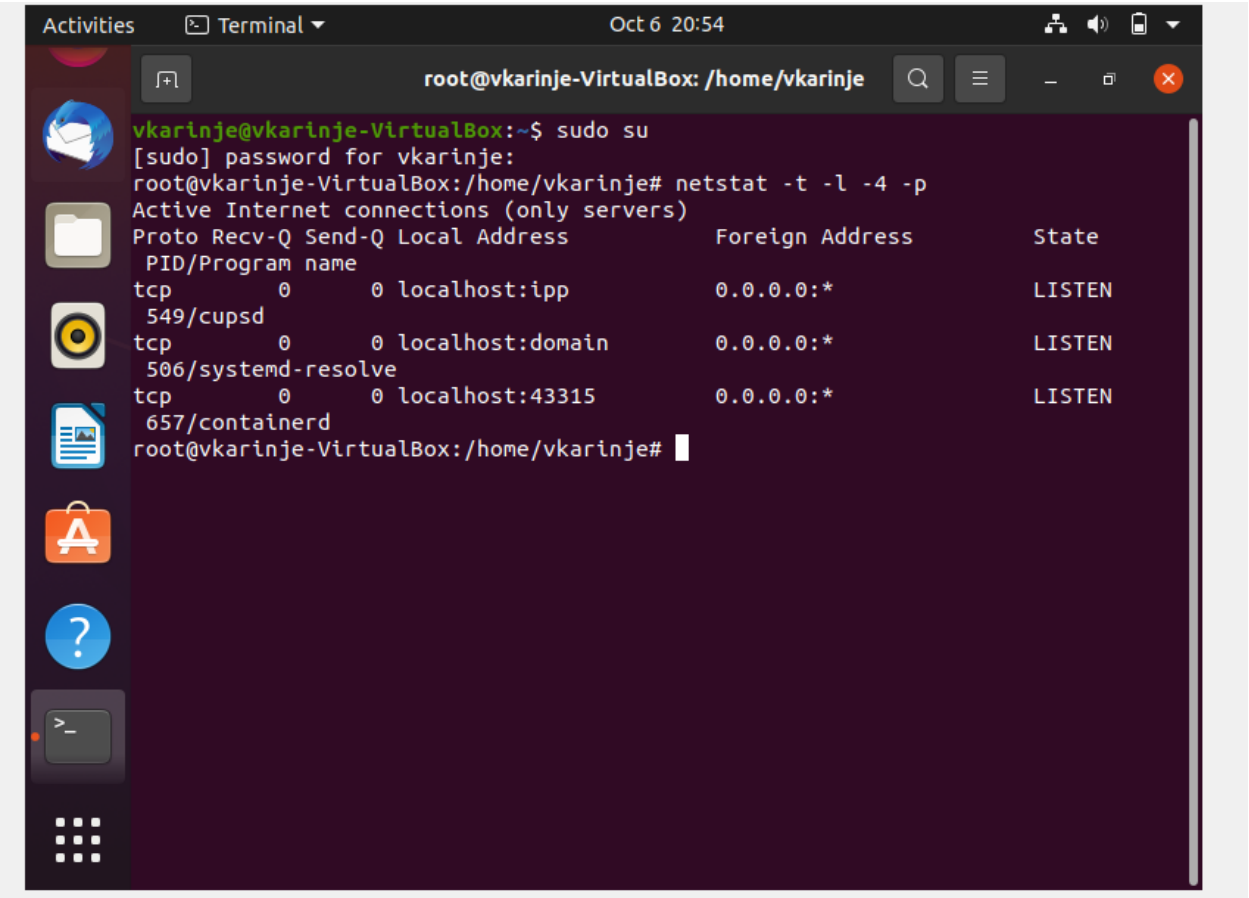
CS 530 INTERNET WEB AND CLOUD SYSTEMS

Name: Varsha Karinje
PSU ID: 925923534

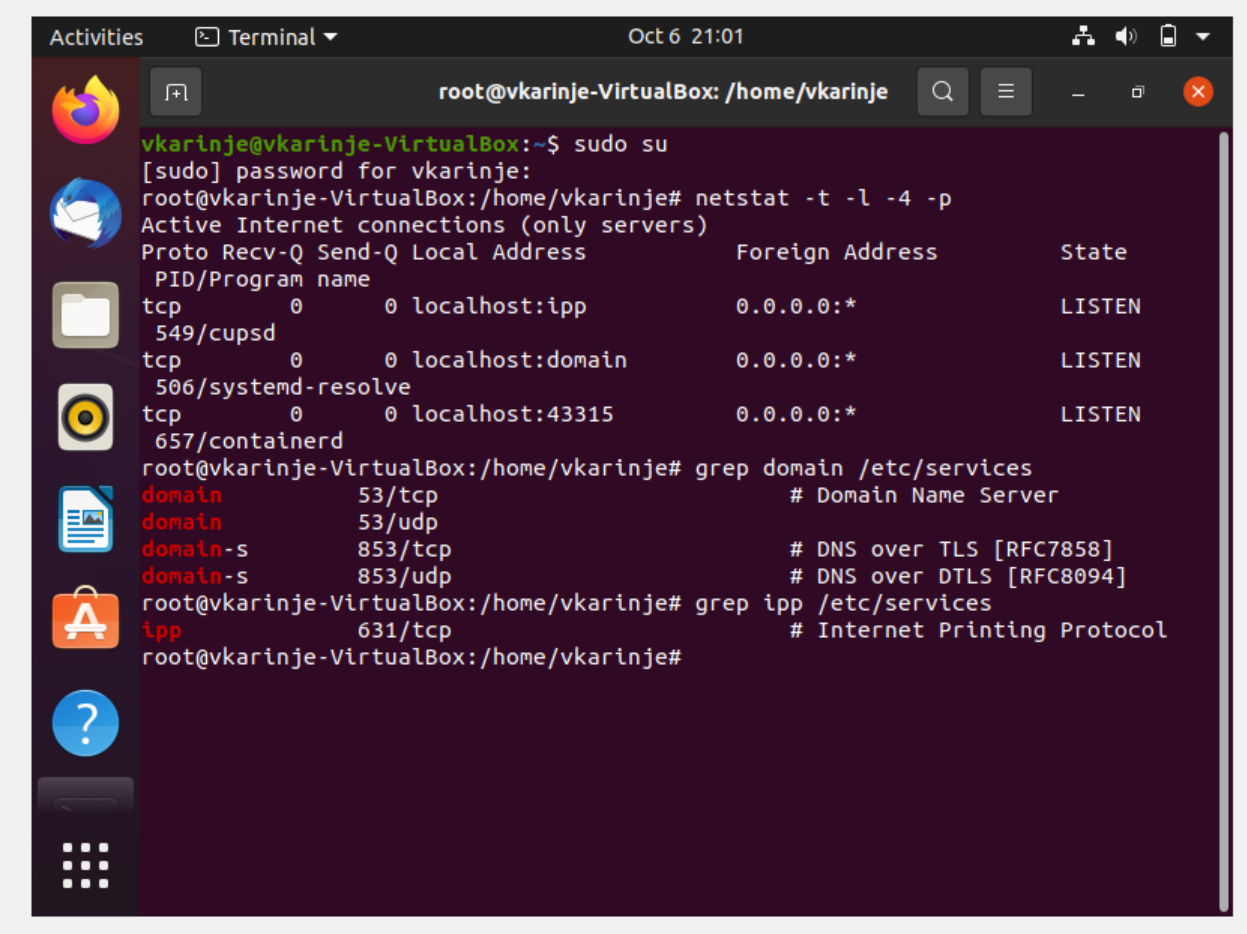
TCP #1 (netstat, lsof, nc)

netstat

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



- 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.



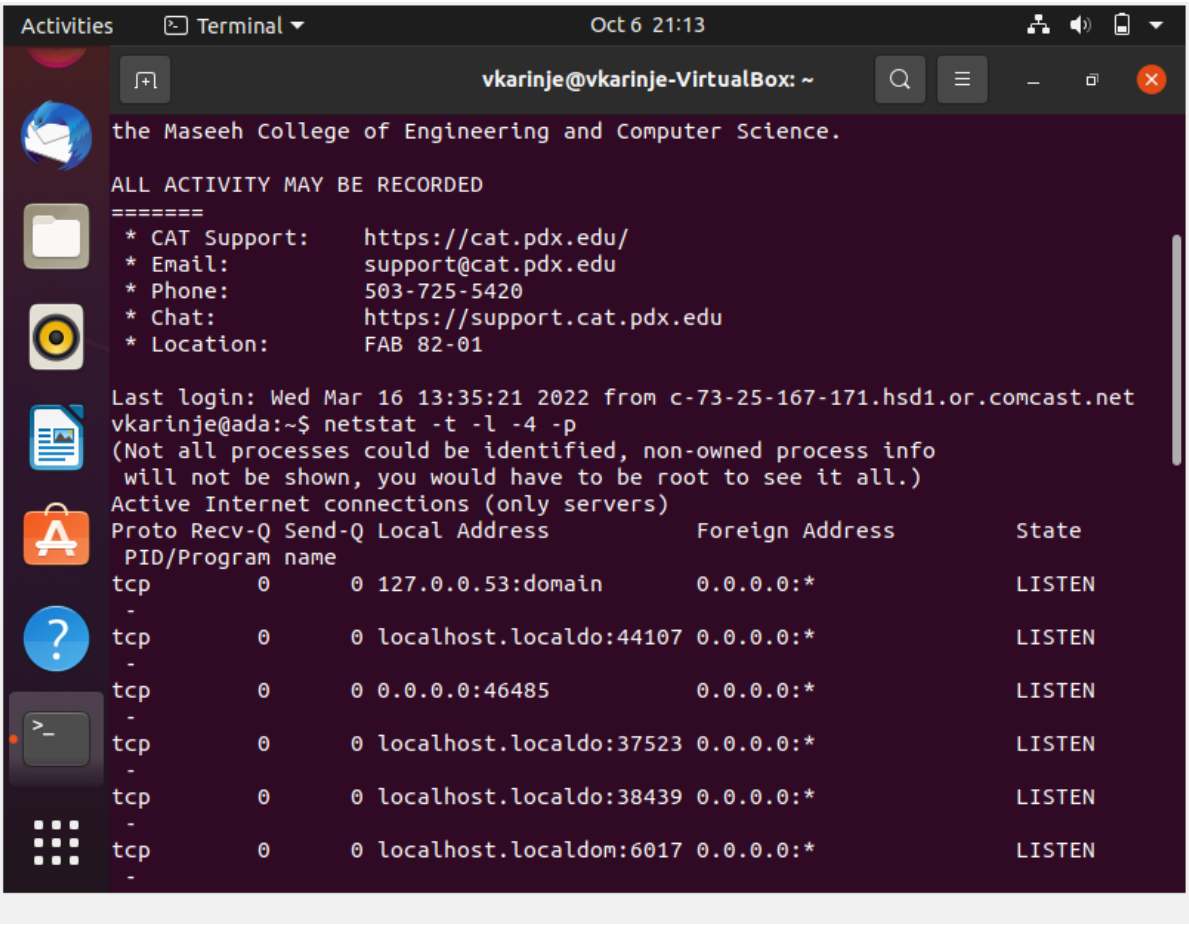
domain 53/tcp #Domain Name Server

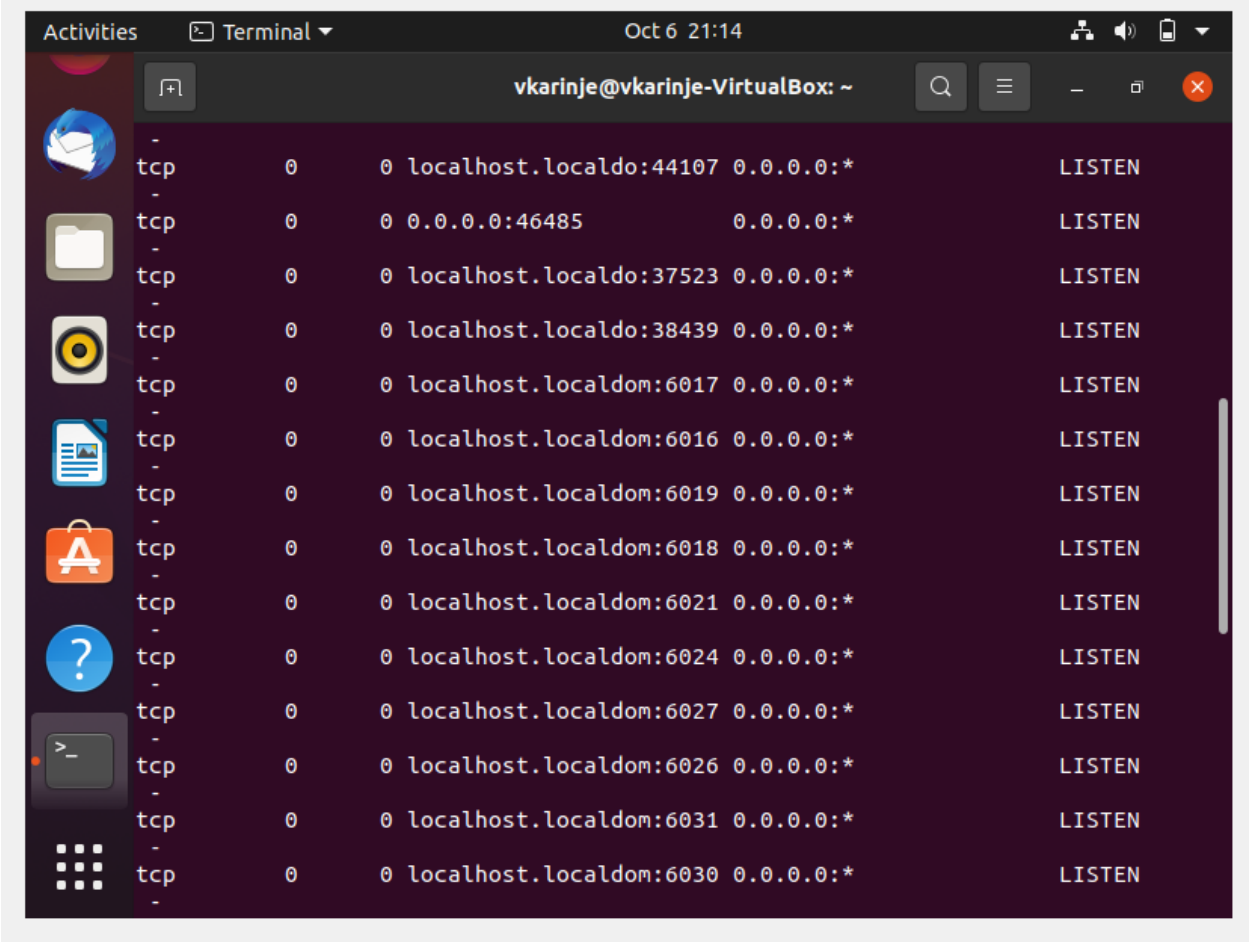
Ipp 631/tcp #Internet Printing Protocol

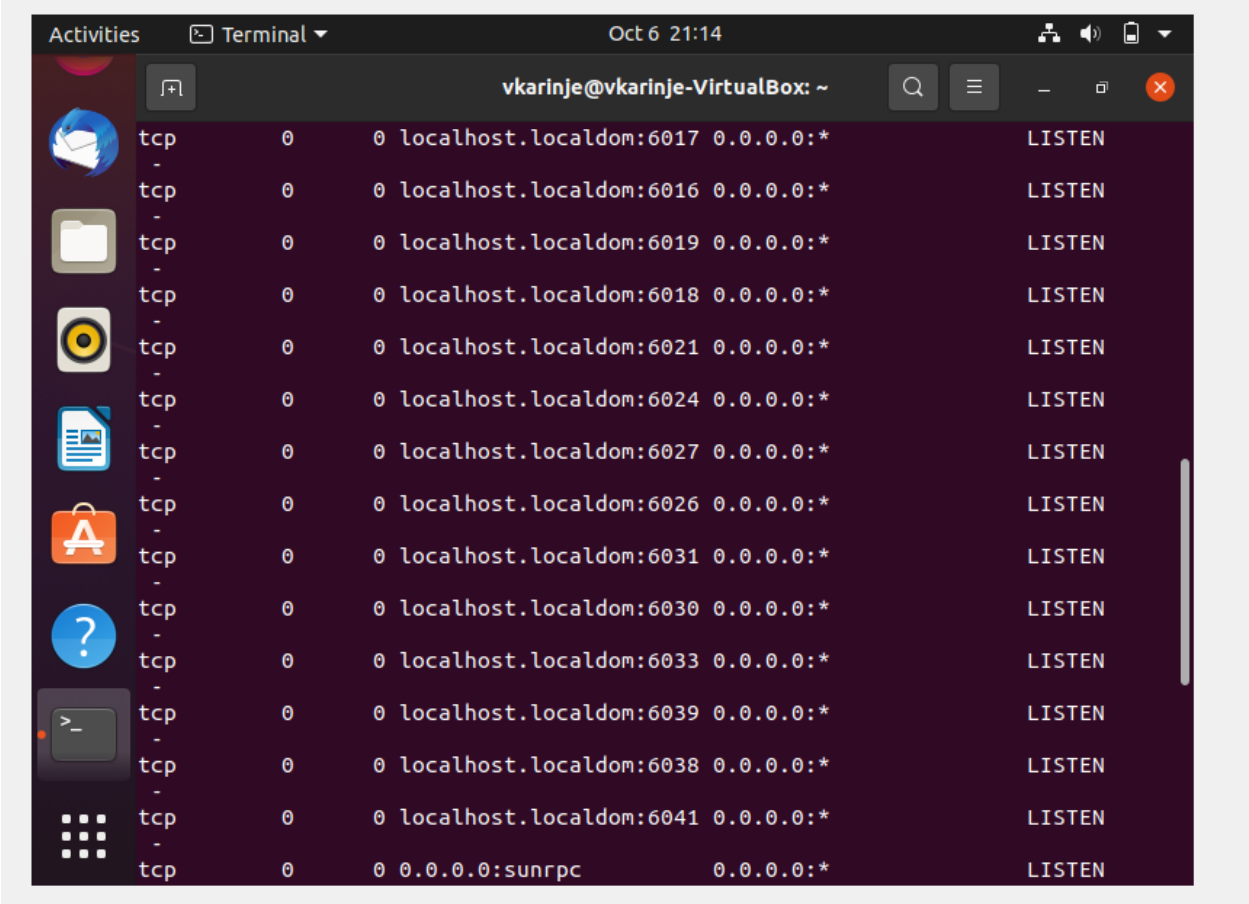
- For ports that only have a number, what service might it be providing based on the name of the program that is being run?

