

Stuart Rimel

CS530: Internet Web & Cloud, Fall 2023

Odin: srime1

** In all the terminal screenshots my Odin name is in the terminal prompt **

Table of Contents:

[2.1: TCP, HTTP](#)

[2.1.1: TCP #1 Sockets](#)

[2.1.2: - Isof](#)

[2.1.3: TCP #2 Throughput](#)

[2.1.4: - iperf](#)

[2.1.5: HTTP #3 Requests](#)

[2.1.6: Asynchronous HTTP requests](#)

[2.2: DNS, Recap](#)

[2.2.1: DNS reconnaissance #1 \(dig\)](#)

[2.2.2: Iterative DNS lookups](#)

[2.2.3: Reverse DNS lookups](#)

[2.2.4: Host enumeration](#)

[2.2.5: Geographic DNS #2](#)

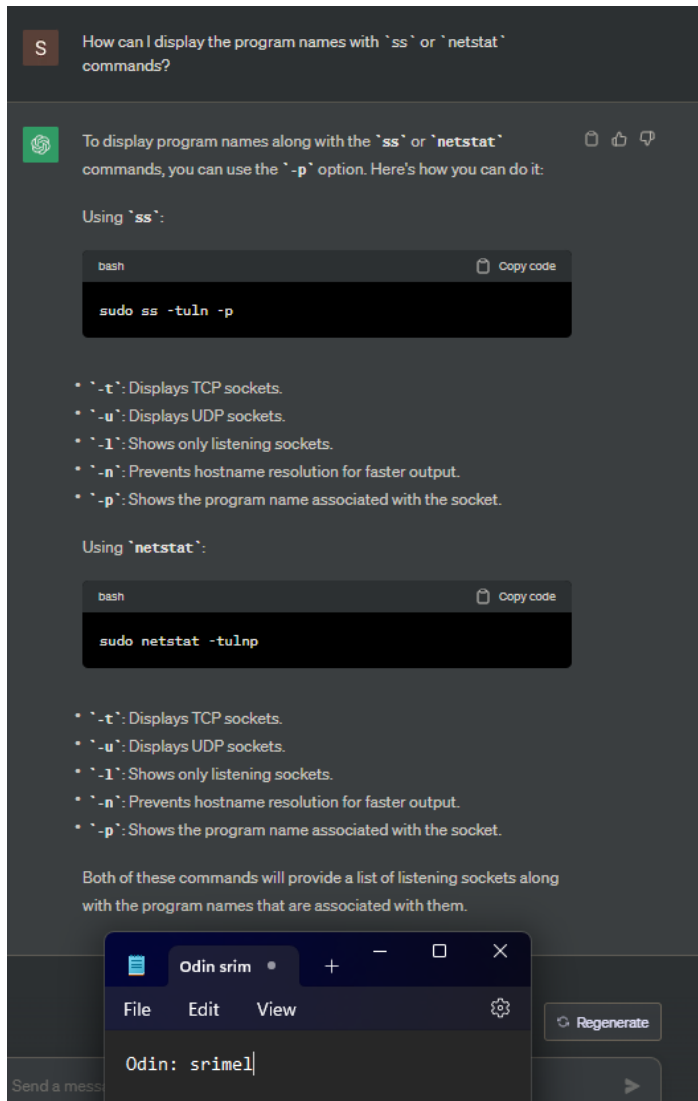
[2.2.6-7: Wireshark Lab #3](#)

[2.2.8: Network Recap Lab #4](#)

[2.2.9-10: Collect trace / Analyze trace](#)

2.1: TCP, HTTP

2.1.1: TCP #1 Sockets



Here is when I ran the command in my course VM:

```
srimel@course-vm:~$ sudo ss -tln -p | grep LISTEN
LISTEN 0      128          0.0.0.0:22      0.0.0.0:*      users: (("sshd",pid=790,fd=3))
LISTEN 0      4096        127.0.0.53:53    0.0.0.0:*      users: (("systemd-resolve",pid=366,fd=14))
LISTEN 0      4096        127.0.0.1:34203  0.0.0.0:*      users: (("containerd",pid=448,fd=10))
LISTEN 0      128         [::]:22         [::]:*         users: (("sshd",pid=790,fd=4))
LISTEN 0      2          [::]:3350       [::]:*         users: (("xrdp-sesman",pid=484,fd=7))
LISTEN 0      2          *:3389          *:             users: (("xrdp",pid=616,fd=11))
srimel@course-vm:~$
```

A service that can be contacted from any interface on the machine would be `sshd` with PID 790.

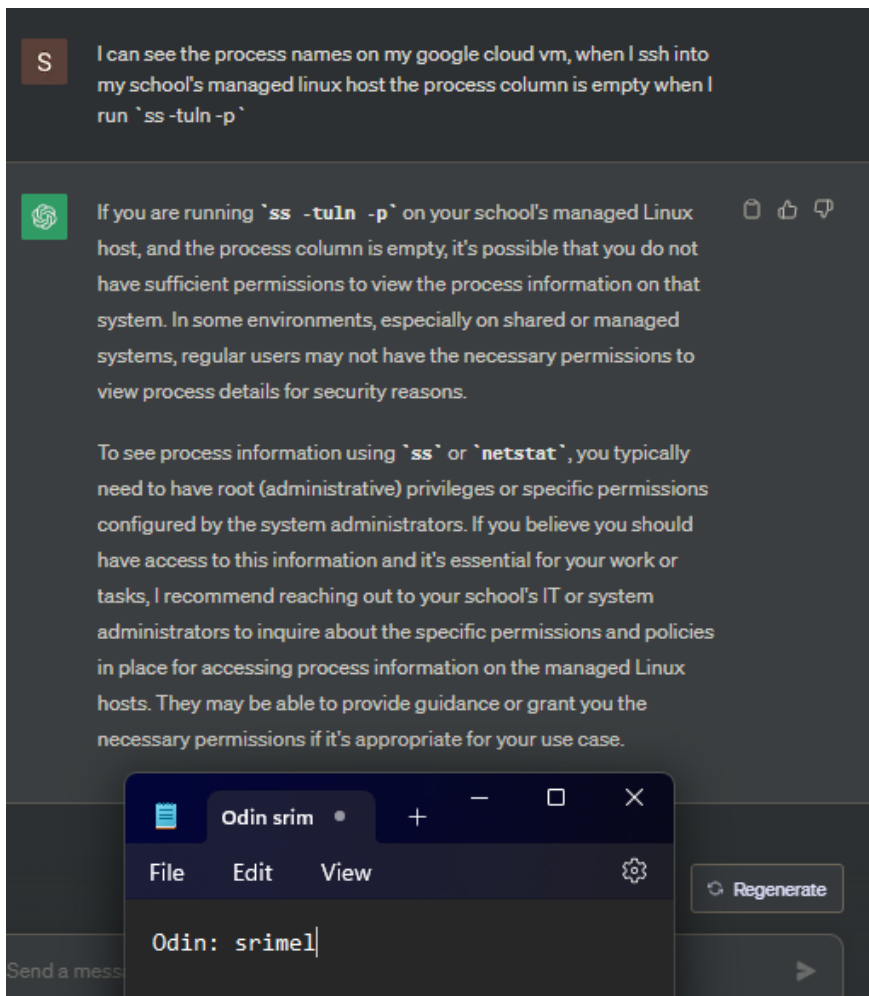
Here is the commands run in linux.cs.pdx.edu:

```

srimel@ada:~$ ss -tln -p
State      Recv-Q    Send-Q    Local Address:Port    Peer Address:Port    Process
LISTEN     0          511       127.0.0.1:39507        0.0.0.0:*
LISTEN     0          128       127.0.0.1:6100        0.0.0.0:*
LISTEN     0          128       127.0.0.1:6101        0.0.0.0:*
LISTEN     0          4096      127.0.0.53%lo:53      0.0.0.0:*
LISTEN     0          128       127.0.0.1:6102        0.0.0.0:*
LISTEN     0          128       0.0.0.0:22            0.0.0.0:*
LISTEN     0          128       127.0.0.1:6103        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       127.0.0.1:6105        0.0.0.0:*
LISTEN     0          100       127.0.0.1:25          0.0.0.0:*
LISTEN     0          128       127.0.0.1:6011        0.0.0.0:*
LISTEN     0          511       127.0.0.1:33277       0.0.0.0:*
LISTEN     0          5         127.0.0.1:5953        0.0.0.0:*
LISTEN     0          128       127.0.0.1:6018        0.0.0.0:*
LISTEN     0          4096      *:113                 *:
LISTEN     0          128       [::1]:6100            [::]:*
LISTEN     0          50        *:1716                 *:
LISTEN     0          128       [::1]:6101            [::]:*
LISTEN     0          128       [::1]:6102            [::]:*
LISTEN     0          128       [::]:22               [::]:*
LISTEN     0          128       [::1]:6103            [::]:*
LISTEN     0          128       [::1]:631             [::]:*
LISTEN     0          128       [::1]:6104            [::]:*
LISTEN     0          128       [::1]:6105            [::]:*
LISTEN     0          100       [::1]:25              [::]:*
LISTEN     0          128       [::1]:6011            [::]:*
LISTEN     0          5         [::1]:5953            [::]:*
LISTEN     0          128       [::1]:6018            [::]:*
srimel@ada:~$ |

