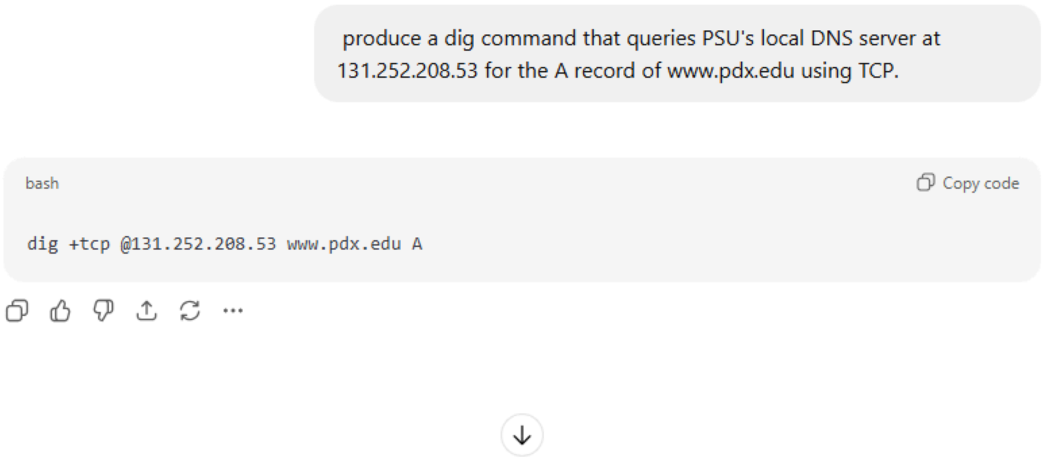
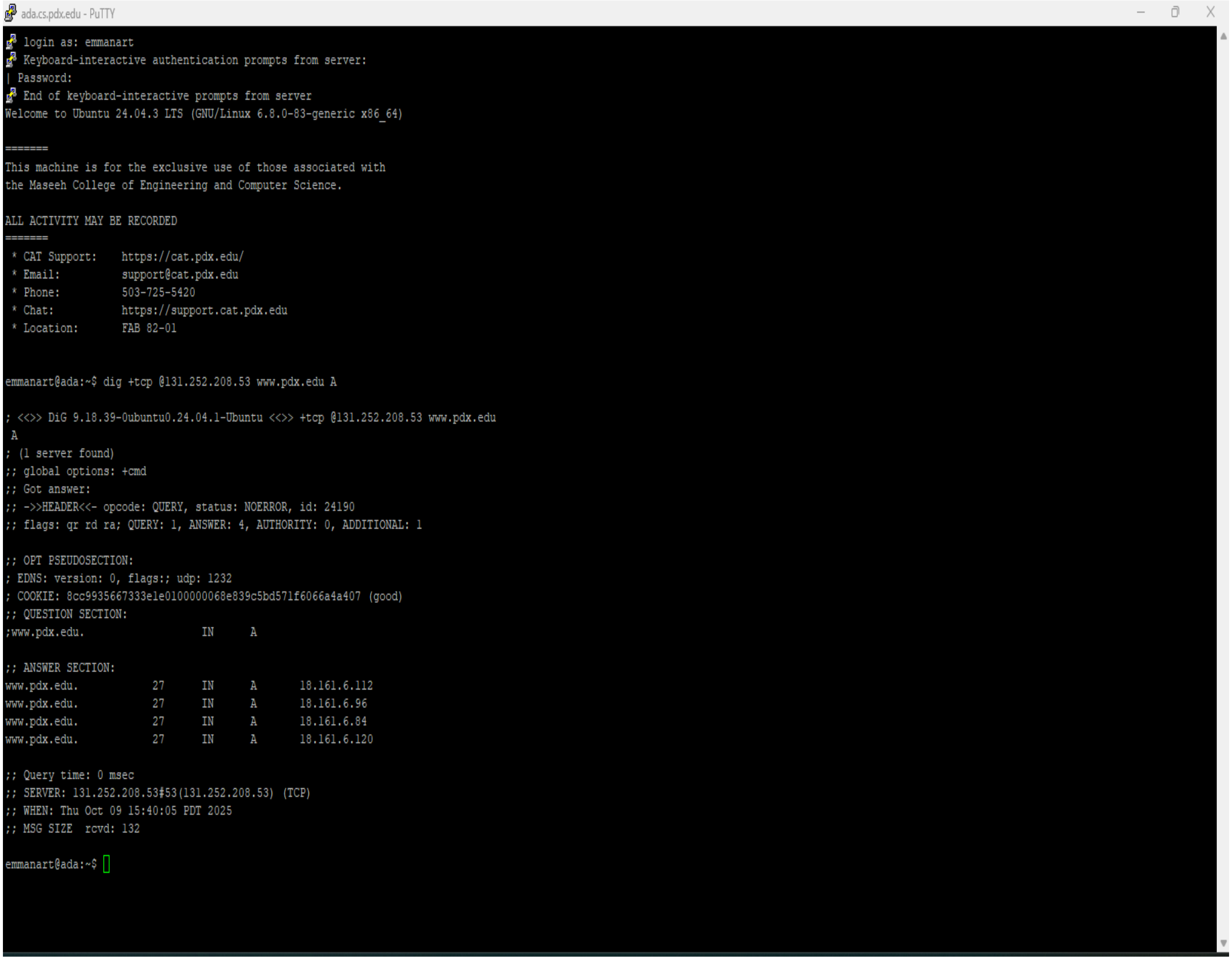
- **Take a screenshot of the prompt and the dig command produced.**



produce a dig command that queries PSU's local DNS server at 131.252.208.53 for the A record of www.pdx.edu using TCP.

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

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



```
login as: emmanart
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-83-generic x86_64)

=======
This machine is for the exclusive use of those associated with
the Maseeh College of Engineering and Computer Science.

ALL ACTIVITY MAY BE RECORDED
=======
 * CAT Support:    https://cat.pdx.edu/
 * Email:          support@cat.pdx.edu
 * Phone:          503-725-5420
 * Chat:           https://support.cat.pdx.edu
 * Location:       FAB 82-01


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

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> +tcp @131.252.208.53 www.pdx.edu
 A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24190
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8cc9935667333e1e0100000068e839c5bd571f6066a4a407 (good)
;; QUESTION SECTION:
;www.pdx.edu.                   IN      A

;; ANSWER SECTION:
www.pdx.edu.            27      IN      A       18.161.6.112
www.pdx.edu.            27      IN      A       18.161.6.96
www.pdx.edu.            27      IN      A       18.161.6.84
www.pdx.edu.            27      IN      A       18.161.6.120

;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (TCP)
;; WHEN: Thu Oct 09 15:40:05 PDT 2025
;; MSG SIZE  rcvd: 132

emmanart@ada:~$ 
```

