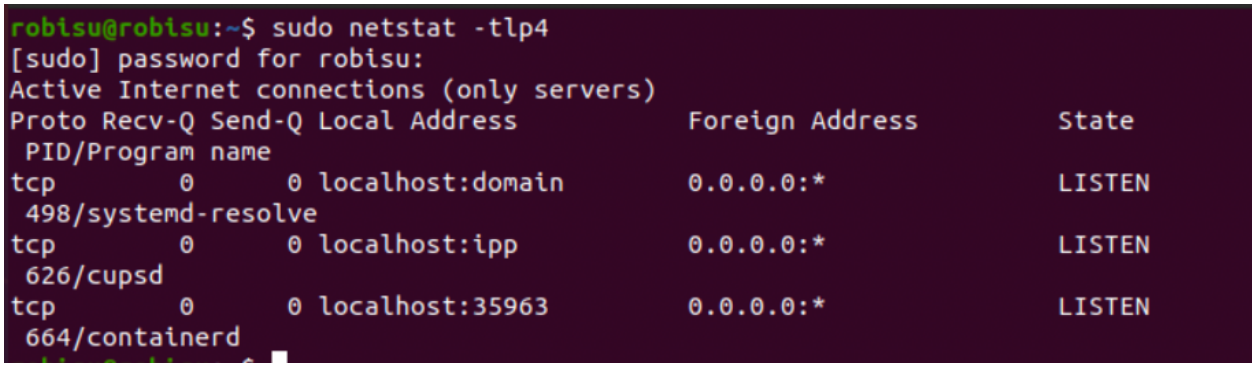
TCP #1

Netstat

Linux VM netstat output:



Port for ‘domain’:

Port for ‘ipp’:

containerd: ‘container daemon” - it is a container runtime, which helps to manage the lifecycle of the host machine, which in this case is the Ubuntu VM itself. It helps with everything from image management, lower-level storage, to network connections of the host.

PSU Linux Lab Machine:

```
[robisu@babbage ~] $ netstat -tlp4
(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 localhost.localdo:44245 0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:38677           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:domain       0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      -
tcp        0      0 localhost.localdo:43607 0.0.0.0:*               LISTEN      -
tcp        0      0 localhost.localdoma:ipp 0.0.0.0:*               LISTEN      -
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*               LISTEN      -
tcp        0      0 localhost.localdom:6010 0.0.0.0:*               LISTEN      -
tcp        0      0 localhost.localdo:42491 0.0.0.0:*               LISTEN      -
tcp        0      0 localhost.localdom:6011 0.0.0.0:*               LISTEN      -
tcp        0      0 localhost.localdom:6012 0.0.0.0:*               LISTEN      -
tcp        0      0 localhost.localdo:43359 0.0.0.0:*               LISTEN      -
tcp        0      0 localhost.localdo:41089 0.0.0.0:*               LISTEN      -
tcp        0      0 localhost.localdo:40323 0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:25069           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN      -
[robisu@babbage ~] $
```

LSOF

Number of open descriptors- **34817**:

```
robisu@robisu:~$ sudo lsof | wc -l
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
34817
robisu@robisu:~$
```

Equivalent to the **netstat** output:

```
robisu@robisu:~$ sudo lsof -sTCP:LISTEN -i4TCP
COMMAND     PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r   498 systemd-resolve   13u  IPv4  20313      0t0  TCP localhost:domai
n (LISTEN)
cupsd       626            root    7u  IPv4  23893      0t0  TCP localhost:ipp (
LISTEN)
container 5295             root   12u  IPv4  83550      0t0  TCP localhost:44419
 (LISTEN)
```

NETCAT

```
robisu@robisu:~$ nc linux.cs.pdx.edu 22
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3
^C
robisu@robisu:~$
```

TCP #2

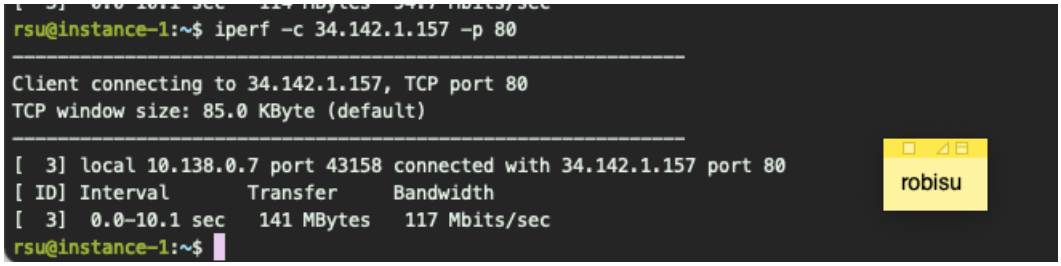
IPERF

Australia:

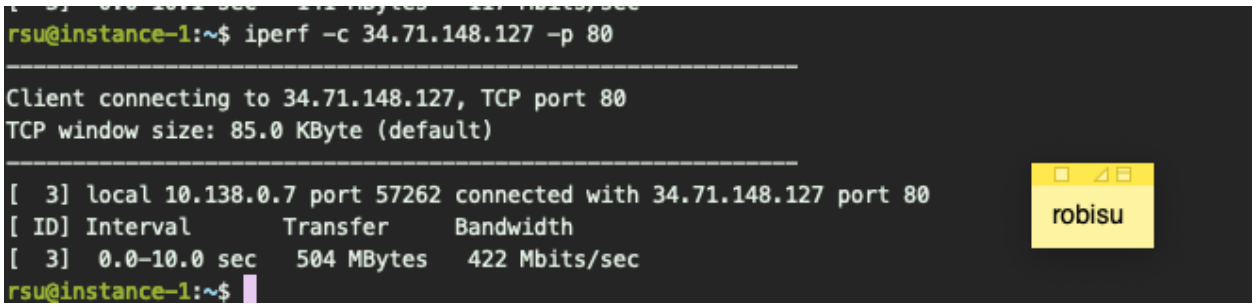
```
rsu@instance-1:~$ iperf -c 34.116.68.173 -p 80
------------------------------------------------------------
Client connecting to 34.116.68.173, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 10.138.0.7 port 56220 connected with 34.116.68.173 port 80
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.1 sec   114 MBytes  94.7 Mbits/sec
rsu@instance-1:~$
```

robisu

Europe:



US East:



Bandwidths:

- Australia: 94.7 mbps
- Europe: 117 mbps
- US East: 422 mbps

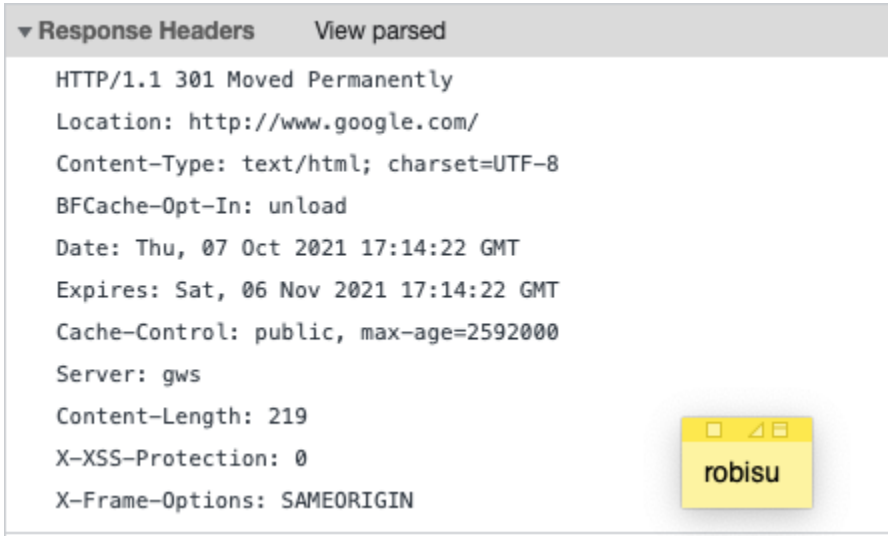
The magnitude of each bandwidth decreases as the distance from us-west1-b increases. The physical distance is what explains this pattern, because of the relative time that it takes for a packet to be acknowledged after it is sent. The network increases the bandwidth by measuring the time from request → acknowledgement, and this is fastest with the nearest location of the VM (which in this case is US East).

HTTP #3

First Request

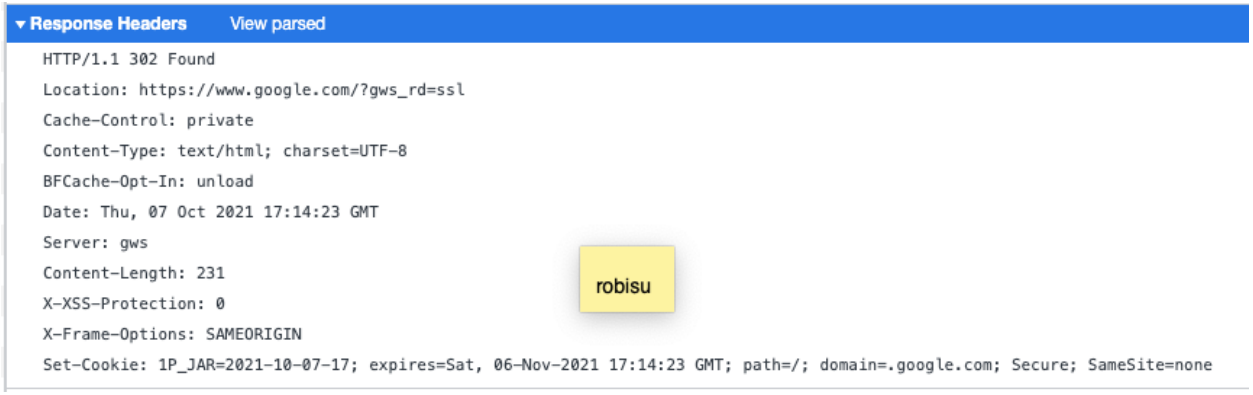
- *What is the URL being requested?*
  - **http://google.com/**
- *What are the Host: (HTTP 1.1) or :authority: (HTTP 2.0) headers sent by the browser?*
  - **Host: google.com**
- *What is the User-Agent: HTTP header that is sent?*

    - **Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36**
- *What is the HTTP status code in the response and what does it mean?*
    - **Status code: 301 Moved Permanently**
    - **“Moved Permanently” - this specific URL has been listed as one that is permanently redirected to a different URL**
- *Look up the status code. Show the associated HTTP response header that is sent in conjunction with this status code for the request.*
    - **HTTP/1.1 301 Moved Permanently**



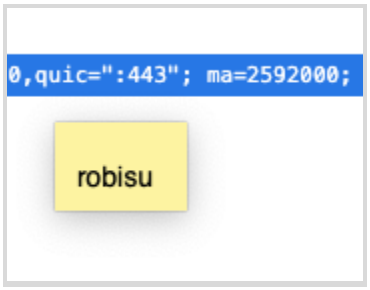
Second Request

- *What is the URL being requested? Is it using HTTP or HTTPS?*
    - **It uses HTTP: http://www.google.com/**
- *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?*
    - **Status code: 302 Found**
    - **Unlike a 301 code, a 302 indicates a *temporary* move to a different URL (one indicated in the Location header in the response)**
- *Show the associated HTTP response header that is sent in conjunction with this status code for the request.* (see below)



Third Request

- *What is the URL being requested? Is it using HTTP or HTTPS?*
    - **HTTPS: https://www.google.com/?gws_rd=ssl**
- *What is the HTTP status code in the response?*
    - **200**
    - **This is the 'OK' response, meaning the requested URL and resource has been found and retrieved successfully**
- *Look for an alt-svc: HTTP response header. Does the server believe the client can use HTTP3/QUIC?*
    - **Yes, it lists that an alternative service is available for the server at port 443 - quic=":443"; ma=2592000**



- *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?*

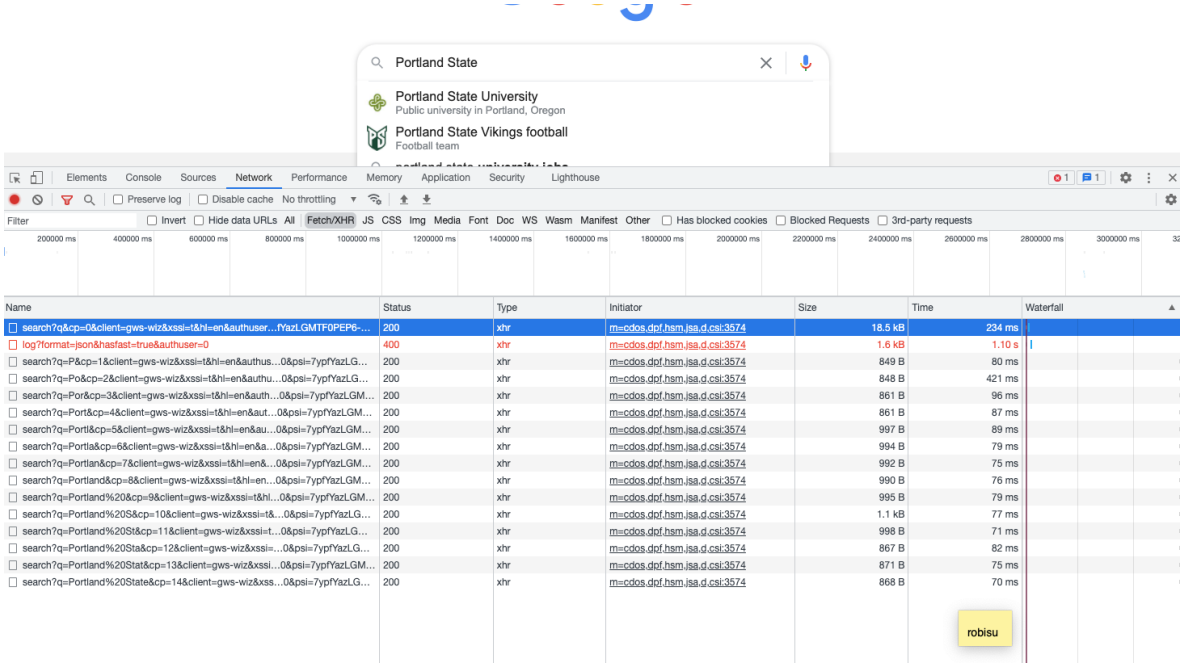
```
set-cookie: 1P_JAR=2021-10-07-17; expires=Sat, 06-Nov-2021 17:14:23 GMT; path=/; domain=.google.com; Secure; SameSite=none
set-cookie: NID=511=Q2aUSPuj-BJ-c-mdBK-owmJxQv_6B43_E1YRUouDLJQFLqVoSp2Fxtg2RCf5TRwzND1Uku_XuZt7TZzEGDdo7NEdlBPs5vvDJX6DrGg0fT3ACNMBGKKnNLyF2RDTpk3Hj-svlYPI1mtnj5tEN8L9dLEFoKiolrmvdsxqoLTLpbQ; expires=Fri, 08-Apr-2022 17:14:23 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none
strict-transport-security: max-age=31536000
x-frame-options: SAMEORIGIN
```