```

On the school's server I cannot see the name of the process. I think I might not have permissions for that. I asked chatGPT about that.



However, I can infer that 0.0.0.0:22 is ssh since it traditional runs on port 22 and it has 0.0.0.0 so any interface can connect.

2.1.2: - lsof

I inadvertently got the `lsof` command suggest from chatGPT while trying to perform the task in 2.1.1:

S will this also show the name of the programs?

The `netstat` command with the `grep 'LISTEN'` portion will show you a list of all TCP sockets in the LISTEN state on the specified IPv4 address, but it won't directly display the names of the programs associated with those sockets. To see the program names, you can use the `lsof` command in combination with `grep`. Here's how you can do it:

```
bash
Copy code
sudo lsof -iTCP -sTCP:LISTEN -n | grep 'LISTEN'
```

Here's what each part of the command does:

- `sudo`: Runs the command with administrator privileges.
- `lsof`: Lists open files, including network sockets.
- `-iTCP`: Specifies that we want to list TCP sockets.
- `-sTCP:LISTEN`: Filters the list to only show sockets in the LISTEN state.
- `-n`: Prevents hostname resolution for faster output.
- `| grep 'LISTEN'`: Uses `grep` to filter the results and only display lines containing 'LISTEN', which shows you the sockets in the LISTEN state.

This command will provide a list of all TCP sockets in the LISTEN state on your IPv4 address along with the associated program names.

Odin: srime1

Here's the command being run in the course-vm:

```
srime1@course-vm:~$ sudo lsof -iTCP -sTCP:LISTEN -n | grep 'LISTEN'
systemd-r 366 systemd-resolve 14u IPv4 15934 0t0 TCP 127.0.0.53:domain (LISTEN)
container 448 root 10u IPv4 18047 0t0 TCP 127.0.0.1:34203 (LISTEN)
xrdp-sesm 484 root 7u IPv6 16374 0t0 TCP [::1]:3350 (LISTEN)
xrdp 616 xrdp 11u IPv6 17680 0t0 TCP *:ms-wbt-server (LISTEN)
sshd 790 root 3u IPv4 17902 0t0 TCP *:ssh (LISTEN)
sshd 790 root 4u IPv6 17913 0t0 TCP *:ssh (LISTEN)
srime1@course-vm:~$
```

2.1.3: TCP #2 Throughput

VM instances

Filter Enter property name or value

Status	Name ↑	Zone	In use by	Internal IP	External IP	Network	Connect
	course-vm	us-west1-b		10.138.0.2 (nic0)		default	SSH ▾ ⋮
	vm-australia-southeast1-b	australia-southeast1-b		10.152.0.2 (nic0)	35.197.160.218 (nic0)	default	SSH ▾ ⋮
	vm-europe-west1-d	europe-west1-d		10.132.0.2 (nic0)	35.205.45.52 (nic0)	default	SSH ▾ ⋮
	vm-us-east1-b	us-east1-b		10.142.0.3 (nic0)	34.75.142.69 (nic0)	default	SSH ▾ ⋮
	vm-us-west1-b	us-west1-b		10.138.0.10 (nic0)	35.199.191.117 (nic0)	default	SSH ▾ ⋮

Related actions

Explore Backup and DR **NEW**
Back up your VMs and set up disaster recovery

Odin: srimel

Monitor VMs
How outlier VMs across metrics like CPU and network

Explore VM logs
View, search, analyze, and download VM instance logs

2.1.4: - iperf

```
srimel@vm-us-west1-b:~$ echo australia && iperf -c 35.197.160.218 -p 80
australia
-----
Client connecting to 35.197.160.218, TCP port 80
TCP window size: 85.0 KByte (default)
-----
[ 1] local 10.138.0.10 port 50276 connected with 35.197.160.218 port 80
[ ID] Interval      Transfer    Bandwidth
[ 1] 0.0000-10.2387 sec 188 MBytes  154 Mbits/sec
srimel@vm-us-west1-b:~$ echo europe-west && iperf -c 35.205.45.52 -p 80
europe-west
-----
Client connecting to 35.205.45.52, TCP port 80
TCP window size: 85.0 KByte (default)
-----
[ 1] local 10.138.0.10 port 60514 connected with 35.205.45.52 port 80
[ ID] Interval      Transfer    Bandwidth
[ 1] 0.0000-10.1604 sec 180 MBytes  149 Mbits/sec
srimel@vm-us-west1-b:~$ echo us-east && iperf -c 34.75.142.69 -p 80
us-east
-----
Client connecting to 34.75.142.69, TCP port 80
TCP window size: 85.0 KByte (default)
-----
[ 1] local 10.138.0.10 port 52920 connected with 34.75.142.69 port 80
[ ID] Interval      Transfer    Bandwidth
[ 1] 0.0000-10.0776 sec 418 MBytes  348 Mbits/sec
srimel@vm-us-west1-b:~$
```

The best bandwidth from us-west is to us-east at 348 Mbits/sec. This makes sense because out of the other location us-east is the closest and non-transatlantic destination. Coming in second place is australia-southeast at 154 Mbits/sec. This is pretty much half of the bandwidth of the connection to us-east and this makes sense because Australia is pretty far away from the states. Coming in last is europe-west at 149 Mbits/sec, this one is a little surprising because europe should be closer to us-west than australia-southeast, but it is only negligibly smaller bandwidth at 149 Mbits/sec.

