec-CH-UA-Full-Version-List
accept-ch: Sec-CH-UA-WoW64
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
cache-control: private, max-age=0
content-encoding: br
content-length: 44773
content-security-policy-report-only: object-src 'none';base-uri 'self';script-src 'nonce-way5iyDn5uHovPmKv0A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http;;report-uri https://csp.withgoogle.com/csp/gws/other-hp
content-type: text/html; charset=UTF-8
cross-origin-opener-policy: same-origin-allow-popups; report-to="gws"
date: Mon, 17 Apr 2023 23:24:06 GMT
```

11) The setting of SameSite=None indicates that the cookie can be sent with cross-site requests, including requests from third-party sites.

The screenshot shows the Network tab in the Chrome DevTools developer tools. A request to `google.com` is selected. In the Headers section, there is a 'Set-Cookie' header with the value:

```

    expires: -1
    origin-trial: Ap+qNlnLzJDKSmEHjzM5ila9898gue1lqgb6ezME51khe1j20qVzfVf06PmQ3lodeu... (long string)
    origin-trial: Avud+Mqz735p1K1V21H01kxdMeIN0dU115d0CPz9dovVlCkX80aqjho101jodRrczov... (long string)
    p3p: CP="This is not a P3P policy! See g.co/p3pHelp for more info."
    permissions-policy: unload(){}
    report-to: {"group": "gws", "max_age": 2592000, "endpoints": [{"url": "https://csp.withgoogle.com/csp/report-to/gws/other"}]}
    server: gws
    set-cookie: 1P_JAR=2023-04-11-02; expires=Thu, 11-May-2023 02:37:18 GMT; path=/; domain=.google.com; Secure; SameSite=None
    set-cookie: AEC-AUEUqfWMJf62jYYeA2z0KtpExFjfqZJH0b1ufqEf91Cb3-ZKAriEFA; expires=Sun, 08-Oct-2023 02:37:18 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=Lax
    set-cookie: NID=511-pvuu0CdeVVY-6kVtCYUE1eIaM2ak1z4W025oKeElXjbVhdZ6lDNMG_NQqNlCuKuHtN8Pzbh851_nXoh-MhNC71-yL30Wtq4fjnP80_Pk0MK10jX950Dnbwgdq1RS4Ph7KH-yzL81Dauf84yZ2koA77gLv8pJg; expires=Wed, 11-Oct-2023 02:37:18 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=None
    strict-transport-security: max-age=31536000
    x-frame-options: SAMEORIGIN
    x-xss-protection: 0
    x-content-type-options: nosniff
  
```

The 'Request Headers' section shows:

```

    authority: www.google.com
    method: GET
    path: /
    sec-ch-ua: "Not A Brand";v="1", "Chromium";v="113", "Google Chrome";v="113"
    sec-ch-ua-mobile: ?0
    sec-ch-ua-platform: "Windows"
    user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.145 Safari/537.36
  
```

## 6. Asynchronous HTTP requests

1) The 2 screenshots below show the request and response headers.

The screenshot shows the Network tab in the Chrome DevTools developer tools. A request to `google.com` is selected. In the Headers section, the 'General' section shows:

```

    Request URL: https://www.google.com/complete/search?q=Portland&z=5&t=p&p=14&client=gws-wiz&xss1=t&hl=en&authuser=0&ps=1&qs=2ZPExOHQ8Q-D4KPoQ_161775722698&dp=1.25
    Request Method: GET
    Status Code: 200
    Remote Address: [2507:f8b0:400a:80a::2004]:443
    Referrer Policy: origin
  
```

The 'Response Headers' section shows:

```

    accept-ch: Sec-CH-UA-Platform
    accept-ch: Sec-CH-UA-Platform-Version
    accept-ch: Sec-CH-UA-Full-Version
    accept-ch: Sec-CH-UA-Arch
    accept-ch: Sec-CH-UA-Model
    accept-ch: Sec-CH-UA-Bitness
    accept-ch: Sec-CH-UA-Full-Version-List
    accept-ch: Sec-CH-UA-WoW64
    alt-svc: h3=":443"; ma=2592000;h3-29=":443"; ma=2592000
    cache-control: private, max-age=3600
    content-disposition: attachment; filename=f.txt
  
```

The screenshot shows the Network tab of the Google Chrome developer tools. A request to `google.com` is selected. In the Headers section, a custom header `Odin ID: vishrut` is visible. The Response tab shows the JSON payload returned by Google.

```
Odin ID: vishrut
[{"q": "Portland State", "r": "1"}]
```

The screenshot below shows that the payload has returned the data that is then rendered on the search page.

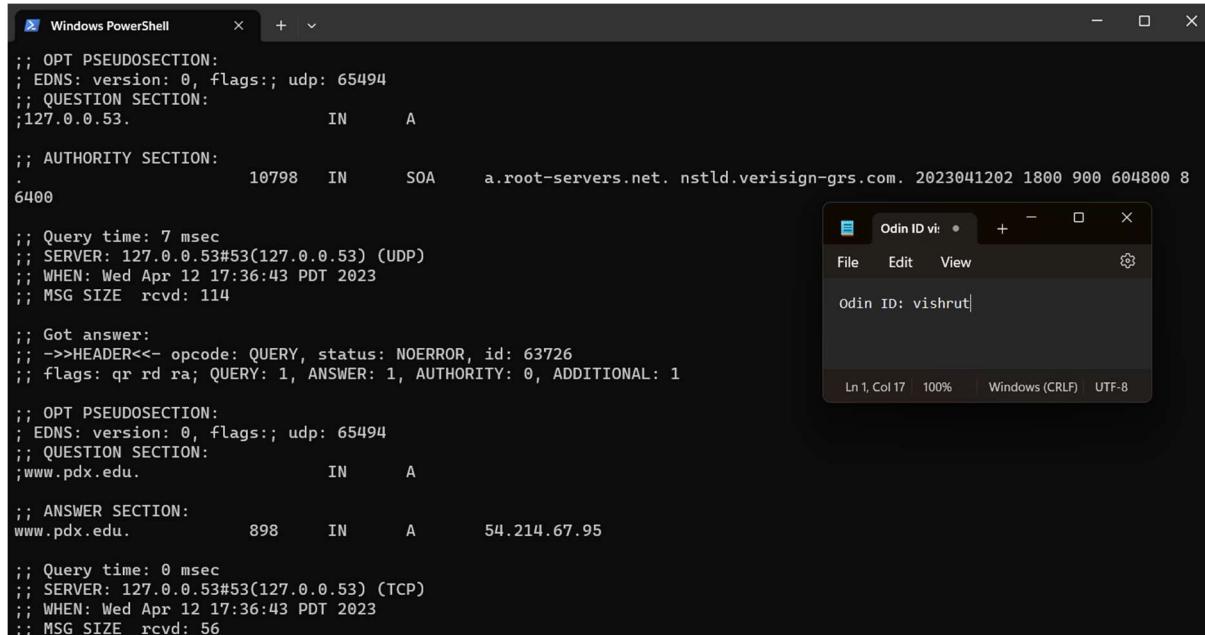
The screenshot shows the Network tab of the Google Chrome developer tools. A request to `google.com` is selected. In the Headers section, a custom header `Odin ID: vishrut` is visible. The Response tab shows the JSON payload returned by Google, which is then rendered as search results on the search page.

