CS 530 Lab Week 2
Max Huecksteadt
PSU ID 969328461

2.1

1. Netstat utility using the four flags, -p, -l, –inet and -tcp

```
mhueck2@mhueck2-VirtualBox:~$ sudo netstat -p -l --inet -tcp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      515/systemd-resolve
tcp        0      0 localhost:35685         0.0.0.0:*               LISTEN      672/containerd
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      649/cupsd
```

ODIN ID:
969328461

2. I found the following mapping for the 'domain' port number:
   domain 53/tcp # Domain Name Server

   And for ipp:
   ipp 631/tcp # Internet Printing Protocol

   The 35685 seems to be providing a container service/utility, based on the name containerd and a quick google.

3. This is a screenshot of the netstat command on the linux server (ada):

```
mhueck2@ada:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 ada.cs.pdx.edu:56078    tanto.cs.pdx:postgresql ESTABLISHED
tcp        0    244 ada.cs.pdx.edu:ssh      73.180.41.138:64263     ESTABLISHED
tcp        0     68 ada.cs.pdx.edu:ssh      76.115.97.233:56990     ESTABLISHED
tcp        0      0 localhost.localdo:40921 localhost.localdo:50140 ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      10.200.138.236:52301    ESTABLISHED
tcp        1      0 ada.cs.pdx.edu:39144    silverfish.cat.pdx.:ipp CLOSE_WAIT
tcp        0      0 ada.cs.pdx.edu:52816    haopenldap.cat.pdx:ldap TIME_WAIT
tcp        0      0 ada.cs.pdx.edu:ssh      used-for-VPN-pack:61167 ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      192.56.44.5:20172       ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      c-24-21-100-196.h:62636 ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      50.53.244.180:55936     ESTABLISHED
tcp        0      0 localhost.localdo:54100 localhost.localdom:6016 TIME_WAIT
tcp        0      0 ada.cs.pdx.edu:ssh      174.127.211.16:54764    ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      10.200.254.244:49246    ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      50.53.244.180:56089     ESTABLISHED
tcp        0      0 localhost.localdo:50140 localhost.localdo:40921 ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      97-115-173-83.ptl:52731 ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      c-24-21-171-224.h:53744 ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      97-120-184-173.ptl:5043 ESTABLISHED
tcp        0      0 localhost.localdo:39591 localhost.localdo:43484 ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      24.22.99.209:56433      ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      c-73-25-157-182.h:62875 ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      50.38.99.11:54897       ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      174.127.211.16:54734    ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      10.200.112.170:61961    ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:ssh      c-24-20-42-159.hs:61964 ESTABLISHED
tcp        0      0 ada.cs.pdx.edu:52800    haopenldap.cat.pdx:ldap TIME_WAIT
tcp        0      0 ada.cs.pdx.edu:ssh      c-73-164-244-126.:50566 ESTABLISHED
```

ODIN ID:
969328461

It appears that the linux server provides ssh for remote access, based on the local addresses column.

4. This is a screenshot of the lsof command with the options comparable to netstat:

```
mhueck2@mhueck2-VirtualBox:~$ sudo lsof -i4 -iTCP -sTCP:LISTEN
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r 515 systemd-resolve   13u  IPv4  20872      0t0  TCP localhost:domain (LISTEN)
cupsd     649            root    7u  IPv4  25194      0t0  TCP localhost:ipp (LISTEN)
container 672            root   10u  IPv4  26329      0t0  TCP localhost:35685 (LISTEN)
mhueck2@mhueck2-VirtualBox:~$
```

ODIN ID:
969328461

5. The version of SSH is OpenSSH 8.9.

```
mhueck2@mhueck2-VirtualBox:~$ nc -v  linux.cs.pdx.edu 22
Connection to linux.cs.pdx.edu 22 port [tcp/ssh] succeeded!
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3
```

ODIN ID:
969328461

6. Here is a screenshot of the measured bandwidth between the various VMs (US West vs US East, Australia, and Western Europe):

```
Last login: Sat Oct  8 00:58:13 2022 from 35.235.241.65
mhueck2@instance-1:~$ iperf -c 34.85.151.189 -p 80
------------------------------------------------------------
Client connecting to 34.85.151.189, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 10.138.0.6 port 43604 connected with 34.85.151.189 port 80
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec   344 MBytes   288 Mbits/sec
mhueck2@instance-1:~$ iperf -c 34.126.198.98 -p 80
------------------------------------------------------------
Client connecting to 34.126.198.98, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 10.138.0.6 port 43620 connected with 34.126.198.98 port 80
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec   113 MBytes  94.1 Mbits/sec
mhueck2@instance-1:~$ iperf -c 34.65.133.235 -p 80
------------------------------------------------------------
Client connecting to 34.65.133.235, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 10.138.0.6 port 52776 connected with 34.65.133.235 port 80
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec   125 MBytes   104 Mbits/sec
```

