

TABLE OF CONTENTS

1. TCP #1: Sockets.....	2
1) Service Contactable from Any Interface on the Machine:.....	3
2. -.....	3
4. -.....	4
5. HTTP #3: Requests.....	5
6. -.....	8
1. DNS reconnaissance #1 (dig).....	9
2. Iterative DNS lookups.....	12
3. Reverse DNS lookups.....	13
4. Host enumeration.....	14
5. Geographic DNS #2.....	15
6. Wireshark Lab #3.....	20
8. Network Recap Lab #4.....	21
9. Collect trace.....	21
10. Analyze trace.....	21

1. TCP #1: Sockets

- Take a screenshot of the prompt and the command that ChatGPT generates

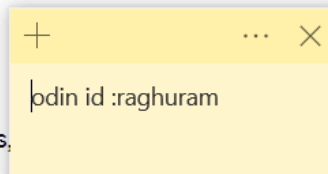
You

find a single command and its command-line flags that, when executed, lists all TCP sockets in a LISTEN state on an IPv4 address, showing the program that is using it



ChatGPT

To list all TCP sockets in a LISTEN state on an IPv4 address, you can use the following command with specific flags in a Unix-like operating system (like Linux):



bash

Copy code

```
sudo ss -tlnp4
```

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

```
raghuran@course-vm:~$ sudo ss -tlnp4
State  Recv-Q  Send-Q  Local Address:Port  Peer Address:Port  Process
LISTEN  0        4096    127.0.0.1:38091      0.0.0.0:*          users: (("containerd",pid=477,fd=8))
LISTEN  0        128     0.0.0.0:22           0.0.0.0:*          users: (("sshd",pid=807,fd=3))
LISTEN  0        4096    127.0.0.53%lo:53     0.0.0.0:*          users: (("systemd-resolve",pid=390,fd=14))
```

- List a service that can be contacted from any interface on the machine. List a service that can only be contacted by local processes.

1) Service Contactable from Any Interface on the Machine:

SSH (Secure Shell)

- IP Address: 0.0.0.0

- Port: 22

2) Service Contactable Only by Local Processes:

System DNS Resolver (systemd-resolve)

- IP Address: 127.0.0.53
- Port: 53
- Run the command again, but do not use `sudo` as this is a machine managed by CAT. Include a screenshot of the output.

```
raghuram@ada:~$ ss -tlnp4
```

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
LISTEN	0	1024	127.0.0.1:36215	0.0.0.0:*	
LISTEN	0	1024	127.0.0.1:36205	0.0.0.0:*	
LISTEN	0	1024	127.0.0.1:32813	0.0.0.0:*	
LISTEN	0	1024	127.0.0.1:33223	0.0.0.0:*	
LISTEN	0	128	0.0.0.0:22	0.0.0.0:*	
LISTEN	0	1024	127.0.0.1:40295	0.0.0.0:*	
LISTEN	0	1024	127.0.0.1:40621	0.0.0.0:*	
LISTEN	0	1024	127.0.0.1:40619	0.0.0.0:*	
LISTEN	0	1024	127.0.0.1:44817	0.0.0.0:*	
LISTEN	0	1024	127.0.0.1:42127	0.0.0.0:*	
LISTEN	0	1024	127.0.0.1:45471	0.0.0.0:*	
LISTEN	0	1024	127.0.0.1:45387	0.0.0.0:*	
LISTEN	0	511	127.0.0.1:45431	0.0.0.0:*	
LISTEN	0	1024	127.0.0.1:45935	0.0.0.0:*	
LISTEN	0	511	127.0.0.1:46749	0.0.0.0:*	
LISTEN	0	4096	127.0.0.53:53	0.0.0.0:*	
LISTEN	0	100	127.0.0.1:25	0.0.0.0:*	
LISTEN	0	128	127.0.0.1:631	0.0.0.0:*	
LISTEN	0	128	127.0.0.1:6104	0.0.0.0:*	
LISTEN	0	128	127.0.0.1:6103	0.0.0.0:*	
LISTEN	0	128	127.0.0.1:6102	0.0.0.0:*	
LISTEN	0	128	127.0.0.1:6101	0.0.0.0:*	
LISTEN	0	128	127.0.0.1:6100	0.0.0.0:*	
LISTEN	0	128	127.0.0.1:6115	0.0.0.0:*	

:

- List the services that this machine provides for external access

Ans : SSH (Secure Shell) Local Address:Port: 0.0.0.0:22

2. -

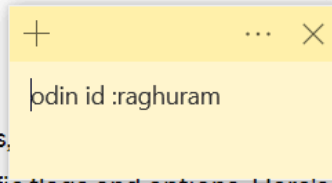
- Take a screenshot of the prompt and the command that ChatGPT generates

You

find a single `lsof` command and its command-line flags that, when executed, lists all TCP sockets in a LISTEN state on an IPv4 address, showing the program that is using it

ChatGPT

To list all TCP sockets in a LISTEN state on an IPv4 address, you can use the `lsof` command with specific flags and options. Here's a suitable command:



```
bash Copy code  
  
lsof -iTCP -sTCP:LISTEN -nP -P
```

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

```
raghurar@course-vm:~$ sudo lsof -iTCP -sTCP:LISTEN -nP -P  
COMMAND  PID    USER      FD  TYPE DEVICE SIZE/OFF NODE NAME  
systemd-r 390  systemd-resolve 14u IPv4 17451      0t0  TCP 127.0.0.53:53 (LISTEN)  
container 477    root       8u  IPv4 18424      0t0  TCP 127.0.0.1:38091 (LISTEN)  
xrdp-sesm 525    root       7u  IPv6 18027      0t0  TCP [::1]:3350 (LISTEN)  
xrdp      656    xrdp      11u IPv6 18180      0t0  TCP *:3389 (LISTEN)  
sshd      807    root       3u  IPv4 19007      0t0  TCP *:22 (LISTEN)  
sshd      807    root       4u  IPv6 19009      0t0  TCP *:22 (LISTEN)  
raghurar@course-vm:~$
```