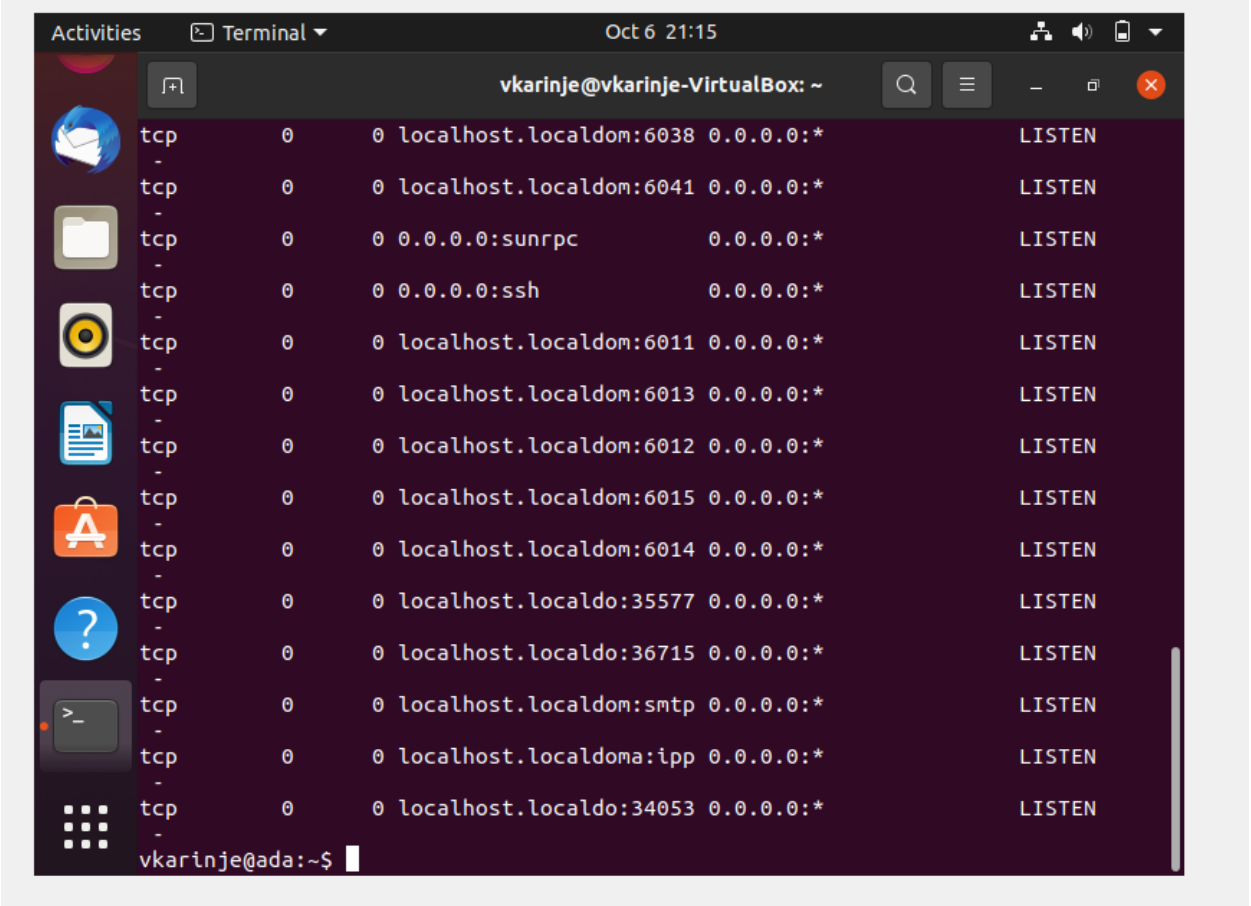
  Based on the name “containerd” for the ports that only have a number, it might be providing network service to docker.

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


Activities
Terminal
Oct 6 21:13
vkarinje@vkarinje-VirtualBox: ~
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: Wed Mar 16 13:35:21 2022 from c-73-25-167-171.hsd1.or.comcast.net
vkarinje@ada:~$ netstat -t -l -4 -p
(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 0 127.0.0.53:domain 0.0.0.0:* LISTEN
-
tcp 0 0 localhost.localdo:44107 0.0.0.0:* LISTEN
-
tcp 0 0 0.0.0.0:46485 0.0.0.0:* LISTEN
-
tcp 0 0 localhost.localdo:37523 0.0.0.0:* LISTEN
-
tcp 0 0 localhost.localdo:38439 0.0.0.0:* LISTEN
-
tcp 0 0 localhost.localdom:6017 0.0.0.0:* LISTEN
-


Activities
Terminal
Oct 6 21:14
vkarinje@vkarinje-VirtualBox: ~
tcp 0 0 localhost.localdo:44107 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:46485 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdo:37523 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdo:38439 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6017 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6016 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6019 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6018 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6021 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6024 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6027 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6026 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6031 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6030 0.0.0.0:* LISTEN


Activities
Terminal
Oct 6 21:14
vkarinje@vkarinje-VirtualBox: ~
tcp 0 0 localhost.localdom:6017 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6016 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6019 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6018 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6021 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6024 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6027 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6026 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6031 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6030 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6033 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6039 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6038 0.0.0.0:* LISTEN
tcp 0 0 localhost.localdom:6041 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:sunrpc 0.0.0.0:* LISTEN



- What services does this machine provide for external access?

  This machine provides ssh for logging into the machine and for executing the commands.
  smtp is used to deliver emails.
  ipp is used for printing information
  domain is the other service provided

lsof

Back on the Ubuntu VM, find the number of open descriptors using the following command.

```
vkarinje@vkarinje-VirtualBox:~$ sudo lsof | wc -l
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
26573
vkarinje@vkarinje-VirtualBox:~$
```

- 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

```
vkarinje@vkarinje-VirtualBox:~$ sudo lsof -iTCP -sTCP:LISTEN
[sudo] password for vkarinje:
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r 516 systemd-resolve   13u  IPv4  20608      0t0  TCP localhost:domain (LISTEN)
cupsd     562            root    6u  IPv6  23069      0t0  TCP ip6-localhost:ipp (LISTEN)
cupsd     562            root    7u  IPv4  23070      0t0  TCP localhost:ipp (LISTEN)
container 651            root   13u  IPv4  25544      0t0  TCP localhost:39431 (LISTEN)
vkarinje@vkarinje-VirtualBox:~$
```

nc

Include for your lab notebook, the version of ssh that is being used

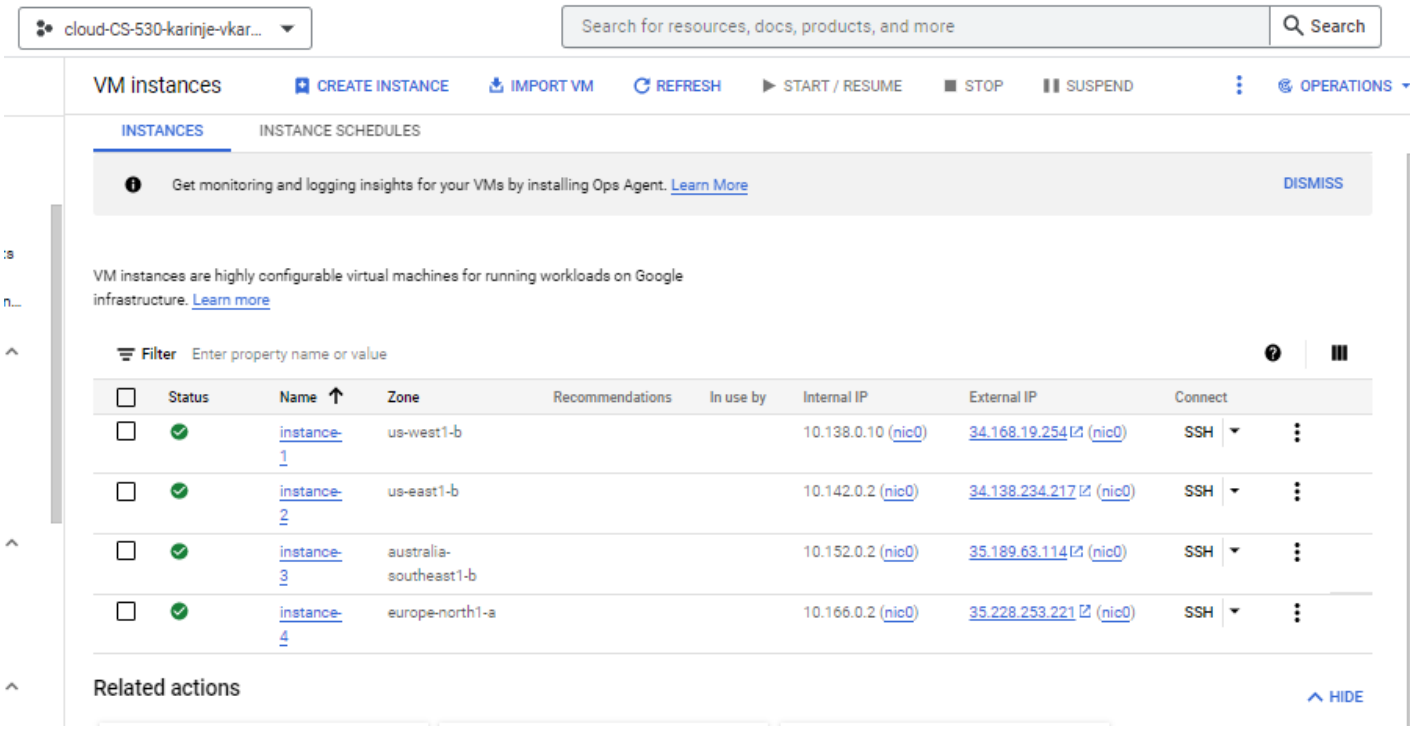
```
vkarinje@vkarinje-VirtualBox:~$ nc linux.cs.pdx.edu 22
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3
```

```
=======
 * 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 Oct  6 21:10:00 2022 from 10.200.235.254
vkarinje@ada:~$ ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 131.252.208.103  netmask 255.255.255.0  broadcast 131.252.208.255
        ether 52:54:00:13:a0:c6  txqueuelen 1000  (Ethernet)
        RX packets 1268051321  bytes 3427301833324 (3.4 TB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1276924673  bytes 1130112770236 (1.1 TB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 203429061  bytes 95399402638 (95.3 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 203429061  bytes 95399402638 (95.3 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vkarinje@ada:~$ nc 131.252.208.255
nc: missing port number
vkarinje@ada:~$ nc 131.252.208.255 22
vkarinje@ada:~$ nc 131.252.208.103 22
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3
```

The version of ssh is 2.0

TCP #2 (iperf)

Creating 4 VMs:one in us-west1-b, one in the US East, one in Australia, and one in Europe. For each machine's configuration, use the following:

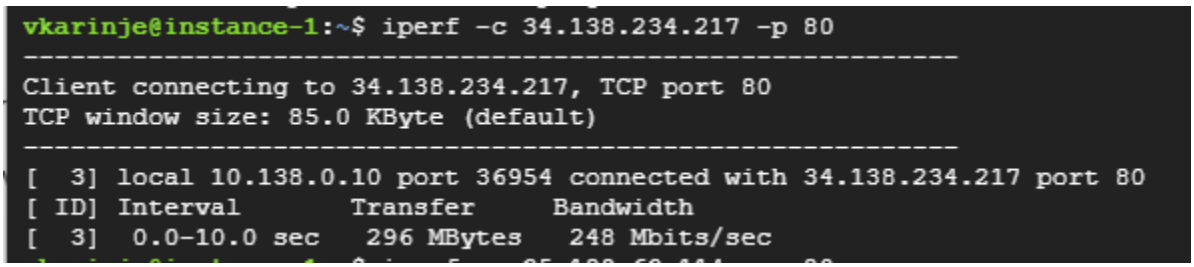


Throughput tests

On your us-west1-b VM, run iperf against each of the VMs created above by pointing the tool to the VM's external IP address.

- 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.

Instance -2 (us-east1-b)



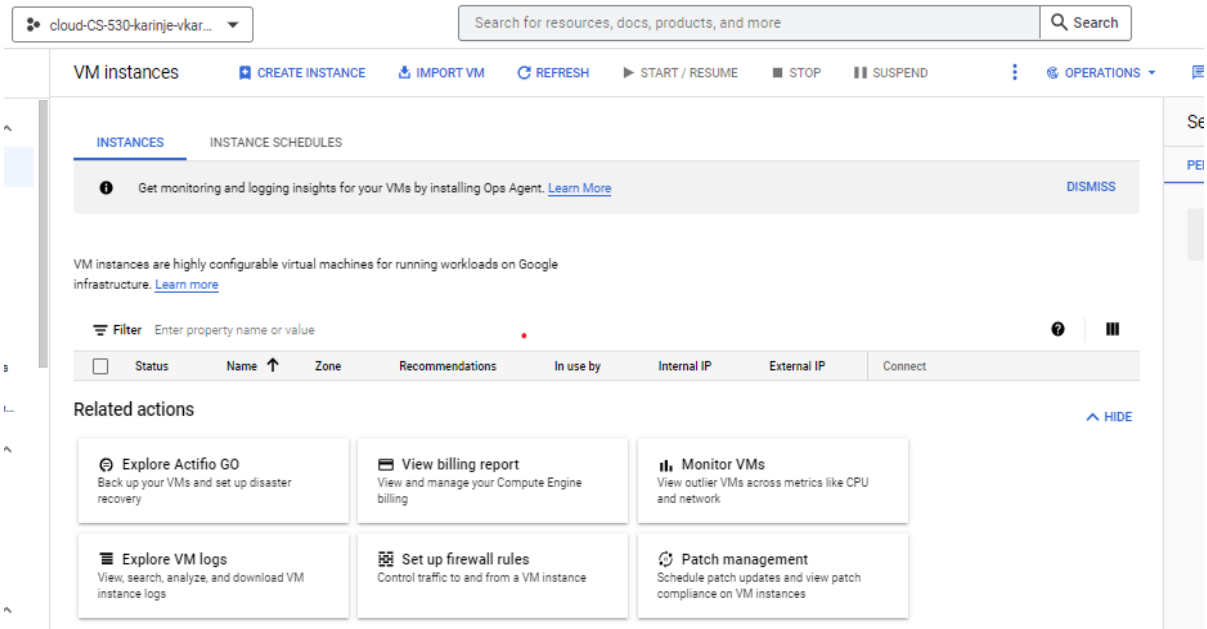
Instance -3 (australia-southeast1-b)

```
vkarinje@instance-1:~$ iperf -c 35.189.63.114  -p 80
------------------------------------------------------------
Client connecting to 35.189.63.114, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 10.138.0.10 port 50790 connected with 35.189.63.114 port 80
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.1 sec   106 MBytes  88.2 Mbits/sec
```