robisu

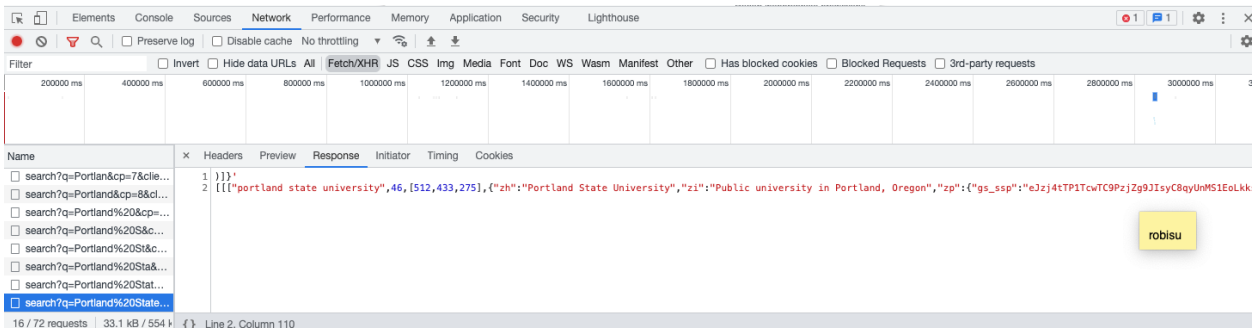
For both cookies above, they are designated as “SameSite=None; Secure”. Which means that they are explicitly designated as cross-site/third-party cookies, and also require a secure context (HTTPS).

Asynchronous Requests

List of requests/responses from typing in the search bar:



Response payload form a single request:



DNS #1

- *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?*
    - **www.pdx.edu : IP Address is 54.214.67.95**

```
[robisu@ada ~] $ dig 131.252.208.53 www.pdx.edu A +tcp

; <<>> DiG 9.16.1-Ubuntu <<>> 131.252.208.53 www.pdx.edu A +tcp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 14652
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e66fed76855d7bc601000000615fa5acb49f442c1c189715 (good)
;; QUESTION SECTION:
;131.252.208.53.                        IN      A

;; AUTHORITY SECTION:
.                       10677   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2021100701 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53)
;; WHEN: Thu Oct 07 18:58:04 PDT 2021
;; MSG SIZE  rcvd: 146

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57641
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e66fed76855d7bc601000000615fa5acb49f442c1c189715 (good)
;; QUESTION SECTION:
;www.pdx.edu.                   IN      A

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

;; Query time: 47 msec
;; SERVER: 131.252.208.53#53(131.252.208.53)
;; WHEN: Thu Oct 07 18:58:04 PDT 2021
;; MSG SIZE  rcvd: 84
```

- **pdx.edu (mail exchange) : IP Address is 74.125.195.26**

```
[robisu@ada ~] $ dig 131.252.208.53 pdx.edu MX +tcp

; <<>> DiG 9.16.1-Ubuntu <<>> 131.252.208.53 pdx.edu MX +tcp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 21886
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 17f8a4df523a26ac01000000615fa5efba84bda634348e90 (good)
;; QUESTION SECTION:
;131.252.208.53.                        IN      A

;; AUTHORITY SECTION:
.                       10610   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2021100701 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53)
;; WHEN: Thu Oct 07 18:59:11 PDT 2021
;; MSG SIZE  rcvd: 146

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57821
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 17f8a4df523a26ac01000000615fa5efba84bda634348e90 (good)
;; QUESTION SECTION:
;pdx.edu.                       IN      MX

;; ANSWER SECTION:
pdx.edu.                72820   IN      MX      5 alt1.aspmx.l.google.com.
pdx.edu.                72820   IN      MX      5 alt2.aspmx.l.google.com.
pdx.edu.                72820   IN      MX      10 alt4.aspmx.l.google.com.
pdx.edu.                72820   IN      MX      1 aspmx.l.google.com.
pdx.edu.                72820   IN      MX      10 alt3.aspmx.l.google.com.

;; ADDITIONAL SECTION:
aspmx.l.google.com.     164     IN      A       74.125.195.26
aspmx.l.google.com.     273     IN      AAAA    2607:f8b0:400e:c08::1b
```

    - **Both www.pdx.edu and PSU's mail services are hosted by external service providers, Amazon and Google respectively (and not locally because they do not start with the prefix 131.252.*)**
- *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.*

Find authoritative server: dig 131.252.208.32 mashimaro.cs.pdx.edu NS +tcp

```
[robisu@ada ~] $ dig 131.252.208.53 mashimaro.cs.pdx.edu NS +tcp

; <<>> DiG 9.16.1-Ubuntu <<>> 131.252.208.53 mashimaro.cs.pdx.edu NS +tcp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 8112
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 15430b93007019e801000000615fa84b6fdcb7f9827415d8 (good)
;; QUESTION SECTION:
;131.252.208.53.                        IN      A

;; AUTHORITY SECTION:
.                       10006   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2021100701 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53)
;; WHEN: Thu Oct 07 19:09:15 PDT 2021
;; MSG SIZE  rcvd: 146

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13671
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 15430b93007019e801000000615fa84b6fdcb7f9827415d8 (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. 2021100703 600 300 1209600 300

;; Query time: 3 msec
;; SERVER: 131.252.208.53#53(131.252.208.53)
;; WHEN: Thu Oct 07 19:09:15 PDT 2021
;; MSG SIZE  rcvd: 147
```