4. -

- 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.

```

raghuram@vm-us-west1-b:~$ iperf -c 10.152.0.2 -p 80
-----
Client connecting to 10.152.0.2, TCP port 80
TCP window size: 85.0 KByte (default)
-----
[ 1] local 10.138.0.11 port 37786 connected with 10.152.0.2 port 80
[ ID] Interval      Transfer    Bandwidth
[ 1] 0.0000-10.1636 sec  189 MBytes  156 Mbits/sec
raghuram@vm-us-west1-b:~$ iperf -c 10.132.0.2 -p 80
-----
Client connecting to 10.132.0.2, TCP port 80
TCP window size: 85.0 KByte (default)
-----
[ 1] local 10.138.0.11 port 55338 connected with 10.132.0.2 port 80
[ ID] Interval      Transfer    Bandwidth
[ 1] 0.0000-10.2053 sec  194 MBytes  159 Mbits/sec
raghuram@vm-us-west1-b:~$ iperf -c 10.142.0.2 -p 80
-----
Client connecting to 10.142.0.2, TCP port 80
TCP window size: 85.0 KByte (default)
-----
[ 1] local 10.138.0.11 port 46802 connected with 10.142.0.2 port 80
[ ID] Interval      Transfer    Bandwidth
[ 1] 0.0000-10.1015 sec  433 MBytes  359 Mbits/sec

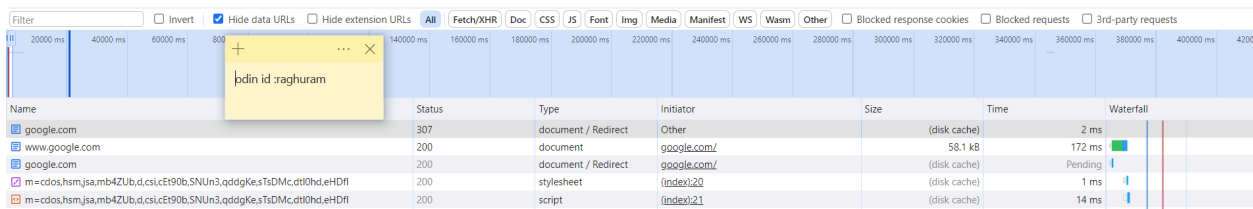
```

The difference is

- The physical proximity of the VMs to each other.
- The quality and capacity of the network connections between the VMs.

5. HTTP #3: Requests

- Take a screenshot of the initial requests for your lab notebook.



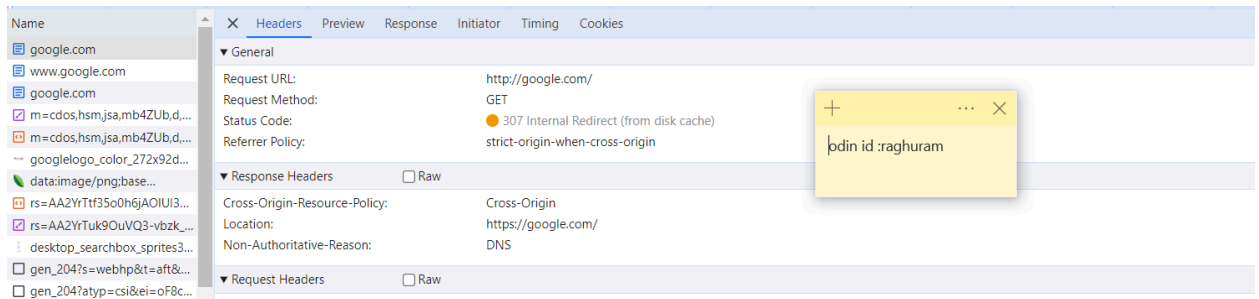
- What is the URL being requested?

http://google.com/

- Explain the HTTP status code that is returned and what the code indicates

307 Internal Redirect (from disk cache) which means temporary redirection that won't modify the original request method or body.

- Take a screenshot indicating the version of the HTTP protocol that is used for each request. (Hint: look at the response status line and **alt-svc**: HTTP response headers indicating HTTP/2 or HTTP/3).



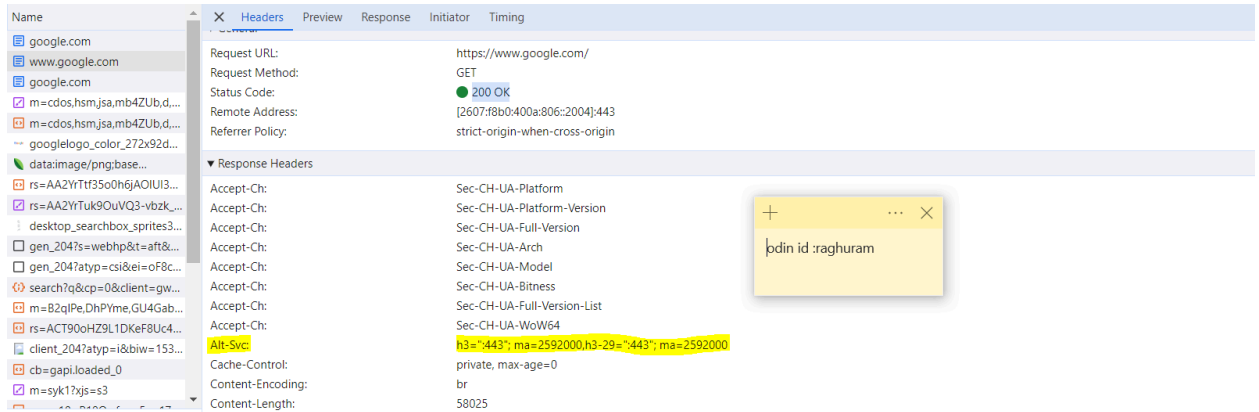
- What is the URL being requested?

https://www.google.com/

- Explain the HTTP status code that is returned and what the code indicates

200 OK code means that **the request was successful**, but the meaning of success depends on the request method

- Take a screenshot indicating the version of the HTTP protocol that is used for each request. (Hint: look at the response status line and **alt-svc**: HTTP response headers indicating HTTP/2 or HTTP/3).



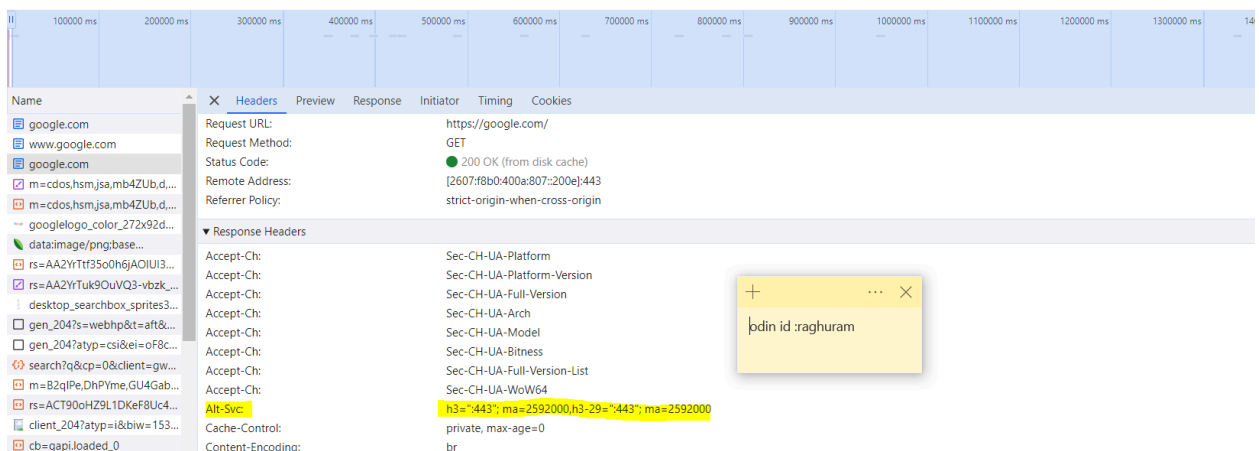
- What is the URL being requested?