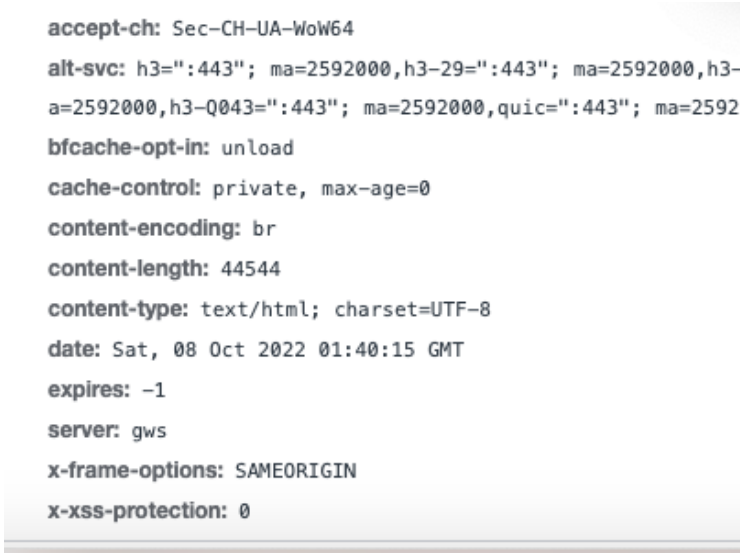
ODIN ID:
969328461

Because we are using TCP, the difference in bandwidth between the VMs can be explained by the client having to wait for a response from the server to ensure the connection was made successfully. Because Europe and Australia are much further than the Eastern US, the transfer takes longer.

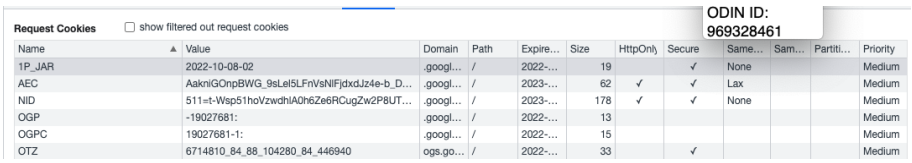
7.

- What is the URL being requested?
  - **Request URL:** https://www.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?
    - ‘www.google.com’, and ‘Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36’
- What is the HTTP status code in the response and what does it mean?
    - 200, which means the request has succeeded
- Look up the status code. Show the associated HTTP response header that is sent in conjunction with this status code for the request.



- What is the URL being requested? Is it using HTTP or HTTPS?
    - https://adservice.google.com/adsid/google/ui , https
- 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?
    - 204 no content, it means a request has succeeded but the client doesn’t need to navigate away from the page.
- Show the associated HTTP response header that is sent in conjunction with this status code for the request.
    - 

- What is the URL being requested? Is it using HTTP or HTTPS? https://ogs.google.com/widget/app/so?origin=https://www.google.com&cn=app&pid=1&spid=538&hl=en, https
- What is the HTTP status code in the response? 200
- Look for an alt-svc: HTTP response header. Does the server believe the client can use HTTP3/QUIC?
    - quic=":443"; ma=2592000- I believe this means the client can use QUIC, using port 443. It is listed as the last of the alternative services so it is not the most preferable, but it is usable.
- 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?
    - 

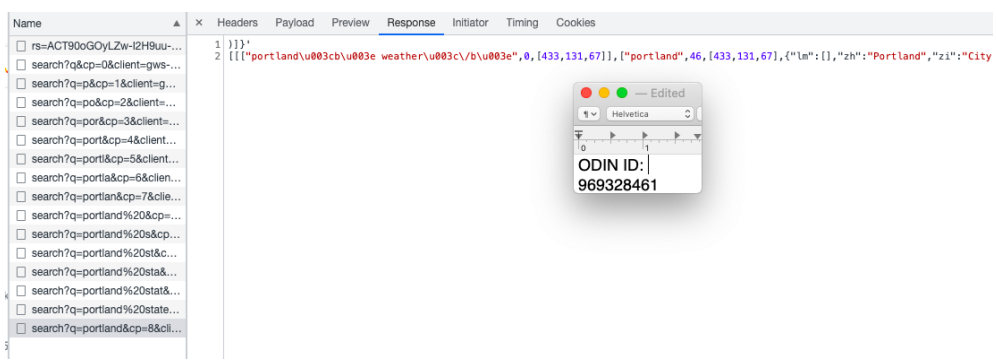
Request Cookies ☐ show filtered out request cookies