Query for mashimaro.cs.pdx.edu: `dig -q cs.pdx.edu mashimaro.cs.pdx.edu A +tcp`

```
[robisu@ada ~] $ dig -q cs.pdx.edu mashimaro.cs.pdx.edu A +tcp

; <<>> DiG 9.16.1-Ubuntu <<>> -q cs.pdx.edu mashimaro.cs.pdx.edu A +tcp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42025
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a8e2fb46a379f46101000000615fa9159c2ca849389e48bb (good)
;; QUESTION SECTION:
;cs.pdx.edu.                    IN      A

;; ANSWER SECTION:
cs.pdx.edu.             6834    IN      A       131.252.208.114

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53)
;; WHEN: Thu Oct 07 19:12:37 PDT 2021
;; MSG SIZE  rcvd: 83

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46926
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a8e2fb46a379f46101000000615fa9159c2ca849389e48bb (good)
;; QUESTION SECTION:
;mashimaro.cs.pdx.edu.          IN      A

;; ANSWER SECTION:
mashimaro.cs.pdx.edu.   14301   IN      A       131.252.220.66

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53)
;; WHEN: Thu Oct 07 19:12:37 PDT 2021
;; MSG SIZE  rcvd: 93
```

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

Find authoritative server: dig 131.252.208.53 thefengs.com NS +tcp

```
;; ANSWER SECTION:
thefengs.com.           21600   IN      NS      ns-cloud2.googledomains.com.
thefengs.com.           21600   IN      NS      ns-cloud4.googledomains.com.
thefengs.com.           21600   IN      NS      ns-cloud1.googledomains.com.
thefengs.com.           21600   IN      NS      ns-cloud3.googledomains.com.

;; ADDITIONAL SECTION:
ns-cloud1.googledomains.com. 329859 IN  A       216.239.32.106
ns-cloud2.googledomains.com. 141375 IN  A       216.239.34.106
ns-cloud3.googledomains.com. 141375 IN  A       216.239.36.106
ns-cloud4.googledomains.com. 141375 IN  A       216.239.38.106
ns-cloud1.googledomains.com. 329859 IN  AAAA    2001:4860:4802:32::6a
ns-cloud2.googledomains.com. 172800 IN  AAAA    2001:4860:4802:34::6a
ns-cloud3.googledomains.com. 172800 IN  AAAA    2001:4860:4802:36::6a
ns-cloud4.googledomains.com. 172800 IN  AAAA    2001:4860:4802:38::6a
```

robisu

Find IP address: dig 216.239.32.106 thefengs.com A +tcp

```
[robisu@ada ~] $ dig 216.239.32.106 thefengs.com A +tcp

; <<>> DiG 9.16.1-Ubuntu <<>> 216.239.32.106 thefengs.com A +tcp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 26756
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 175398a6948868610100000615faa5e2a7da2e3c355f867 (good)
;; QUESTION SECTION:
;216.239.32.106.                        IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2021100701 1800 900 604800 86400

;; Query time: 11 msec
;; SERVER: 131.252.208.53#53(131.252.208.53)
;; WHEN: Thu Oct 07 19:18:06 PDT 2021
;; MSG SIZE  rcvd: 146

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36767
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 175398a6948868610100000615faa5e2a7da2e3c355f867 (good)
;; QUESTION SECTION:
;thefengs.com.                  IN      A

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

;; Query time: 63 msec
;; SERVER: 131.252.208.53#53(131.252.208.53)
;; WHEN: Thu Oct 07 19:18:06 PDT 2021
;; MSG SIZE  rcvd: 85
```

- *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)*
    - **In the request header for a web/HTTP request, the 'Host' field will specify the domain name, which distinguishes the site at the IP address.**

DNS Iterative Lookups

Root Servers:

```
Last login: Thu Oct  7 18:40:32 2021 from c-73-11-56-88.hsd1.ut.comcast.net
[robisu@ada ~] $ dig

; <<>> DiG 9.16.1-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64157
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e006b4005ed82ad4010000006160b4cc328176e6c03e1d6e (good)
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       507306  IN      NS      f.root-servers.net.
.                       507306  IN      NS      g.root-servers.net.
.                       507306  IN      NS      i.root-servers.net.
.                       507306  IN      NS      b.root-servers.net.
.                       507306  IN      NS      j.root-servers.net.
.                       507306  IN      NS      k.root-servers.net.
.                       507306  IN      NS      m.root-servers.net.
.                       507306  IN      NS      d.root-servers.net.
.                       507306  IN      NS      l.root-servers.net.
.                       507306  IN      NS      a.root-servers.net.
.                       507306  IN      NS      h.root-servers.net.
.                       507306  IN      NS      e.root-servers.net.
.                       507306  IN      NS      c.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     349997  IN      A       198.41.0.4
b.root-servers.net.     349998  IN      A       199.9.14.201
c.root-servers.net.     349996  IN      A       192.33.4.12
d.root-servers.net.     349997  IN      A       199.7.91.13
e.root-servers.net.     349997  IN      A       192.203.230.10
f.root-servers.net.     349997  IN      A       192.5.5.241
g.root-servers.net.     349996  IN      A       192.112.36.4
h.root-servers.net.     349997  IN      A       198.97.190.53
i.root-servers.net.     349997  IN      A       192.36.148.17
j.root-servers.net.     349998  IN      A       192.58.128.30
k.root-servers.net.     349997  IN      A       193.0.14.129
l.root-servers.net.     349998  IN      A       199.7.83.42
m.root-servers.net.     349996  IN      A       202.12.27.33
a.root-servers.net.     436413  IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     436413  IN      AAAA    2001:500:200::b
c.root-servers.net.     436413  IN      AAAA    2001:500:2::c
d.root-servers.net.     436413  IN      AAAA    2001:500:2d::d
e.root-servers.net.     436413  IN      AAAA    2001:500:a8::e
f.root-servers.net.     436413  IN      AAAA    2001:500:2f::f
g.root-servers.net.     436413  IN      AAAA    2001:500:12::d0d
h.root-servers.net.     436413  IN      AAAA    2001:500:1::53
i.root-servers.net.     436413  IN      AAAA    2001:7fe::53
j.root-servers.net.     436413  IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     436413  IN      AAAA    2001:7fd::1
l.root-servers.net.     436413  IN      AAAA    2001:500:9f::42
m.root-servers.net.     436413  IN      AAAA    2001:dc3::35
```

com. servers:

```
[robisu@ada ~] $ dig @192.5.5.241 console.cloud.google.com NS +tcp +norecurse

; <<>> DiG 9.16.1-Ubuntu <<>> @192.5.5.241 console.cloud.google.com NS +tcp +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49387
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65535
;; QUESTION SECTION:
;console.cloud.google.com.      IN      NS

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

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

;; Query time: 7 msec
;; SERVER: 192.5.5.241#53(192.5.5.241)
;; WHEN: Fri Oct 08 16:03:50 PDT 2021
;; MSG SIZE  rcvd: 849
```