`https://google.com/`

- Explain the HTTP status code that is returned and what the code indicates

200 OK (from disk cache) that the response was indeed served from cache. Browser will serve this response from cache until the response expires

- Take a screenshot indicating the version of the HTTP protocol that is used for each request. (Hint: look at the response status line and `alt-svc`: HTTP response headers indicating HTTP/2 or HTTP/3).

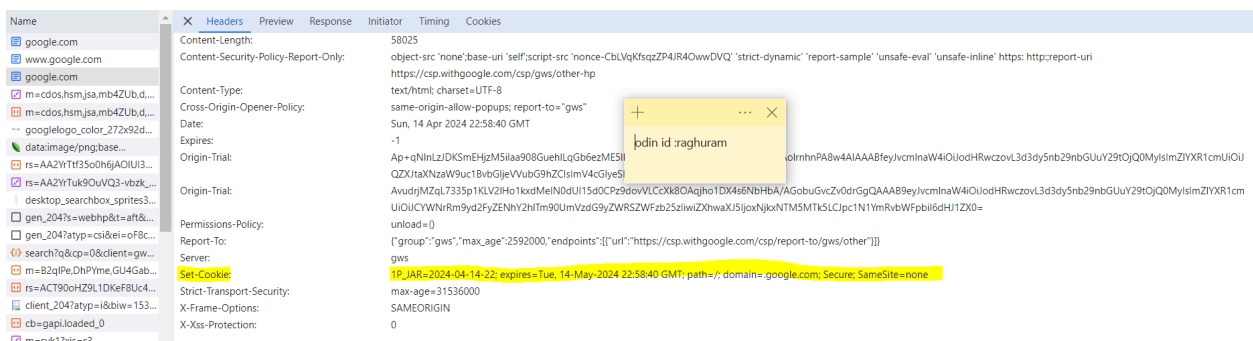


- Show the URLs the browser is redirected to via this header.

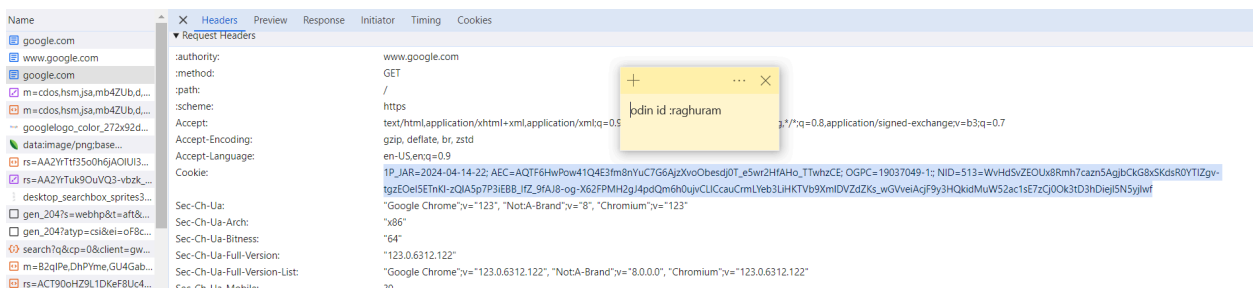
<https://www.google.com/>

<https://google.com/>

- Take a screenshot of when cookies are set via **Set-Cookie:**

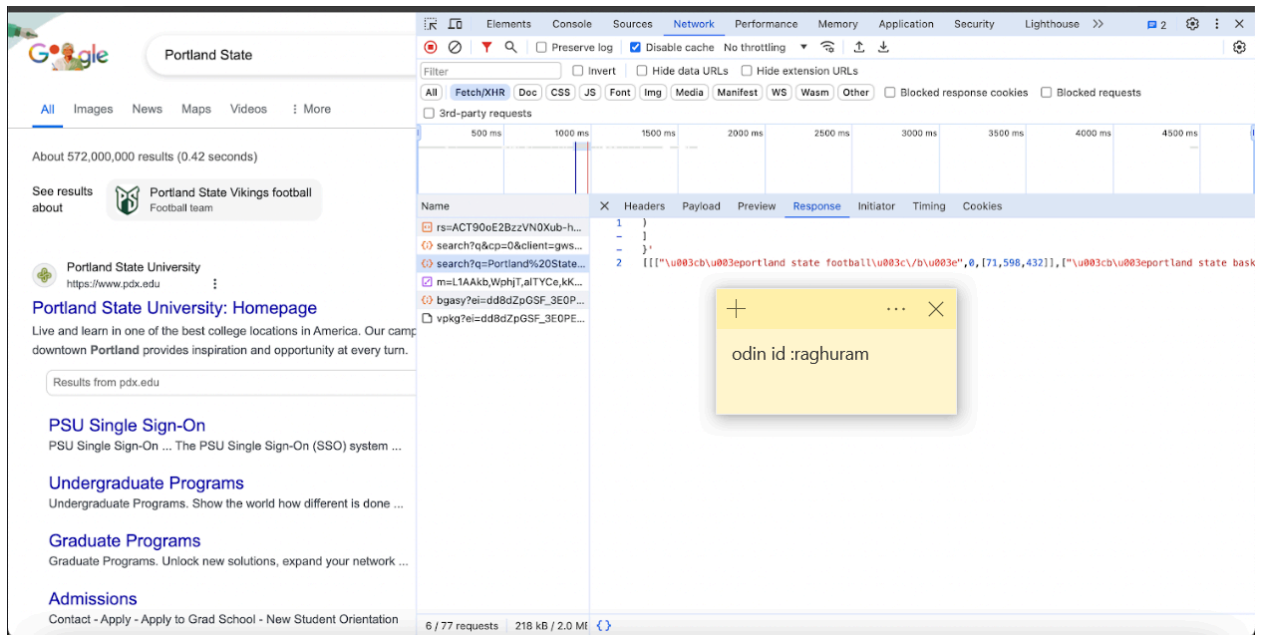


- Take a screenshot of when cookies are attached via **Cookie:**



6. -

- 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"