Instance -4 (europe-north1-a)

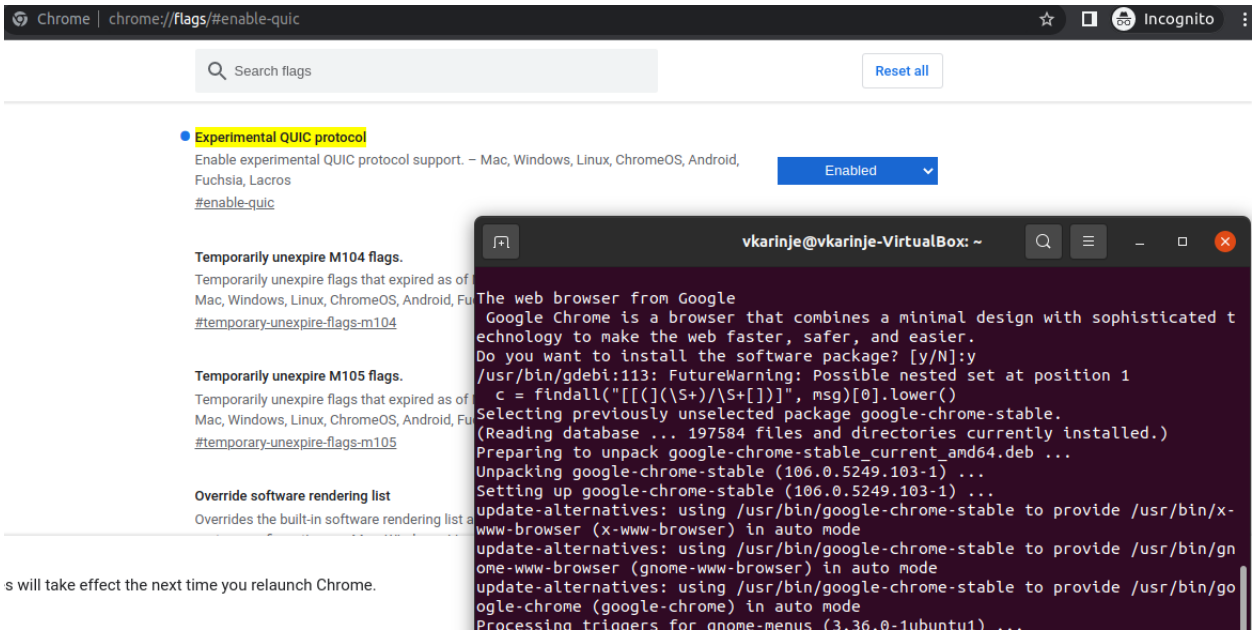
```
vkarinje@instance-1:~$ iperf -c 35.228.253.221  -p 80
------------------------------------------------------------
Client connecting to 35.228.253.221, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 10.138.0.10 port 47144 connected with 35.228.253.221 port 80
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.1 sec   115 MBytes  96.2 Mbits/sec
vkarinje@instance-1:~$
```

The bandwidth between us-west1-b and us-east1-b is 248 Mbits/sec
The bandwidth between us-west1-b and australia-southeast1-b is 88.2 Mbits/sec
The bandwidth between us-west1-b and europe-north1-a is 96.2 Mbits/sec
Hence, we can say that the maximum bandwidth is allocated to the instance that is located closer to us-west1-b.

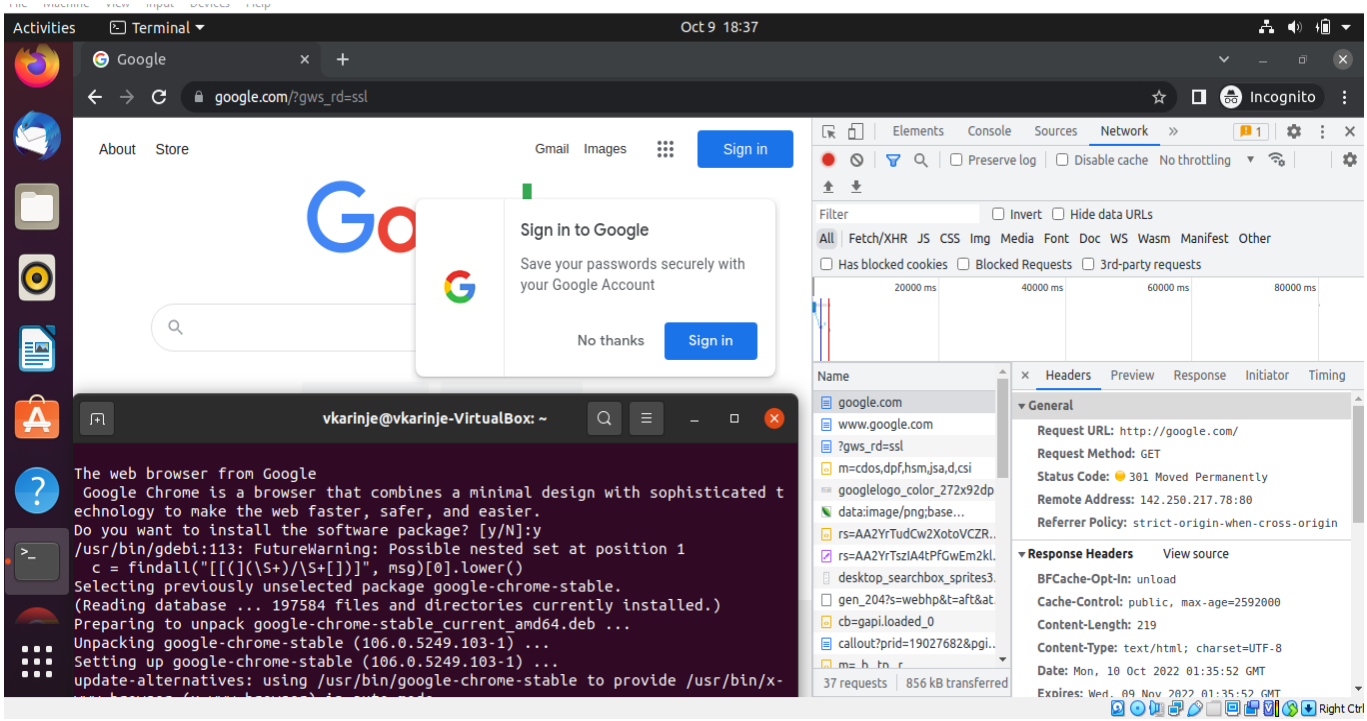


HTTP # 3 (Browser Tools)

Bring up an Incognito window (Ctrl+Shift+N). Then, in the address bar, visit chrome://flags/#enable-quic. If the option exists, find and enable QUIC (HTTP 3).



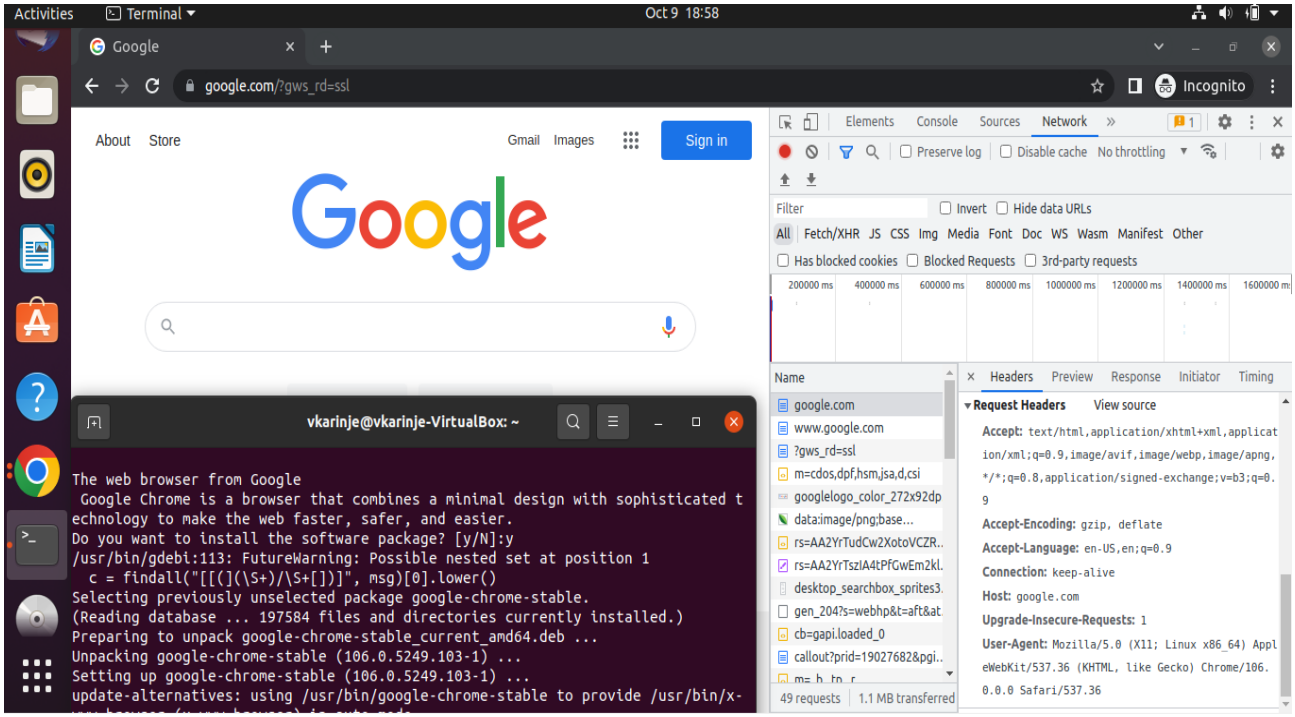
Developer Tools



- What is the URL being requested?

  The requested URL is http://google.com/

- 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?



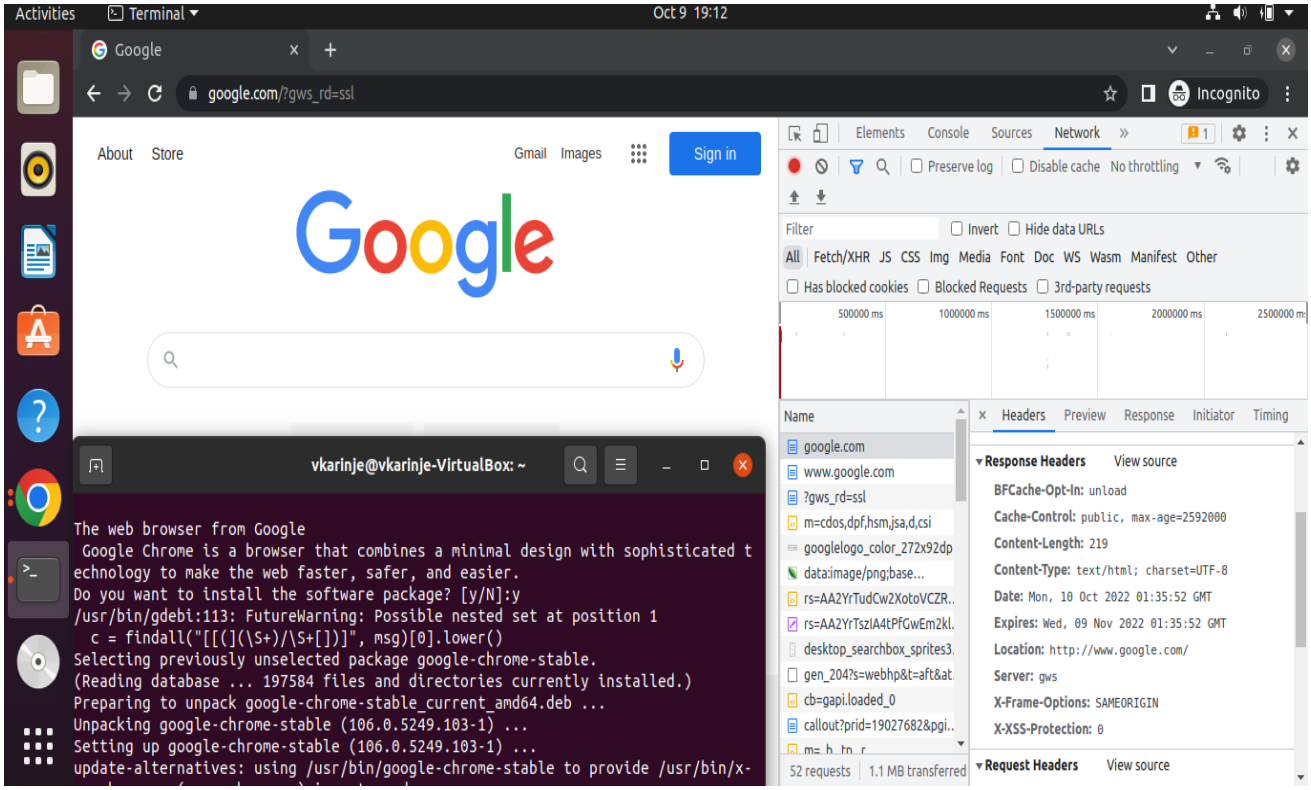
Host is google.com

User-Agent is Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36

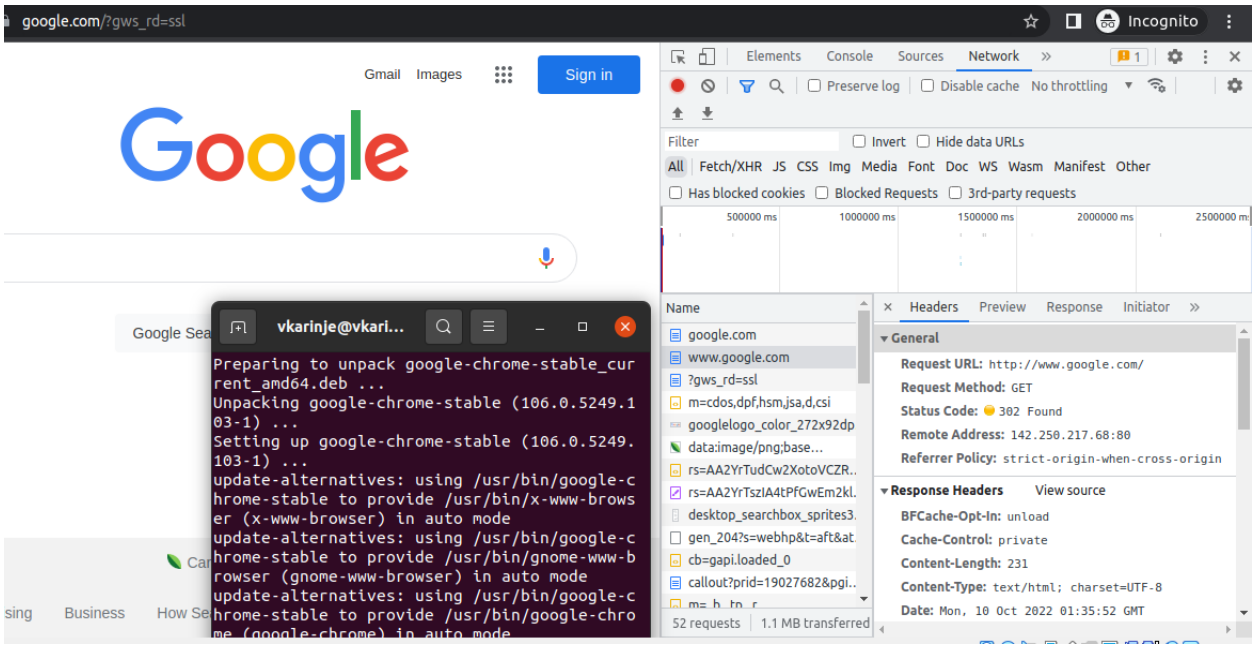
- What is the HTTP status code in the response and what does it mean?

  The HTTP status code in the response is 301(Moved Permanently) and it means that the requested resource has been moved to the URL given by the location headers . The browser will redirect to the new URL.

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



Click on the second request to bring up its connection details. Answer the following questions in your lab notebook.