google.com. authoritative servers:

```
[robisu@ada ~] $ dig @192.41.162.30 console.cloud.google.com NS +tcp +norecurse

; <<>> DiG 9.16.1-Ubuntu <<>> @192.41.162.30 console.cloud.google.com NS +tcp +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7407
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;console.cloud.google.com.      IN      NS

;; AUTHORITY SECTION:
google.com.             172800  IN      NS      ns2.google.com.
google.com.             172800  IN      NS      ns1.google.com.
google.com.             172800  IN      NS      ns3.google.com.
google.com.             172800  IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns2.google.com.         172800  IN      AAAA    2001:4860:4802:34::a
ns2.google.com.         172800  IN      A       216.239.34.10
ns1.google.com.         172800  IN      AAAA    2001:4860:4802:32::a
ns1.google.com.         172800  IN      A       216.239.32.10
ns3.google.com.         172800  IN      AAAA    2001:4860:4802:36::a
ns3.google.com.         172800  IN      A       216.239.36.10
ns4.google.com.         172800  IN      AAAA    2001:4860:4802:38::a
ns4.google.com.         172800  IN      A       216.239.38.10

;; Query time: 27 msec
;; SERVER: 192.41.162.30#53(192.41.162.30)
;; WHEN: Fri Oct 08 16:04:14 PDT 2021
;; MSG SIZE  rcvd: 301
```

lowest authoritative server for console.cloud.google.com (same as the authoritative server group as was discovered in the previous step, so to find the IP Address, I can query the same IP for the “Answer” instead of “Name Server” → see next screenshot):

```
[robisu@ada ~] $ dig @216.239.34.10 console.cloud.google.com NS +tcp +norecurse

; <<>> DiG 9.16.1-Ubuntu <<>> @216.239.34.10 console.cloud.google.com NS +tcp +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18510
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;console.cloud.google.com.      IN      NS

;; ANSWER SECTION:
console.cloud.google.com. 300   IN      CNAME   www3.l.google.com.

;; AUTHORITY SECTION:
l.google.com.           60      IN      SOA     ns1.google.com. dns-admin.google.com. 401726889 900 900 1800 60

;; Query time: 7 msec
;; SERVER: 216.239.34.10#53(216.239.34.10)
;; WHEN: Fri Oct 08 16:04:37 PDT 2021
;; MSG SIZE  rcvd: 124
```

Final IP Address for console.cloud.google.com:

```
[robisu@ada ~] $ dig @216.239.34.10 console.cloud.google.com A +tcp +norecurse

; <<>> DiG 9.16.1-Ubuntu <<>> @216.239.34.10 console.cloud.google.com A +tcp +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21394
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;console.cloud.google.com.      IN      A

;; ANSWER SECTION:
console.cloud.google.com. 300   IN      CNAME   www3.l.google.com.
www3.l.google.com.      300     IN      A       172.217.14.238

;; Query time: 7 msec
;; SERVER: 216.239.34.10#53(216.239.34.10)
;; WHEN: Fri Oct 08 16:32:23 PDT 2021
;; MSG SIZE  rcvd: 90
```

Reverse DNS Lookups

List IPv4 Addresses pointed to by espn.go.com:

```
[robisu@ada ~] $ IP=`dig @ns-1573.awsdns-04.co.uk. espn.go.com. A +tcp | egrep 99. | awk '{print $5}'`
[robisu@ada ~] $ echo $IP
99.84.74.93 99.84.74.53 99.84.74.55 99.84.74.46
[robisu@ada ~] $
```

Reverse Lookup Loop for DNS Names:

```
[robisu@ada ~] $ for i in `echo $IP`; do dig -x $i | egrep server- | awk '{print $5}'; done
server-99-84-74-93.hio50.r.cloudfront.net.
server-99-84-74-53.hio50.r.cloudfront.net.
server-99-84-74-55.hio50.r.cloudfront.net.
server-99-84-74-46.hio50.r.cloudfront.net.
[robisu@ada ~] $
```

Host Enumeration

For loop to do reverse lookups on the range of subnets at 131.252.220.0/24:

```
[robisu@ada ~] $ for i in `echo 131.252.220.{0..255}`; do dig -x $i | egrep cs.pdx.edu | awk '{print $5}'; done > 220hosts.txt
[robisu@ada ~] $
```

Print hosts with car manufacturer names:

```
[robisu@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.
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.
[robisu@ada ~] $
```

DNS #2

- *What geographic locations do ipinfo.io and DB-IP return?*
    - For 131.252.208.53 : Portland, OR

Geolocation data from DB-IP (Product: Full, 2021-10-1)

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

robisu

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

robisu

- For 198.82.247.66: Blacksburg, VA

Geolocation data from IP2Location (Product: DB6, updated on 2021-10-1)

IP Address	Country	Region	City
198.82.247.66	United States of America	Virginia	Blacksburg
ISP	**Organization**	**Latitude**	**Longitude**
Virginia Polytechnic Institute and State Univ.	Not Available	37.2557	-80.4315

robisu

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

robisu

- *Record each result for your lab notebook.*

```
Last login: Fri Oct  8 15:58:40 2021 from c-71-230-228-230.hsd1.or.comcast.net
[robisu@ada ~] $ dig @131.252.208.53 www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> @131.252.208.53 www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30656
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5f7c1608979c87d3010000006163230db9a6236b2bcc64dc (good)
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         176     IN      A       142.250.217.100

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53)
;; WHEN: Sun Oct 10 10:29:49 PDT 2021
;; MSG SIZE  rcvd: 87
```

```
[robisu@ada ~] $ dig @198.82.247.66 www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> @198.82.247.66 www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47930
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 6837437b5cf6371bda36eeb86163234645bdf5f822175ff7 (good)
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         84      IN      A       172.217.9.196

;; Query time: 63 msec
;; SERVER: 198.82.247.66#53(198.82.247.66)
;; WHEN: Sun Oct 10 10:30:46 PDT 2021
;; MSG SIZE  rcvd: 87
```

- *What is the geographic distance between each pair of DNS server and web server?*
    - **From Blacksburg,VA to Washington, DC: ~200 miles**
    - **From Portland, OR to Seattle, WA: ~150 miles**
- *Do the routes reveal any information on the accuracy of the geographic locations given? (Answer might be no)*

- **Not really...for all four of the IP Addresses, when I examine the hops in between the PSU-network machine and the destination host, most of the geolocation data from the two different sources, ipinfo.io and DB-IP, does not match for one IP. In one case, one source sites Tokyo, Japan while the other is Montreal, Quebec:**

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

IP Address	Country	Region	City
108.170.235.159	Japan	Tokyo	Tokyo
ISP	**Organization**	**Latitude**	**Longitude**
Google LLC	Google LLC (google.com)	35.6895	139.6917

Geolocation data from DB-IP (Product: Full, 2021-10-1)