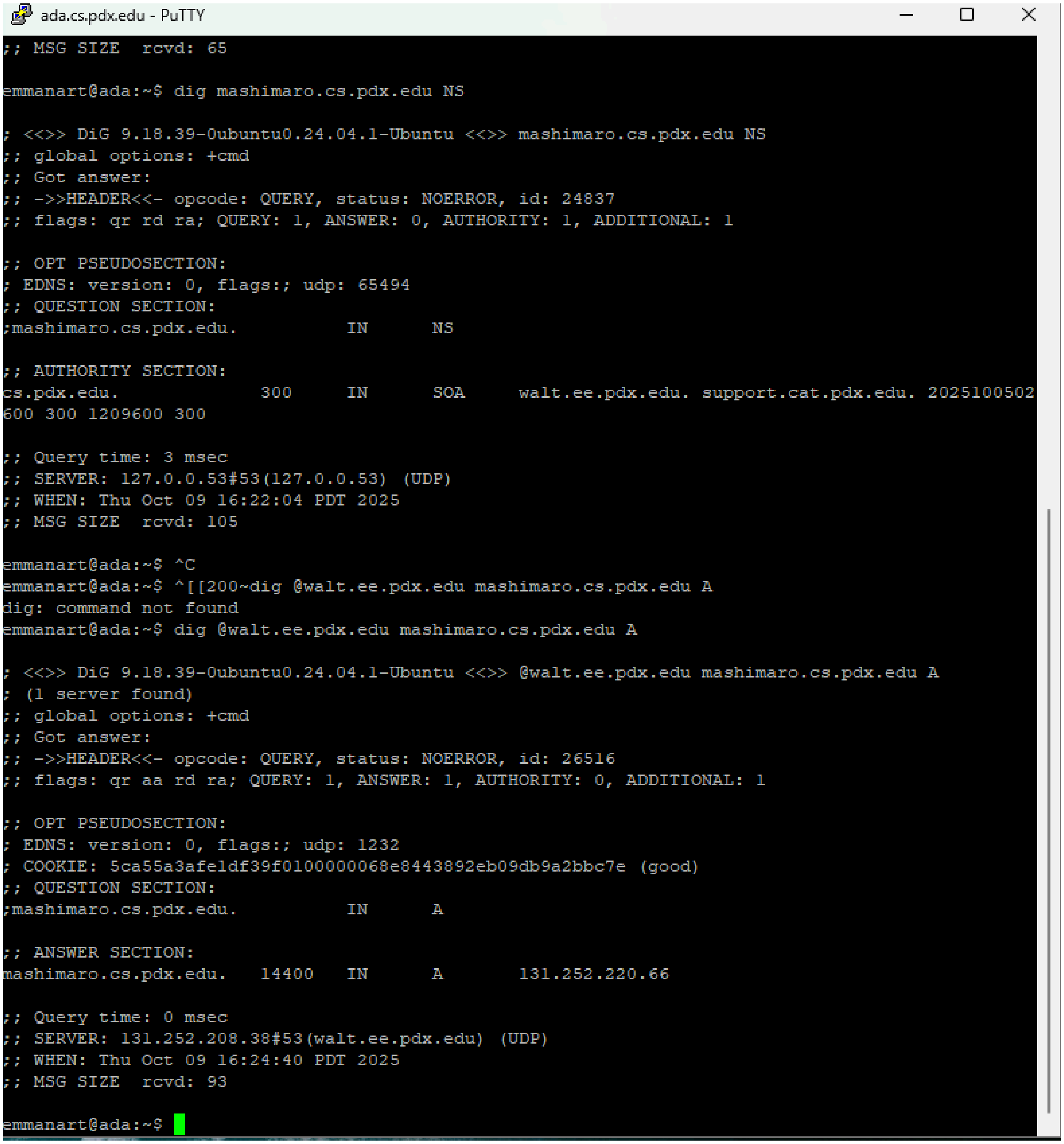
- What cloud provider hosts the web site for www.pdx.edu?

  Amazon Web Services

- What cloud provider handles mail for pdx.edu?

  Google

- Take a screenshot of the results for both records for your lab notebook for mashimaro.cs.pdx.edu



```
;; MSG SIZE  rcvd: 65

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

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> mashimaro.cs.pdx.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24837
;; 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. 2025100502
600 300 1209600 300

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Oct 09 16:22:04 PDT 2025
;; MSG SIZE  rcvd: 105

emmanart@ada:~$ ^C
emmanart@ada:~$ ^[[200~dig @walt.ee.pdx.edu mashimaro.cs.pdx.edu A
dig: command not found
emmanart@ada:~$ dig @walt.ee.pdx.edu mashimaro.cs.pdx.edu A

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> @walt.ee.pdx.edu mashimaro.cs.pdx.edu A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26516
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 5ca55a3afe1df39f0100000068e8443892eb09db9a2bbc7e (good)
;; QUESTION SECTION:
;mashimaro.cs.pdx.edu.          IN      A

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

;; Query time: 0 msec
;; SERVER: 131.252.208.38#53(walt.ee.pdx.edu) (UDP)
;; WHEN: Thu Oct 09 16:24:40 PDT 2025
;; MSG SIZE  rcvd: 93

emmanart@ada:~$ 
```