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

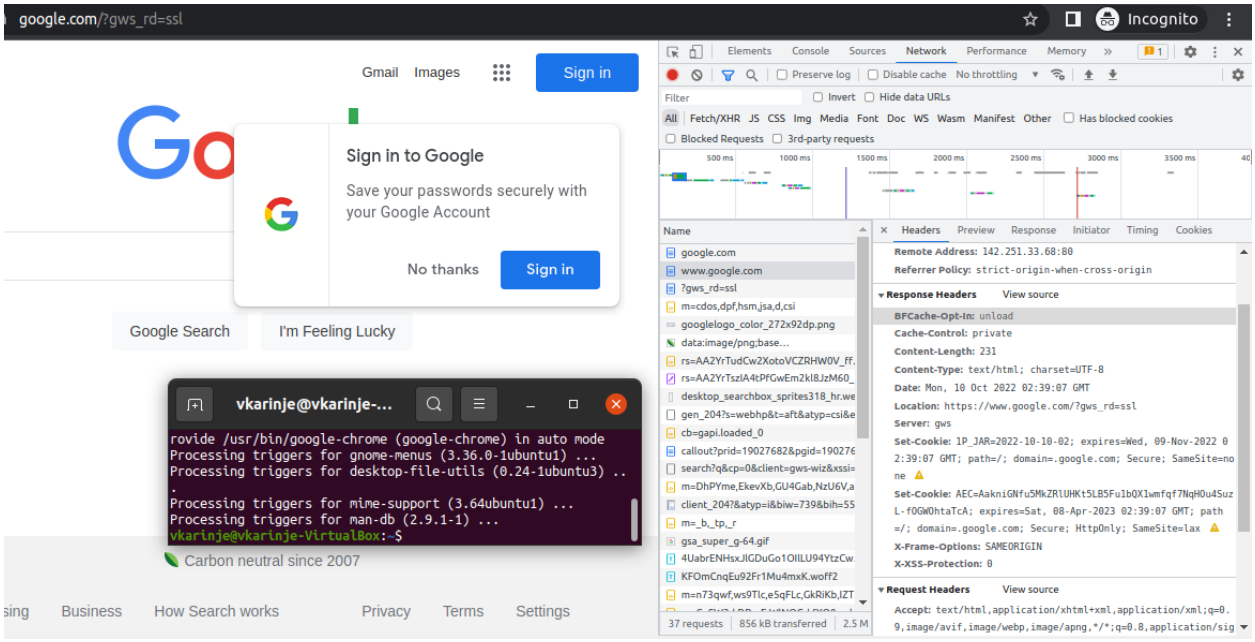
The URL being requested is http://www.google.com/

It is using HTTP

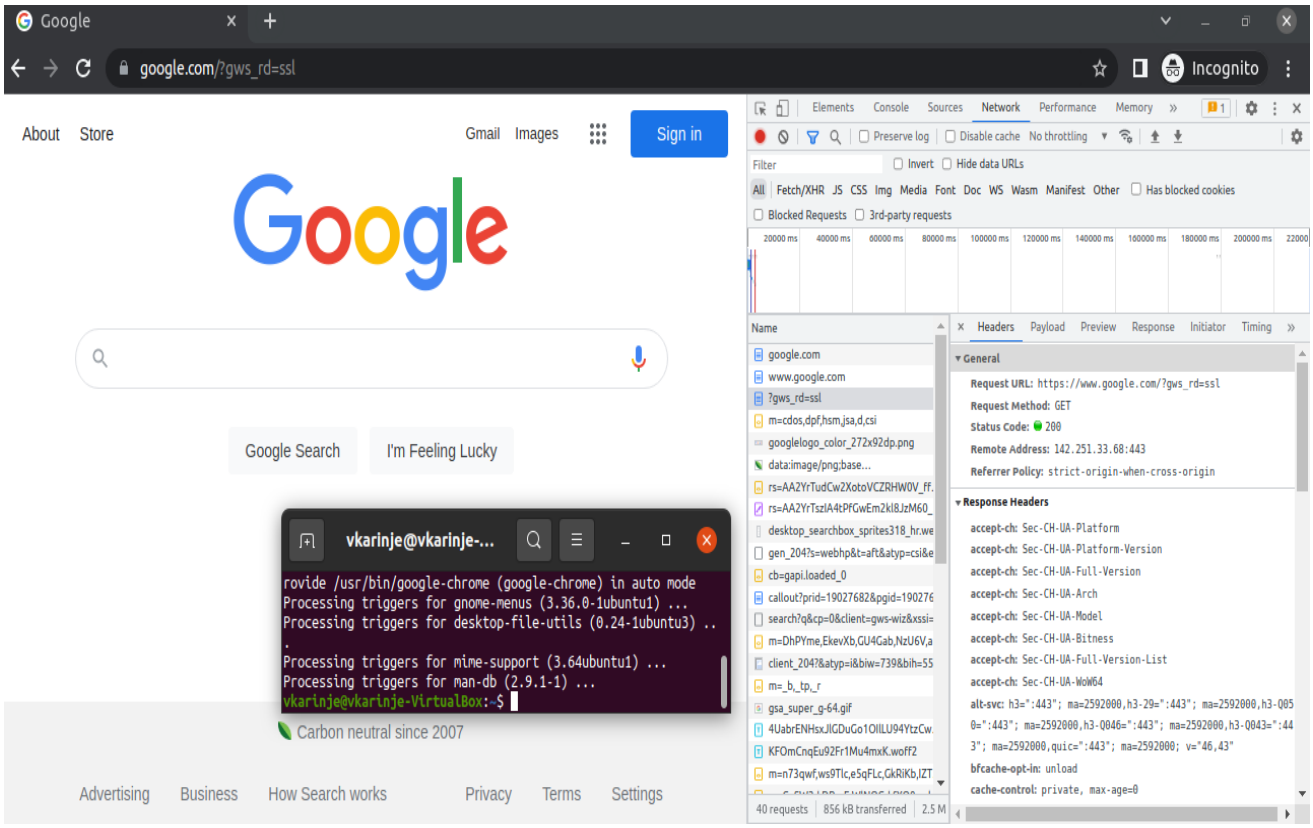
- What is the HTTP status code in the response and what does it mean? Is it different from the first status code? If so, what is the semantic difference?

  The HTTP status code is 302 Found and it means that the requested resource has been temporarily moved to the URL that is given by the location header. Yes, it is different from the first status code. 301 indicates that a page has been moved permanently to a new location whereas, 302 means that a page has been moved to a new location but is just temporary.

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



Click on the third request to bring up its connection details. Answer the following questions in your lab notebook.



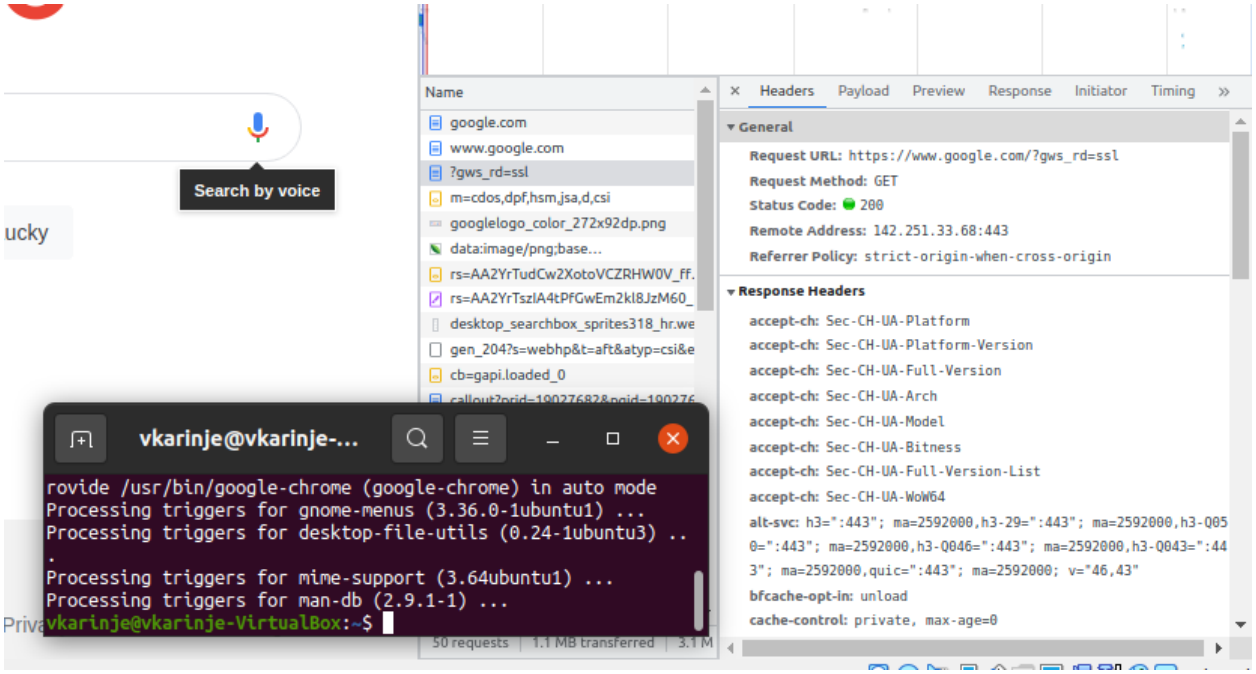
- What is the URL being requested? Is it using HTTP or HTTPS?

  The URL being requested is https://www.google.com/?gws_rd=ssl. It is using HTTPS.

- What is the HTTP status code in the response?

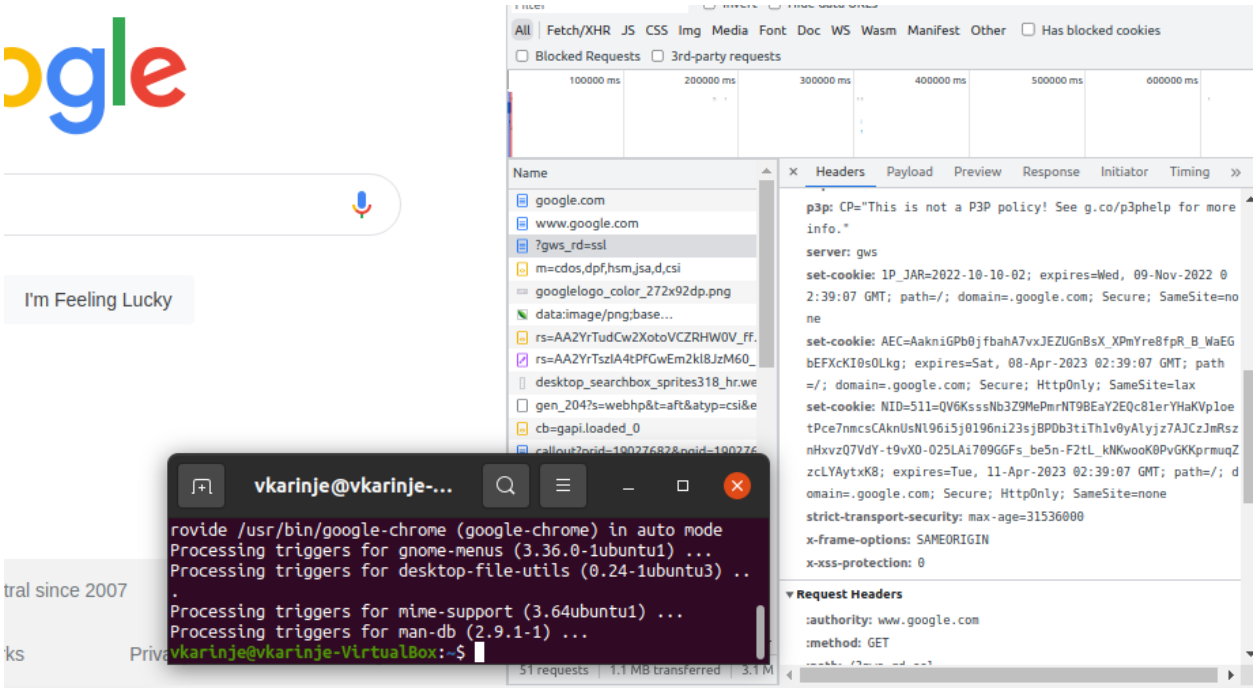
  The HTTP status code in the response is 200.

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



Yes, the server believes the client can use HTTP3/QUIC.

- 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?



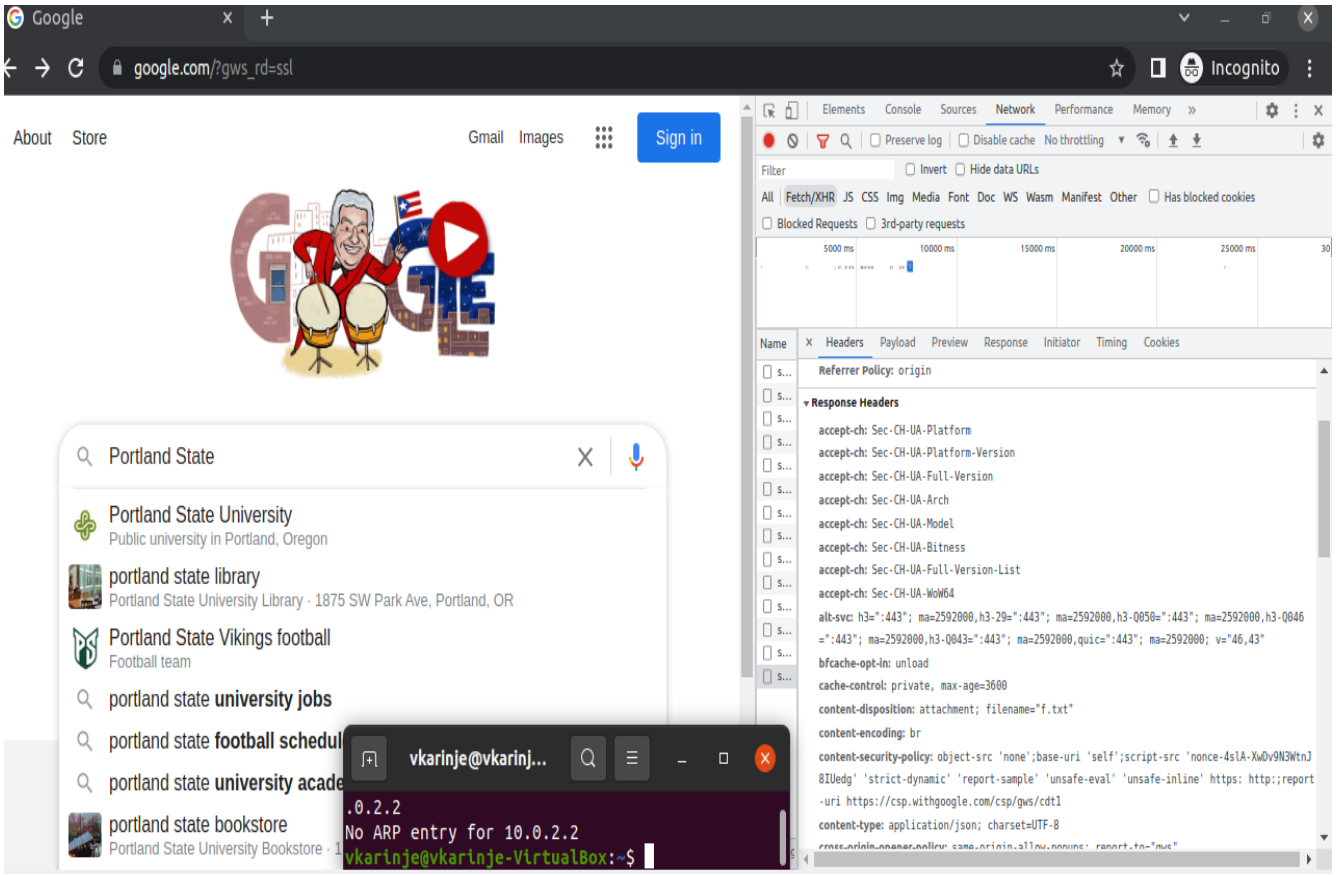
SameSite=none

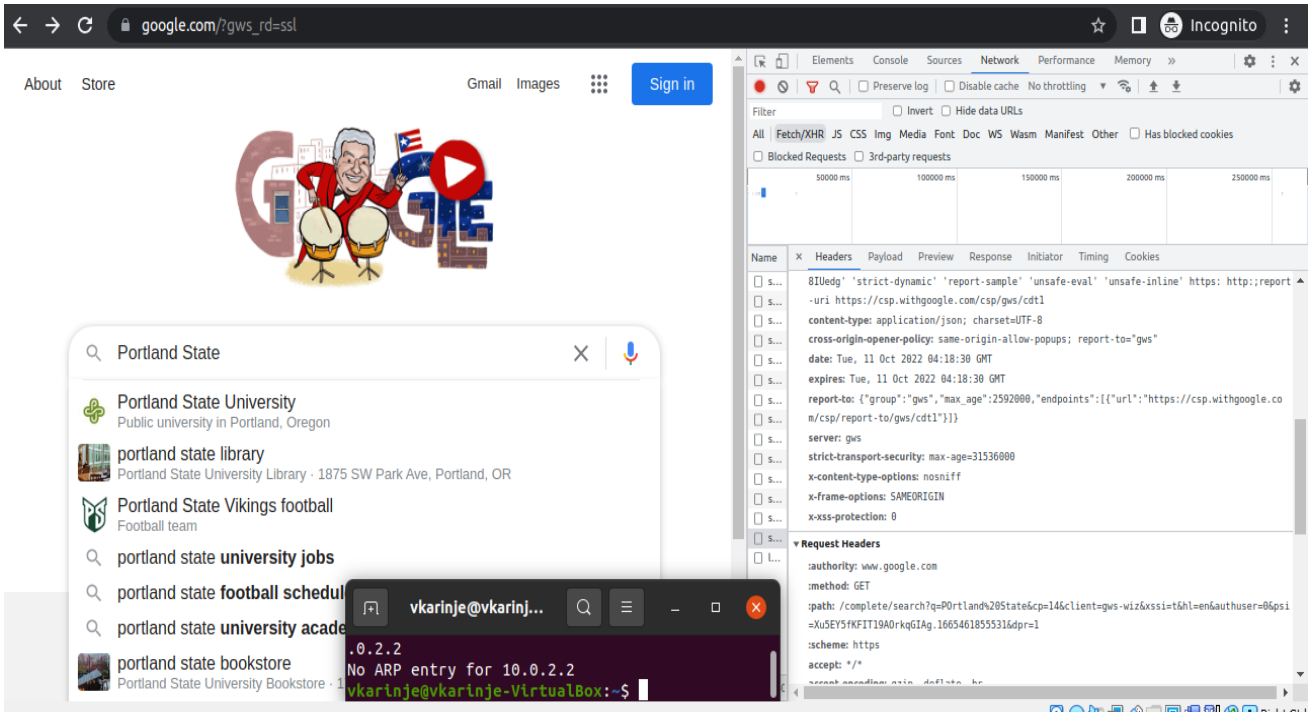
The Set-Cookie of the HTTP response header has an attribute SameSite which allows us to declare if the cookie should be restricted to first-party or the same-site.