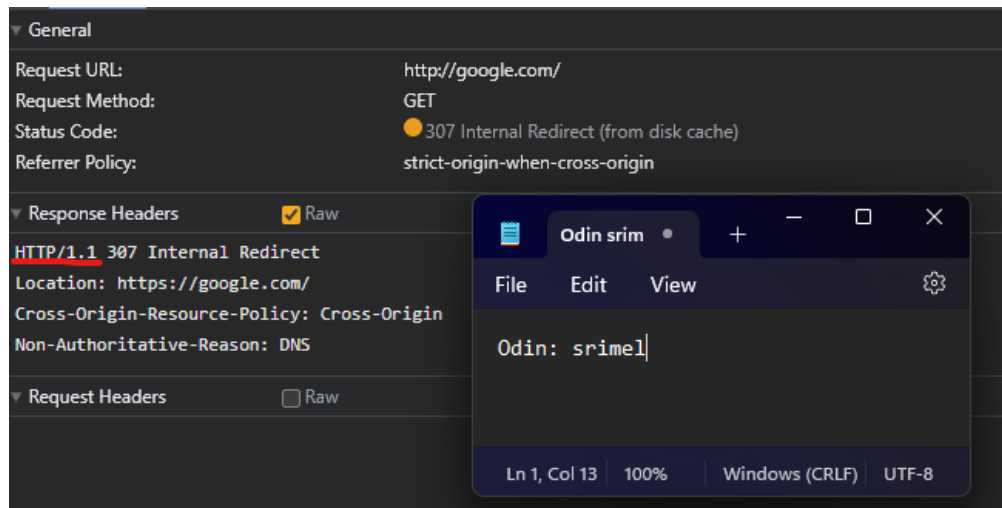
2.1.5: HTTP #3 Requests

Top three requests:

Name	Status	Type	Initiator	Size	Time	Waterfall
google.com	307	document / Redir...	Other	(disk cache)	1 ms	
google.com	301	document / Redir...	google.com/	24 B	27 ms	
www.google.com	200	document	google.com/	52.1 kB	135 ms	
	200	script	(index):25	273 kB	23 ms	
	200	png	(index):66	3.5 kB	24 ms	
	200	png	(index):121	(memory cache)	0 ms	
	200	script	(index):118	74.9 kB	17 ms	
	200	stylesheet	(index):118	668 B	16 ms	
	200	webp	(index):125	689 B	22 ms	

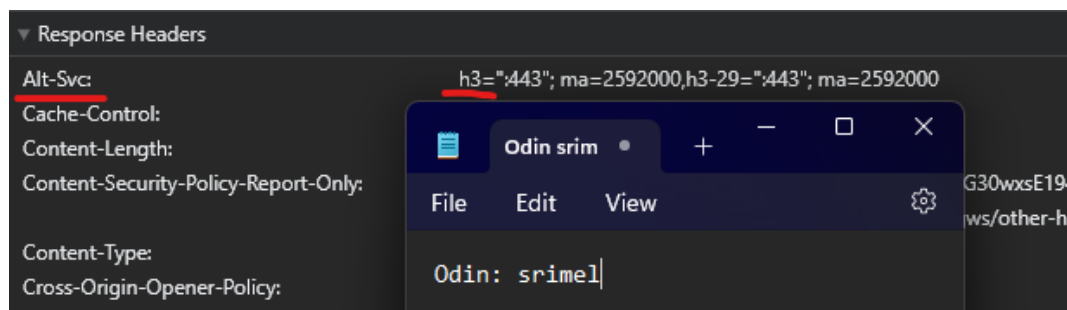
Request #1:

- URL: <http://google.com/>
- Status Code: 307 Internal Redirect
 - Successful response, but will redirect
- Using HTTP/1.1



Request #2:

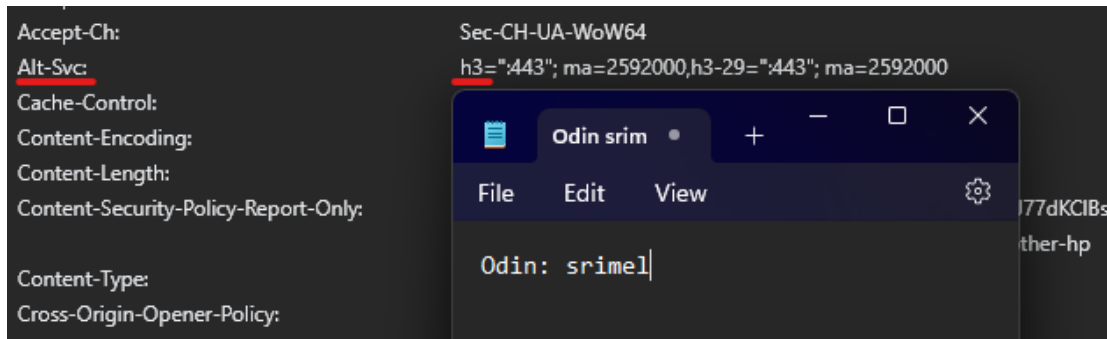
- URL: <https://google.com/>
- Status Code: 301 Moved Permanently
 - Requested resource has been moved to a different location
- Using HTTP/3



Request #3:

- URL: <https://www.google.com/>
- Status Code: 200 OK
 - Successful response

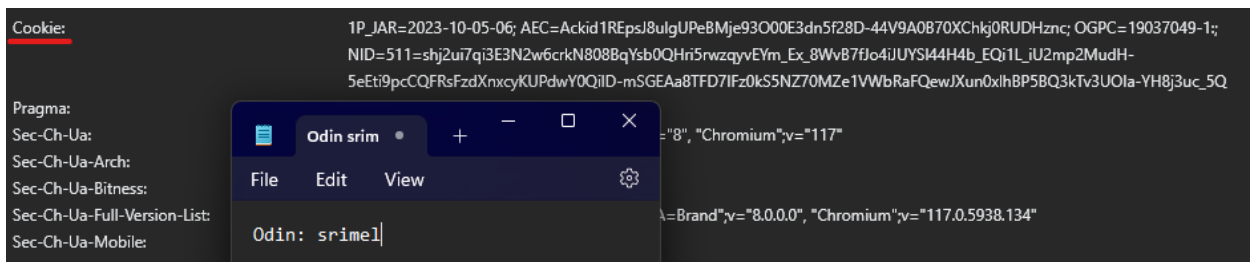
- Using HTTP/3



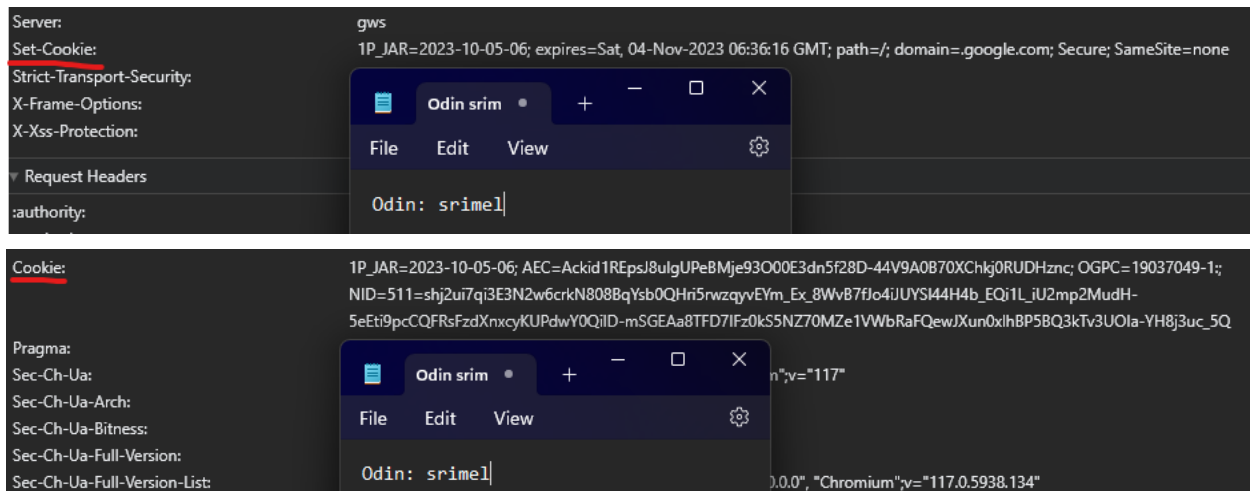
First redirection URL: <https://google.com/>

Second redirection URL: <https://www.google.com/>

Cookies for Request #2: <https://google.com/>



Cookies for Request #3: <https://www.google.com/>



2.1.6: Asynchronous HTTP requests

Requests and response listings for typing 'Portland State' in google search:

Name	Status	Type	Initiator	Size	Time	Waterfall
<input type="checkbox"/> rs=ACT90oEm0gndJDakKWHMl-hMvs_yCIMZIA	200	fetch	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	111 kB	31 ms	
<input type="checkbox"/> search?q&cp=0&client=gws-wiz&xssi=t&gs_pcr=2&hl=e...pr=...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	2.0 kB	111 ms	
<input type="checkbox"/> hpba?vet=10ahUKEwj_9be6pd6BAxWKGTOIHffJAVsQj-OKCBs...H...	200	xhr	m=slb_wiz_aa.abd.syn8.syo7.syo8...	122 B	51 ms	
<input type="checkbox"/> search?q=P&cp=1&client=gws-wiz&xssi=t&gs_pcr=unde...0&p...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	800 B	47 ms	
<input type="checkbox"/> search?q=Po&cp=2&client=gws-wiz&xssi=t&gs_pcr=und...0&...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	733 B	48 ms	
<input type="checkbox"/> search?q=Por&cp=3&client=gws-wiz&xssi=t&gs_pcr=un...0&p...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	827 B	214 ms	
<input type="checkbox"/> search?q=Port&cp=4&client=gws-wiz&xssi=t&gs_pcr=u...0&ps...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	958 B	67 ms	
<input type="checkbox"/> search?q=Portl&cp=5&client=gws-wiz&xssi=t&gs_pcr=...0&psi...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	992 B	65 ms	
<input type="checkbox"/> search?q=Portla&cp=6&client=gws-wiz&xssi=t&gs_pcr...0&psi...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	991 B	68 ms	
<input type="checkbox"/> search?q=Portlan&cp=7&client=gws-wiz&xssi=t&gs_pcr...0&psi...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	989 B	59 ms	
<input type="checkbox"/> search?q=Portland&cp=8&client=gws-wiz&xssi=t&gs_pc...0&ps...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	985 B	73 ms	
<input type="checkbox"/> search?q=Portland%20&cp=9&client=gws-wiz&xssi=t&gs...0&p...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	972 B	62 ms	
<input type="checkbox"/> search?q=Portland%20S&cp=10&client=gws-wiz&xssi=t&...0&...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	678 B	64 ms	
<input type="checkbox"/> search?q=Portland%20St&cp=11&client=gws-wiz&xssi=t...0&ps...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	585 B	59 ms	
<input type="checkbox"/> search?q=Portland%20Sta&cp=12&client=gws-wiz&xssi=...0&p...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	955 B	61 ms	
<input type="checkbox"/> search?q=Portland%20Stat&cp=13&client=gws-wiz&xssi...0&ps...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	955 B	70 ms	
<input type="checkbox"/> search?q=Portland%20State&cp=14&client=gws-wiz&xss...0&p...	200	xhr	m=cdos,hsm.jsa.mb4ZUlb.d.csi.c...	954 B	63 ms	

Odin srim

File Edit View

Odin: sriml

/ 3.4 MB resources | Finish: 21.2 min | DOMContentLoaded: 225 ms | Load: 511 ms

×	Headers	Payload	Preview	Response	Initiator	Timing	Cookies
1)						
-]						
-	}]'						
2	[[["portland state university",46,[512,433,131],{"lm":[],"zh":"Portland State University","zi":"Public university in Portland, Oregon","zp":{"g						

Odin srim

File Edit View

Odin: sriml

2.2: DNS, Recap

2.2.1: DNS reconnaissance #1 (dig)

S Produce a linux dig command that queries 131.252.208.53 for the 'A' record of 'www.pdx.edu'. This must be done using TCP as well.

You can use the `dig` command with the `+tcp` option to specify that the query should be sent over TCP instead of the default UDP. Here's the command to query the 'A' record of 'www.pdx.edu' from the DNS server at IP address 131.252.208.53 using TCP:

```
bash
dig +tcp @131.252.208.53 A www.pdx.edu
```

This command will send a DNS query to the specified DNS server over TCP and request the 'A' record for 'www.pdx.edu'.

Odin: srimel

Getting A records:

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

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> +tcp @131.252.208.53 A www.pdx.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51427
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: b7ad4bf961986af001000000651e6a5a9f3bd68e01545ddc (good)
;; QUESTION SECTION:
;www.pdx.edu.                IN      A

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

;; Query time: 67 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (TCP)
;; WHEN: Thu Oct 05 00:48:42 PDT 2023
;; MSG SIZE rcvd: 132

srimel@ada:~$
```

Getting MX records:

```

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

; <<>> DiG 9.18.12-Ubuntu0.22.04.2-Ubuntu <<>> +tcp @131.252.208.53 MX pdx.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22822
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: f207492a914be8e101000000651e6de84455dadc750af608 (good)
;; QUESTION SECTION:
;pdx.edu.                IN      MX

;; ANSWER SECTION:
pdx.edu.                51669   IN      MX      5 alt1.aspmx.l.google.com.
pdx.edu.                51669   IN      MX      1 aspmx.l.google.com.
pdx.edu.                51669   IN      MX      10 alt4.aspmx.l.google.com.
pdx.edu.                51669   IN      MX      10 alt3.aspmx.l.google.com.
pdx.edu.                51669   IN      MX      5 alt2.aspmx.l.google.com.

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (TCP)
;; WHEN: Thu Oct 05 01:03:52 PDT 2023
;; MSG SIZE rcvd: 182

srimel@ada:~$ |
[0] 0: bash*

```

Searching all the IPs on iplocation.net showed that amazon for the ISP and Organization, so I would have to say that the cloud provider is AWS in this case.

The mail cloud provider for pdx.edu is Google.

Authoritative server for mashimaro.cs.pdx.edu:

```

srimel@ada:~$ dig +tcp @131.252.208.53 NS mashimaro.cs.pdx.edu

; <<>> DiG 9.18.12-Ubuntu0.22.04.2-Ubuntu <<>> +tcp @131.252.208.53 NS mashimaro.cs.pdx.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7172
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 1247f2eb62f852e901000000651e6ee06c71a1fc2b63c44f (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. 2023100302 600 300 1209600 300

;; Query time: 3 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (TCP)
;; WHEN: Thu Oct 05 01:08:00 PDT 2023
;; MSG SIZE rcvd: 147

srimel@ada:~$ |
[0] 0: bash*

```

Query authoritative server for A record:

```

srime1@ada:~$ dig +tcp @131.252.208.53 A walt.ee.pdx.edu

; <<>> DiG 9.18.12-Ubuntu0.22.04.2-Ubuntu <<>> +tcp @131.252.208.53 A walt.ee.pdx.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25598
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e35bdca610f87add01000000651e6f76fc3c101d47b32f95 (good)
;; QUESTION SECTION:
;walt.ee.pdx.edu.                IN      A

;; ANSWER SECTION:
walt.ee.pdx.edu.                6662    IN      A      131.252.208.38

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (TCP)
;; WHEN: Thu Oct 05 01:10:30 PDT 2023
;; MSG SIZE rcvd: 88

srime1@ada:~$ |
[0] 0: bash*

```

2.2.2: Iterative DNS lookups

Dig with no args, showing ip of f root server:

```

c.root-servers.net. 2984 IN A 192.203.230.10
f.root-servers.net. 2984 IN A 192.5.5.241
g.root-servers.net. 2984 IN A 192.33.4.12

```

Query list:

1. dig +tcp +norecurse @192.5.5.241 NS console.cloud.google.com
2. dig +tcp +norecurse @192.12.94.30 NS console.cloud.google.com
3. dig +tcp +norecurse @216.239.34.10 NS console.cloud.google.com

Answer to query:

```
srimel@ada:~$ dig +tcp +norecurse @216.239.34.10 NS console.cloud.google.com

; <<> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<> +tcp +norecurse @216.239.34.10 NS console.cloud.google
.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6437
;; 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. 570642618 900 90
0 1800 60

;; Query time: 11 msec
;; SERVER: 216.239.34.10#53(216.239.34.10) (TCP)
;; WHEN: Thu Oct 05 01:41:37 PDT 2023
;; MSG SIZE rcvd: 124

srimel@ada:~$ |
```

2.2.3: Reverse DNS lookups

ChatGPT prompt/answer:

S

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



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

bash

Copy code