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

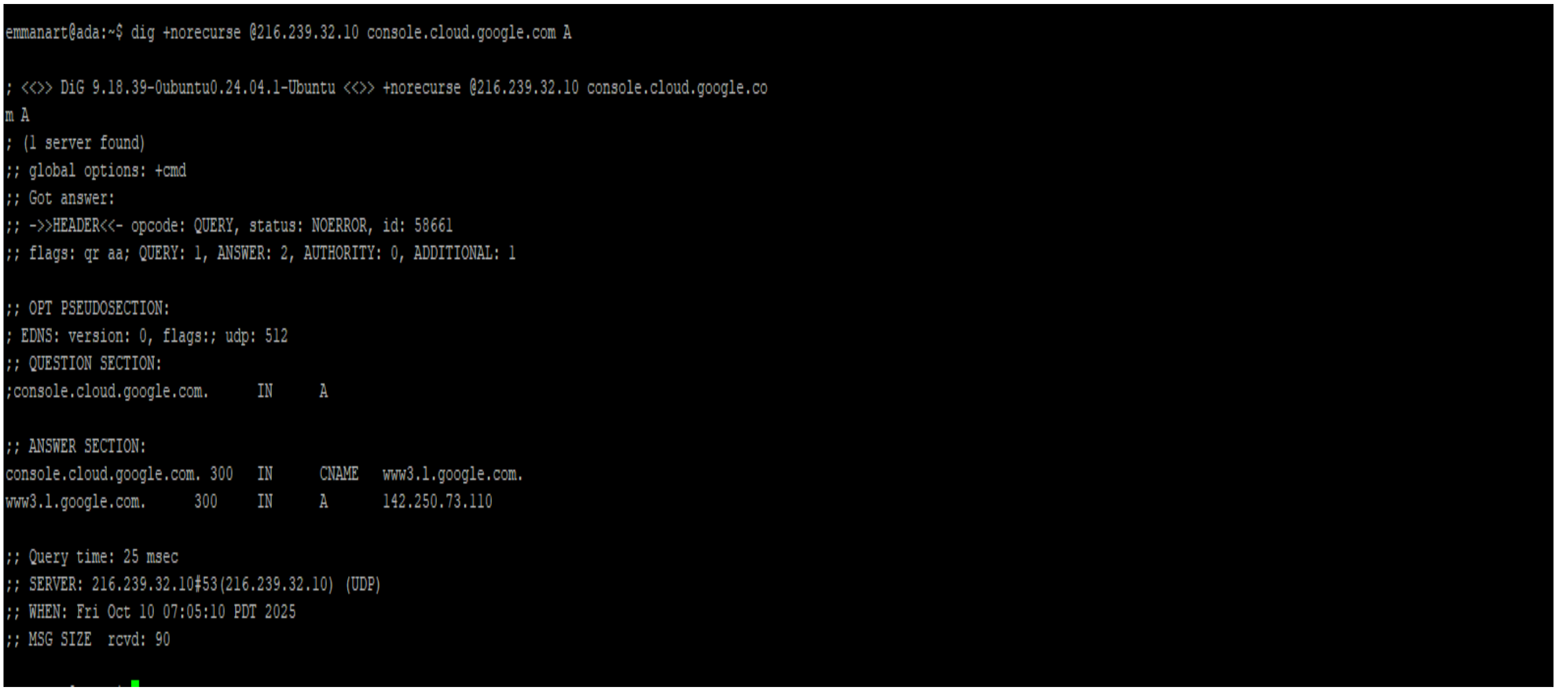
dig f.root-servers.net A

dig +norecurse @192.5.5.241 console.cloud.google.com A

dig +norecurse@192.5.6.30 console.cloud.google.com A dig +norecurse@216.239.32.10 console.cloud.google.com A

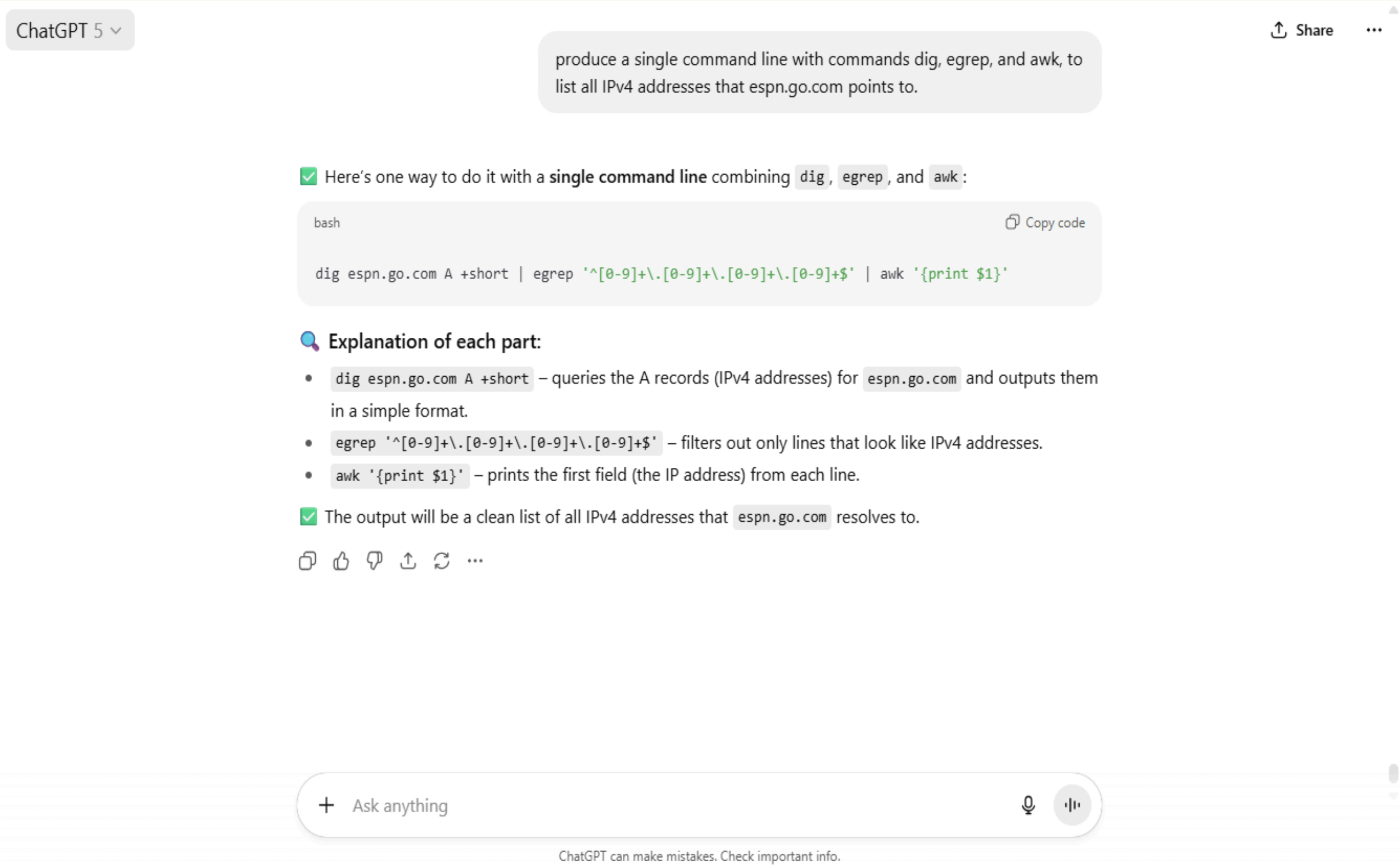
192.5.5.241

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



```
emmanart@ada:~$ dig +norecurse @216.239.32.10 console.cloud.google.com A

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> +norecurse @216.239.32.10 console.cloud.google.co
m A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58661
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
console.cloud.google.com. 300   IN      CNAME   www3.l.google.com.
www3.l.google.com.      300     IN      A       142.250.73.110

;; Query time: 25 msec
;; SERVER: 216.239.32.10#53(216.239.32.10) (UDP)
;; WHEN: Fri Oct 10 07:05:10 PDT 2025
;; MSG SIZE  rcvd: 90
```

- Take a screenshot of the prompt and the command produced that lists all IPv4 addresses that espn.go.com points to.



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

✅ Here's one way to do it with a **single command line** combining `dig`, `egrep`, and `awk`:

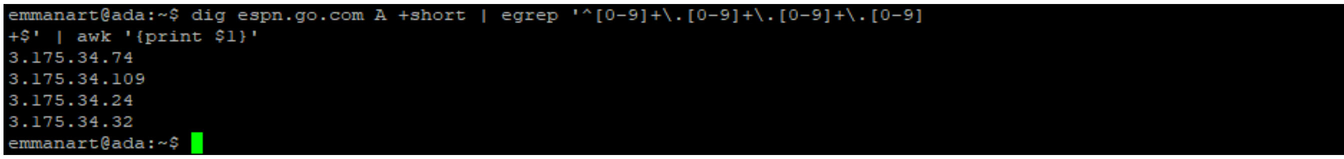
```bash
dig espn.go.com A +short | egrep '^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$' | awk '{print $1}'
```

🔍 **Explanation of each part:**

- `dig espn.go.com A +short` – queries the A records (IPv4 addresses) for `espn.go.com` and outputs them in a simple format.
- `egrep '^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$'` – filters out only lines that look like IPv4 addresses.
- `awk '{print $1}'` – prints the first field (the IP address) from each line.