```
Odin ID: vishrut
[{"q": "Portland State", "r": "1"}]
```

## 02.2: DNS, Recap

### 1. DNS #1 (dig)

- 1) The ANSWER section of the A record for [www.pdx.edu](http://www.pdx.edu) indicates the IP address where PSU's web services are hosted. The ANSWER section of the MX record for pdx.edu indicates the hostnames of the mail servers where PSU's email services are hosted.



```
Windows PowerShell

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

;; AUTHORITY SECTION:
.          10798   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023041202 1800 900 604800 8
6400

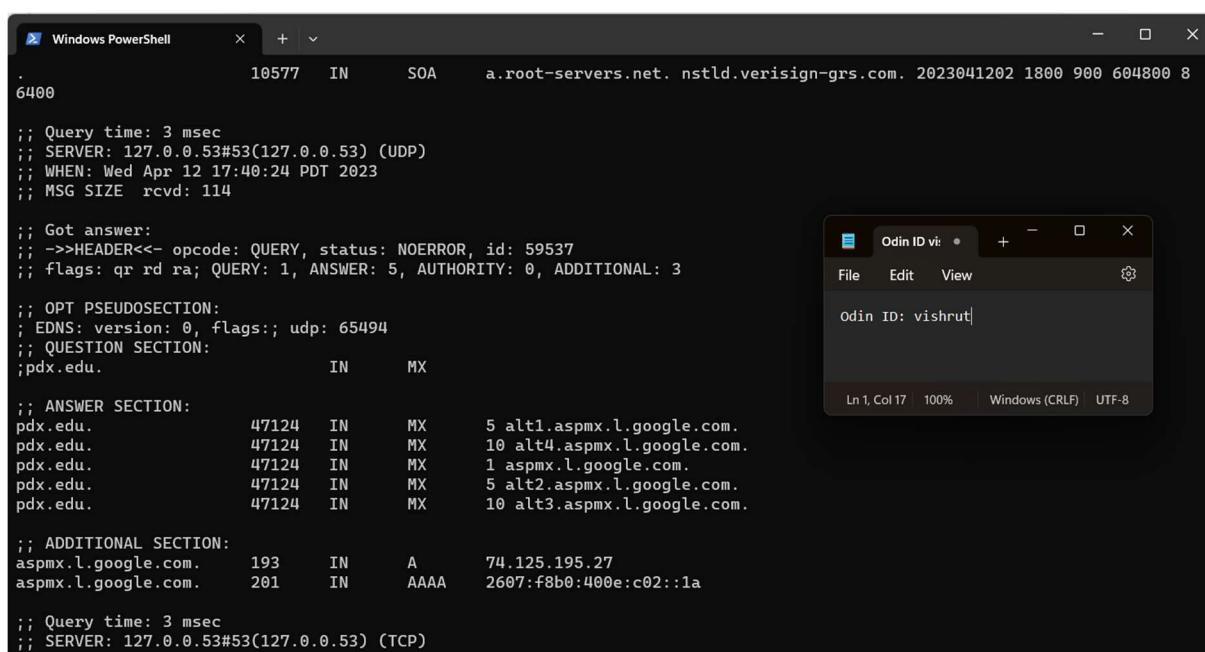
;; Query time: 7 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 17:36:43 PDT 2023
;; MSG SIZE  rcvd: 114

;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 63726
;; 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.      898     IN      A      54.214.67.95

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
;; WHEN: Wed Apr 12 17:36:43 PDT 2023
;; MSG SIZE  rcvd: 56
```



```
Windows PowerShell

.          10577   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023041202 1800 900 604800 8
6400

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 17:40:24 PDT 2023
;; MSG SIZE  rcvd: 114

;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 59537
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 3