```
dig +short espn.go.com | egrep -o '([0-9]{1,3}\.){3}[0-9]{1,3}' | awk '!seen[$0]++'
```

Here's a breakdown of what each part of the command does:

1. `dig +short espn.go.com`: This command uses `dig` to query the DNS for the IPv4 addresses associated with `espn.go.com` and returns the results in a short format (only the IP addresses).
2. `egrep -o '([0-9]{1,3}\.){3}[0-9]{1,3}'`: This part of the command uses `egrep` with a regular expression to extract IPv4 addresses from the output of `dig`. The regular expression `'([0-9]{1,3}\.){3}[0-9]{1,3}'` matches IPv4 addresses in the form of `XXX.XXX.XXX.XXX`, where `XXX` represents one to three digits. The `-o` option tells `egrep` to only output the matched IP addresses.
3. `awk '!seen[$0]++'`: Finally, `awk` is used to remove duplicate IP addresses from the list. It keeps track of seen IP addresses and only prints each unique address once.

This command should provide you with a list of unique IPv4 addresses associated with `espn.go.com`.



File

Edit

View



Odin: srimel

Results from command ChatGPT produced:

```
srime1@ada:~$ dig +short espn.go.com | egrep -o '([0-9]{1,3}\.){3}[0-9]{1,3}' | awk '!seen[$0]++'
18.161.6.80
18.161.6.94
18.161.6.38
18.161.6.89
srime1@ada:~$
```

I stored those in an environment variable named 'IPS' then ran the following command for reverse lookup:

```
srime1@ada:~$ for i in `echo $IPS`
> do
> dig +tcp -x $i | egrep '^([0-9])' | awk '{print $5}'
> done
server-18-161-6-89.hio52.r.cloudfront.net.
server-18-161-6-94.hio52.r.cloudfront.net.
server-18-161-6-38.hio52.r.cloudfront.net.
server-18-161-6-80.hio52.r.cloudfront.net.
srime1@ada:~$ |
[0] 0: bash*
```

2.2.4: Host enumeration

```
srime1@ada:~$ cat 220hosts.txt | head -190 | 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.
srime1@ada:~$ |
```

2.2.5: Geographic DNS #2

Geographic locations

131.252.208.53

- Ipinfo.io
 - Portland, Oregon 97204
 - lat/long: 45.5234, -122.6762
- DB-IP
 - Portland, Oregon 97207
 - lat/long: 45.584, -122.728

198.82.247.66

- Ipinfo.io
 - Blacksburg, Virginia 24062
 - lat/long: 37.2296, -80.4139
- DB-IP
 - Blacksburg, Virginia 24061
 - lat/long: 37.2037, -80.4143

131.252.208.53 resolves to 142.251.215.228:

142.251.215.228 has geo coordinates: 47.6062, -122.3321

```
srinel@ada:~$ dig +tcp @131.252.208.53 A www.google.com

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> +tcp @131.252.208.53 A www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61128
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 244e0b655d35fe9f01000000651f96dfa1b2556efd17ef5f (good)
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.                175     IN      A      142.251.215.228

;; Query time: 3 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (TCP)
;; WHEN: Thu Oct 05 22:10:55 PDT 2023
;; MSG SIZE rcvd: 87

srinel@ada:~$ |
```

198.82.247.66 resolves to 6 addresses, but taking the first one is 142.251.111.104

142.251.111.104 has geo coordinates: 39.0437, -77.4875


```

srinel@ada:~$ dig +tcp @198.82.247.66 A www.google.com

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> +tcp @198.82.247.66 A www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52966
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 32e31591a88c38e666a82892651f974d354403684803d778 (good)
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.                186     IN      A      142.251.111.104
www.google.com.                186     IN      A      142.251.111.147
www.google.com.                186     IN      A      142.251.111.99
www.google.com.                186     IN      A      142.251.111.103
www.google.com.                186     IN      A      142.251.111.105
www.google.com.                186     IN      A      142.251.111.106

;; AUTHORITY SECTION:
google.com.                    135004  IN      NS      ns4.google.com.
google.com.                    135004  IN      NS      ns1.google.com.
google.com.                    135004  IN      NS      ns2.google.com.
google.com.                    135004  IN      NS      ns3.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.                307953  IN      A      216.239.32.10
ns2.google.com.                307953  IN      A      216.239.34.10
ns3.google.com.                307953  IN      A      216.239.36.10
ns4.google.com.                307953  IN      A      216.239.38.10
ns1.google.com.                135004  IN      AAAA   2001:4860:4802:32::a
ns2.google.com.                135004  IN      AAAA   2001:4860:4802:34::a
ns3.google.com.                335045  IN      AAAA   2001:4860:4802:36::a
ns4.google.com.                135004  IN      AAAA   2001:4860:4802:38::a

;; Query time: 67 msec
;; SERVER: 198.82.247.66#53(198.82.247.66) (TCP)
;; WHEN: Thu Oct 05 22:12:45 PDT 2023
;; MSG SIZE rcvd: 415

srinel@ada:~$ |
[0] 0:bash*

```

Traceroutes:

```

Odin: srinel
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)  0.526 ms  0.463 ms  0.347 ms

```

```

Odin: srimel
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) 1.817 ms 1.755 ms 1.796 ms
 2 CORE1.net.pdx.edu (131.252.5.142) 0.839 ms 0.773 ms 0.663 ms
 3 131.252.5.213 (131.252.5.213) 0.368 ms 0.513 ms 0.332 ms
 4 port-psu-pe-01.net.linkoregon.org (199.165.177.48) 0.417 ms 0.314 ms 0.375 ms
 5 eugn-oh-vpn-01.net.linkoregon.org (207.98.126.3) 10.193 ms 10.163 ms 10.138 ms
 6 bois-gtwy-pe-01.net.linkoregon.org (207.98.126.135) 10.085 ms 10.166 ms 10.110 ms
 7 bois-gtwy-pe-01-loren.net.linkoregon.org (163.253.5.65) 9.991 ms 9.902 ms 9.969 ms
 8 hundredge-0-0-0-24.703.core1.bois.net.internet2.edu (163.253.5.64) 12.348 ms 12.229 ms 12.187 ms
 9 fourhundredge-0-0-0-0.4079.core2.salt.net.internet2.edu (163.253.1.249) 64.755 ms 64.679 ms 64.611 ms
10 fourhundredge-0-0-0-21.4079.core1.salt.net.internet2.edu (163.253.1.28) 64.604 ms fourhundredge-0-0-0-2
2.4079.core1.salt.net.internet2.edu (163.253.1.30) 64.253 ms fourhundredge-0-0-0-23.4079.core1.salt.net.int
ernet2.edu (163.253.1.32) 64.114 ms
11 fourhundredge-0-0-0-0.4079.core1.denv.net.internet2.edu (163.253.1.170) 65.464 ms 65.368 ms fourhundre
dge-0-0-0-0.4079.core2.kans.net.internet2.edu (163.253.1.251) 66.284 ms
12 fourhundredge-0-0-0-0.4079.core1.kans.net.internet2.edu (163.253.1.243) 64.141 ms 64.050 ms fourhundre
dge-0-0-0-22.4079.core1.kans.net.internet2.edu (163.253.1.54) 63.948 ms
13 fourhundredge-0-0-0-3.4079.core2.chic.net.internet2.edu (163.253.1.244) 65.098 ms 65.789 ms 65.660 ms
14 fourhundredge-0-0-0-3.4079.core2.eqch.net.internet2.edu (163.253.2.19) 65.931 ms 65.399 ms 65.263 ms
15 fourhundredge-0-0-0-0.4079.core2.clev.net.internet2.edu (163.253.2.16) 64.752 ms 65.635 ms 65.271 ms
16 fourhundredge-0-0-0-3.4079.core2.ashb.net.internet2.edu (163.253.1.138) 64.685 ms 64.460 ms 64.353 ms
17 192.122.175.14 (192.122.175.14) 63.307 ms 63.201 ms 63.065 ms
18 vtacs-1.msap.cns.vt.edu (192.70.187.18) 66.011 ms 65.906 ms 65.928 ms
19 isb-core.xe-7-0-0.0.cns.vt.edu (128.173.0.202) 67.976 ms 67.870 ms 67.892 ms
20 cas-core.lo0.2000.cns.vt.edu (198.82.1.143) 67.510 ms 67.402 ms 67.225 ms
21 jeru.cns.vt.edu (198.82.247.66) 67.715 ms 67.642 ms 67.597 ms

```