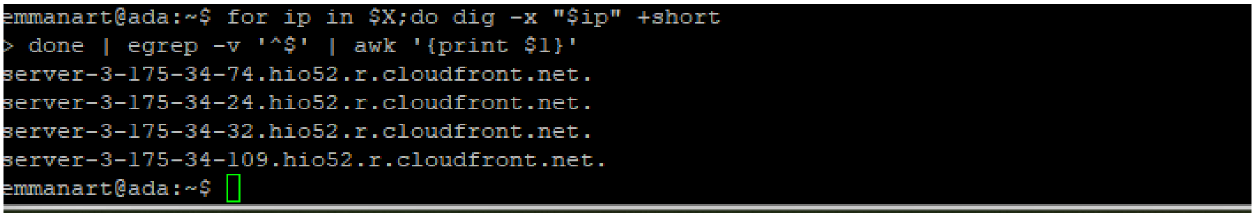
✅ The output will be a clean list of all IPv4 addresses that `espn.go.com` resolves to.

- Take a screenshot of its results of the dig command for espn go for your lab notebook of the above



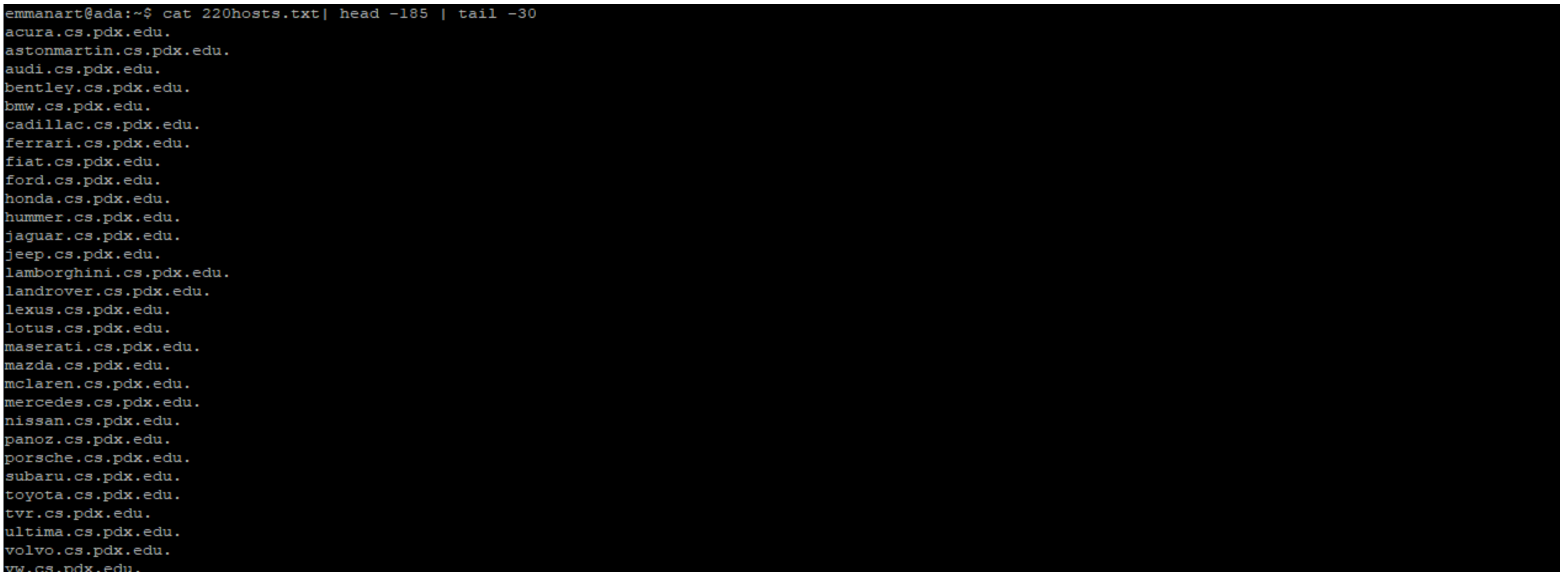
```
emmanart@ada:~$ dig espn.go.com A +short | egrep '^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]
+$' | awk '{print $1}'
3.175.34.74
3.175.34.109
3.175.34.24
3.175.34.32
emmanart@ada:~$
```

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



```
emmanart@ada:~$ for ip in $X;do dig -x "$ip" +short
> done | egrep -v '^$' | awk '{print $1}'
server-3-175-34-74.hio52.r.cloudfront.net.
server-3-175-34-24.hio52.r.cloudfront.net.
server-3-175-34-32.hio52.r.cloudfront.net.
server-3-175-34-109.hio52.r.cloudfront.net.
emmanart@ada:~$
```

- Take a screenshot of the results in your lab notebook (car manufacturers)



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

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

  For 131.252.208.53, it's Portland State University, Portland Oregon. For 198.82.247.66., it's Virginia Polytechnic Institute and State University in BlacksBurg, Virginia