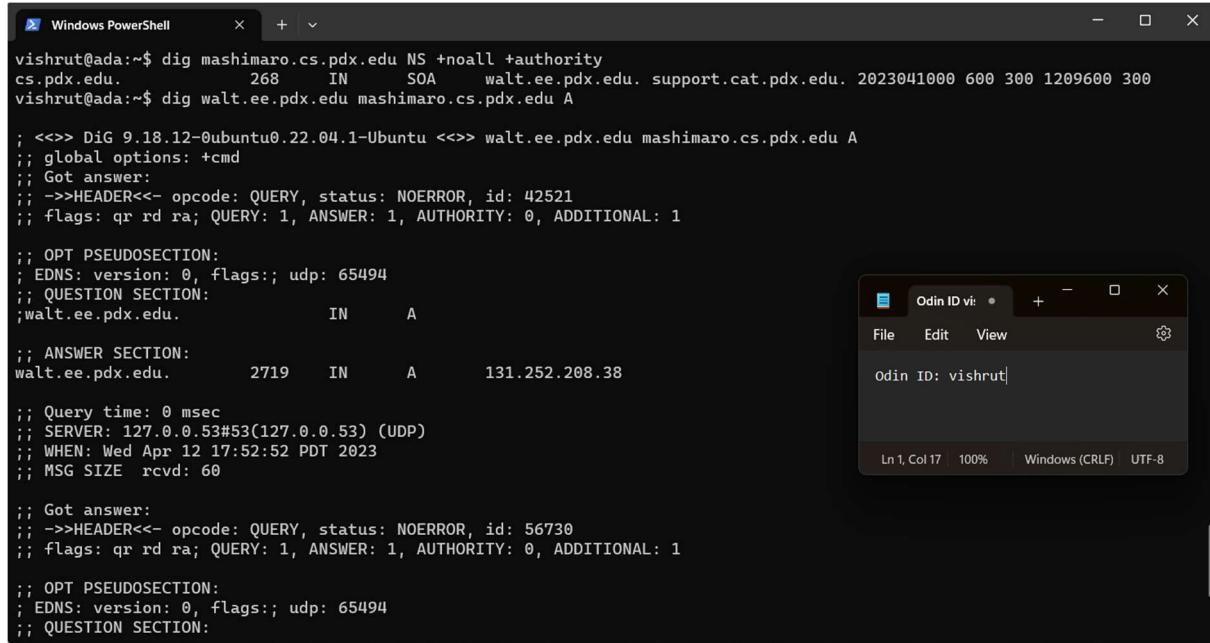
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;pdx.edu.          IN      MX

;; ANSWER SECTION:
pdx.edu.        47124   IN      MX      5 alt1.aspmx.l.google.com.
pdx.edu.        47124   IN      MX      10 alt4.aspmx.l.google.com.
pdx.edu.        47124   IN      MX      1 aspmx.l.google.com.
pdx.edu.        47124   IN      MX      5 alt2.aspmx.l.google.com.
pdx.edu.        47124   IN      MX      10 alt3.aspmx.l.google.com.

;; ADDITIONAL SECTION:
aspmx.l.google.com. 193     IN      A       74.125.195.27
aspmx.l.google.com. 201     IN      AAAA    2607:f8b0:400e:c02::1a

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
```

- 2) The screenshot below shows the authoritative server of mashimaro.cs.pdx.edu and also the result after querying walt.ee.pdx.edu for the A record of mashimaro.cs.pdx.edu.



```
vishrut@ada:~$ dig mashimaro.cs.pdx.edu NS +noall +authority
mashimaro.cs.pdx.edu. 268 IN SOA walt.ee.pdx.edu. support.cat.pdx.edu. 2023041000 600 300 1209600 300
vishrut@ada:~$ dig walt.ee.pdx.edu mashimaro.cs.pdx.edu A
; <>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <>> walt.ee.pdx.edu mashimaro.cs.pdx.edu A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 42521
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

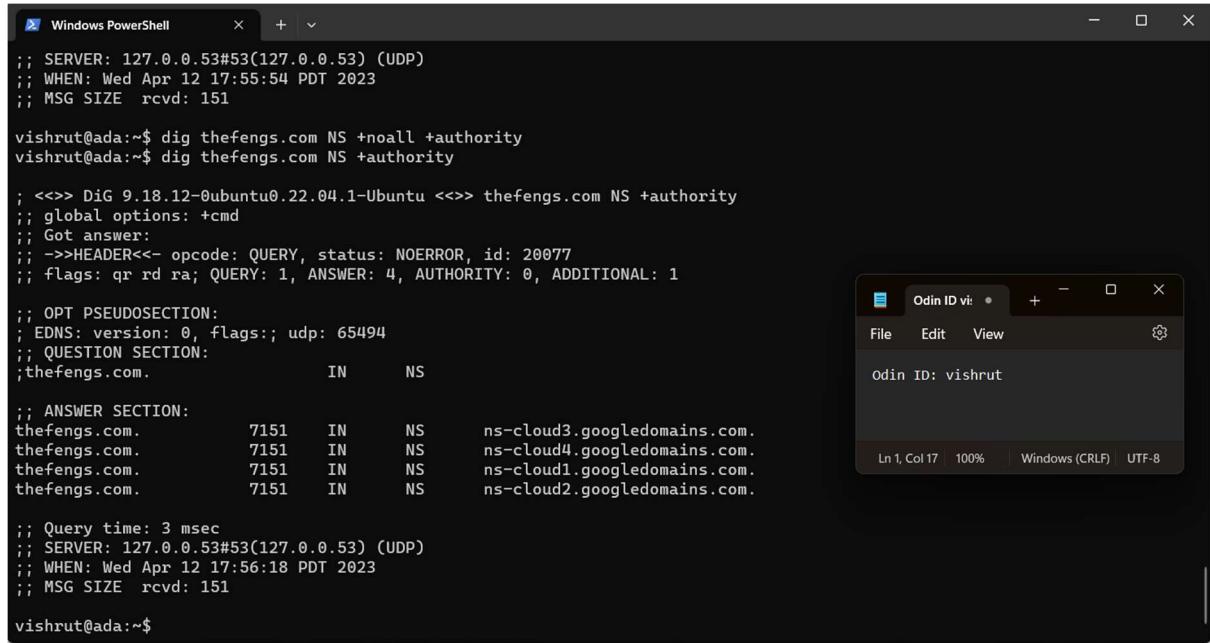
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;walt.ee.pdx.edu. IN A
;; ANSWER SECTION:
walt.ee.pdx.edu. 2719 IN A 131.252.208.38

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 17:52:52 PDT 2023
;; MSG SIZE rcvd: 60