02.2: DNS, Recap

1. DNS reconnaissance #1 (dig)

- Take a screenshot of the prompt and the dig command produced.

```

raghuram@ada:~$ dig @131.252.208.53 www.pdx.edu A +tcp

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> @131.252.208.53 www.pdx.edu A +tcp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8248
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d1e2c429f9a78f0301000000661c756823a0b4b8f69e7650 (good)
;; QUESTION SECTION:
;www.pdx.edu.                IN      A

;; ANSWER SECTION:
www.pdx.edu.                 60      IN      A      18.161.6.84
www.pdx.edu.                 60      IN      A      18.161.6.96
www.pdx.edu.                 60      IN      A      18.161.6.112
www.pdx.edu.                 60      IN      A      18.161.6.120

;; Query time: 75 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (TCP)
;; WHEN: Sun Apr 14 17:31:36 PDT 2024
;; MSG SIZE rcvd: 132

```

- Take a screenshot of the records returned for your lab notebook.

```

raghuram@ada:~$ dig @131.252.208.53 pdx.edu MX +tcp

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> @131.252.208.53 pdx.edu MX +tcp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12869
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8f13d65d8c0cfe7e01000000661c85327a1bfe6a66fbf42b (good)
;; QUESTION SECTION:
;pdx.edu.                                IN      MX

;; ANSWER SECTION:
pdx.edu.      76866      IN      MX      10 alt3.aspmx.l.google.com.
pdx.edu.      76866      IN      MX      10 alt4.aspmx.l.google.com.
pdx.edu.      76866      IN      MX      1 aspmx.l.google.com.
pdx.edu.      76866      IN      MX      5 alt1.aspmx.l.google.com.
pdx.edu.      76866      IN      MX      5 alt2.aspmx.l.google.com.

;; ADDITIONAL SECTION:
aspmx.l.google.com. 233      IN      A      142.250.107.27

;; Query time: 3 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (TCP)
;; WHEN: Sun Apr 14 18:38:58 PDT 2024
;; MSG SIZE rcvd: 198

```

- What cloud provider hosts the web site for www.pdx.edu?

Amazon Web services (AWS)

- What cloud provider handles mail for pdx.edu?

Google's mail servers like alt3.aspmx.l.google.com

- Take a screenshot of the results for both records for your lab notebook.

```

raghuram@ada:~$ dig mashimaro.cs.pdx.edu NS

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> mashimaro.cs.pdx.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46577
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
cs.pdx.edu.      300      IN      SOA      walt.ee.pdx.edu. support.cat.pdx.edu. 2024040800 600 300 1209600 300

;; Query time: 7 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Apr 14 19:01:09 PDT 2024
;; MSG SIZE rcvd: 105

```

```
raghuram@ada:~$ dig mashimaro.cs.pdx.edu A

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> mashimaro.cs.pdx.edu A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27850
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
mashimaro.cs.pdx.edu.      2224    IN      A      131.252.220.66

;; Query time: 0 msec
```

2. Iterative DNS lookups

- List all of the iterative dig commands performed for the lookup

dig

dig f.root-servers.net console.cloud.google.com NS +tcp

dig a.root-servers.net console.cloud.google.com. A +tcp

- Take a screenshot of the results of the final query for your lab notebook.

```

raghuram@course-vm:~$ dig a.root-servers.net console.cloud.google.com. A +tcp

; <<> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<> a.root-servers.net console.cloud.google.com. A +tcp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33675
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;a.root-servers.net.          IN      A

;; ANSWER SECTION:
a.root-servers.net.          259200  IN      A      198.41.0.4

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Apr 15 06:04:35 UTC 2024
;; MSG SIZE rcvd: 63

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26211
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; 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 142.250.107.101
www3.l.google.com. 300 IN A 142.250.107.139
www3.l.google.com. 300 IN A 142.250.107.102
www3.l.google.com. 300 IN A 142.250.107.113
www3.l.google.com. 300 IN A 142.250.107.138
www3.l.google.com. 300 IN A 142.250.107.100

```

3. Reverse DNS lookups

- Take a screenshot of the prompt and the command produced

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

| ChatGPT

To produce a list of all IPv4 addresses that `espn.go.com` points to using `dig`, `egrep`, and `awk`, you can use the following single command line:

```
bash Copy code  
  
dig espn.go.com A +short | egrep -o "([0-9]{1,3}[\.]){3}[0-9]{1,3}" | awk '{print $1}'
```

Here's what each part of this pipeline does:

1. `dig espn.go.com A +short`: Performs a DNS lookup for `espn.go.com`, which are the IPv4 addresses. The `+short` option simplifies the output to just the

- Take a screenshot of its results for your lab notebook

```
raghuram@course-vm:~$ dig espn.go.com A +short | egrep -o "([0-9]{1,3}[\.]){3}[0-9]{1,3}" | awk '{print $1}'  
18.65.229.14  
18.65.229.26  
18.65.229.61  
18.65.229.93
```

- Take a screenshot of the command and its results for your lab notebook

```
raghuram@course-vm:~$ for ip in $(dig espn.go.com A +short | egrep -o "([0-9]{1,3}[\.]){3}[0-9]{1,3}"); do  
  dig -x $ip +short | awk '{print $1}'  
done  
server-18-65-229-26.sea73.r.cloudfront.net.  
server-18-65-229-14.sea73.r.cloudfront.net.  
server-18-65-229-93.sea73.r.cloudfront.net.  
server-18-65-229-61.sea73.r.cloudfront.net.
```

4. Host enumeration

- Take a screenshot of the results in your lab notebook










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

5. Geographic DNS #2










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

131.252.208.53





















































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

 IP ADDRESS: 131.252.208.53	 ISP: Not available
 COUNTRY: United States 	 ORGANIZATION: AS6366 Portland State University
 REGION: Oregon	 LATITUDE: 45.5234
 CITY: Portland	 LONGITUDE: -122.6762

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

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

POPULAR ARTICLES

-  Find IP address of a network
-  Find IP addresses of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network










 **Shop new & noteworthy finds**












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

198.82.247.66



























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

 IP ADDRESS: 198.82.247.66	 ISP: Not available
 COUNTRY: United States 	 ORGANIZATION: AS1312 Virginia Polytechnic Institute and State Univ.
 REGION: Virginia	 LATITUDE: 37.2296
 CITY: Blacksburg	 LONGITUDE: -80.4139

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

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

POPULAR ARTICLES

-  Find IP address of a network
-  Find IP addresses of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network
-  Find IP address of a private network

 **Tongyu AX1800 Dual**
\$70.99 ✓prime

 **Tongyu AX1800 Dual**
\$70.99 ✓prime

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

For 131.252.208.208.53

```
raghuram@ada:~$ dig @131.252.208.53 www.google.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> @131.252.208.53 www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57207
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d6e9e54353cceb001000000661cd59bd9ba9135e28e60b5 (good)
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.                 50      IN      A      142.250.217.100

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Mon Apr 15 00:22:03 PDT 2024
;; MSG SIZE rcvd: 87
```