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

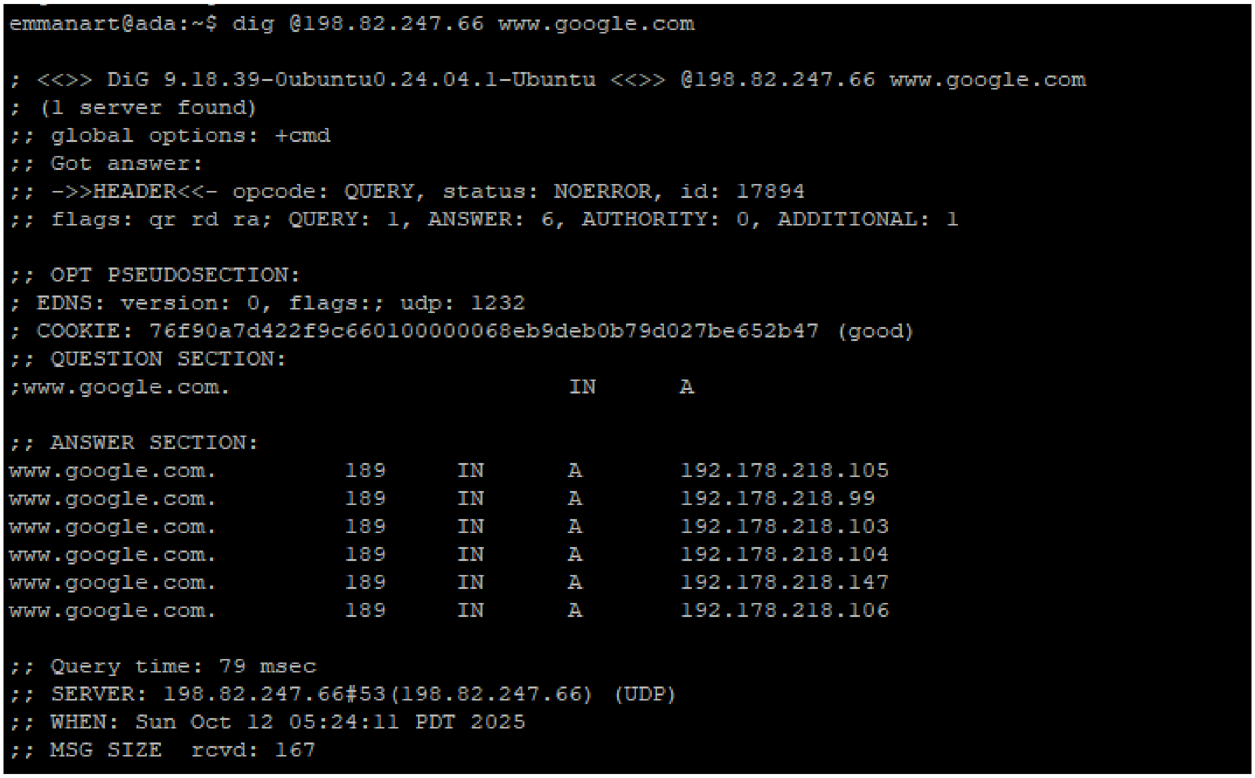
  For the Portland State University address resolution for google, one ip address at the end of the resolution was 142.250.217.100 . For the Virginia Polytechnic address resolution for google, one ip address at the end of the resolution was 192.178.218.105

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

  For 142.250.217.100 it's Seattle Washington and for 192.178.218.105 it's Yuki Japan, Leesburg Virginia US, Mountain View California US

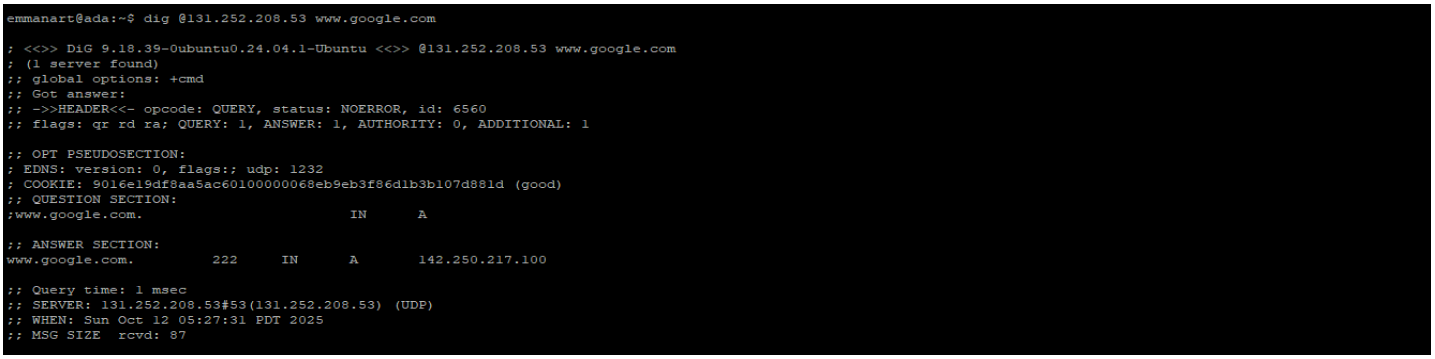
- Take a screenshot of the results for your lab notebook.

  Virginia



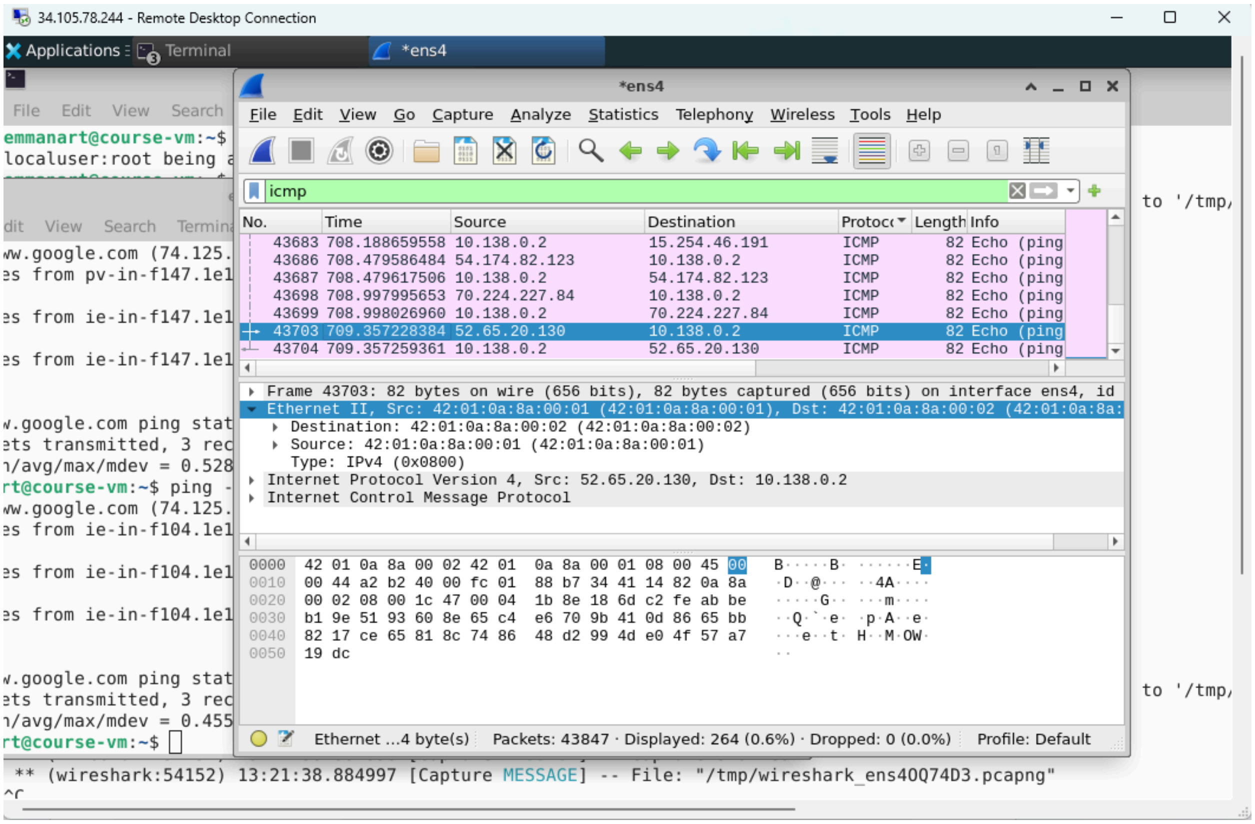
```
emmanart@ada:~$ dig @198.82.247.66 www.google.com

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> @198.82.247.66 www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17894
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 76f90a7d422f9c660100000068eb9deb0b79d027be652b47 (good)
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         189     IN      A       192.178.218.105
www.google.com.         189     IN      A       192.178.218.99
www.google.com.         189     IN      A       192.178.218.103
www.google.com.         189     IN      A       192.178.218.104
www.google.com.         189     IN      A       192.178.218.147
www.google.com.         189     IN      A       192.178.218.106

;; Query time: 79 msec
;; SERVER: 198.82.247.66#53(198.82.247.66) (UDP)
;; WHEN: Sun Oct 12 05:24:11 PDT 2025
;; MSG SIZE  rcvd: 167
```