IP Address	Country	Region	City
108.170.235.159	Canada	Quebec	Montreal
ISP	**Organization**	**Latitude**	**Longitude**
Google LLC	Google LLC	45.5017	-73.5673

robisu

List of all 4 traceroute results:

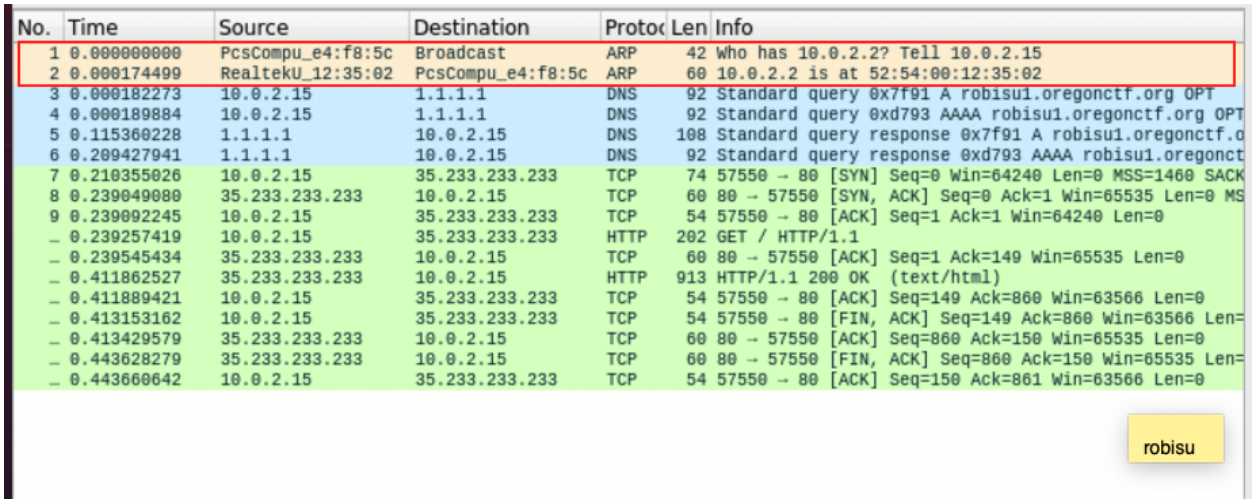
```
[robisu@ada ~] $ traceroute 131.252.208.53
traceroute to 131.252.208.53 (131.252.208.53), 30 hops max, 60 byte packets
 1  rdns.cat.pdx.edu (131.252.208.53)  1.078 ms  1.013 ms  0.968 ms
[robisu@ada ~] $ traceroute 198.82.247.66
traceroute to 198.82.247.66 (198.82.247.66), 30 hops max, 60 byte packets
 1  radiant.seas.pdx.edu (131.252.208.212)  1.255 ms  4.419 ms  4.386 ms
 2  CORE1.net.pdx.edu (131.252.5.142)  0.796 ms  0.750 ms  0.703 ms
 3  131.252.5.213 (131.252.5.213)  4.144 ms  4.098 ms  4.054 ms
 4  ptck-pe1-gw.nero.net (199.165.177.18)  4.008 ms  3.962 ms  3.917 ms
 5  hundredge-0-0-0-24.701.core1.port.net.internet2.edu (198.71.45.218)  4.524 ms  4.464 ms  4.402 ms
 6  163.253.1.231 (163.253.1.231)  5.389 ms  5.231 ms  5.217 ms
 7  ae-17.4070.rtsw.seat.net.internet2.edu (163.253.0.191)  4.156 ms  4.268 ms  4.084 ms
 8  ae-1.4079.rtsw.minn.net.internet2.edu (162.252.70.173)  45.944 ms  45.968 ms  45.823 ms
 9  ae-1.4079.rtsw.eqch.net.internet2.edu (162.252.70.106)  44.672 ms  44.645 ms  44.616 ms
10  ae-0.4079.rtsw3.eqch.net.internet2.edu (162.252.70.163)  45.300 ms  45.160 ms  45.125 ms
11  ae-1.4079.rtsw.clev.net.internet2.edu (162.252.70.130)  51.416 ms  51.446 ms  51.358 ms
12  ae-0.4079.rtsw.ashb.net.internet2.edu (162.252.70.128)  58.288 ms  58.260 ms  58.194 ms
13  192.122.175.14 (192.122.175.14)  58.024 ms  59.179 ms  59.153 ms
14  vtacs-1.msap.cns.vt.edu (192.70.187.18)  66.129 ms  65.733 ms  64.954 ms
15  isb-core.et-5-1-0.0.cns.vt.edu (128.173.0.206)  65.269 ms  64.943 ms  64.841 ms
16  cas-core.lo0.2000.cns.vt.edu (198.82.1.143)  64.821 ms  64.949 ms  64.881 ms
17  jeru.cns.vt.edu (198.82.247.66)  64.629 ms  64.656 ms  64.597 ms
[robisu@ada ~] $ traceroute 142.250.217.100
traceroute to 142.250.217.100 (142.250.217.100), 30 hops max, 60 byte packets
 1  radiant.seas.pdx.edu (131.252.208.212)  1.317 ms  1.265 ms  1.243 ms
 2  CORE1.net.pdx.edu (131.252.5.142)  0.616 ms  0.592 ms  0.557 ms
 3  131.252.5.213 (131.252.5.213)  1.039 ms  0.955 ms  0.959 ms
 4  google-b.nwax.net (198.32.195.33)  4.029 ms  3.981 ms  3.932 ms
 5  108.170.245.97 (108.170.245.97)  4.856 ms  4.808 ms  4.974 ms
 6  142.251.55.203 (142.251.55.203)  3.944 ms  3.990 ms 142.251.55.201 (142.251.55.201)  3.978 ms
 7  sea09s30-in-f4.1e100.net (142.250.217.100)  3.931 ms  3.995 ms  3.977 ms
[robisu@ada ~] $ traceroute 172.217.9.196
traceroute to 172.217.9.196 (172.217.9.196), 30 hops max, 60 byte packets
 1  radiant.seas.pdx.edu (131.252.208.212)  1.183 ms  1.110 ms  4.056 ms
 2  CORE1.net.pdx.edu (131.252.5.142)  0.695 ms  0.680 ms  0.647 ms
 3  131.252.5.213 (131.252.5.213)  3.858 ms  3.819 ms  3.778 ms
 4  google.nwax.net (198.32.195.34)  4.089 ms  3.983 ms  4.056 ms
 5  108.170.245.124 (108.170.245.124)  4.591 ms 74.125.243.194 (74.125.243.194)  4.816 ms 108.170.245.108 (108.170.245.108)  4.486 ms
 6  142.251.64.22 (142.251.64.22)  11.481 ms  11.315 ms  11.296 ms
 7  142.250.231.200 (142.250.231.200)  49.021 ms 72.14.239.196 (72.14.239.196)  49.315 ms  49.943 ms
 8  142.251.67.133 (142.251.67.133)  150.511 ms 142.251.67.143 (142.251.67.143)  60.925 ms 142.251.67.133 (142.251.67.133)  150.964 ms
 9  209.85.252.39 (209.85.252.39)  73.648 ms 142.251.49.206 (142.251.49.206)  72.545 ms 209.85.252.47 (209.85.252.47)  72.266 ms
10  216.239.63.233 (216.239.63.233)  73.659 ms 216.239.35.163 (216.239.35.163)  71.626 ms 72.14.233.182 (72.14.233.182)  73.464 ms
11  108.170.246.1 (108.170.246.1)  71.938 ms  71.877 ms  71.798 ms
12  108.170.235.159 (108.170.235.159)  73.337 ms  73.327 ms  73.622 ms
13  iad30s14-in-f4.1e100.net (172.217.9.196)  72.958 ms  72.816 ms  71.655 ms
[robisu@ada ~] $
```