```

Odin: srimel
traceroute to 142.251.215.228 (142.251.215.228), 30 hops max, 60 byte packets
 1 radiant.seas.pdx.edu (131.252.208.212) 1.195 ms 1.221 ms 1.213 ms
 2 CORE1.net.pdx.edu (131.252.5.142) 8.308 ms 8.205 ms 8.100 ms
 3 131.252.5.213 (131.252.5.213) 0.507 ms 0.406 ms 0.357 ms
 4 google.nwax.net (198.32.195.34) 4.238 ms 4.272 ms 4.152 ms
 5 108.170.245.113 (108.170.245.113) 4.046 ms 4.197 ms 108.170.245.97 (108.170.245.97) 4.866 ms
 6 142.251.241.137 (142.251.241.137) 4.366 ms 4.368 ms 216.239.56.223 (216.239.56.223) 4.570 ms
 7 sea09s35-in-f4.1e100.net (142.251.215.228) 3.716 ms 4.165 ms 4.255 ms

```

```

Odin: srimel
traceroute to 142.251.111.104 (142.251.111.104), 30 hops max, 60 byte packets
 1 radiant.seas.pdx.edu (131.252.208.212) 0.866 ms 0.864 ms 0.919 ms
 2 CORE1.net.pdx.edu (131.252.5.142) 0.901 ms 0.819 ms 0.741 ms
 3 131.252.5.213 (131.252.5.213) 0.458 ms 0.482 ms 0.347 ms
 4 google.nwax.net (198.32.195.34) 3.763 ms 3.775 ms 4.096 ms
 5 74.125.243.194 (74.125.243.194) 4.808 ms 74.125.243.195 (74.125.243.195) 4.487 ms 74.125.243.194 (74.125.243.194) 5.220 ms
 6 142.251.235.210 (142.251.235.210) 26.230 ms 172.253.76.192 (172.253.76.192) 10.922 ms 10.696 ms
 7 192.178.74.222 (192.178.74.222) 51.605 ms 192.178.74.210 (192.178.74.210) 50.681 ms 192.178.74.212 (192.178.74.212) 87.900 ms
 8 192.178.72.195 (192.178.72.195) 59.589 ms 192.178.72.198 (192.178.72.198) 59.352 ms 192.178.72.195 (192.178.72.195) 59.768 ms
 9 * 192.178.81.232 (192.178.81.232) 73.423 ms *
10 142.250.209.59 (142.250.209.59) 72.941 ms 72.106 ms 142.250.209.110 (142.250.209.110) 72.542 ms
11 142.251.68.23 (142.251.68.23) 73.773 ms 142.251.68.9 (142.251.68.9) 71.741 ms 142.251.66.245 (142.251.66.245) 70.777 ms
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 bk-in-f104.1e100.net (142.251.111.104) 72.108 ms 71.829 ms 72.222 ms

```

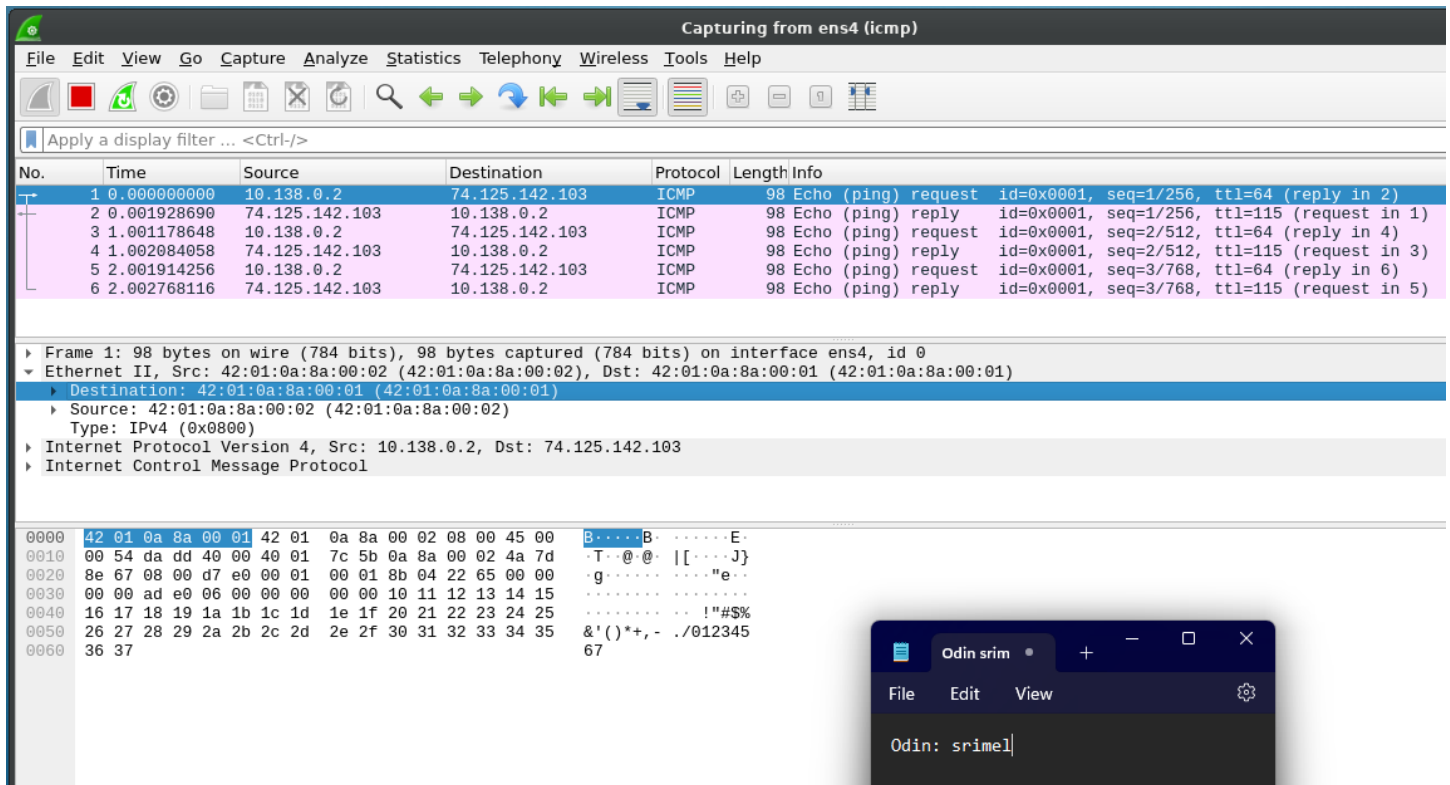
2.2.6-7: Wireshark Lab #3

IP address of VM:

- Public: 35.233.163.193
- Private: 10.138.0.2

Name of ethernet interface: ens4 10.138.2/32

Default router IP: 10.138.0.1



Capturing from ens4 (icmp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.138.0.2	74.125.142.103	ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 2)
2	0.001928690	74.125.142.103	10.138.0.2	ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=115 (request in 1)
3	1.001178648	10.138.0.2	74.125.142.103	ICMP	98	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 4)
4	1.002084058	74.125.142.103	10.138.0.2	ICMP	98	Echo (ping) reply id=0x0001, seq=2/512, ttl=115 (request in 3)
5	2.001914256	10.138.0.2	74.125.142.103	ICMP	98	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 6)
6	2.002768116	74.125.142.103	10.138.0.2	ICMP	98	Echo (ping) reply id=0x0001, seq=3/768, ttl=115 (request in 5)

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface ens4, id 0

Ethernet II, Src: 42:01:0a:8a:00:02 (42:01:0a:8a:00:02), 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:00:02 (42:01:0a:8a:00:02)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.138.0.2, Dst: 74.125.142.103

Internet Control Message Protocol

0000 42 01 0a 8a 00 01 42 01 0a 8a 00 02 08 00 45 00 B.....B.....E..

0010 00 54 da dd 40 00 40 01 7c 5b 0a 8a 00 02 4a 7d .T..@.. | [....J}

0020 8e 67 08 00 d7 e0 00 01 00 01 8b 04 22 65 00 00 .g....."e..

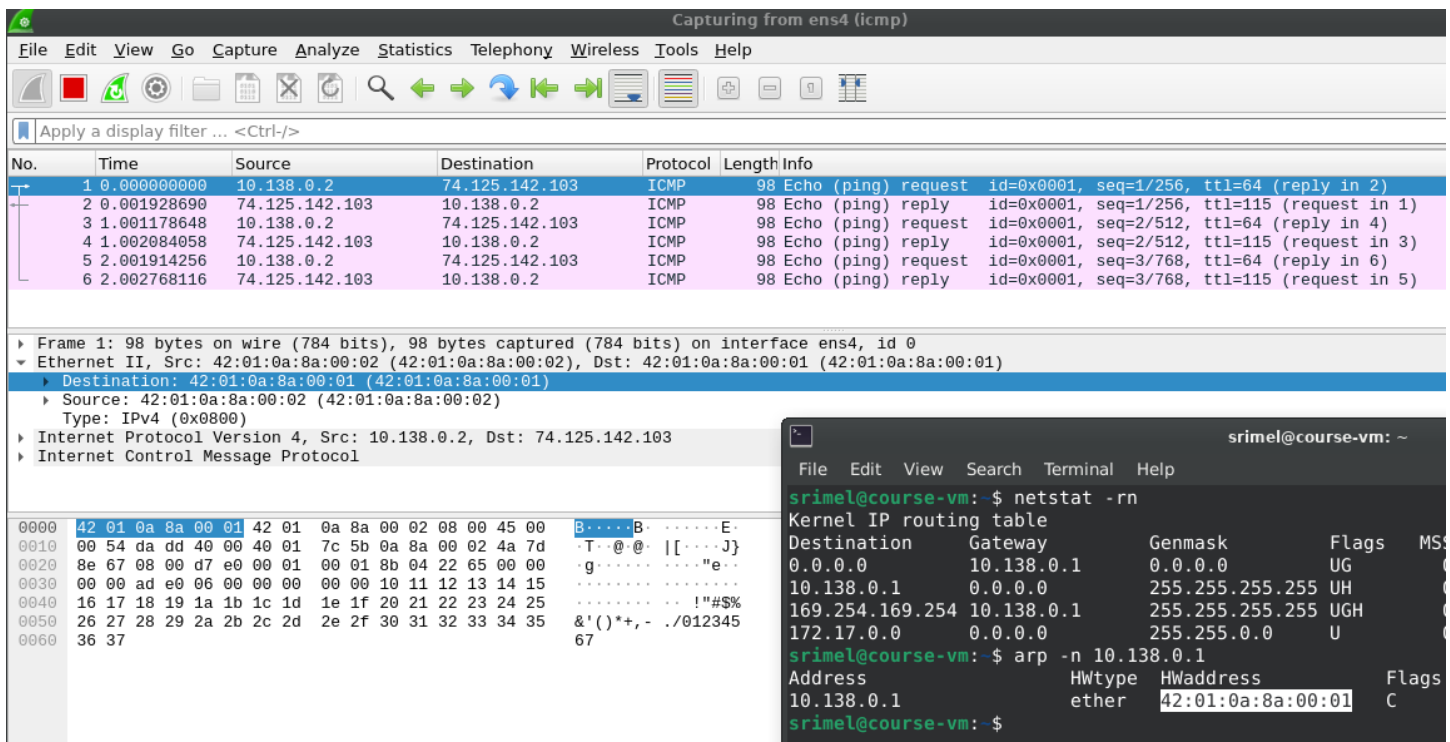
0030 00 00 ad e0 06 00 00 00 00 00 10 11 12 13 14 15 !"#\$\$%

0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 &'()*+,-./012345

0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 67

0060 36 37

For the first packet, the destination MAC address corresponds to the interface on the default router.



Capturing from ens4 (icmp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.138.0.2	74.125.142.103	ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 2)
2	0.001928690	74.125.142.103	10.138.0.2	ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=115 (request in 1)
3	1.001178648	10.138.0.2	74.125.142.103	ICMP	98	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 4)
4	1.002084058	74.125.142.103	10.138.0.2	ICMP	98	Echo (ping) reply id=0x0001, seq=2/512, ttl=115 (request in 3)
5	2.001914256	10.138.0.2	74.125.142.103	ICMP	98	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 6)
6	2.002768116	74.125.142.103	10.138.0.2	ICMP	98	Echo (ping) reply id=0x0001, seq=3/768, ttl=115 (request in 5)

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface ens4, id 0

Ethernet II, Src: 42:01:0a:8a:00:02 (42:01:0a:8a:00:02), 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:00:02 (42:01:0a:8a:00:02)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.138.0.2, Dst: 74.125.142.103

Internet Control Message Protocol

0000 42 01 0a 8a 00 01 42 01 0a 8a 00 02 08 00 45 00 B.....B.....E..

0010 00 54 da dd 40 00 40 01 7c 5b 0a 8a 00 02 4a 7d .T..@.. | [....J}

0020 8e 67 08 00 d7 e0 00 01 00 01 8b 04 22 65 00 00 .g....."e..

0030 00 00 ad e0 06 00 00 00 00 00 10 11 12 13 14 15 !"#\$\$%

0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 &'()*+,-./012345

0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 67

0060 36 37