;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 56730
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
```

- 3) The screenshots below show the authoritative server for thefengs.com and the result after querying that server for the A record of thefengs.com.



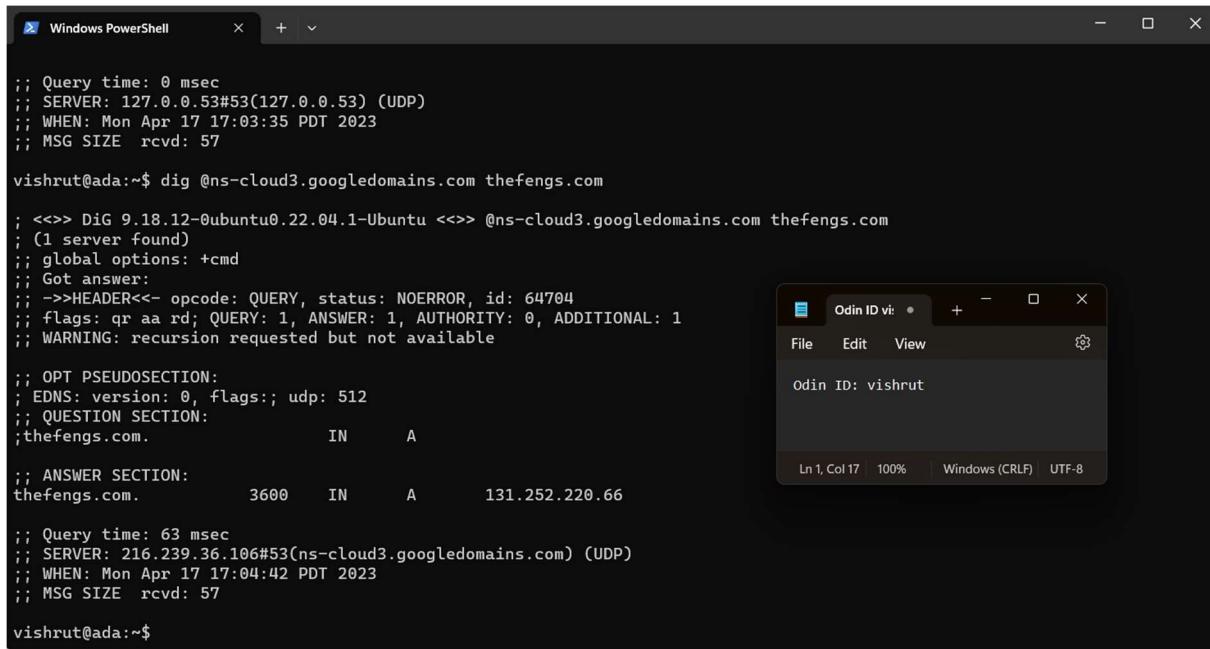
```
vishrut@ada:~$ dig thefengs.com NS +noall +authority
vishrut@ada:~$ dig thefengs.com NS +authority

; <>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <>> thefengs.com NS +authority
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 20077
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;thefengs.com. IN NS
;; ANSWER SECTION:
thefengs.com. 7151 IN NS ns-cloud3.googledomains.com.
thefengs.com. 7151 IN NS ns-cloud4.googledomains.com.
thefengs.com. 7151 IN NS ns-cloud1.googledomains.com.
thefengs.com. 7151 IN NS ns-cloud2.googledomains.com.

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 17:56:18 PDT 2023
;; MSG SIZE rcvd: 151

vishrut@ada:~$
```



```

; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Apr 17 17:03:35 PDT 2023
;; MSG SIZE rcvd: 57

vishrut@ada:~$ dig @ns-cloud3.googledomains.com thefengs.com

; <>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <>> @ns-cloud3.googledomains.com thefengs.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 64704
;; 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

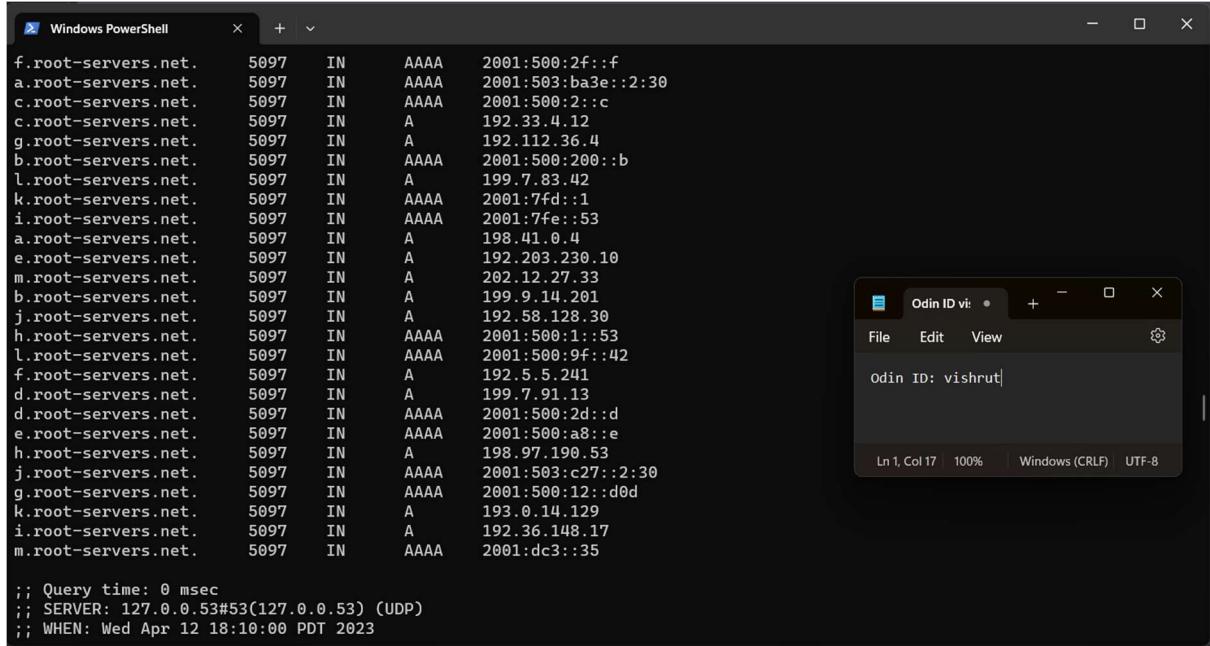
;; ANSWER SECTION:
thefengs.com.      3600    IN      A       131.252.220.66