ODIN ID: 969328461

Name	Value	Domain	Path	Expire...	Size	HttpOnly	Secure	Same...	Sam...	Partiti...	Priority
1P_JAR	2022-10-08-02	.googl...	/	2022-...	19		✓	None			Medium
AEC	AakniGOnpBWG_9sLel5LFnVsNlFjdxdJz4e-b_D...	.googl...	/	2023-...	62	✓	✓	Lax			Medium
NID	511=t-Wsp51hoVzwdhlA0h6Ze6RCugZw2P8UT...	.googl...	/	2023-...	178	✓	✓	None			Medium
OGP	-19027681:	.googl...	/	2022-...	13						Medium
OGPC	19027681-1:	.googl...	/	2022-...	15						Medium
OTZ	6714810_84_88_104280_84_446940	ogs.go...	/	2022-...	33		✓				Medium

    - 1P_JAR and NID are set without Samesite restrictions in place. This means that the cookies for the domain google.com match the current website (google.com).

This is the response from the request of 'portland state' in the google search bar. The far right of the screenshot shows 'city' which comes up in the search dropdown as 'city in oregon'.



2.2

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?

    The dig results show that www.pdx.edu hosts its own address, and that the mail services are run by google mail servers: aspmx.l.google.com (and alternates).

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

```
mhueck2@ada:~$ dig mashimaro.cs.pdx.edu -t "NS" +tcp

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> mashimaro.cs.pdx.edu -t NS +tcp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51756
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 16a0b13283f21b4b010000006341b9508c1c4915725ab50b (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. 20221003

;; Query time: 3 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (TCP)
;; WHEN: Sat Oct 08 10:54:24 PDT 2022
;; MSG SIZE  rcvd: 147
```

— Edited

Helvetica

ODIN ID:
969328461

```
mhueck2@ada:~$ dig walt.ee.pdx.edu -t "A" +tcp

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> walt.ee.pdx.edu -t A +tcp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18725
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: bb3036602233e35c010000006341b965d542a38ff476a745 (good)
;; QUESTION SECTION:
;walt.ee.pdx.edu.               IN      A

;; ANSWER SECTION:
walt.ee.pdx.edu.        4512    IN      A       131.252.208.38

;; Query time: 3 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (TCP)
;; WHEN: Sat Oct 08 10:54:45 PDT 2022
;; MSG SIZE  rcvd: 88
```

— Edit

Helvetica

ODIN ID:
969328461

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

   This is the A record for the authoritative server that hosts thefengs.com: 216.239.36.106

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

   The request uses an HTTP header such as GET

5.First I used dig with no arguments to find the IP address for the F root server.

```
mhueck2@ada:~$ dig

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5725
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9cce6eac4c107d6e010000006341be39d275ab10fb179b41 (good)
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       123874  IN      NS      k.root-servers.net.
.                       123874  IN      NS      e.root-servers.net.
.                       123874  IN      NS      c.root-servers.net.
.                       123874  IN      NS      a.root-servers.net.
.                       123874  IN      NS      d.root-servers.net.
.                       123874  IN      NS      i.root-servers.net.
.                       123874  IN      NS      f.root-servers.net.
.                       123874  IN      NS      b.root-servers.net.
.                       123874  IN      NS      h.root-servers.net.
.                       123874  IN      NS      m.root-servers.net.
.                       123874  IN      NS      g.root-servers.net.
.                       123874  IN      NS      j.root-servers.net.
.                       123874  IN      NS      l.root-servers.net.
```

ODIN ID:
969328461

Then I used dig at that IP address (192.5.5.241) to find the edu servers:

```
mhueck2@ada:~$ dig www.cs.pdx.edu  @192.5.5.241 -t "NS" +tcp +norecurse

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> www.cs.pdx.edu @192.5.5.241 -t NS +tcp +norecurse
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20780
;; 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      NS

;; 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.
```

ODIN ID:
969328461

I used the F edu-server IP address to find the pdx.edu domain:

```
mhueck2@ada:~$ dig www.cs.pdx.edu  @192.35.51.30 -t "NS" +tcp +norecurse

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> www.cs.pdx.edu @192.35.51.30 -t NS +tcp +norecurse
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61807
;; 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      NS

;; 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: Sat Oct 08 12:15:44 PDT 2022
;; MSG SIZE  rcvd: 164
```

ODIN ID:
969328461

Which leads to the pdx.edu domain where cs.pdx.edu is hosted.