Pdx



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

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> @131.252.208.53 www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6560
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9016e19df8aa5ac60100000068eb9eb3f86d1b3b107d881d (good)
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         222     IN      A       142.250.217.100

;; Query time: 1 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Sun Oct 12 05:27:31 PDT 2025
;; MSG SIZE  rcvd: 87
```

- In a terminal, using commands from prior labs, find the addresses and interfaces on the VM. Make a note of:
    1. The IP address of the VM: 10.138.0.2/32
    2. The name of the local virtual ethernet interface: ens4
    3. The IP address of the default router: 10.138.0.1
- Take a screenshot of the bytes in the packet dump window as shown below


34.105.78.244 - Remote Desktop Connection
Applications
Terminal
*ens4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
emmanart@course-vm:~$
localuser:root being a
```

```
ww.google.com (74.125.
es from pv-in-f147.1e1

es from ie-in-f147.1e1

es from ie-in-f147.1e1

w.google.com ping stat
ets transmitted, 3 rec
n/avg/max/mdev = 0.528
rt@course-vm:~$ ping -
ww.google.com (74.125.
es from ie-in-f104.1e1

es from ie-in-f104.1e1

es from ie-in-f104.1e1

w.google.com ping stat
ets transmitted, 3 rec
n/avg/max/mdev = 0.455
rt@course-vm:~$
```

icmp

```
No.   Time          Source          Destination     Protocol Length Info
43683 708.188659558 10.138.0.2      15.254.46.191   ICMP     82 Echo (ping
43686 708.479586484 54.174.82.123   10.138.0.2      ICMP     82 Echo (ping
43687 708.479617506 10.138.0.2      54.174.82.123   ICMP     82 Echo (ping
43698 708.997995653 70.224.227.84   10.138.0.2      ICMP     82 Echo (ping
43699 708.998026960 10.138.0.2      70.224.227.84   ICMP     82 Echo (ping
43703 709.357228384 52.65.20.130    10.138.0.2      ICMP     82 Echo (ping
43704 709.357259361 10.138.0.2      52.65.20.130    ICMP     82 Echo (ping
```

```
Frame 43703: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface ens4, id
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:
    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: 52.65.20.130, Dst: 10.138.0.2
Internet Control Message Protocol
```

```
0000  42 01 0a 8a 00 02 42 01  0a 8a 00 01 08 00 45 00   B·····B· ······E·
0010  00 44 a2 b2 40 00 fc 01  88 b7 34 41 14 82 0a 8a   ·D··@··· ··4A····
0020  00 02 08 00 1c 47 00 04  1b 8e 18 6d c2 fe ab be   ·····G·· ···m····
0030  b1 9e 51 93 60 8e 65 c4  e6 70 9b 41 0d 86 65 bb   ··Q·`·e· ·p·A··e·
0040  82 17 ce 65 81 8c 74 86  48 d2 99 4d e0 4f 57 a7   ···e··t· H··M·OW·
0050  19 dc                                              ··
```

Ethernet ...4 byte(s) | Packets: 43847 · Displayed: 264 (0.6%) · Dropped: 0 (0.0%) | Profile: Default

```
to '/tmp/
to '/tmp/
** (wireshark:54152) 13:21:38.884997 [Capture MESSAGE] -- File: "/tmp/wireshark_ens40Q74D3.pcapng"
^C
```

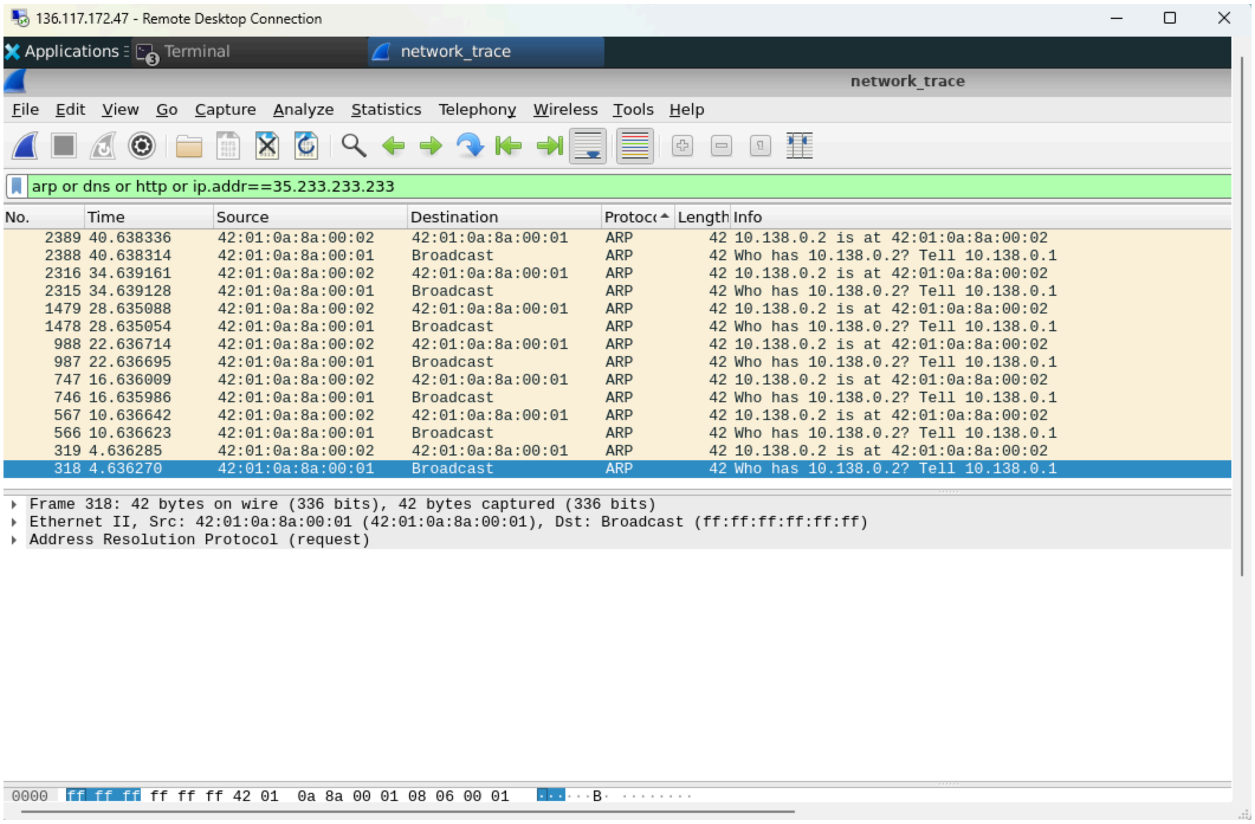
- Does the destination MAC address correspond to an interface on the VM, an interface on the default router or an interface on Google's web site? It corresponds to the interface of the default router
- Does the destination MAC address correspond to an interface on the VM, an interface on the default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