; Query time: 63 msec
;; SERVER: 216.239.36.106#53(ns-cloud3.googledomains.com) (UDP)
;; WHEN: Mon Apr 17 17:04:42 PDT 2023
;; MSG SIZE rcvd: 57

vishrut@ada:~$
```

4) When a web request hits port 80 of 131.252.220.66, the server uses the HTTP protocol to determine which site to serve from. Specifically, the HTTP protocol uses the ‘Host’ header in the HTTP request to determine which site to serve.

5) The screenshots below show the result of the DNS iterative lookup of www.amazon.co.uk



```

Windows PowerShell - f.root-servers.net.      5097   IN      AAAA    2001:500:2f::f
Windows PowerShell - a.root-servers.net.      5097   IN      AAAA    2001:503:ba3e::2:30
Windows PowerShell - c.root-servers.net.      5097   IN      AAAA    2001:500:2::c
Windows PowerShell - c.root-servers.net.      5097   IN      A      192.33.4.12
Windows PowerShell - g.root-servers.net.      5097   IN      A      192.112.36.4
Windows PowerShell - b.root-servers.net.      5097   IN      AAAA    2001:500:200::b
Windows PowerShell - l.root-servers.net.      5097   IN      A      199.7.83.42
Windows PowerShell - k.root-servers.net.      5097   IN      AAAA    2001:7fd::1
Windows PowerShell - i.root-servers.net.      5097   IN      AAAA    2001:7fe::53
Windows PowerShell - a.root-servers.net.      5097   IN      A      198.41.0.4
Windows PowerShell - e.root-servers.net.      5097   IN      A      192.203.230.10
Windows PowerShell - m.root-servers.net.      5097   IN      A      202.12.27.33
Windows PowerShell - b.root-servers.net.      5097   IN      A      199.9.14.201
Windows PowerShell - j.root-servers.net.      5097   IN      A      192.58.128.30
Windows PowerShell - h.root-servers.net.      5097   IN      AAAA    2001:500:1::53
Windows PowerShell - l.root-servers.net.      5097   IN      AAAA    2001:500:9f::42
Windows PowerShell - f.root-servers.net.      5097   IN      A      192.5.5.241
Windows PowerShell - d.root-servers.net.      5097   IN      A      199.7.91.13
Windows PowerShell - d.root-servers.net.      5097   IN      AAAA    2001:500:2d::d
Windows PowerShell - e.root-servers.net.      5097   IN      AAAA    2001:500:a8::e
Windows PowerShell - h.root-servers.net.      5097   IN      A      198.97.190.53
Windows PowerShell - j.root-servers.net.      5097   IN      AAAA    2001:503:c27::2:30
Windows PowerShell - g.root-servers.net.      5097   IN      AAAA    2001:500:12::d0d
Windows PowerShell - k.root-servers.net.      5097   IN      A      193.0.14.129
Windows PowerShell - i.root-servers.net.      5097   IN      A      192.36.148.17
Windows PowerShell - m.root-servers.net.      5097   IN      AAAA    2001:dc3::35

; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 18:10:00 PDT 2023
```

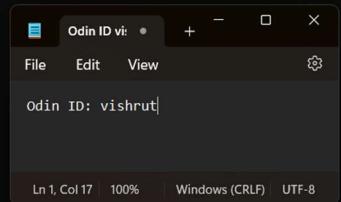
Windows PowerShell

```
vishruti@ada:~$ dig @192.5.5.241 +norecurse www.amazon.co.uk. NS +tcp
; <>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <>> @192.5.5.241 +norecurse www.amazon.co.uk. NS +tcp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58035
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 17

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65535
;; QUESTION SECTION:
;www.amazon.co.uk.      IN      NS

;; 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   2001:502:ad09::3
nsb.nic.uk.    172800  IN      A       156.154.101.3
nsb.nic.uk.    172800  IN      AAAA   2001:502:2eda::3
nsc.nic.uk.    172800  IN      A       156.154.102.3
```



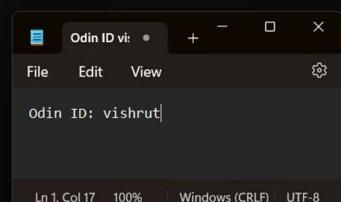
Windows PowerShell

```
vishruti@ada:~$ dig @nsa.nic.uk. +norecurse www.amazon.co.uk. NS +tcp
; <>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <>> @nsa.nic.uk. +norecurse www.amazon.co.uk. NS +tcp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32703
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 556592ea96d8c730100000064375b97ad5d742b03aee5be (good)
;; QUESTION SECTION:
;www.amazon.co.uk.      IN      NS

;; AUTHORITY SECTION:
amazon.co.uk.    172800  IN      NS      pdns4.ultradrns.org.
amazon.co.uk.    172800  IN      NS      pdns5.ultradrns.info.
amazon.co.uk.    172800  IN      NS      ns1.p31.dyne.net.
amazon.co.uk.    172800  IN      NS      pdns3.ultradrns.org.
amazon.co.uk.    172800  IN      NS      pdns2.ultradrns.net.
amazon.co.uk.    172800  IN      NS      ns3.p31.dyne.net.
amazon.co.uk.    172800  IN      NS      pdns1.ultradrns.net.
amazon.co.uk.    172800  IN      NS      ns2.p31.dyne.net.
amazon.co.uk.    172800  IN      NS      pdns6.ultradrns.co.uk.
amazon.co.uk.    172800  IN      NS      ns4.p31.dyne.net.

;; Query time: 19 msec
;; SERVER: 156.154.100.3#53(nsa.nic.uk.) (TCP)
;; WHEN: Wed Apr 12 18:32:07 PDT 2023
```



```

Windows PowerShell

vishrut@ada:~$ dig @ns1.p31.dynect.net. +norecurse www.amazon.co.uk. NS +tcp

; <>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <>> @ns1.p31.dynect.net. +norecurse www.amazon.co.uk. NS +tcp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8629
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b8fb69a0fc48a65b0832676664375c12d26a4b791f6fe041 (good)
; QUESTION SECTION:
;www.amazon.co.uk.           IN      NS

;; ANSWER SECTION:
www.amazon.co.uk.     1800    IN      CNAME   tp.bfbdc3ca1-frontier.amazon.co.uk.