6. Here are the results from the reverse DNS lookup:

```
mhueck2@mhueck2-VirtualBox:~$ X=`dig espn.go.com -4 | egrep 99. | awk '
{print $5}'`
mhueck2@mhueck2-VirtualBox:~$ echo $X
99.84.66.98 99.84.66.55 99.84.66.108 99.84.66.17
mhueck2@mhueck2-VirtualBox:~$ for i in `echo $X`; do dig -x $i | egrep
net | awk '{print $5}'; done
server-99-84-66-98.hio50.r.cloudfront.net.
server-99-84-66-55.hio50.r.cloudfront.net.
server-99-84-66-108.hio50.r.cloudfront.net.
server-99-84-66-17.hio50.r.cloudfront.net.
mhueck2@mhueck2-VirtualBox:~$
```

ODIN ID:
969328461

Here is a screenshot of all of the car manufacturer domains on the 131.252.220.0/24 subnet:

```
mhueck2@ada:~$ cat 220hosts.txt --number | head -189 | tail +160
   160  acura.cs.pdx.edu.
   161  astonmartin.cs.pdx.edu.
   162  audi.cs.pdx.edu.
   163  bentley.cs.pdx.edu.
   164  bmw.cs.pdx.edu.
   165  cadillac.cs.pdx.edu.
   166  ferrari.cs.pdx.edu.
   167  fiat.cs.pdx.edu.
   168  ford.cs.pdx.edu.
   169  honda.cs.pdx.edu.
   170  hummer.cs.pdx.edu.
   171  jaguar.cs.pdx.edu.
   172  jeep.cs.pdx.edu.
   173  lamborghini.cs.pdx.edu.
   174  landrover.cs.pdx.edu.
   175  lexus.cs.pdx.edu.
   176  lotus.cs.pdx.edu.
   177  maserati.cs.pdx.edu.
   178  mazda.cs.pdx.edu.
   179  mclaren.cs.pdx.edu.
   180  mercedes.cs.pdx.edu.
   181  nissan.cs.pdx.edu.
   182  panoz.cs.pdx.edu.
   183  porsche.cs.pdx.edu.
   184  subaru.cs.pdx.edu.
   185  toyota.cs.pdx.edu.
   186  tvr.cs.pdx.edu.
   187  ultima.cs.pdx.edu.
   188  volvo.cs.pdx.edu.
   189  vw.cs.pdx.edu.
```

— Edited

Helvetica

ODIN ID:
969328461

8. Ipinfo.io returns pdx.edu (portland state university), and DB-IP returns Portland state university (for 131.252.208.53).

Ipinfo.io returns Virginia Polytechnic Institute and State Univ. (vt.edu) and DB-IP returns Virginia Polytechnic Institute and State Univ.

9. Using dig to resolve the first PSU server, I got 142.250.69.196 and www.google.com.
For the Virginia polytechnic, I got the same result.

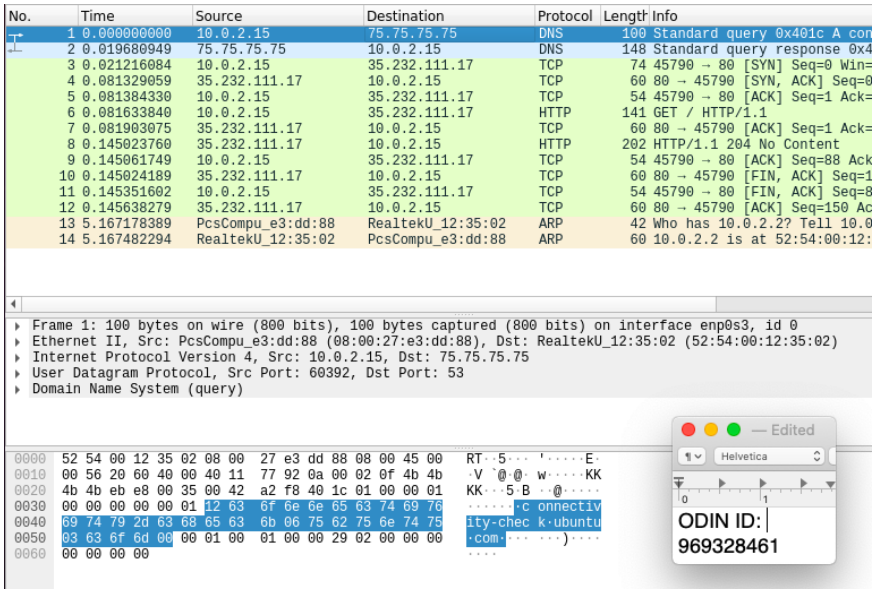
10. Both ipinfo.io and DB-IP return a google server in Seattle, Washington. Approximately 2700 miles between Virginia and Seattle and approx 170 between Portland and Seattle.