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

For 198.82.247.66.

```

raghuram@ada:~$ dig @198.82.247.66 www.google.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> @198.82.247.66 www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53283
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3611a04105e24998fd23e157661cd5f9db45981359284997 (good)
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.                145     IN      A      142.251.16.99
www.google.com.                145     IN      A      142.251.16.103
www.google.com.                145     IN      A      142.251.16.147
www.google.com.                145     IN      A      142.251.16.104
www.google.com.                145     IN      A      142.251.16.105
www.google.com.                145     IN      A      142.251.16.106










;; Query time: 63 msec
;; SERVER: 198.82.247.66#53(198.82.247.66) (UDP)
;; WHEN: Mon Apr 15 00:23:37 PDT 2024
;; MSG SIZE rcvd: 167



```

- What are the geographic coordinates of each DNS server and the IP address it resolves for www.google.com?

For ip address 142.250.217.100

Geolocation data from IP2Location (Product: DB6, 2024-4-1)

 IP ADDRESS: 142.250.217.100	 ISP: Google LLC
 COUNTRY: United States 	 ORGANIZATION: Not available
 REGION: California	 LATITUDE: 37.4060
 CITY: Mountain View	 LONGITUDE: -122.0785

 is my website down?
 Subnet Calculator

+

...

×

ipdin id:raghuram

work printer?

private network

How to wire my 45 cable?










What is the difference between public and private IP address?

What is static and dynamic IP addresses?

- What are the geographic coordinates of each DNS server and the IP address it resolves for www.google.com?

For ip address 142.251.16.99

Geolocation data from IP2Location (Product: DB6, 2024-4-1)

 IP ADDRESS: 142.251.16.99	 ISP: Google LLC
 COUNTRY: United States 	 ORGANIZATION: Not available
 REGION: California	 LATITUDE: 37.4060
 CITY: Mountain View	 LONGITUDE: -122.0785

TRY IT FREE

Subscription Req

+ ... X

pdin id :raghuram

Subnet Calculator

- Take a screenshot of the results for your lab notebook.

```
raghuram@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) 0.602 ms 0.453 ms 0.347 ms
```

```
raghuram@ada:~$ traceroute 198.82.247.66
traceroute to 198.82.247.66 (198.82.247.66), 30 hops max, 60 byte packets
 1 glados.cat.pdx.edu (131.252.208.21) 4.428 ms 4.224 ms 4.108 ms
 2 0015-opnsense.cat.pdx.edu (10.208.91.1) 0.114 ms 0.087 ms 0.092 ms
 3 CORE1.net.pdx.edu (131.252.5.142) 1.456 ms 1.372 ms 1.269 ms
 4 131.252.5.213 (131.252.5.213) 0.473 ms 0.366 ms 0.461 ms
 5 e0-28.switch4.pdx1.he.net (216.218.230.89) 27.169 ms * 26.930 ms
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 eqix-ash.vt.edu (206.126.236.139) 57.584 ms 57.484 ms 57.370 ms
11 192.70.187.20 (192.70.187.20) 64.827 ms 64.796 ms 64.573 ms
12 isb-core.xe-7-0-0.0.cns.vt.edu (128.173.0.202) 65.234 ms 65.226 ms 65.347 ms
13 cas-core.lo0.2000.cns.vt.edu (198.82.1.143) 64.686 ms 64.330 ms 64.595 ms
14 jeru.cns.vt.edu (198.82.247.66) 64.456 ms 64.264 ms 64.172 ms
```

```

raghuram@ada:~$ traceroute 142.251.16.99
traceroute to 142.251.16.99 (142.251.16.99), 30 hops max, 60 byte packets
 1 glados.cat.pdx.edu (131.252.208.21)  5.688 ms  5.559 ms  5.438 ms
 2 0015-opnsense.cat.pdx.edu (10.208.91.1)  1.406 ms  1.325 ms  1.232 ms
 3 CORE1.net.pdx.edu (131.252.5.142)  1.865 ms  1.771 ms  1.680 ms
 4 131.252.5.213 (131.252.5.213)  0.807 ms  0.710 ms  0.617 ms
 5 google.nwax.net (198.32.195.34)  3.882 ms  3.955 ms  4.184 ms
 6 108.170.255.175 (108.170.255.175)  5.171 ms  192.178.105.35 (192.178.105.35)  4.270 ms  192.178.105.129 (192.178.105.129)  4.265 ms
 7 108.170.255.196 (108.170.255.196)  4.433 ms  5.328 ms  192.178.105.148 (192.178.105.148)  16.268 ms
 8 * 216.239.50.20 (216.239.50.20)  11.683 ms *
 9 142.250.213.63 (142.250.213.63)  52.507 ms * *
10 192.178.81.226 (192.178.81.226)  67.872 ms  67.750 ms *
11 172.253.51.73 (172.253.51.73)  64.305 ms 142.250.209.59 (142.250.209.59)  66.552 ms 172.253.51.73 (172.253.51.73)  76.949 ms
12 142.251.68.15 (142.251.68.15)  64.899 ms 142.251.227.157 (142.251.227.157)  63.741 ms 64.816 ms
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * bl-in-f99.1e100.net (142.251.16.99)  65.357 ms

```

```

raghuram@ada:~$ traceroute 142.250.217.100
traceroute to 142.250.217.100 (142.250.217.100), 30 hops max, 60 byte packets
 1 glados.cat.pdx.edu (131.252.208.21)  1.244 ms  1.093 ms  0.976 ms
 2 0015-opnsense.cat.pdx.edu (10.208.91.1)  0.200 ms  0.150 ms  0.094 ms
 3 CORE1.net.pdx.edu (131.252.5.142)  8.107 ms  8.038 ms  7.927 ms
 4 131.252.5.213 (131.252.5.213)  0.492 ms  0.399 ms  0.400 ms
 5 google.nwax.net (198.32.195.34)  4.211 ms  4.237 ms  4.226 ms
 6 192.178.105.35 (192.178.105.35)  4.621 ms  4.982 ms 108.170.255.123 (108.170.255.123)  4.848 ms
 7 142.251.55.201 (142.251.55.201)  4.835 ms 142.251.55.203 (142.251.55.203)  4.578 ms 4.752 ms
 8 sea09s30-in-f4.1e100.net (142.250.217.100)  4.300 ms 4.188 ms 4.115 ms