;; AUTHORITY SECTION:
bfbdc3ca1-frontier.amazon.co.uk. 900 IN NS      ns-1078.awsdns-06.org.
bfbdc3ca1-frontier.amazon.co.uk. 900 IN NS      ns-248.awsdns-31.com.
bfbdc3ca1-frontier.amazon.co.uk. 900 IN NS      ns-853.awsdns-42.net.
bfbdc3ca1-frontier.amazon.co.uk. 900 IN NS      ns-1624.awsdns-11.co.uk.

;; Query time: 15 msec
;; SERVER: 108.59.161.31#53(ns1.p31.dynect.net.) (TCP)
;; WHEN: Wed Apr 12 18:34:10 PDT 2023
;; MSG SIZE rcvd: 261

vishrut@ada:~$ |

```

## 2. Reverse DNS lookups

The screenshot below shows the result of running a single command line with commands dig, egrep, and awk, to list all IPv4 addresses that espn.go.com points to.

And also the result of looping over the IPv4 addresses and performing reverse lookups to get the DNS server names.

```

Windows PowerShell

/vishrut@ada:~$ dig +short espn.go.com | egrep '^[[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$' | awk '{ print $1 }'
18.161.6.89
18.161.6.94
18.161.6.38
18.161.6.80
vishrut@ada:~$ X='dig +short espn.go.com | egrep '^[[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$' | awk '{ print $1 }'
vishrut@ada:~$ for ip in X; do
    host $ip
done
Host X not found: 2(SERVFAIL)
vishrut@ada:~$ for ip in `echo $X`; do
    host $ip;
done
17.66.84.99.in-addr.arpa domain name pointer server-99-84-66-17.hio50.r.cloudfront.net.
98.66.84.99.in-addr.arpa domain name pointer server-99-84-66-98.hio50.r.cloudfront.net.
55.66.84.99.in-addr.arpa domain name pointer server-99-84-66-55.hio50.r.cloudfront.net.
108.66.84.99.in-addr.arpa domain name pointer server-99-84-66-108.hio50.r.cloudfront.net.
vishrut@ada:~$ for ip in `echo $X`; do
    host $ip;
done | egrep -v 'not found' | awk '{ print $NF }'
server-99-84-66-17.hio50.r.cloudfront.net.
server-99-84-66-98.hio50.r.cloudfront.net.
server-99-84-66-55.hio50.r.cloudfront.net.
server-99-84-66-108.hio50.r.cloudfront.net.
vishrut@ada:~$ |

```

### 3. Host enumeration

The screenshot below shows the set of car manufacturers names.

A screenshot of a Windows PowerShell window titled "Windows PowerShell". The command `cat 220hosts.txt | head -185 | tail -30` was run, displaying a list of car manufacturer names ending with ".cs.pdx.edu". To the right, a small window titled "Odin ID vi" shows the text "Odin ID: vishrut".

```
vw.cs.pdx.edu.  
vishrut@ada:~$ cat 220hosts.txt | head -185 | tail -30  
acura.cs.pdx.edu.  
astonmartin.cs.pdx.edu.  
audi.cs.pdx.edu.  
bentley.cs.pdx.edu.  
bmw.cs.pdx.edu.  
cadillac.cs.pdx.edu.  
ferari.cs.pdx.edu.  
fiat.cs.pdx.edu.  
ford.cs.pdx.edu.  
honda.cs.pdx.edu.  
hummer.cs.pdx.edu.  
jaguar.cs.pdx.edu.  
jeep.cs.pdx.edu.  
lamborghini.cs.pdx.edu.  
landrover.cs.pdx.edu.  
lexus.cs.pdx.edu.  
lotus.cs.pdx.edu.  
maserati.cs.pdx.edu.  
mazda.cs.pdx.edu.  
mclaren.cs.pdx.edu.  
mercedes.cs.pdx.edu.  
nissan.cs.pdx.edu.  
panoz.cs.pdx.edu.  
porsche.cs.pdx.edu.  
subaru.cs.pdx.edu.  
toyota.cs.pdx.edu.  
tvr.cs.pdx.edu.  
ultima.cs.pdx.edu.  
volvo.cs.pdx.edu.  
vw.cs.pdx.edu.  
vishrut@ada:~$ |
```

### 4. DNS #2 (Geographic DNS)

#### 1) Result of ipinfo.io and DB-IP

A screenshot of a web page comparing geolocation data from three sources: ipinfo.io, DB-IP, and IPRegistry.co. All three sources show the same results for the IP address 131.252.208.53, which is associated with Portland State University in Portland, Oregon, United States.

**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 (pdx.edu)

Odin ID vi window:  
Odin ID: vishrut

DNS Lookup links:  
Who is Hosting a Website  
Domain Age Checker  
Is my website down?  
Subnet Calculator

Popular Articles:  
Find IP address of a network printer?  
Find IP addresses of a private network  
How to wire a RJ-45 cable?  
What is the difference between public and private IP address?  
What is static and dynamic IP addresses?  
What is an IP Address?

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

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

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

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

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

Subnet Calculator window:

- Odin ID: vishrut
- What is static and dynamic IP addresses?
- What is an IP Address?
- What is a Proxy Server?
- My IP address is hacked. What do I do?

ADVERTISEMENT: COMCAST BUSINESS Get products that grow as you grow. GET IT NOW! (855) 335-7919

2)

```
porsche.cs.pdx.edu.
subaru.cs.pdx.edu.
toyota.cs.pdx.edu.
tvr.cs.pdx.edu.
ultima.cs.pdx.edu.
volvo.cs.pdx.edu.
vw.cs.pdx.edu.
vishrut@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: 16614
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e32fb2d1b5b4512901000000643766bbea199aacc16b9ed9 (good)
; QUESTION SECTION:
;www.google.com.           IN      A

;; ANSWER SECTION:
www.google.com.        153     IN      A      142.251.33.100

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Wed Apr 12 19:19:39 PDT 2023
;; MSG SIZE  rcvd: 87

vishrut@ada:~$
```

Subnet Calculator window:

- Odin ID: vishrut

```

Windows PowerShell
vishrut@ada:~$ 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: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a01f77242e87f5c44adeb1d36437674e1d032adda9efb7a5 (good)
; QUESTION SECTION:
;www.google.com.           IN      A