11. Using traceroute on 142.250.69.196, the last address is sea30s08-in-f4.1e100.net, which seems like it could be a Seattle address (based on the 'sea'). The PSU IP address shows rdns.cat.pdx.edu, which of course is a PSU address in Portland. Finally, the Virginia address ends with jeru.cns.vt.edu, which is clearly the vt or Virginia tech domain. So, besides the ambiguous seattle address, the IP locator is accurate in this case.

12. Changing the default DNS server to 1.1.1.1 and performing a rDNS lookup yields:
1.1.1.1.in-addr.arpa. 606 IN PTR one.one.one.one
so seemingly the server is also called one.one.one.one.

13. Here is the packet analysis from wireshark: the website oregonctf.org is resolved to an IP address through a DNS server (75.75.75.75). Then there is a TCP handshake to establish a connection between the host and the oregonctf website, and the server responds to a GET request from the host. Finally, the router (at my house) performs ARP to find my device, and connects to it.

One DNS request is made, and it looks like 5 TCP connections are simultaneously made (from 10.0.2.15 outbound). There is one HTTP GET request made.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	75.75.75.75	DNS	100	Standard query 0x401c A con
2	0.019680949	75.75.75.75	10.0.2.15	DNS	148	Standard query response 0x4
3	0.021216084	10.0.2.15	35.232.111.17	TCP	74	45790 → 80 [SYN] Seq=0 Win=
4	0.081329059	35.232.111.17	10.0.2.15	TCP	60	80 → 45790 [SYN, ACK] Seq=0
5	0.081384330	10.0.2.15	35.232.111.17	TCP	54	45790 → 80 [ACK] Seq=1 Ack=
6	0.081633840	10.0.2.15	35.232.111.17	HTTP	141	GET / HTTP/1.1
7	0.081903075	35.232.111.17	10.0.2.15	TCP	60	80 → 45790 [ACK] Seq=1 Ack=
8	0.145023760	35.232.111.17	10.0.2.15	HTTP	202	HTTP/1.1 204 No Content
9	0.145061749	10.0.2.15	35.232.111.17	TCP	54	45790 → 80 [ACK] Seq=88 Ack
10	0.145024189	35.232.111.17	10.0.2.15	TCP	60	80 → 45790 [FIN, ACK] Seq=1
11	0.145351602	10.0.2.15	35.232.111.17	TCP	54	45790 → 80 [FIN, ACK] Seq=8
12	0.145638279	35.232.111.17	10.0.2.15	TCP	60	80 → 45790 [ACK] Seq=150 Ac
13	5.167178389	PcsCompu_e3:dd:88	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0
14	5.167482294	RealtekU_12:35:02	PcsCompu_e3:dd:88	ARP	60	10.0.2.2 is at 52:54:00:12:

```
Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_e3:dd:88 (08:00:27:e3:dd:88), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 60392, Dst Port: 53
Domain Name System (query)
```

```
0000  52 54 00 12 35 02 08 00  27 e3 dd 88 08 00 45 00   RT··5··· '·····E·
0010  00 56 20 60 40 00 40 11  77 92 0a 00 02 0f 4b 4b   ·V `@·@· w·····KK
0020  4b 4b eb e8 00 35 00 42  a2 f8 40 1c 01 00 00 01   KK···5·B ··@·····
0030  00 00 00 00 00 01 12 63  6f 6e 6e 65 63 74 69 76   ·····c onnectiv
0040  69 74 79 2d 63 68 65 63  6b 06 75 62 75 6e 74 75   ity-chec k·ubuntu
0050  03 63 6f 6d 00 00 01 00  01 00 00 29 02 00 00 00   ·com····· ···)····
0060  00 00 00 00                                        ····
```

— Edited

Helvetica

ODIN ID:
969328461