```

6. Wireshark Lab #3

- Take a screenshot of the bytes in the packet dump window as shown below

The screenshot shows the Wireshark interface with a packet capture on interface ens4. The packet list shows a series of ICMP Echo (ping) requests and replies. The packet details pane shows the selected packet (No. 17) with its Ethernet II header, IP header, and ICMP Echo (ping) request details. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
7	56.412229737	10.138.0.10	108.177.98.104	ICMP	98	Echo (ping) request id=0x0001, seq=3/768
8	56.412626156	108.177.98.104	10.138.0.10	ICMP	98	Echo (ping) reply id=0x0001, seq=3/768
9	64.117382999	10.138.0.10	108.177.98.103	ICMP	98	Echo (ping) request id=0x0002, seq=1/256
10	64.118195344	108.177.98.103	10.138.0.10	ICMP	98	Echo (ping) reply id=0x0002, seq=1/256
11	65.119443121	10.138.0.10	108.177.98.103	ICMP	98	Echo (ping) request id=0x0002, seq=2/512
12	65.119828755	108.177.98.103	10.138.0.10	ICMP	98	Echo (ping) reply id=0x0002, seq=2/512
13	66.120653619	10.138.0.10	108.177.98.103	ICMP	98	Echo (ping) request id=0x0002, seq=3/768
14	66.121020705	108.177.98.103	10.138.0.10	ICMP	98	Echo (ping) reply id=0x0002, seq=3/768
15	69.424468404	10.138.0.10	108.177.98.103	ICMP	98	Echo (ping) request id=0x0003, seq=1/256
16	69.424821024	108.177.98.103	10.138.0.10	ICMP	98	Echo (ping) reply id=0x0003, seq=1/256
17	70.441510960	10.138.0.10	108.177.98.103	ICMP	98	Echo (ping) request id=0x0003, seq=2/512
18	70.441883087	108.177.98.103	10.138.0.10	ICMP	98	Echo (ping) reply id=0x0003, seq=2/512
19	71.442654344	10.138.0.10	108.177.98.103	ICMP	98	Echo (ping) request id=0x0003, seq=3/768
20	71.443119624	108.177.98.103	10.138.0.10	ICMP	98	Echo (ping) reply id=0x0003, seq=3/768
21	225.866584574	47.254.241.127	10.138.0.10	ICMP	50	Echo (ping) request id=0x3368, seq=52205
22	225.866633324	10.138.0.10	47.254.241.127	ICMP	50	Echo (ping) reply id=0x3368, seq=52205

Frame 17: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface ens4, id 0
 Ethernet II, Src: 42:01:0a:8a:00:01 (42:01:0a:8a:00:01), Dst: 42:01:0a:8a:00:0a (42:01:0a:8a:00:0a)
 Destination: 42:01:0a:8a:00:0a (42:01:0a:8a:00:0a)
 Address: 42:01:0a:8a:00:0a (42:01:0a:8a:00:0a)
01.... = LG bit: Locally administered address (this is NOT the factory default)
0.... = IG bit: Individual address (unicast)
 Source: 42:01:0a:8a:00:01 (42:01:0a:8a:00:01)
 Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 128.9.29.131, Dst: 10.138.0.10
 Internet Control Message Protocol

- Does the destination MAC address correspond to an interface on the VM, an interface on the default router or an interface on Google's web site?

destination MAC address correspond an interface on the default router

- Does the destination MAC address correspond to an interface on the VM, an interface on the default router or an interface on Google's web site?

destination MAC address correspond to an interface on the VM

8. Network Recap Lab #4

- Find the IP address of <OdinId>.oregonctf.org, replacing <OdinId> with your OdinId

```
raghुरam@course-vm:~$ dig raghुरam.oregonctf.org

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> raghुरam.oregonctf.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 51634
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

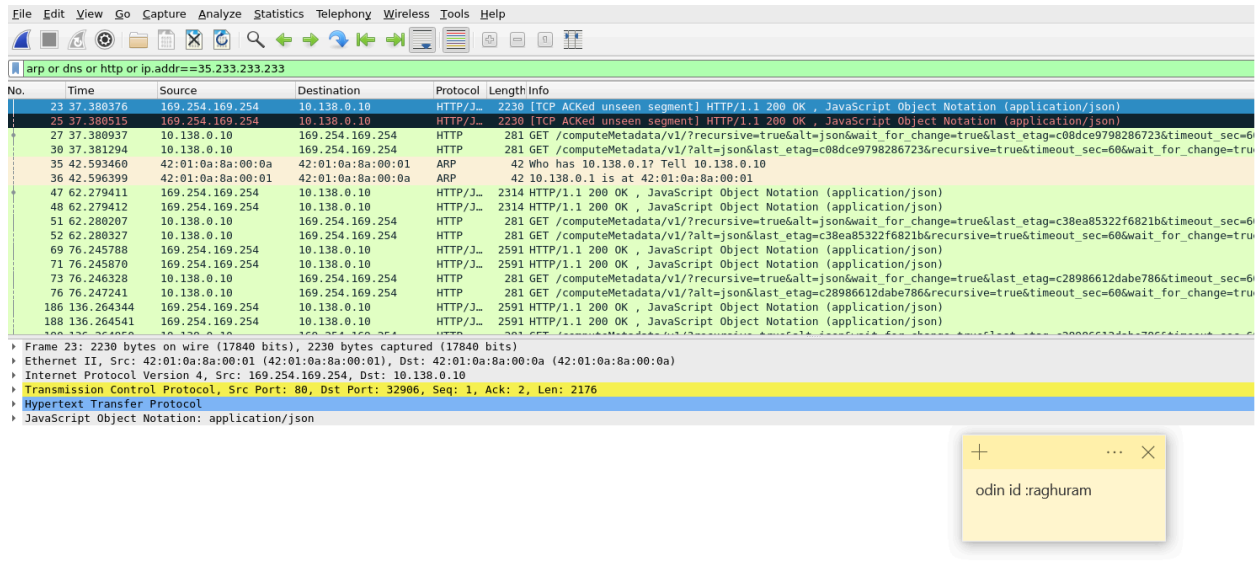
;; ANSWER SECTION:
raghुरam.oregonctf.org. 3600    IN      A      35.233.233.233

;; Query time: 72 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Apr 16 02:09:24 UTC 2024
;; MSG SIZE rcvd: 67
```