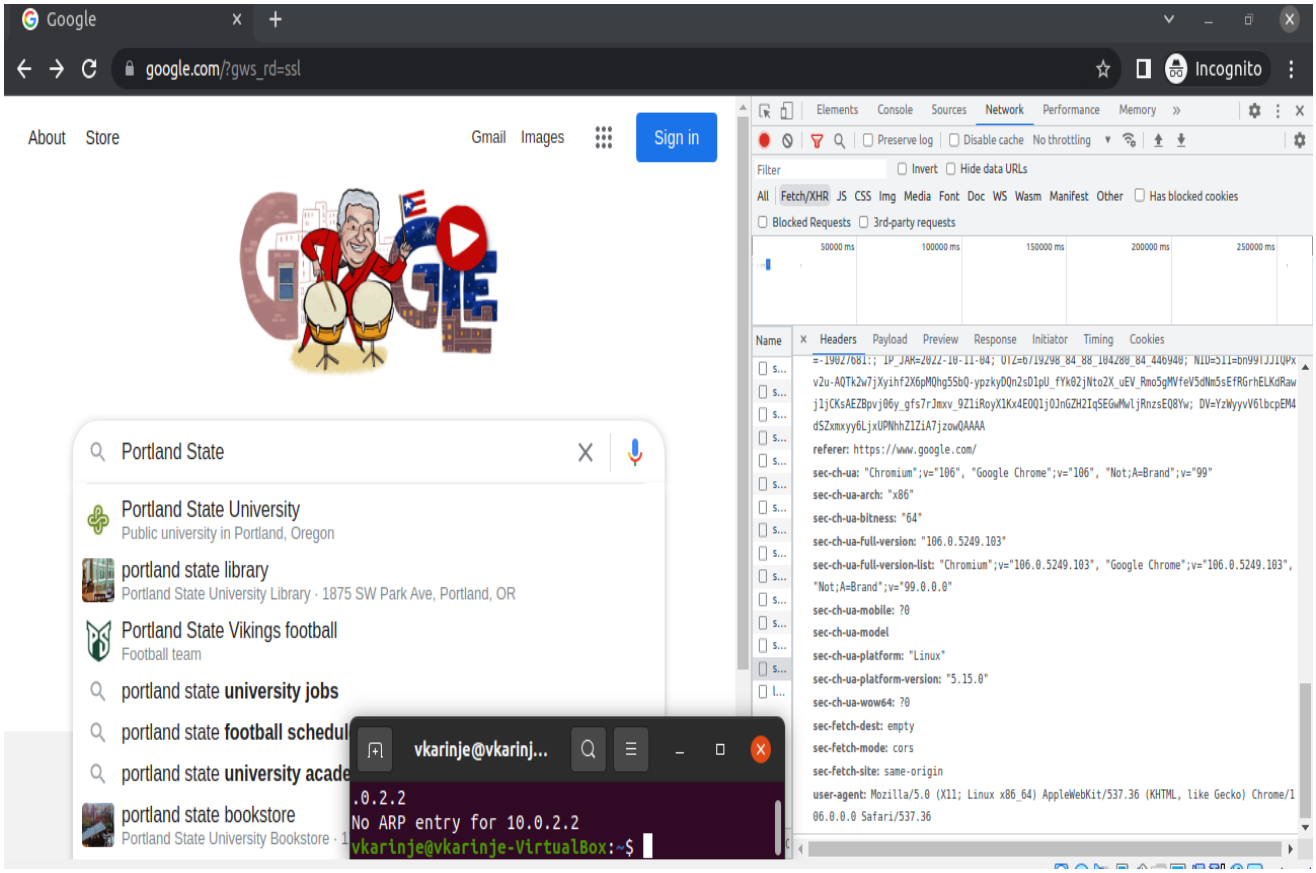
Asynchronous HTTP requests

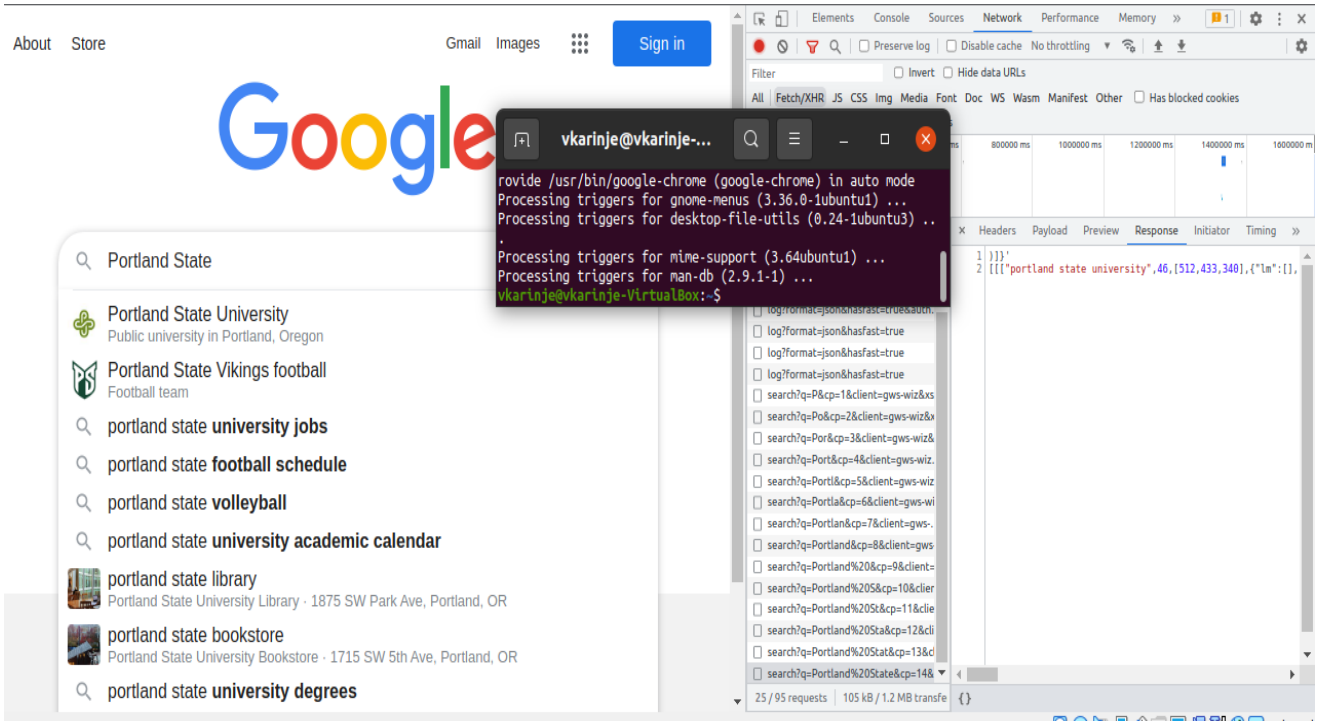
- Show the requests and responses in the listing. Click on the last request sent, then click on the response to see that its payload has returned the data that is then rendered on the search page similar to what is shown below for "rabbid".

Ans:




google.com/?gws_rd=ssl
Incognito
About
Store
Gmail
Images
Sign in
Portland State
Portland State University
Public university in Portland, Oregon
portland state library
Portland State University Library · 1875 SW Park Ave, Portland, OR
Portland State Vikings football
Football team
portland state university jobs
portland state football schedul
portland state university acade
portland state bookstore
Portland State University Bookstore
vkarinje@vkarinj...
.0.2.2
No ARP entry for 10.0.2.2
vkarinje@vkarinje-VirtualBox:~$
Elements
Console
Sources
Network
Performance
Memory
Preserve log
Disable cache
No throttling
Filter
Invert
Hide data URLs
All
Fetch/XHR
JS
CSS
Img
Media
Font
Doc
WS
Wasm
Manifest
Other
Has blocked cookies
Blocked Requests
3rd-party requests
Name
Headers
Payload
Preview
Response
Initiator
Timing
Cookies
Request Headers


Google
google.com/?gws_rd=ssl
Incognito
About
Store
Gmail
Images
Sign in
Portland State
Portland State University
Public university in Portland, Oregon
portland state library
Portland State University Library · 1875 SW Park Ave, Portland, OR
Portland State Vikings football
Football team
portland state university jobs
portland state football schedul
portland state university acade
portland state bookstore
Portland State University Bookstore
vkarinje@vkarinj...
.0.2.2
No ARP entry for 10.0.2.2
vkarinje@vkarinje-VirtualBox:~$
Elements
Console
Sources
Network
Performance
Memory
Preserve log
Disable cache
No throttling
Filter
Invert
Hide data URLs
All
Fetch/XHR
JS
CSS
Img
Media
Font
Doc
WS
Wasm
Manifest
Other
Has blocked cookies
Blocked Requests
3rd-party requests
Name
Headers
Payload
Preview
Response
Initiator
Timing
Cookies


About
Store
Gmail
Images
Sign in
Google
Portland State
Portland State University
Public university in Portland, Oregon
Portland State Vikings football
Football team
portland state university jobs
portland state football schedule
portland state volleyball
portland state university academic calendar
portland state library
Portland State University Library · 1875 SW Park Ave, Portland, OR
portland state bookstore
Portland State University Bookstore · 1715 SW 5th Ave, Portland, OR
portland state university degrees
vkarinje@vkarinje-...
rovide /usr/bin/google-chrome (google-chrome) in auto mode
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
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) ...
vkarinje@vkarinje-VirtualBox:~$
Elements
Console
Sources
Network
Performance
Memory
Headers
Payload
Preview
Response
Initiator
Timing
Cookies
)]}'
[[["portland state university",46,[512,433,340],{"lm":[],"zh":"Portland State Universit

02.2 : DNS,Recap

DNS #1 (dig)

DNS reconnaissance

- Use dig to query the local DNS server 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?

A record

```
vkarinje@ada:~$ dig www.pdx.edu -4 A

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> www.pdx.edu -4 A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8217
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d7268c9756133d03010000006343909cc44d86035ab66db3 (good)
;; QUESTION SECTION:
;www.pdx.edu.                   IN      A

;; ANSWER SECTION:
www.pdx.edu.            900     IN      A       54.214.67.95

;; Query time: 55 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Sun Oct 09 20:25:16 PDT 2022
;; MSG SIZE  rcvd: 84

vkarinje@ada:~$
```

The IP address is 54.214.67.95

MX Record

```
vkarinje@ada:~$ dig www.pdx.edu -4 MX

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> www.pdx.edu -4 MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4417
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 50edc415919795da0100000063439134e2c0a39e9c0bd512 (good)
;; 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: 59 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Sun Oct 09 20:27:48 PDT 2022
;; MSG SIZE  rcvd: 144

vkarinje@ada:~$
```

PSU's mail/web services come from ns-cloud-e1.googledomains.com.hostmaster.pdx.edu

- 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.

```
vkarinje@ada:~$ dig mashimaro.cs.pdx.edu -4 NS

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> mashimaro.cs.pdx.edu -4 NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26471
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7a5ebf8d99c232ea010000006343930dedca95fb93d4fa86 (good)
;; QUESTION SECTION:
;mashimaro.cs.pdx.edu.          IN      NS

;; AUTHORITY SECTION:
cs.pdx.edu.             300     IN      SOA     walt.ee.pdx.edu. support.cat.pdx.edu. 2022100301 600 300 1209600 300

;; Query time: 3 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Sun Oct 09 20:35:41 PDT 2022
;; MSG SIZE  rcvd: 147
```

The authoritative server for mashimaro.cs.pdx.edu is walt.ee.pdx.edu

```
vkarinje@ada:~$ dig @walt.ee.pdx.edu mashimaro.cs.pdx.edu -4 A

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> @walt.ee.pdx.edu mashimaro.cs.pdx.edu -4 A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24383
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4016762d93dbc7ac0100000634393e990201649567cc720 (good)
;; QUESTION SECTION:
;mashimaro.cs.pdx.edu.          IN      A

;; ANSWER SECTION:
mashimaro.cs.pdx.edu.   14400   IN      A       131.252.220.66

;; Query time: 0 msec
;; SERVER: 131.252.208.38#53(walt.ee.pdx.edu) (UDP)
;; WHEN: Sun Oct 09 20:39:21 PDT 2022
;; MSG SIZE  rcvd: 93

vkarinje@ada:~$
```

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

```
vkarinje@ada:~$ dig thefengs.com -4 NS

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> thefengs.com -4 NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21584
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 1f1bff7f9bc708260100000634394c5c6b478441d69416e (good)
;; QUESTION SECTION:
;thefengs.com.                  IN      NS

;; ANSWER SECTION:
thefengs.com.           4673    IN      NS      ns-cloud1.googledomains.com.
thefengs.com.           4673    IN      NS      ns-cloud3.googledomains.com.
thefengs.com.           4673    IN      NS      ns-cloud2.googledomains.com.
thefengs.com.           4673    IN      NS      ns-cloud4.googledomains.com.

;; ADDITIONAL SECTION:
ns-cloud1.googledomains.com. 141160 IN  A       216.239.32.106
ns-cloud2.googledomains.com. 141160 IN  A       216.239.34.106
ns-cloud3.googledomains.com. 141160 IN  A       216.239.36.106
ns-cloud4.googledomains.com. 144897 IN  A       216.239.38.106
ns-cloud1.googledomains.com. 141160 IN  AAAA    2001:4860:4802:32::6a
ns-cloud2.googledomains.com. 141160 IN  AAAA    2001:4860:4802:34::6a
ns-cloud3.googledomains.com. 141160 IN  AAAA    2001:4860:4802:36::6a
ns-cloud4.googledomains.com. 144897 IN  AAAA    2001:4860:4802:38::6a

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Sun Oct 09 20:43:01 PDT 2022
;; MSG SIZE  rcvd: 358
```

The authoritative server for the fengs.com is ns-cloud1.googledomains.com

```
vkarinje@ada:~$ dig @ns-cloud1.googledomains.com thefengs.com -4 A

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> @ns-cloud1.googledomains.com thefengs.com -4 A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5212
;; 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: 51 msec
;; SERVER: 216.239.32.106#53(ns-cloud1.googledomains.com) (UDP)
;; WHEN: Sun Oct 09 20:52:03 PDT 2022
;; MSG SIZE  rcvd: 57

vkarinje@ada:~$
```

- 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)

  The site “thefengs.com” is mentioned by the HOST of the protocol header. This is how the server knows which site to serve from.