  It corresponds to the interface of the VM

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

  35.233.233.233

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

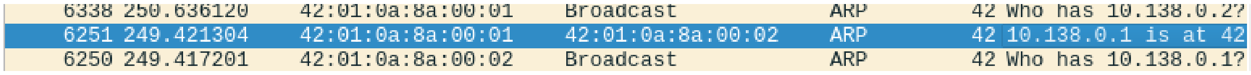

136.117.172.47 - Remote Desktop Connection
Applications
Terminal
network_trace
network_trace
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

```
No.   Time       Source             Destination        Protoc  Length Info
 2389 40.638336  42:01:0a:8a:00:02  42:01:0a:8a:00:01  ARP        42 10.138.0.2 is at 42:01:0a:8a:00:02
 2388 40.638314  42:01:0a:8a:00:01  Broadcast          ARP        42 Who has 10.138.0.2? Tell 10.138.0.1
 2316 34.639161  42:01:0a:8a:00:02  42:01:0a:8a:00:01  ARP        42 10.138.0.2 is at 42:01:0a:8a:00:02
 2315 34.639128  42:01:0a:8a:00:01  Broadcast          ARP        42 Who has 10.138.0.2? Tell 10.138.0.1
 1479 28.635088  42:01:0a:8a:00:02  42:01:0a:8a:00:01  ARP        42 10.138.0.2 is at 42:01:0a:8a:00:02
 1478 28.635054  42:01:0a:8a:00:01  Broadcast          ARP        42 Who has 10.138.0.2? Tell 10.138.0.1
  988 22.636714  42:01:0a:8a:00:02  42:01:0a:8a:00:01  ARP        42 10.138.0.2 is at 42:01:0a:8a:00:02
  987 22.636695  42:01:0a:8a:00:01  Broadcast          ARP        42 Who has 10.138.0.2? Tell 10.138.0.1
  747 16.636009  42:01:0a:8a:00:02  42:01:0a:8a:00:01  ARP        42 10.138.0.2 is at 42:01:0a:8a:00:02
  746 16.635986  42:01:0a:8a:00:01  Broadcast          ARP        42 Who has 10.138.0.2? Tell 10.138.0.1
  567 10.636642  42:01:0a:8a:00:02  42:01:0a:8a:00:01  ARP        42 10.138.0.2 is at 42:01:0a:8a:00:02
  566 10.636623  42:01:0a:8a:00:01  Broadcast          ARP        42 Who has 10.138.0.2? Tell 10.138.0.1
  319 4.636285   42:01:0a:8a:00:02  42:01:0a:8a:00:01  ARP        42 10.138.0.2 is at 42:01:0a:8a:00:02
  318 4.636270   42:01:0a:8a:00:01  Broadcast          ARP        42 Who has 10.138.0.2? Tell 10.138.0.1

 Frame 318: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
 Ethernet II, Src: 42:01:0a:8a:00:01 (42:01:0a:8a:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 42 01  0a 8a 00 01 08 06 00 01   ······B· ········
```

ARP

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



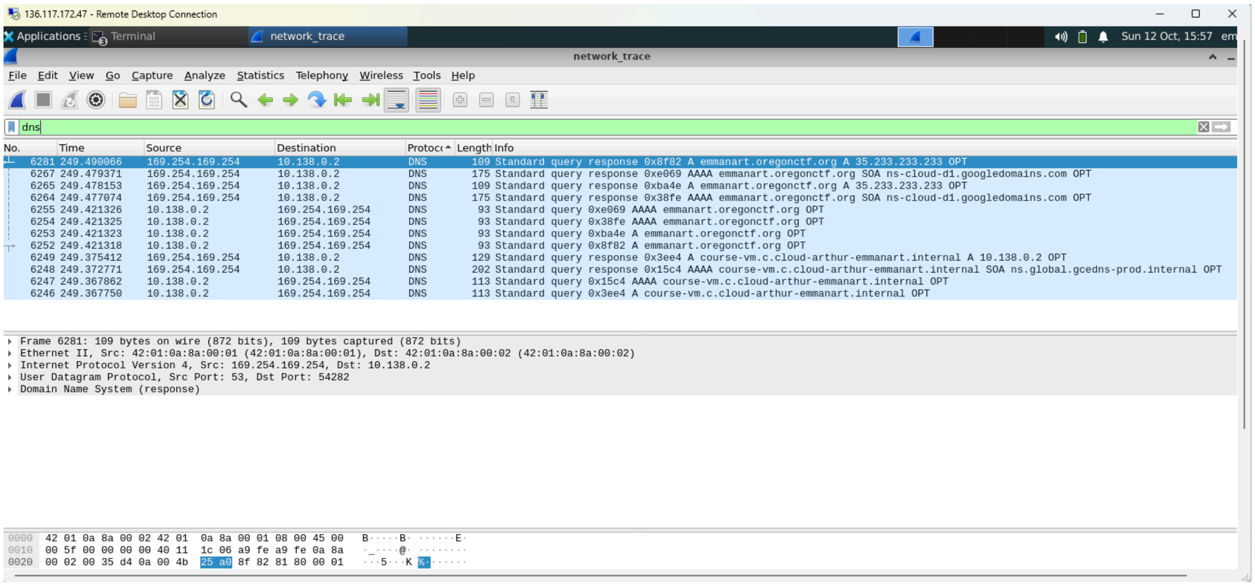
```
6338 250.636120   42:01:0a:8a:00:01   Broadcast           ARP        42 Who has 10.138.0.2?
6251 249.421304   42:01:0a:8a:00:01   42:01:0a:8a:00:02   ARP        42 10.138.0.1 is at 42
6250 249.417201   42:01:0a:8a:00:02   Broadcast           ARP        42 Who has 10.138.0.1?
```

Packet numbers: 6250 (ARP request) and 6251 (ARP reply)

- What is this hardware address?