9. Collect trace

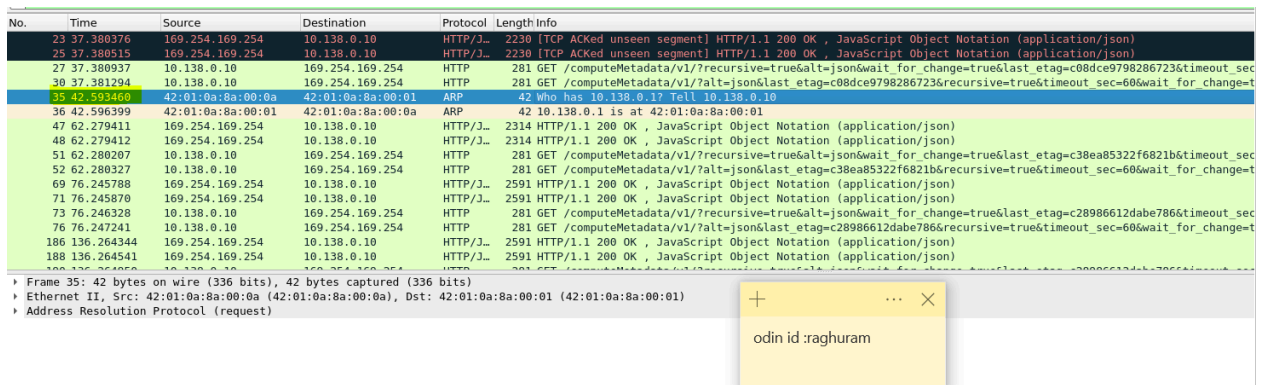
10. Analyze trace

- Take a screenshot of the all of the packets returned within Wireshark that includes their packet numbers



ARP

- What packet numbers in the trace are the result of the VM attempting to get the hardware address of the default router?



- What is this hardware address?

42:01:0a:8a:00:0a

DNS

- What packet numbers in the trace correspond to the DNS request for the web site?

No.	Time	Source	Destination	Protocol	Length	Info
73	76.246328	10.138.0.10	169.254.169.254	HTTP	281	GET /computeMetadata/v1/?recursive=true&alt=json&wait_for_change=true&last_etag=c28986612dabe7866&timeout_sec=60&wait_for_change=t
76	76.247241	10.138.0.10	169.254.169.254	HTTP	281	GET /computeMetadata/v1/?alt=json&last_etag=c28986612dabe7866&recursive=true&timeout_sec=60&wait_for_change=t
186	136.264344	169.254.169.254	10.138.0.10	HTTP/1.1	200	OK , JavaScript Object Notation (application/json)
188	136.264541	169.254.169.254	10.138.0.10	HTTP/1.1	200	OK , JavaScript Object Notation (application/json)
198	136.264950	10.138.0.10	169.254.169.254	HTTP	281	GET /computeMetadata/v1/?recursive=true&alt=json&wait_for_change=true&last_etag=c28986612dabe7866&timeout_sec=60&wait_for_change=t
193	136.265675	10.138.0.10	169.254.169.254	HTTP	281	GET /computeMetadata/v1/?alt=json&last_etag=c28986612dabe7866&recursive=true&timeout_sec=60&wait_for_change=t
428	192.120279	10.138.0.10	169.254.169.254	DNS	115	Standard query 0x5a08 A course-vm.c.cloud-nataraja-raghuram.internal OPT
429	192.120377	10.138.0.10	169.254.169.254	DNS	115	Standard query response 0x5a08 A course-vm.c.cloud-nataraja-raghuram.internal OPT
430	192.126598	169.254.169.254	10.138.0.10	DNS	131	Standard query response 0x5a08 A course-vm.c.cloud-nataraja-raghuram.internal A 10.138.0.10 OPT
431	192.126716	169.254.169.254	10.138.0.10	DNS	204	Standard query response 0x5a08 AAAA course-vm.c.cloud-nataraja-raghuram.internal SOA ns.global.gcedns-prod.1
432	192.147866	42:01:0a:8a:00:0a	Broadcast	ARP	42	Who has 10.138.0.17 Tell 10.138.0.10
433	192.150157	42:01:0a:8a:00:01	42:01:0a:8a:00:0a	ARP	42	10.138.0.1 is at 42:01:0a:8a:00:01
435	192.150173	10.138.0.10	169.254.169.254	DNS	93	Standard query 0x6560 AAAA raghuram.oregonctf.org OPT
437	192.220512	169.254.169.254	10.138.0.10	DNS	175	Standard query response 0x6560 AAAA raghuram.oregonctf.org SOA ns-cloud-d1.googledomains.com OPT
440	192.221119	10.138.0.10	35.233.233.233	TCP	74	39576 → 80 [SYN] Seq=0 Win=65520 Len=0 MSS=1420 SACK_PERM=1 TSval=3013755882 TSecr=0 WS=128
443	192.223838	35.233.233.233	10.138.0.10	TCP	74	80 → 39576 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1420 SACK_PERM=1 TSval=3261793782 TSecr=3013755882 WS=128
Frame 435: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)						
Ethernet II, Src: 42:01:0a:8a:00:0a (42:01:0a:8a:00:0a), Dst: 42:01:0a:8a:00:01 (42:01:0a:8a:00:01)						
Internet Protocol Version 4, Src: 10.138.0.10, Dst: 169.254.169.254						
User Datagram Protocol, Src Port: 48743, Dst Port: 53						
Domain Name System (query)						

+

...

×

odin id :raghuram

- What is the IP address of the local DNS server being queried?

169.254.169.254

TCP

- What packet numbers in the trace correspond to the initial TCP handshake for the web request?