Network Recap #3

Analyze Network Trace

Wireshark Packet Trace

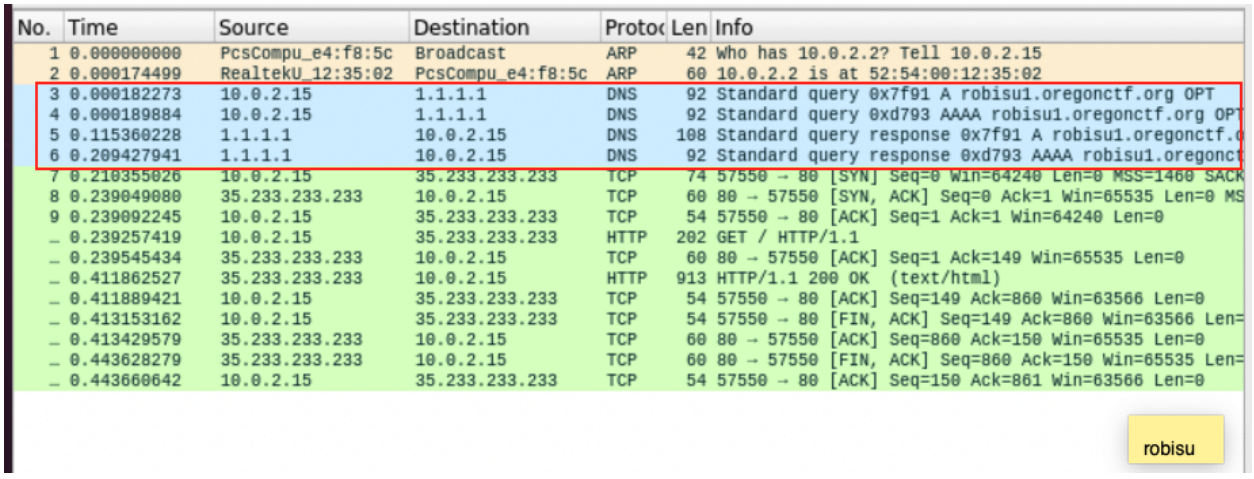
ARP Packets



No.	Time	Source	Destination	Protoc	Len	Info
1	0.000000000	PcsCompu_e4:f8:5c	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
2	0.000174499	RealtekU_12:35:02	PcsCompu_e4:f8:5c	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
3	0.000182273	10.0.2.15	1.1.1.1	DNS	92	Standard query 0x7f91 A robisu1.oregonctf.org OPT
4	0.000189884	10.0.2.15	1.1.1.1	DNS	92	Standard query 0xd793 AAAA robisu1.oregonctf.org OPT
5	0.115360228	1.1.1.1	10.0.2.15	DNS	108	Standard query response 0x7f91 A robisu1.oregonctf.o
6	0.209427941	1.1.1.1	10.0.2.15	DNS	92	Standard query response 0xd793 AAAA robisu1.oregonct
7	0.210355026	10.0.2.15	35.233.233.233	TCP	74	57550 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
8	0.239049080	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
9	0.239092245	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
_	0.239257419	10.0.2.15	35.233.233.233	HTTP	202	GET / HTTP/1.1
_	0.239545434	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [ACK] Seq=1 Ack=149 Win=65535 Len=0
_	0.411862527	35.233.233.233	10.0.2.15	HTTP	913	HTTP/1.1 200 OK (text/html)
_	0.411889421	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [ACK] Seq=149 Ack=860 Win=63566 Len=0
_	0.413153162	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [FIN, ACK] Seq=149 Ack=860 Win=63566 Len=
_	0.413429579	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [ACK] Seq=860 Ack=150 Win=65535 Len=0
_	0.443628279	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [FIN, ACK] Seq=860 Ack=150 Win=65535 Len=
_	0.443660642	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [ACK] Seq=150 Ack=861 Win=63566 Len=0

The first two packets represent the machine's broadcast message in order to discover the MAC address for the default router/gateway, as illustrated with the **Info** section of the two packets. Line 2 shows the response from the gateway device (Realtek).