DNS iterative lookups

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

  Finding IP address of F root server

Iterative query to IP address of F root

```
vkarinje@ada:~$ dig @192.5.5.241 +norecurse +tcp www.cs.pdx.edu

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> @192.5.5.241 +norecurse +tcp www.cs.pdx.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1206
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65535
;; QUESTION SECTION:
;www.cs.pdx.edu.                        IN      A

;; AUTHORITY SECTION:
edu.                    172800  IN      NS      l.edu-servers.net.
edu.                    172800  IN      NS      b.edu-servers.net.
edu.                    172800  IN      NS      c.edu-servers.net.
edu.                    172800  IN      NS      d.edu-servers.net.
edu.                    172800  IN      NS      e.edu-servers.net.
edu.                    172800  IN      NS      f.edu-servers.net.
edu.                    172800  IN      NS      g.edu-servers.net.
edu.                    172800  IN      NS      a.edu-servers.net.
edu.                    172800  IN      NS      h.edu-servers.net.
edu.                    172800  IN      NS      i.edu-servers.net.
edu.                    172800  IN      NS      j.edu-servers.net.
edu.                    172800  IN      NS      k.edu-servers.net.
edu.                    172800  IN      NS      m.edu-servers.net.

;; ADDITIONAL SECTION:
l.edu-servers.net.      172800  IN      A       192.41.162.30
l.edu-servers.net.      172800  IN      AAAA    2001:500:d937::30
b.edu-servers.net.      172800  IN      A       192.33.14.30
b.edu-servers.net.      172800  IN      AAAA    2001:503:231d::2:30
c.edu-servers.net.      172800  IN      A       192.26.92.30
c.edu-servers.net       172800  IN      AAAA    2001:503:83eb::30
```

```
;; ADDITIONAL SECTION:
l.edu-servers.net.      172800  IN      A       192.41.162.30
l.edu-servers.net.      172800  IN      AAAA    2001:500:d937::30
b.edu-servers.net.      172800  IN      A       192.33.14.30
b.edu-servers.net.      172800  IN      AAAA    2001:503:231d::2:30
c.edu-servers.net.      172800  IN      A       192.26.92.30
c.edu-servers.net.      172800  IN      AAAA    2001:503:83eb::30
d.edu-servers.net.      172800  IN      A       192.31.80.30
d.edu-servers.net.      172800  IN      AAAA    2001:500:856e::30
e.edu-servers.net.      172800  IN      A       192.12.94.30
e.edu-servers.net.      172800  IN      AAAA    2001:502:1ca1::30
f.edu-servers.net.      172800  IN      A       192.35.51.30
f.edu-servers.net.      172800  IN      AAAA    2001:503:d414::30
g.edu-servers.net.      172800  IN      A       192.42.93.30
g.edu-servers.net.      172800  IN      AAAA    2001:503:eea3::30
a.edu-servers.net.      172800  IN      A       192.5.6.30
a.edu-servers.net.      172800  IN      AAAA    2001:503:a83e::2:30
h.edu-servers.net.      172800  IN      A       192.54.112.30
h.edu-servers.net.      172800  IN      AAAA    2001:502:8cc::30
i.edu-servers.net.      172800  IN      A       192.43.172.30
i.edu-servers.net.      172800  IN      AAAA    2001:503:39c1::30
j.edu-servers.net.      172800  IN      A       192.48.79.30
j.edu-servers.net.      172800  IN      AAAA    2001:502:7094::30
k.edu-servers.net.      172800  IN      A       192.52.178.30
k.edu-servers.net.      172800  IN      AAAA    2001:503:d2d::30
m.edu-servers.net.      172800  IN      A       192.55.83.30
m.edu-servers.net.      172800  IN      AAAA    2001:501:b1f9::30

;; Query time: 0 msec
;; SERVER: 192.5.5.241#53(192.5.5.241) (TCP)
;; WHEN: Sun Oct 09 21:03:30 PDT 2022
;; MSG SIZE  rcvd: 838

vkarinje@ada:~$
```

Finding IP address of f.edu-servers.net

```
vkarinje@ada:~$ dig f.edu-servers.net

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> f.edu-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60552
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 1997fc7366fd836c0100000063439a260037dd68b2ded53f (good)
;; QUESTION SECTION:
;f.edu-servers.net.             IN      A

;; ANSWER SECTION:
f.edu-servers.net.      59235   IN      A       192.35.51.30

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Sun Oct 09 21:05:58 PDT 2022
;; MSG SIZE  rcvd: 90

vkarinje@ada:~$
```

Iterative query to IP address of f.edu-servers.net

```
vkarinje@ada:~$ dig @192.35.51.30 +norecurse +tcp www.cs.pdx.edu

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> @192.35.51.30 +norecurse +tcp www.cs.pdx.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42230
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.cs.pdx.edu.                        IN      A

;; AUTHORITY SECTION:
pdx.edu.                172800  IN      NS      ns-cloud-e1.googledomains.com.
pdx.edu.                172800  IN      NS      ns-cloud-e2.googledomains.com.
pdx.edu.                172800  IN      NS      ns-cloud-e3.googledomains.com.
pdx.edu.                172800  IN      NS      ns-cloud-e4.googledomains.com.

;; Query time: 19 msec
;; SERVER: 192.35.51.30#53(192.35.51.30) (TCP)
;; WHEN: Sun Oct 09 21:08:07 PDT 2022
;; MSG SIZE  rcvd: 164

vkarinje@ada:~$
```

Finding IP address of NS at google domains

```
vkarinje@ada:~$ dig ns-cloud-e1.googledomains.com

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> ns-cloud-e1.googledomains.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50573
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 08a364790551547801000000063439b41b5f597fcee949b44 (good)
;; QUESTION SECTION:
;ns-cloud-e1.googledomains.com. IN      A

;; ANSWER SECTION:
ns-cloud-e1.googledomains.com. 240876 IN A      216.239.32.110

;; Query time: 3 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Sun Oct 09 21:10:41 PDT 2022
;; MSG SIZE  rcvd: 102
```

Iterative query to IP address of NS at google domains

```
vkarinje@ada:~$ dig @216.239.32.110 +norecurse +tcp www.cs.pdx.edu

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> @216.239.32.110 +norecurse +tcp www.cs.pdx.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53025
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.cs.pdx.edu.                        IN      A

;; AUTHORITY SECTION:
cs.pdx.edu.             14400   IN      NS      dns0.pdx.edu.
cs.pdx.edu.             14400   IN      NS      walt.ee.pdx.edu.
cs.pdx.edu.             14400   IN      NS      dns1.pdx.edu.

;; ADDITIONAL SECTION:
walt.ee.pdx.edu.        14400   IN      A       131.252.208.38
dns1.pdx.edu.           14400   IN      A       131.252.120.129
dns0.pdx.edu.           14400   IN      A       131.252.120.128

;; Query time: 51 msec
;; SERVER: 216.239.32.110#53(216.239.32.110) (TCP)
;; WHEN: Sun Oct 09 21:12:30 PDT 2022
;; MSG SIZE  rcvd: 151

vkarinje@ada:~$
```

Finding IP address of dns0.pdx.edu

```
vkarinje@ada:~$ dig dns0.pdx.edu

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> dns0.pdx.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61019
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: eeb04587b55a243e0100000063439cb7c5bfadedab4a3f8e (good)
;; QUESTION SECTION:
;dns0.pdx.edu.                  IN      A

;; ANSWER SECTION:
dns0.pdx.edu.           11664   IN      A       131.252.120.128

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Sun Oct 09 21:16:55 PDT 2022
;; MSG SIZE  rcvd: 85

vkarinje@ada:~$
```

Iterative query to ip address of dns0.pdx.edu

```
vkarinje@ada:~$ dig @131.252.120.128 +norecurse +tcp www.cs.pdx.edu

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> @131.252.120.128 +norecurse +tcp www.cs.pdx.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28691
;; flags: qr aa ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 6148b7ba6dbb801e05c2247863439d35f184c49a92a9336c (good)
;; QUESTION SECTION:
;www.cs.pdx.edu.                        IN      A

;; ANSWER SECTION:
www.cs.pdx.edu.         14400   IN      CNAME   vhost-therest.cat.pdx.edu.
vhost-therest.cat.pdx.edu. 14400 IN     A       131.252.208.114

;; AUTHORITY SECTION:
cat.pdx.edu.            14400   IN      NS      dns0.pdx.edu.
cat.pdx.edu.            14400   IN      NS      dns1.pdx.edu.
cat.pdx.edu.            14400   IN      NS      walt.ee.pdx.edu.

;; ADDITIONAL SECTION:
dns0.pdx.edu.           9740    IN      A       131.252.120.128
walt.ee.pdx.edu.        14400   IN      A       131.252.208.38

;; Query time: 0 msec
;; SERVER: 131.252.120.128#53(131.252.120.128) (TCP)
;; WHEN: Sun Oct 09 21:19:01 PDT 2022
;; MSG SIZE  rcvd: 211

vkarinje@ada:~$
```

Now we found the result vhost-therest.cat.pdx.edu which is the canonical name for www.cs.pdx.edu.

Reverse DNS lookups

Aliases and reverse lookups

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

```
vkarinje@ada:~$ dig espn.go.com | egrep 'espn.go.com' | awk ' {print $5}'
<<>>

99.84.66.55
99.84.66.108
99.84.66.17
99.84.66.98
vkarinje@ada:~$
```

- 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.

```
vkarinje@ada:~$ X=(`dig espn.go.com | egrep 'espn.go.com' | awk ' {print $5}'`)
vkarinje@ada:~$ for i in "${X[@]}"; do echo `dig -x $i | egrep 'ANSWER SECTION' -A1 | awk '/.in-addr.arpa./ {print $5}'` ; done

server-99-84-66-55.hio50.r.cloudfront.net.
server-99-84-66-17.hio50.r.cloudfront.net.
server-99-84-66-108.hio50.r.cloudfront.net.
server-99-84-66-98.hio50.r.cloudfront.net.
vkarinje@ada:~$
```

Host enumeration

- Using a `for` loop, perform a reverse DNS lookup for each IP address on the `131.252.220.0/24` subnet. Note that some addresses on the subnet do not have names bound to them and will not return a record. Take the output of the loop and pipe it to `egrep` and `awk` to list just the names of the hosts, then redirect the final output to a file called `220hosts.txt` output using the `>` character to perform output redirection to a file.

Ans:

```
vkarinje@ada:~$ for i in {1..255}; do dig -x 131.252.220.$i | egrep PTR | awk '{print $5}'; done > 220hosts.txt
vkarinje@ada:~$ cat 220hosts.txt | head -374 | tail -59
acura.cs.pdx.edu.

astonmartin.cs.pdx.edu.

audi.cs.pdx.edu.

bentley.cs.pdx.edu.

bmw.cs.pdx.edu.

cadillac.cs.pdx.edu.

ferrari.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.
vkarinje@ada:~$
```

DNS #2 (Geographic DNS)

Visit https://www.iplocation.net/ and lookup the geographical location of the following DNS servers: 131.252.208.53 and 198.82.247.66.

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

  Ans: ipinfo.io and DB-IP return the geographic location as Oregon, Portland (Portland State University) for ip address 131.252.208.53.

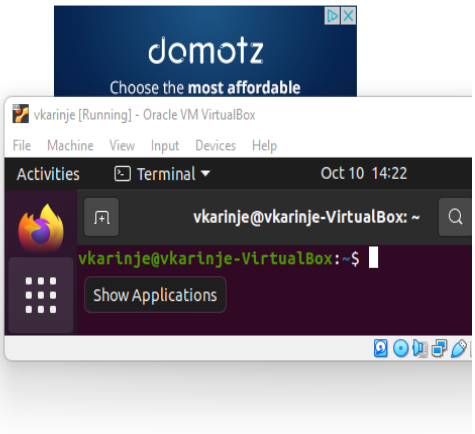
ISP	Organization	Latitude	Longitude
Portland State University	Not Available	45.5213	-122.6859

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

IP Address	Country	Region	City
131.252.208.53	United States	Oregon	Portland
ISP	**Organization**	**Latitude**	**Longitude**
Portland State University	Portland State University (pdx.edu)	45.5234	-122.6762

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

IP Address	Country	Region	City
131.252.208.53	United States	Oregon	Portland (North Portland)
ISP	**Organization**	**Latitude**	**Longitude**
Portland State University	Portland State University	45.584	-122.728



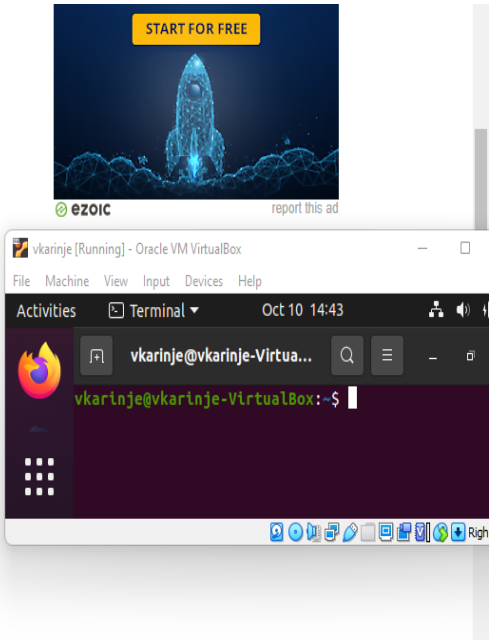
ipinfo.io and DB-IP return the geographic location as Virginia, Blacksburg (Virginia Polytechnic Institute and State University) for ip address 198.82.247.66.

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

IP Address	Country	Region	City
198.82.247.66	United States	Virginia	Blacksburg
ISP	**Organization**	**Latitude**	**Longitude**
Virginia Polytechnic Institute and State Univ.	Virginia Polytechnic Institute and State Univ. (vt.edu)	37.2296	-80.4139

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

IP Address	Country	Region	City
198.82.247.66	United States	Virginia	Blacksburg (Farmview - Ramble)
ISP	**Organization**	**Latitude**	**Longitude**
Virginia Polytechnic Institute and State Univ.	Virginia Polytechnic Institute and State Univ.	37.2037	-80.4143



Then, using dig, resolve www.google.com from each of the DNS servers (dig @<DNS_server_IP> www.google.com).

```
Last login: Mon Oct 10 13:53:01 2022 from c-73-11-13-21.hsd1.or.comcast.net
vkarinje@ada:~$ dig @131.252.208.53 www.google.com

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> @131.252.208.53 www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61758
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 0c70c2d403af4b25010000006344 92dd0021c934fb9f4466 (good)
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         150     IN      A       142.251.211.228

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Mon Oct 10 14:47:09 PDT 2022
;; MSG SIZE  rcvd: 87

vkarinje@ada:~$
```

```
vkarinje@ada:~$ dig @198.82.247.66 www.google.com

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> @198.82.247.66 www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59623
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a7368b74ca7e7273dcc34ce56344937332757c4a0f77fb69 (good)
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         110     IN      A       142.251.45.4

;; Query time: 71 msec
;; SERVER: 198.82.247.66#53(198.82.247.66) (UDP)
;; WHEN: Mon Oct 10 14:49:39 PDT 2022
;; MSG SIZE  rcvd: 87

vkarinje@ada:~$
```

Go back to https://www.iplocation.net/ and lookup the geographical location of each IP address returned. What geographic locations do ipinfo.io and DB-IP return?

Ans: ipinfo.io and DB-IP return Washington, Seattle for ip address 142.251.211.228.

ISP	Organization	Latitude	Longitude
Google LLC	Not Available	37.4060	-122.0785

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

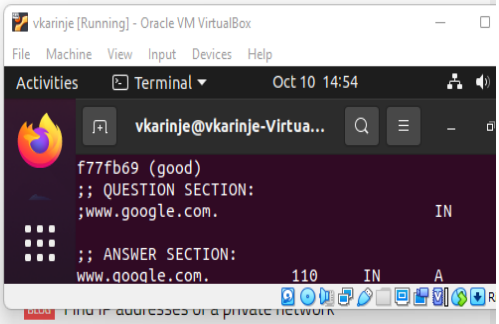
IP Address	Country	Region	City
142.251.211.228	United States	Washington	Seattle

ISP	Organization	Latitude	Longitude
Google LLC	Google LLC (google.com)	47.6062	-122.3321

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

IP Address	Country	Region	City
142.251.211.228	United States	Washington	Seattle

ISP	Organization	Latitude	Longitude
Google LLC	Google LLC	47.6062	-122.332



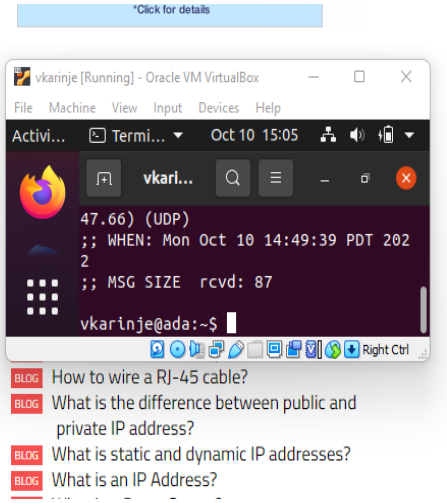
ipinfo.io returns Virginia, Alexandria and DB-IP returns District of Columbia, Washington D.C. for Ip address 142.251.45.4.