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
arp or dns or http or ip.addr==35.233.233.233					
No.	Time	Source	Destination	Protocol	Length Info
193	136.265675	10.138.0.10	169.254.169.254	HTTP	281 GET /computeMetadata/v1/?alt=json&last_etag=c28986612dabe786&recursive=true&timeout_sec=60&wait_for_change=t
428	192.120279	10.138.0.10	169.254.169.254	DNS	115 Standard query 0x5a08 A course-vm.c.cloud-nataraja-raghuram.internal OPT
429	192.120377	10.138.0.10	169.254.169.254	DNS	115 Standard query 0x5a08 AAAA course-vm.c.cloud-nataraja-raghuram.internal OPT
430	192.126598	169.254.169.254	10.138.0.10	DNS	131 Standard query response 0x5a08 A course-vm.c.cloud-nataraja-raghuram.internal A 10.138.0.10 OPT
431	192.126716	169.254.169.254	10.138.0.10	DNS	204 Standard query response 0x5a08 AAAA course-vm.c.cloud-nataraja-raghuram.internal SOA ns.global.gcedns-prod.i
432	192.147866	42:01:0a:8a:00:0a	Broadcast	ARP	42 Who has 10.138.0.1? Tell 10.138.0.10
433	192.150157	42:01:0a:8a:00:01	42:01:0a:8a:00:0a	ARP	42 10.138.0.1 is at 42:01:0a:8a:00:01
435	192.150173	10.138.0.10	169.254.169.254	DNS	93 Standard query 0x6560 AAAA raghuram.oregonctf.org OPT
437	192.220512	169.254.169.254	10.138.0.10	DNS	175 Standard query response 0x6560 AAAA raghuram.oregonctf.org SOA ns-cloud-dl.googledomains.com OPT
440	192.221119	10.138.0.10	35.233.233.233	TCP	74 39576 → 80 [SYN] Seq=0 Win=65520 Len=0 MSS=1420 SACK_PERM=1 TSval=3013755882 TSecr=0 WS=128
443	192.223838	35.233.233.233	10.138.0.10	TCP	74 80 → 39576 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1420 SACK_PERM=1 TSval=3261793782 TSecr=3013755882 WS=
444	192.223878	10.138.0.10	35.233.233.233	TCP	66 39576 → 80 [ACK] Seq=1 Ack=1 Win=65408 Len=0 TSval=3013755885 TSecr=3261793782
445	192.224002	10.138.0.10	35.233.233.233	HTTP	203 GET / HTTP/1.1
448	192.224529	35.233.233.233	10.138.0.10	TCP	66 80 → 39576 [ACK] Seq=1 Ack=138 Win=64640 Len=0 TSval=3261793783 TSecr=3013755885
451	192.224938	35.233.233.233	10.138.0.10	TCP	7106 80 → 39576 [PSH, ACK] Seq=1 Ack=138 Win=64640 Len=7048 TSval=3261793784 TSecr=3013755885 [TCP segment of a r
452	192.224953	10.138.0.10	35.233.233.233	TCP	66 39576 → 80 [ACK] Seq=138 Ack=7041 Win=61056 Len=0 TSval=3013755886 TSecr=3261793784
453	192.225023	35.233.233.233	10.138.0.10	HTTP	203 HTTP/1.1 200 OK (text/html)
Frame 440: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)					
Ethernet II, Src: 42:01:0a:8a:00:0a (42:01:0a:8a:00:0a), Dst: 42:01:0a:8a:00:01 (42:01:0a:8a:00:01)					
Destination: 42:01:0a:8a:00:01 (42:01:0a:8a:00:01)					
Source: 42:01:0a:8a:00:0a (42:01:0a:8a:00:0a)					
Type: IPv4 (0x0800)					
Internet Protocol Version 4, Src: 10.138.0.10, Dst: 35.233.233.233					
0100 = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 60					
Identification: 0x4573 (17779)					
Flags: 0x40, Don't fragment					
...0 0000 0000 0000 = Fragment Offset: 0					
Time to Live: 64					
Protocol: TCP (6)					
Header Checksum: 0xdce2 [validation disabled]					
[Header checksum status: Unverified]					
Source address: 10.138.0.10					

- How long does it take to perform the initial TCP handshake?

0.002661 seconds

HTTP

- What packet numbers in the trace correspond to the actual HTTP request and response?

Applications : raghuram@course-vm: network_trac

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp or dns or http or ip.addr==35.233.233.233

No.	Time	Source	Destination	Protocol	Length	Info
430	192.126598	169.254.169.254	10.138.0.10	DNS	131	Standard query response 0x5a08 A course-vm.c.cloud-nataraja-raghuram.internal A 10.138.0.10 OPT
431	192.126716	169.254.169.254	10.138.0.10	DNS	204	Standard query response 0xda66 AAAA course-vm.c.cloud-nataraja-raghuram.internal SOA ns.global.gcedns-prod.i
432	192.147866	42:01:0a:8a:00:0a	Broadcast	ARP	42	Who has 10.138.0.1? Tell 10.138.0.10
433	192.150157	42:01:0a:8a:00:01	42:01:0a:8a:00:0a	ARP	42	10.138.0.1 is at 42:01:0a:8a:00:01
435	192.150173	10.138.0.10	169.254.169.254	DNS	93	Standard query 0x6560 AAAA raghuram.oregonctf.org OPT
437	192.220512	169.254.169.254	10.138.0.10	DNS	175	Standard query response 0x6560 AAAA raghuram.oregonctf.org SOA ns-cloud-dl.googledomains.com OPT
440	192.221119	10.138.0.10	35.233.233.233	TCP	74	39576 → 80 [SYN] Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM=1 TSval=3013755882 TSecr=0 WS=128
443	192.223838	35.233.233.233	10.138.0.10	TCP	74	80 → 39576 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1420 SACK_PERM=1 TSval=3261793782 TSecr=3013755882 WS=
444	192.223878	10.138.0.10	35.233.233.233	TCP	66	39576 → 80 [ACK] Seq=1 Ack=1 Win=65408 Len=0 TSval=3013755885 TSecr=3261793782
445	192.224002	10.138.0.10	35.233.233.233	HTTP	203	GET / HTTP/1.1
448	192.224529	35.233.233.233	10.138.0.10	TCP	66	80 → 39576 [ACK] Seq=1 Ack=138 Win=64640 Len=0 TSval=3261793783 TSecr=3013755885
451	192.224938	35.233.233.233	10.138.0.10	TCP	7106	80 → 39576 [PSH, ACK] Seq=1 Ack=138 Win=64640 Len=7040 TSval=3261793784 TSecr=3013755885 [TCP segment of a r
452	192.224953	10.138.0.10	35.233.233.233	TCP	66	39576 → 80 [ACK] Seq=138 Ack=7041 Win=61056 Len=0 TSval=3013755886 TSecr=3261793784
453	192.225037	35.233.233.233	10.138.0.10	HTTP	792	HTTP/1.1 200 OK (text/html)
454	192.225045	10.138.0.10	35.233.233.233	TCP	66	39576 → 80 [ACK] Seq=138 Ack=7767 Win=60416 Len=0 TSval=3013755886 TSecr=3261793784
461	192.226163	10.138.0.10	35.233.233.233	TCP	66	39576 → 80 [FIN, ACK] Seq=138 Ack=7767 Win=64128 Len=0 TSval=3013755887 TSecr=3261793784

Frame 445: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits)

Ethernet II, Src: 42:01:0a:8a:00:0a (42:01:0a:8a:00:0a), Dst: 42:01:0a:8a:00:01 (42:01:0a:8a:00:01)

- Destination: 42:01:0a:8a:00:01 (42:01:0a:8a:00:01)
- Source: 42:01:0a:8a:00:0a (42:01:0a:8a:00:0a)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.138.0.10, Dst: 35.233.233.233

- Version: 4
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 189
- Identification: 0x4575 (17781)
- Flags: 0x40, Don't fragment
- Fragment Offset: 0
- Time to Live: 64
- Protocol: TCP (6)
- Header Checksum: 0xdc5f [validation disabled]
- Header checksum status: Unverified
- Source Address: 10.138.0.10

odin id : raghuram

- How long does it take to process the HTTP request after the handshake?

0.001035 seconds