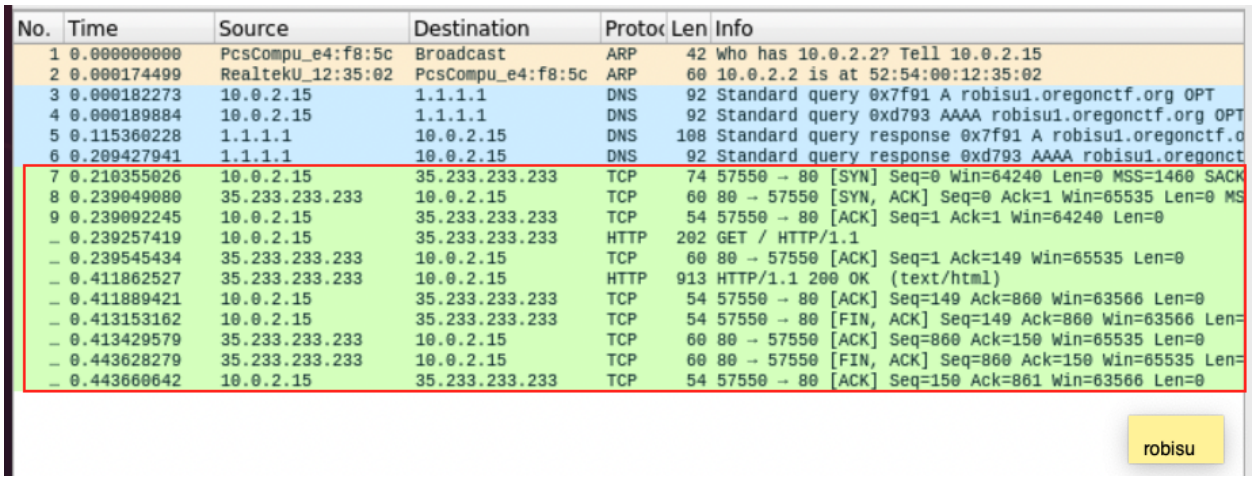
DNS Packets



No.	Time	Source	Destination	Protoc	Len	Info
1	0.000000000	PcsCompu_e4:f8:5c	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
2	0.000174499	RealtekU_12:35:02	PcsCompu_e4:f8:5c	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
3	0.000182273	10.0.2.15	1.1.1.1	DNS	92	Standard query 0x7f91 A robisu1.oregonctf.org OPT
4	0.000189884	10.0.2.15	1.1.1.1	DNS	92	Standard query 0xd793 AAAA robisu1.oregonctf.org OPT
5	0.115360228	1.1.1.1	10.0.2.15	DNS	108	Standard query response 0x7f91 A robisu1.oregonctf.o
6	0.209427941	1.1.1.1	10.0.2.15	DNS	92	Standard query response 0xd793 AAAA robisu1.oregonct
7	0.210355026	10.0.2.15	35.233.233.233	TCP	74	57550 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
8	0.239049080	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
9	0.239092245	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
_	0.239257419	10.0.2.15	35.233.233.233	HTTP	202	GET / HTTP/1.1
_	0.239545434	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [ACK] Seq=1 Ack=149 Win=65535 Len=0
_	0.411862527	35.233.233.233	10.0.2.15	HTTP	913	HTTP/1.1 200 OK (text/html)
_	0.411889421	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [ACK] Seq=149 Ack=860 Win=63566 Len=0
_	0.413153162	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [FIN, ACK] Seq=149 Ack=860 Win=63566 Len=
_	0.413429579	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [ACK] Seq=860 Ack=150 Win=65535 Len=0
_	0.443628279	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [FIN, ACK] Seq=860 Ack=150 Win=65535 Len=
_	0.443660642	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [ACK] Seq=150 Ack=861 Win=63566 Len=0

The next packets, Lines 3-6, show the DNS protocol in order to discover the IP address for the domain 'robisu1.oregonctf.org'. The queries are sent out for both IPv4 and IPv6, which are denoted by types **A** and **AAAA.**

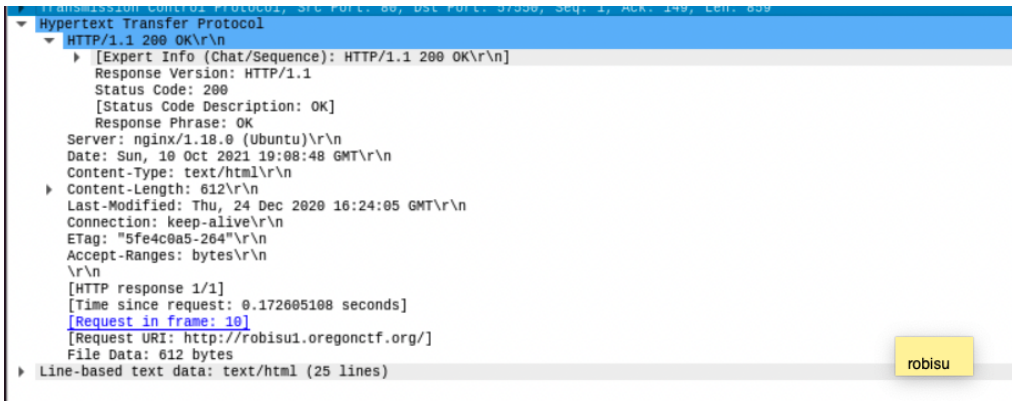
TCP and HTTP Packets



No.	Time	Source	Destination	Protoc	Len	Info
1	0.000000000	PcsCompu_e4:f8:5c	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
2	0.000174499	RealtekU_12:35:02	PcsCompu_e4:f8:5c	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
3	0.000182273	10.0.2.15	1.1.1.1	DNS	92	Standard query 0x7f91 A robisu1.oregonctf.org OPT
4	0.000189884	10.0.2.15	1.1.1.1	DNS	92	Standard query 0xd793 AAAA robisu1.oregonctf.org OPT
5	0.115360228	1.1.1.1	10.0.2.15	DNS	108	Standard query response 0x7f91 A robisu1.oregonctf.o
6	0.209427941	1.1.1.1	10.0.2.15	DNS	92	Standard query response 0xd793 AAAA robisu1.oregonct
7	0.210355026	10.0.2.15	35.233.233.233	TCP	74	57550 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
8	0.239049080	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
9	0.239092245	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
_	0.239257419	10.0.2.15	35.233.233.233	HTTP	202	GET / HTTP/1.1
_	0.239545434	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [ACK] Seq=1 Ack=149 Win=65535 Len=0
_	0.411862527	35.233.233.233	10.0.2.15	HTTP	913	HTTP/1.1 200 OK (text/html)
_	0.411889421	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [ACK] Seq=149 Ack=860 Win=63566 Len=0
_	0.413153162	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [FIN, ACK] Seq=149 Ack=860 Win=63566 Len=
_	0.413429579	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [ACK] Seq=860 Ack=150 Win=65535 Len=0
_	0.443628279	35.233.233.233	10.0.2.15	TCP	60	80 → 57550 [FIN, ACK] Seq=860 Ack=150 Win=65535 Len=
_	0.443660642	10.0.2.15	35.233.233.233	TCP	54	57550 → 80 [ACK] Seq=150 Ack=861 Win=63566 Len=0

The remaining packets represent the TCP protocol exchange with the IP address discovered from DNS, as well as the HTTP exchange from the application layer. The first three **lines 7, 8**, **and 9**, are the sender and recipient establishing the initial random sequence number for the subsequent packets (in a 3-way handshake). Once this is established and acknowledged, then the HTTP request is sent (and acknowledged by the server), HTTP response is received (and acknowledged by the client), before a TCP packet is sent with a message that the client has finished sending all requests (indicated with the FIN code/flag in the TCP packet).

- *How many DNS requests are made?*
  - **Two DNS requests (IPv4 and IPv6)**
- *How many TCP connections does the browser initiate simultaneously to the site?*
  - **A single TCP connection is sent, indicated by the single port (80) that it connects to.**
- *How many HTTP GET requests are there for embedded objects?*
  - **There is a single GET request (‘GET /’) made, with a single response with ‘text/html’ objects.**



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Server: nginx/1.18.0 (Ubuntu)\r\n
  Date: Sun, 10 Oct 2021 19:08:48 GMT\r\n
  Content-Type: text/html\r\n
  Content-Length: 612\r\n
  Last-Modified: Thu, 24 Dec 2020 16:24:05 GMT\r\n
  Connection: keep-alive\r\n
  ETag: "5fe4c0a5-264"\r\n
  Accept-Ranges: bytes\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.172605108 seconds]
  [Request in frame: 10]
  [Request URI: http://robisu1.oregonctf.org/]
  File Data: 612 bytes
Line-based text data: text/html (25 lines)
```