;; ANSWER SECTION:
www.google.com.    166    IN      A      172.253.62.105
www.google.com.    166    IN      A      172.253.62.147
www.google.com.    166    IN      A      172.253.62.103
www.google.com.    166    IN      A      172.253.62.106
www.google.com.    166    IN      A      172.253.62.104
www.google.com.    166    IN      A      172.253.62.99

;; Query time: 67 msec
;; SERVER: 198.82.247.66#53(198.82.247.66) (UDP)
;; WHEN: Wed Apr 12 19:22:06 PDT 2023
;; MSG SIZE rcvd: 167

vishrut@ada:~$
```

3) Below are the distances between each DNS server and the IP address

142.251.33.100 to 172.253.62.105 -> 2016 n mi, 3734 km

142.251.33.100 to 172.253.62.103 -> 2016 n mi, 3734 km

142.251.33.100 to 172.253.62.147 -> 611 n mi, 1132 km

142.251.33.100 to 172.253.62.104 -> 2016 n mi, 3734 km

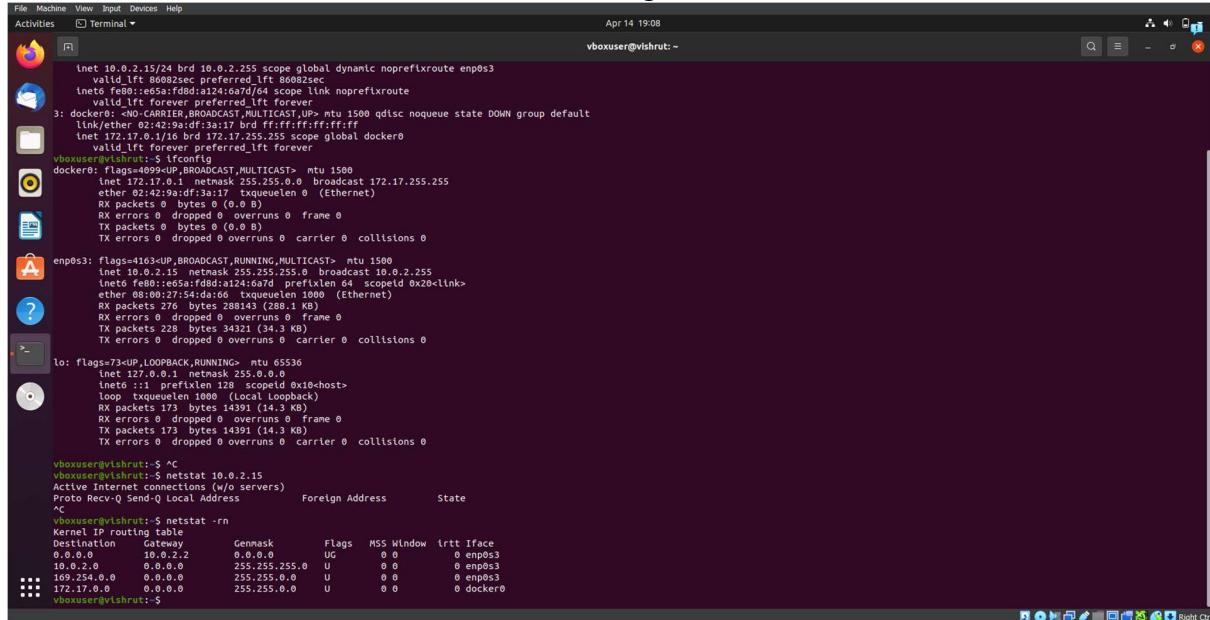
142.251.33.100 to 172.253.62.106 -> 2016 n mi, 3734 km

142.251.33.100 to 172.253.62.99 -> 2016 n mi, 3734 km

4) No, there is no clear indication of the geographic location of the servers in the traceroute.

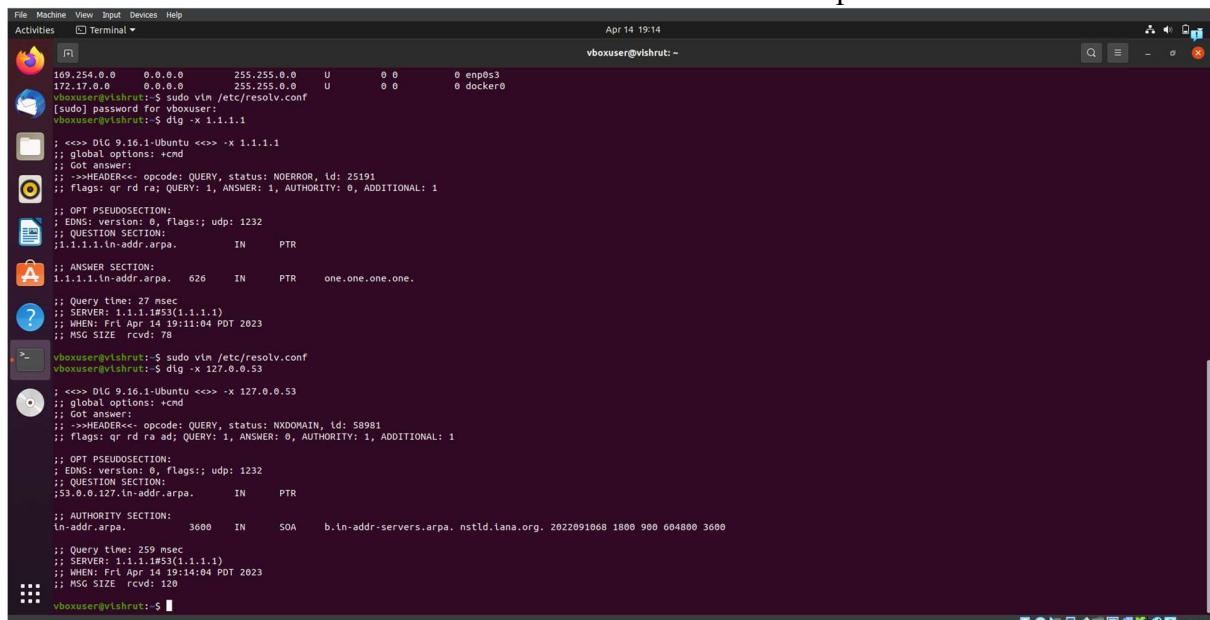
## 5. Network Recap Lab #3

The screenshot below shows the results of ifconfig and the netstat commands.



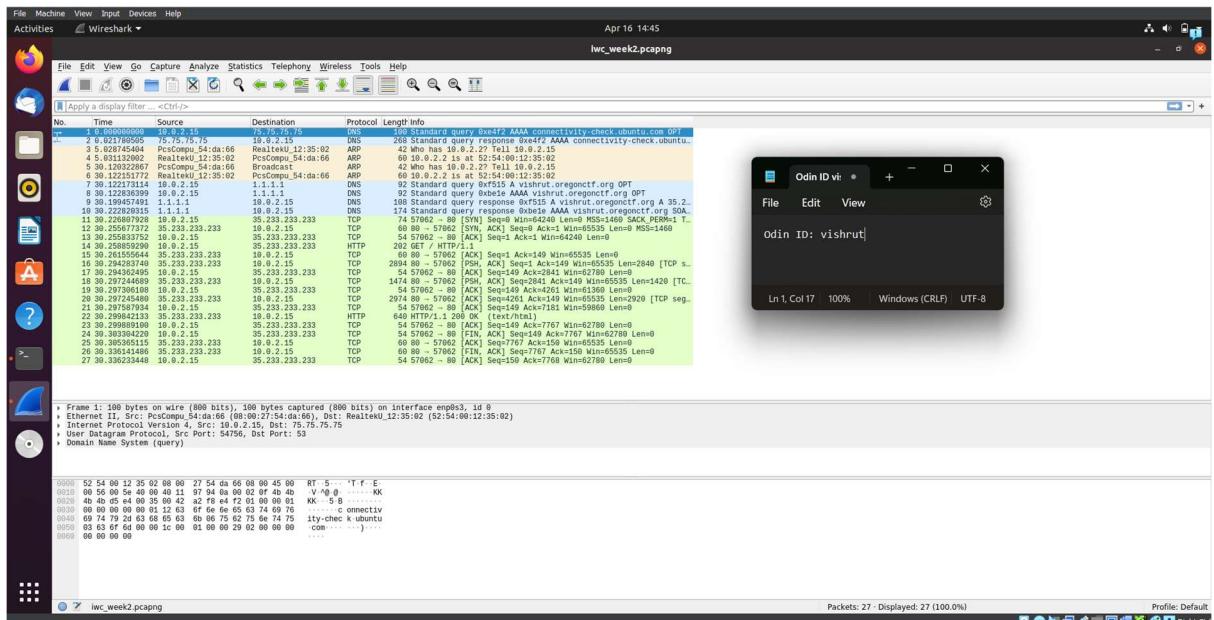
```
File Machine View Input Devices Help
Activities Terminal Apr 14 19:08
vboxuser@vishrut: ~
ifconfig
inet 10.0.2.15 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
    valid_lft 86082sec preferred_lft 86082sec
    inet6 fe80::e65af:fd8d:a124:6a7d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:9a:df:3a:17 brd ff:ff:ff:ff:ff:ff
    txqueuelen 0 (Ethernet)
        valid_lft forever preferred_lft forever
vboxuser@vishrut: ~$ ifconfig
docker0: flags=4099UP,BROADCAST,MULTICAST mtu 1500
    inet 172.17.0.1 brd 172.17.0.255 broadcast 172.17.255.255
        netmask 255.255.255.0
        ether 02:42:9a:df:3a:17 txqueuelen 0 (Ethernet)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
enp0s3: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
    inet 10.0.2.15 brd 255.255.255.0 broadcast 10.0.2.255
        netmask 255.255.255.0
        ether 08:00:27:54:d4:7d txqueuelen 1000 (Ethernet)
            RX packets 173 bytes 14391 (14.3 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 228 bytes 34321 (34.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
    inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
            RX packets 173 bytes 14391 (14.3 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 173 bytes 14391 (14.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
vboxuser@vishrut: ~$ ^C
vboxuser@vishrut: ~$ netstat -an
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
*.*.vboxuser@vishrut: ~$ 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          0 enp0s3
10.0.2.0        0.0.0.0    255.255.255.0 U          0 0          0 enp0s3
169.254.0.0     0.0.0.0    255.255.0.0   U          0 0          0 enp0s3
172.17.0.0      0.0.0.0    255.255.0.0   U          0 0          0 docker0
vboxuser@vishrut: ~$
```

The screenshot below shows the result of the reverse DNS lookup on the DNS server.