```
srimel@course-vm: ~  
File Edit View Search Terminal Help  
srimel@course-vm:~$ netstat -rn  
Kernel IP routing table  
Destination Gateway Genmask Flags MSS  
0.0.0.0 10.138.0.1 0.0.0.0 UG  
10.138.0.1 0.0.0.0 255.255.255.255 UH  
169.254.169.254 10.138.0.1 255.255.255.255 UGH  
172.17.0.0 0.0.0.0 255.255.0.0 U  
srimel@course-vm:~$ arp -n 10.138.0.1  
Address HWtype HWaddress Flags  
10.138.0.1 ether 42:01:0a:8a:00:01 C  
srimel@course-vm:~$
```

For the second packet, the destination MAC address corresponds to the VM network interface.

The image displays a Wireshark packet capture from interface ens4 (icmp) and a terminal window showing network configuration and ARP table management.

Wireshark Packet Capture:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.138.0.2	74.125.142.103	ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 2)
2	0.001928690	74.125.142.103	10.138.0.2	ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=115 (request in 1)
3	1.001178648	10.138.0.2	74.125.142.103	ICMP	98	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 4)
4	1.002084058	74.125.142.103	10.138.0.2	ICMP	98	Echo (ping) reply id=0x0001, seq=2/512, ttl=115 (request in 3)
5	2.001914256	10.138.0.2	74.125.142.103	ICMP	98	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 6)
6	2.002768116	74.125.142.103	10.138.0.2	ICMP	98	Echo (ping) reply id=0x0001, seq=3/768, ttl=115 (request in 5)

Frame 2 Details:

- Ethernet II, Src: 42:01:0a:8a:00:01 (42:01:0a:8a:00:01), Dst: 42:01:0a:8a:00:02 (42:01:0a:8a:00:02)
- Destination: 42:01:0a:8a:00:02 (42:01:0a:8a:00:02)
- Source: 42:01:0a:8a:00:01 (42:01:0a:8a:00:01)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 74.125.142.103, Dst: 10.138.0.2
- Internet Control Message Protocol

Terminal Output:

```
srimel@course-vm: ~  
File Edit View Search Terminal Help  
srimel@course-vm:~$ arp -n 10.138.0.1  
Address HWtype HWaddress Flags  
10.138.0.1 ether 42:01:0a:8a:00:01 C  
srimel@course-vm:~$ arp -n 10.138.0.2  
10.138.0.2 (10.138.0.2) -- no entry  
srimel@course-vm:~$ ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue st  
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
inet 127.0.0.1/8 scope host lo  
valid lft forever preferred_lft forever  
inet6 ::1/128 scope host  
valid lft forever preferred_lft forever  
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 qdis  
link/ether 42:01:0a:8a:00:02 brd ff:ff:ff:ff:ff:ff  
inet 10.138.0.2/32 metric 100 scope global dynamic e  
valid lft 84935sec preferred_lft 84935sec  
inet6 fe80::4001:aff:fe8a:2/64 scope link  
valid lft forever preferred_lft forever
```

2.2.8: Network Recap Lab #4

IP address of srimel.oregonctf.org: 35.233.233.233

```
srimel@course-vm:~$ dig +tcp srimel.oregonctf.org  
  
;<<>> DiG 9.18.12-Ubuntu0.22.04.3-Ubuntu <<>> +tcp srimel.oregonctf.org  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63598  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:;; udp: 65494  
;; QUESTION SECTION:  
srimel.oregonctf.org. IN A  
  
;; ANSWER SECTION:  
srimel.oregonctf.org. 3573 IN A 35.233.233.233  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)  
;; WHEN: Sun Oct 08 01:47:52 UTC 2023  
;; MSG SIZE rcvd: 65
```

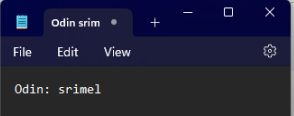
Deleting arp entry for default router:

```
srime1@course-vm:~$ arp -an
? (10.138.0.1) at 42:01:0a:8a:00:01 [ether] on ens4
srime1@course-vm:~$ sudo arp -d 10.138.0.1; arp -an
srime1@course-vm:~$
```

2.2.9-10: Collect trace / Analyze trace

No.	Time	Source	Destination	Protocol	Length	Info
2850	46.511525	10.138.0.2	169.254.169.254	DNS	110	Standard query 0x8bbc A course-vm.c.cloud-rimel-srime1.internal OPT
2851	46.511607	10.138.0.2	169.254.169.254	DNS	110	Standard query 0xc8bc AAAA course-vm.c.cloud-rimel-srime1.internal OPT
2852	46.517744	169.254.169.254	10.138.0.2	DNS	199	Standard query response 0xc8bc AAAA course-vm.c.cloud-rimel-srime1.internal SOA ns.global.qcdns-prod.internal OPT
2853	46.517925	169.254.169.254	10.138.0.2	DNS	126	Standard query response 0x8bbc A course-vm.c.cloud-rimel-srime1.internal A 10.138.0.2 OPT
2854	46.529069	42:01:0a:8a:00:02	Broadcast	ARP	42	Who has 10.138.0.1? Tell 10.138.0.2
2855	46.545238	42:01:0a:8a:00:01	42:01:0a:8a:00:02	ARP	42	10.138.0.1 is at 42:01:0a:8a:00:01
2856	46.545246	10.138.0.2	169.254.169.254	DNS	91	Standard query 0x222d AAAA srime1.oregonctf.org OPT
2872	46.618949	169.254.169.254	10.138.0.2	DNS	173	Standard query response 0x222d AAAA srime1.oregonctf.org SOA ns-cloud-d1.googledomains.com OPT
2873	46.619358	10.138.0.2	35.233.233.233	TCP	74	40098 → 80 [SYN] Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM=1 TSval=3006037289 TSecr=0 WS=128
2874	46.620162	35.233.233.233	10.138.0.2	TCP	74	80 → 40098 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1420 SACK_PERM=1 TSval=178854269 TSecr=3006037289 WS=128
2875	46.620130	10.138.0.2	35.233.233.233	TCP	66	40098 → 80 [ACK] Seq=1 Ack=1 Win=65408 Len=0 TSval=3006037290 TSecr=178854269
2876	46.620201	10.138.0.2	35.233.233.233	HTTP	201	GET / HTTP/1.1
2877	46.620664	35.233.233.233	10.138.0.2	TCP	66	80 → 40098 [ACK] Seq=1 Ack=136 Win=64640 Len=0 TSval=178854270 TSecr=3006037290
2878	46.620824	35.233.233.233	10.138.0.2	TCP	7106	80 → 40098 [PSH, ACK] Seq=1 Ack=136 Win=64640 Len=7040 TSval=178854270 TSecr=3006037290 [TCP segment of a reassembled PDU]
2879	46.620824	35.233.233.233	10.138.0.2	HTTP	792	HTTP/1.1 200 OK (text/html)
2880	46.620842	10.138.0.2	35.233.233.233	TCP	66	40098 → 80 [ACK] Seq=136 Ack=7041 Win=61956 Len=0 TSval=3006037291 TSecr=178854270
2881	46.620849	10.138.0.2	35.233.233.233	TCP	66	40098 → 80 [ACK] Seq=136 Ack=7767 Win=60416 Len=0 TSval=3006037291 TSecr=178854270
2882	46.621822	10.138.0.2	35.233.233.233	TCP	66	40098 → 80 [FIN, ACK] Seq=136 Ack=7767 Win=64128 Len=0 TSval=3006037292 TSecr=178854270
2883	46.623013	35.233.233.233	10.138.0.2	TCP	66	80 → 40098 [FIN, ACK] Seq=7767 Ack=137 Win=64640 Len=0 TSval=178854272 TSecr=3006037292
2884	46.623028	10.138.0.2	35.233.233.233	TCP	66	40098 → 80 [ACK] Seq=137 Ack=7768 Win=64128 Len=0 TSval=3006037293 TSecr=178854272
2958	50.469953	169.254.169.254	10.138.0.2	HTTP/J..	2193	[TCP ACKed unseen segment] HTTP/1.1 200 OK, JavaScript Object Notation (application/json)
2960	50.470343	10.138.0.2	169.254.169.254	HTTP	280	GET /computeMetadata/v1/?recursive=true&alt=json&wait_for_change=true&last_etag=1c812f1437177f8&timeout_sec=60 HTTP/1.1
2982	53.564743	169.254.169.254	10.138.0.2	HTTP/J..	2193	[TCP ACKed unseen segment] HTTP/1.1 200 OK, JavaScript Object Notation (application/json)
2984	53.565333	10.138.0.2	169.254.169.254	HTTP	281	GET /computeMetadata/v1/?recursive=true&alt=json&wait_for_change=true&last_etag=1c812f1437177f8 HTTP/1.1

Frame 2850: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: 42:01:0a:8a:00:02 (42:01:0a:8a:00:02), Dst: 42:01:0a:8a:00:01 (42:01:0a:8a:00:01)
Internet Protocol Version 4, Src: 10.138.0.2, Dst: 169.254.169.254
User Datagram Protocol, Src Port: 56096, Dst Port: 53
Domain Name System (query)



ARP

- Packet numbers 2854-5 are attempting to get hardware address of default router
- The default router hardware address: 42:01:0a:8a:00:01

DNS

- Packets 2856-7 correspond to the DNS request for the website
- IP address of the local DNS server being queried: 169.254.169.254

TCP

- Packets 2873-5 seem to correspond to the initial TCP handshake for the web request
- Time for initial TCP handshake: 0.000772

HTTP

- Packets 2876, 2879 seem to correspond with the first HTTP request and response
- Time to process the HTTP request after the handshake: 0.000623