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

IP Address	Country	Region	City
142.251.45.4	United States	Virginia	Alexandria
ISP	**Organization**	**Latitude**	**Longitude**
Google LLC	Google LLC (google.com)	38.8048	-77.0469

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

IP Address	Country	Region	City
142.251.45.4	United States	District of Columbia	Washington D.C.
ISP	**Organization**	**Latitude**	**Longitude**
Google LLC	Google LLC	38.9072	-77.0369



- What is the geographic distance between each pair of DNS server and web server?

Ans: The geographical distance between 131.252.208.53 (DNS server, PSU, Portland, OR) and 142.251.211.228 (google.com, Washington, Seattle) is 173.8 miles.

The geographical distance between 198.82.247.66 (DNS server, Virginia, Blacksburg) and 142.251.45.4 (google.com, District of Columbia, Washington DC) is 269.5 miles.

The geographical distance between 198.82.247.66 (DNS server, Virginia, Blacksburg) and 142.251.45.4 (google.com, Virginia, Alexandria) is 175 miles.

Perform a traceroute to all 4 IP addresses from a PSU network.

```
vkarinje@ada:~$ traceroute 131.252.208.53
traceroute to 131.252.208.53 (131.252.208.53), 30 hops max, 60 byte packets
 1  rdns.cat.pdx.edu (131.252.208.53)  0.576 ms  0.541 ms  0.505 ms
vkarinje@ada:~$
```

```
vkarinje@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 (131.252.208.212)  1.025 ms  3.319 ms  3.292 ms
 2  CORE1.net.pdx.edu (131.252.5.142)  0.765 ms  0.724 ms  0.677 ms
 3  131.252.5.213 (131.252.5.213)  3.056 ms  3.010 ms  2.965 ms
 4  port-psu-pe-01.net.linkoregon.org (199.165.177.48)  2.920 ms  2.873 ms  2.826 ms
 5  eugn-oh-vpn-01.net.linkoregon.org (207.98.126.3)  10.438 ms  10.495 ms  10.504 ms
 6  bois-gtwy-pe-01.net.linkoregon.org (207.98.126.135)  10.481 ms  10.509 ms  10.336 ms
 7  bois-gtwy-pe-01-loren.net.linkoregon.org (163.253.5.65)  10.231 ms  10.164 ms  10.200 ms
 8  hundredge-0-0-0-24.703.core1.bois.net.internet2.edu (163.253.5.64)  13.532 ms  13.488 ms  13.457 ms
 9  fourhundredge-0-0-0-0.4079.core2.salt.net.internet2.edu (163.253.1.249)  64.716 ms  64.746 ms  64.665 ms
10  fourhundredge-0-0-0-21.4079.core1.salt.net.internet2.edu (163.253.1.28)  67.772 ms  64.504 ms  65.329 ms
11  fourhundredge-0-0-0-0.4079.core1.denv.net.internet2.edu (163.253.1.170)  65.401 ms  65.374 ms fourhundredge-0-0-0-0.4079.core2.kans.net.in
ternet2.edu (163.253.1.251)  64.549 ms
12  fourhundredge-0-0-0-0.4079.core1.kans.net.internet2.edu (163.253.1.243)  66.701 ms  65.747 ms  65.698 ms
13  fourhundredge-0-0-0-3.4079.core2.chic.net.internet2.edu (163.253.1.244)  65.037 ms  66.861 ms  66.725 ms
14  fourhundredge-0-0-0-3.4079.core2.eqch.net.internet2.edu (163.253.2.19)  65.408 ms  65.003 ms  66.919 ms
15  fourhundredge-0-0-0-0.4079.core2.clev.net.internet2.edu (163.253.2.16)  65.605 ms  64.661 ms  64.534 ms
16  fourhundredge-0-0-0-3.4079.core2.ashb.net.internet2.edu (163.253.1.138)  65.937 ms  65.885 ms  66.125 ms
17  192.122.175.14 (192.122.175.14)  63.371 ms  63.690 ms  63.587 ms
18  vtacs-1.msap.cns.vt.edu (192.70.187.18)  69.253 ms  70.171 ms  69.047 ms
19  isb-core.et-5-1-0.0.cns.vt.edu (128.173.0.206)  69.679 ms  69.678 ms  69.380 ms
20  cas-core.lo0.2000.cns.vt.edu (198.82.1.143)  69.596 ms  69.438 ms  69.394 ms
21  jeru.cns.vt.edu (198.82.247.66)  69.460 ms  69.616 ms  69.808 ms
vkarinje@ada:~$
```

```
vkarinje@ada:~$ traceroute 142.251.211.228
traceroute to 142.251.211.228 (142.251.211.228), 30 hops max, 60 byte packets
 1  radiant.seas.pdx.edu (131.252.208.212)  1.582 ms  1.663 ms  1.751 ms
 2  CORE1.net.pdx.edu (131.252.5.142)  0.755 ms  1.338 ms  1.293 ms
 3  131.252.5.213 (131.252.5.213)  1.163 ms  1.192 ms  1.211 ms
 4  google.nwax.net (198.32.195.34)  4.478 ms  4.425 ms  4.613 ms
 5  74.125.243.193 (74.125.243.193)  4.795 ms 74.125.243.177 (74.125.243.177)  5.117 ms  5.073 ms
 6  216.239.43.121 (216.239.43.121)  4.883 ms  5.097 ms 216.239.43.231 (216.239.43.231)  4.955 ms
 7  sea30s13-in-f4.1e100.net (142.251.211.228)  4.778 ms  4.479 ms  4.966 ms
vkarinje@ada:~$
```

```
vkarinje@ada:~$ traceroute 142.251.45.4
traceroute to 142.251.45.4 (142.251.45.4), 30 hops max, 60 byte packets
 1  radiant.seas.pdx.edu (131.252.208.212)  4.749 ms  4.837 ms  4.917 ms
 2  CORE1.net.pdx.edu (131.252.5.142)  0.741 ms  0.707 ms  0.665 ms
 3  131.252.5.213 (131.252.5.213)  0.940 ms  1.631 ms  1.206 ms
 4  google.nwax.net (198.32.195.34)  4.172 ms  4.278 ms  4.043 ms
 5  74.125.243.179 (74.125.243.179)  14.549 ms  14.484 ms 74.125.243.194 (74.125.243.194)  5.566 ms
 6  142.251.68.202 (142.251.68.202)  10.866 ms  10.716 ms 216.239.41.34 (216.239.41.34)  24.771 ms
 7  142.251.226.161 (142.251.226.161)  51.740 ms * 142.251.226.159 (142.251.226.159)  53.116 ms
 8  * 142.251.64.254 (142.251.64.254)  65.872 ms 142.251.65.6 (142.251.65.6)  65.592 ms
 9  * 142.250.236.134 (142.250.236.134)  64.726 ms *
10  142.251.49.163 (142.251.49.163)  67.913 ms  67.903 ms 216.239.35.163 (216.239.35.163)  66.687 ms
11  108.170.240.97 (108.170.240.97)  66.027 ms 108.170.246.1 (108.170.246.1)  64.923 ms 108.170.240.97 (108.170.240.97)  65.571 ms
12  142.251.70.83 (142.251.70.83)  65.601 ms 142.251.70.85 (142.251.70.85)  65.080 ms  66.565 ms
13  iad66s01-in-f4.1e100.net (142.251.45.4)  66.773 ms  65.669 ms  65.595 ms
vkarinje@ada:~$
```

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

  Ans: No, the routes do not reveal any information on the accuracy of the geographic locations given.

Network Recap Lab #3

- Use the ip command to find the IP address of the VM and the name of the local virtual ethernet interface.

  Ans:

```
Connection to linux.cs.pdx.edu closed.
vkarinje@vkarinje-VirtualBox:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:54:c5:2d:85  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=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::ba8:278:f326:5248  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:4a:49:f1  txqueuelen 1000  (Ethernet)
        RX packets 302827  bytes 431484486 (431.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 93419  bytes 7059506 (7.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 195276  bytes 11767157 (11.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 195276  bytes 11767157 (11.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vkarinje@vkarinje-VirtualBox:~$
```

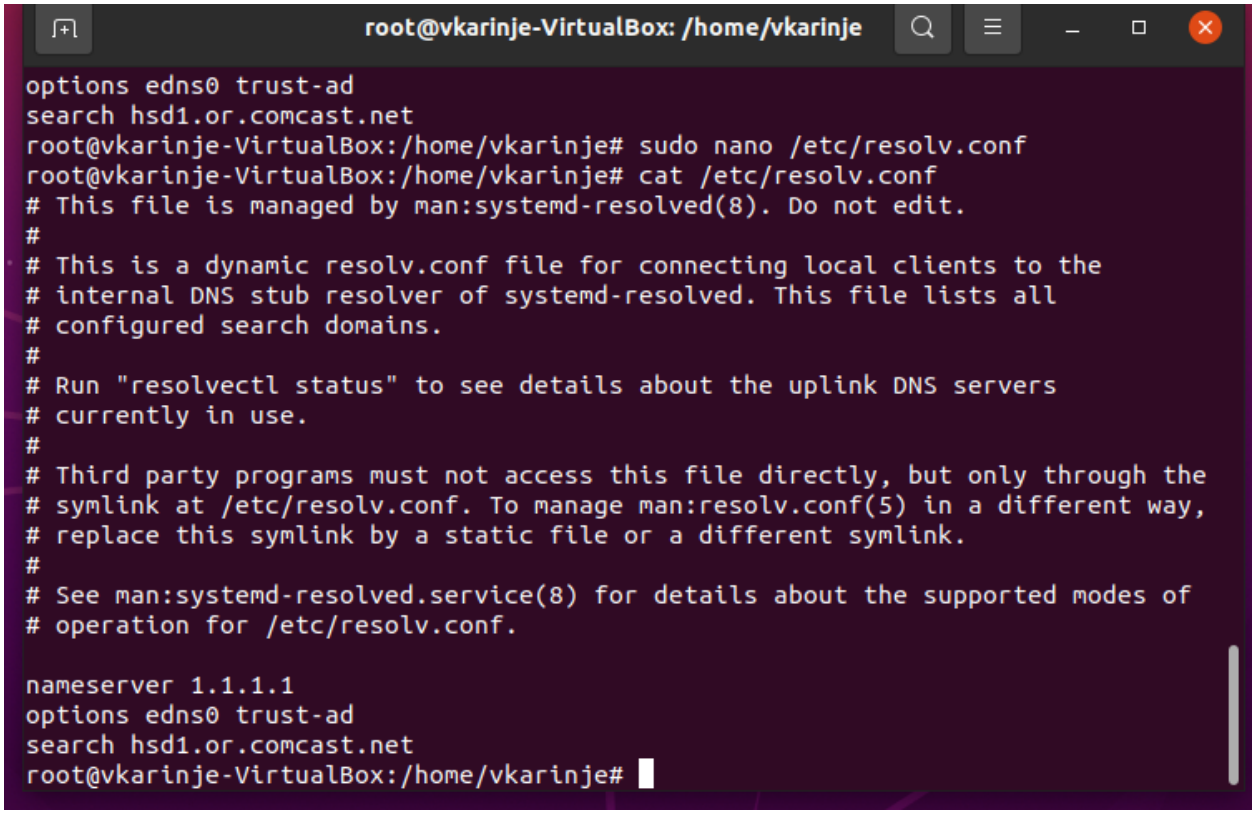
- Use netstat to find the IP address of the default router

  Ans:

```
vkarinje@vkarinje-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          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
vkarinje@vkarinje-VirtualBox:~$
```

- Temporarily change the default DNS server by performing `sudo vim /etc/resolv.conf` and changing the IP address of the nameserver to `1.1.1.1`. Note that this will be overwritten upon next DHCP renew

Ans:



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

Ans:

```
vkarinje@vkarinje-VirtualBox:~$ dig -x 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: 44754
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;1.1.1.1.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
1.1.1.1.in-addr.arpa.   631     IN      PTR     one.one.one.one.

;; Query time: 28 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Oct 10 15:51:24 PDT 2022
;; MSG SIZE  rcvd: 78

vkarinje@vkarinje-VirtualBox:~$
```

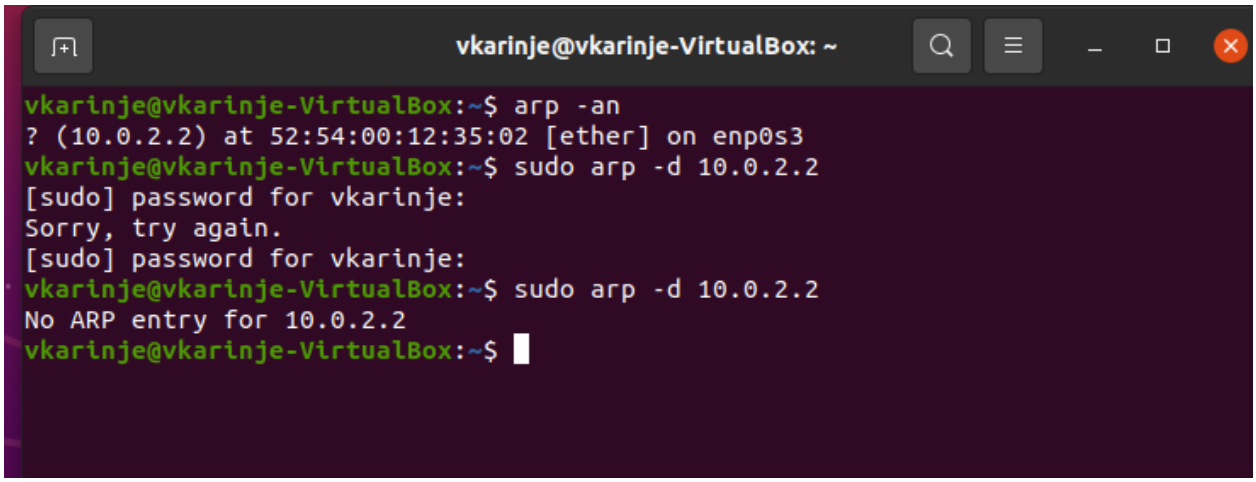
Dump ARP table

Examine the output of the command below to see all of the entries in the table and their numeric IP addresses.

```
vkarinje@vkarinje-VirtualBox:~$ arp -an
? (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
vkarinje@vkarinje-VirtualBox:~$
```

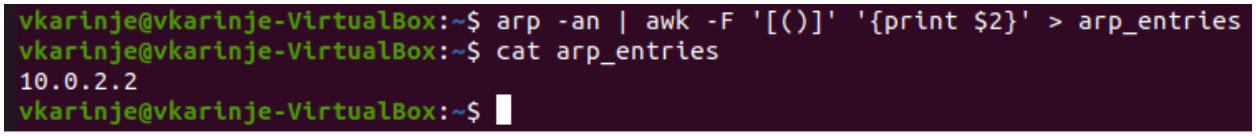
In order to delete the ARP entry of a particular IP address we simply run the command:

```
vkarinje@vkarinje-VirtualBox:~$ sudo arp -d 10.0.2.2
vkarinje@vkarinje-VirtualBox:~$ arp -an
vkarinje@vkarinje-VirtualBox:~$
```



Use a single command-line to create a file that contains each IP address that appears in the machine's ARP table and places the results in a file called `arp_entries`. The command should be similar to the one below:

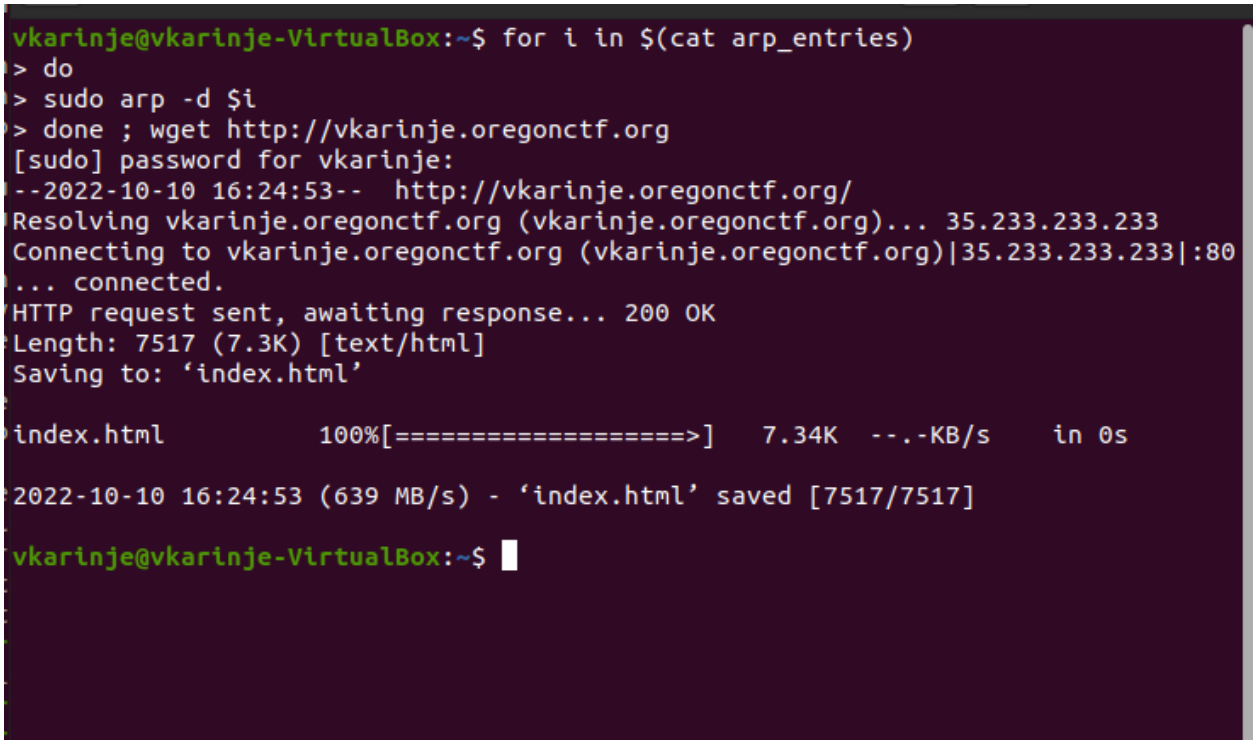
Ans :



Collect and analyze the network trace of a connection

Clear ARP table and retrieve site

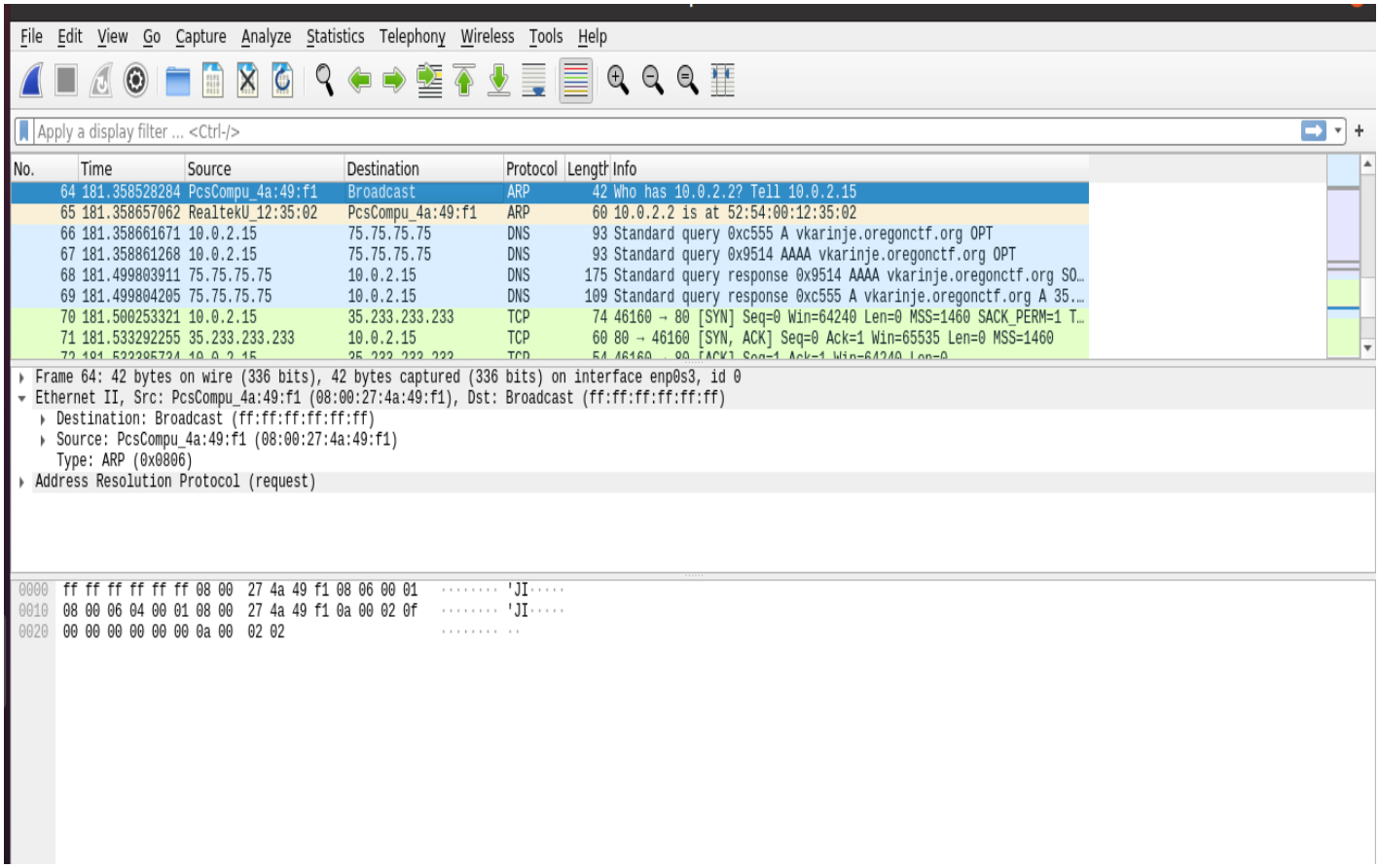
Then clear the ARP table and immediately retrieve `http://<OdinId>.oregonctf.org` (replacing `<OdinId>` with your Odin Id).



Analyze trace

Stop the packet capture and inspect it.

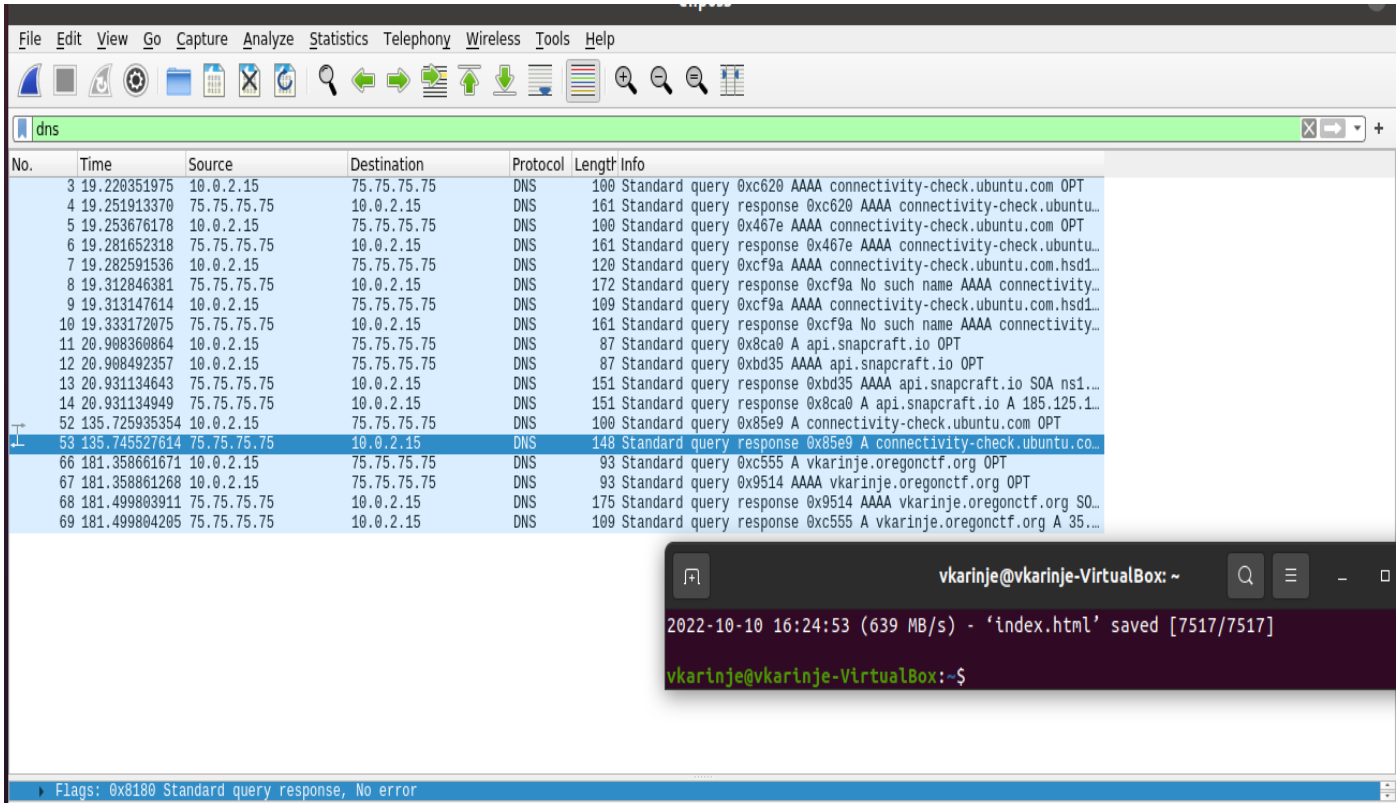
- Take a screenshot of the trace within Wireshark and include an annotation of the packets in the trace to explain the purpose of each of the packets being exchanged.



A broadcast request is sent from the source . Source asks who has the IP address 10.0.2.2. The target server responds with its MAC address.

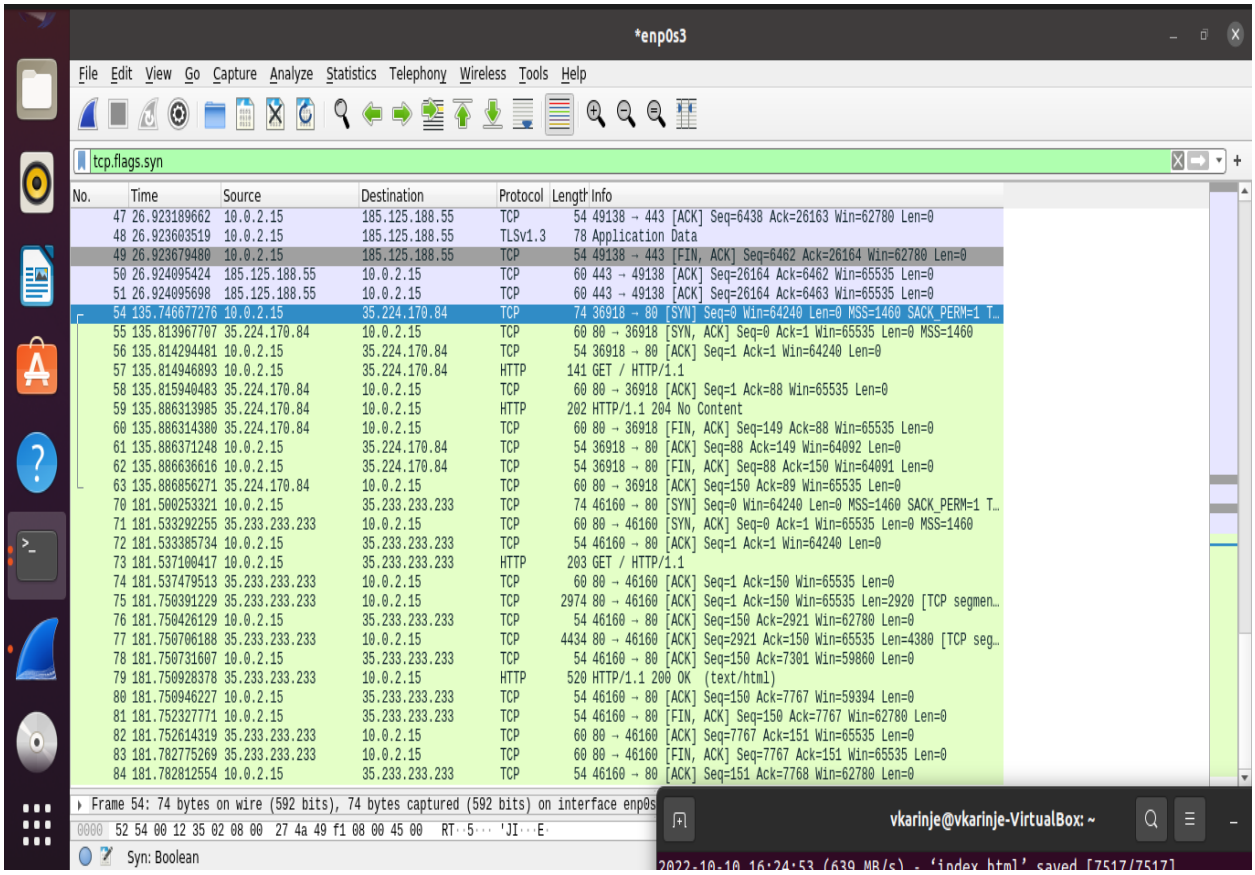
- How many DNS requests are made?

  Ans: There are 18 DNS requests made.



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

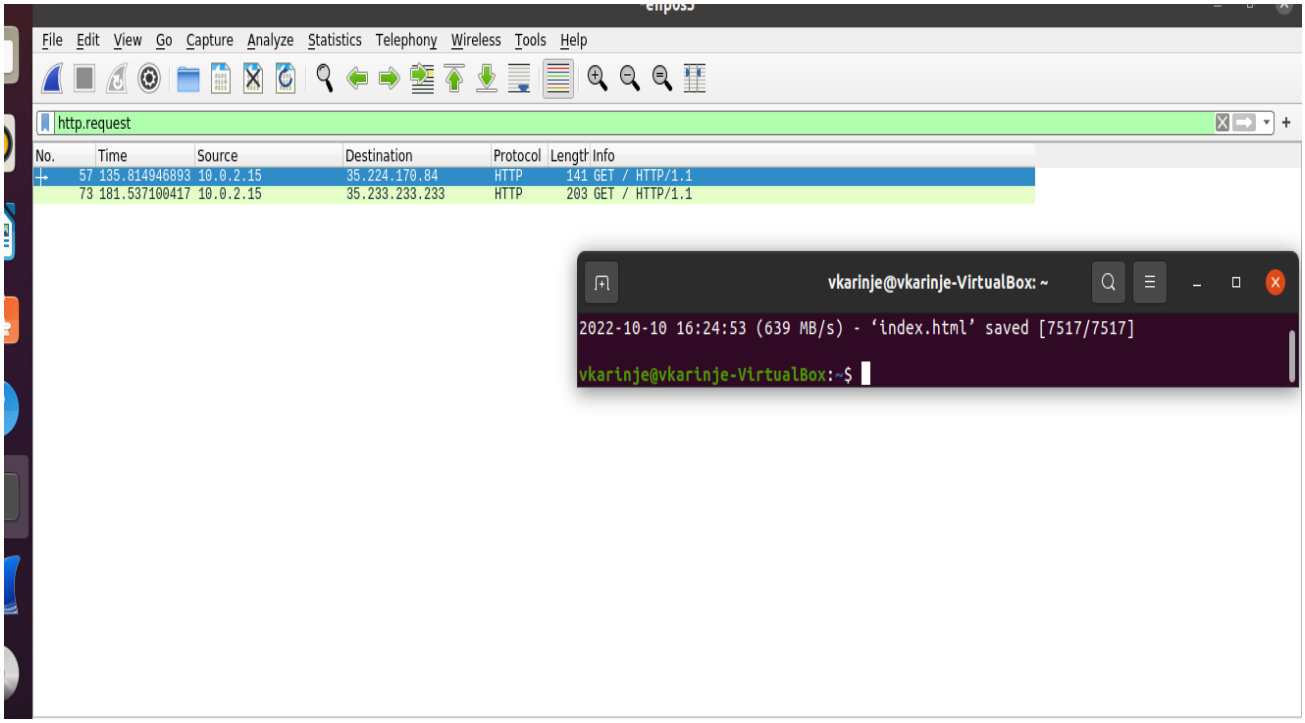
  Ans: 21 TCP connections



- How many HTTP GET requests are there for embedded objects?

  Ans: There are two HTTP GET requests made for embedded objects

Ans:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request
No. Time Source Destination Protocol Length Info
57 135.814946893 10.0.2.15 35.224.170.84 HTTP 141 GET / HTTP/1.1
73 181.537100417 10.0.2.15 35.233.233.233 HTTP 203 GET / HTTP/1.1
vkarinje@vkarinje-VirtualBox: ~
2022-10-10 16:24:53 (639 MB/s) - 'index.html' saved [7517/7517]
vkarinje@vkarinje-VirtualBox:~$