```
File Machine View Input Devices Help
Activities Terminal Apr 14 19:14
vboxuser@vishrut: ~
dig +short 1.1.1.1
; <>> DIG 9.16.1-Ubuntu <>> -x 1.1.1.1
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 25191
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
;; QUESTION SECTION:
;1.1.1.1.in-addr.arpa. IN PTR
;; ANSWER SECTION:
1.1.1.1.in-addr.arpa. 626 IN PTR one.one.one.one.
;; Query time: 27 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Fri Apr 14 19:14:04 PDT 2023
;; MSG SIZE rcvd: 78
vboxuser@vishrut: ~$ sudo vim /etc/resolv.conf
[vudo] password for vboxuser:
vboxuser@vishrut: ~$ dig +short 127.0.0.53
; <>> DIG 9.16.1-Ubuntu <>> -x 127.0.0.53
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 58981
;; flags: qr rd ra ad; 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. nstld.iana.org. 2022091068 1800 900 604800 3600
;; Query time: 259 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Fri Apr 14 19:14:04 PDT 2023
;; MSG SIZE rcvd: 120
vboxuser@vishrut: ~$
```

## 6. Collect and analyze the network trace of a connection



- 1) There are 3 DNS requests
- 2) There are 7 TCP connections initiated by the browser simultaneously to the site.
- 3) There is 1 HTTP GET request for the embedded object.