Hardware address of the default router: 42:01:0a:8a:00:01

DNS


136.117.172.47 - Remote Desktop Connection
Applications
Terminal
network_trace
Sun 12 Oct, 15:57
network_trace
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns
```

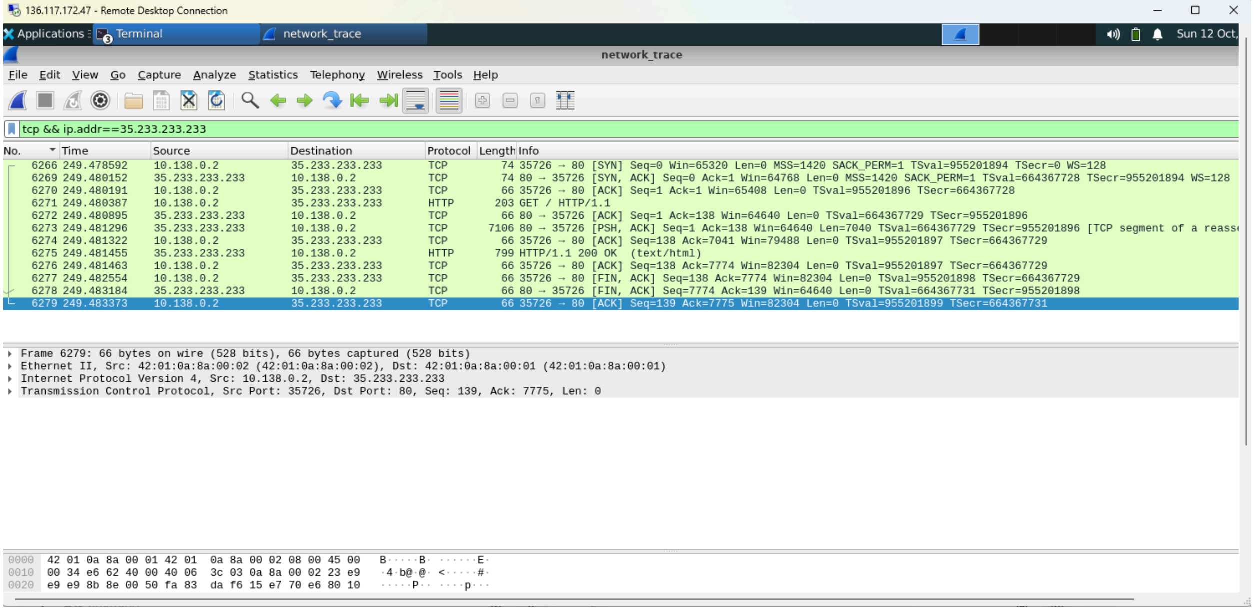
```
No.   Time       Source           Destination      Protocol Length Info
6281 249.490066 169.254.169.254 10.138.0.2       DNS      109 Standard query response 0x8f82 A emmanart.oregonctf.org A 35.233.233.233 OPT
6267 249.479371 169.254.169.254 10.138.0.2       DNS      175 Standard query response 0xe069 AAAA emmanart.oregonctf.org SOA ns-cloud-d1.googledomains.com OPT
6265 249.478153 169.254.169.254 10.138.0.2       DNS      109 Standard query response 0xba4e A emmanart.oregonctf.org A 35.233.233.233 OPT
6264 249.477074 169.254.169.254 10.138.0.2       DNS      175 Standard query response 0x38fe AAAA emmanart.oregonctf.org SOA ns-cloud-d1.googledomains.com OPT
6255 249.421326 10.138.0.2      169.254.169.254  DNS       93 Standard query 0xe069 AAAA emmanart.oregonctf.org OPT
6254 249.421325 10.138.0.2      169.254.169.254  DNS       93 Standard query 0x38fe AAAA emmanart.oregonctf.org OPT
6253 249.421323 10.138.0.2      169.254.169.254  DNS       93 Standard query 0xba4e A emmanart.oregonctf.org OPT
6252 249.421318 10.138.0.2      169.254.169.254  DNS       93 Standard query 0x8f82 A emmanart.oregonctf.org OPT
6249 249.375412 169.254.169.254 10.138.0.2       DNS      129 Standard query response 0x3ee4 A course-vm.c.cloud-arthur-emmanart.internal A 10.138.0.2 OPT
6248 249.372771 169.254.169.254 10.138.0.2       DNS      202 Standard query response 0x15c4 AAAA course-vm.c.cloud-arthur-emmanart.internal SOA ns.global.gcedns-prod.internal OPT
6247 249.367862 10.138.0.2      169.254.169.254  DNS      113 Standard query 0x15c4 AAAA course-vm.c.cloud-arthur-emmanart.internal OPT
6246 249.367750 10.138.0.2      169.254.169.254  DNS      113 Standard query 0x3ee4 A course-vm.c.cloud-arthur-emmanart.internal OPT
```

```
▸ Frame 6281: 109 bytes on wire (872 bits), 109 bytes captured (872 bits)
▸ 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)
▸ Internet Protocol Version 4, Src: 169.254.169.254, Dst: 10.138.0.2
▸ User Datagram Protocol, Src Port: 53, Dst Port: 54282
▸ Domain Name System (response)
```

```
0000  42 01 0a 8a 00 02 42 01  0a 8a 00 01 08 00 45 00   B·····B· ······E·
0010  00 5f 00 00 00 00 40 11  1c 06 a9 fe a9 fe 0a 8a   ·_····@· ········
0020  00 02 00 35 d4 0a 00 4b  25 a0 8f 82 81 80 00 01   ···5···K %·······
```

- What packet numbers in the trace correspond to the DNS request for the web site? Packet 6246, 6247, 6252, 6253, 6255
- What is the IP address of the local DNS server being queried? 169.254.169.254

TCP

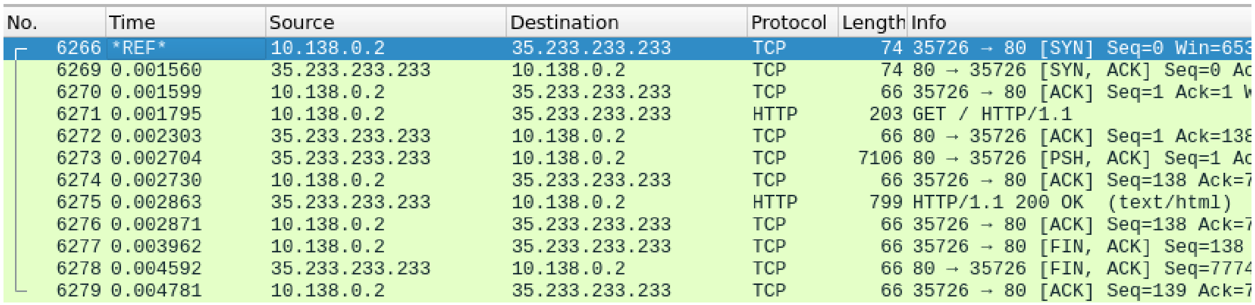

136.117.172.47 - Remote Desktop Connection
Applications
Terminal
network_trace
Sun 12 Oct,
network_trace
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp && ip.addr==35.233.233.233
```

```
No.   Time       Source          Destination     Protocol Length Info
6266 249.478592 10.138.0.2      35.233.233.233  TCP       74 35726 → 80 [SYN] Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM=1 TSval=955201894 TSecr=0 WS=128
6269 249.480152 35.233.233.233  10.138.0.2      TCP       74 80 → 35726 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1420 SACK_PERM=1 TSval=664367728 TSecr=955201894 WS=128
6270 249.480191 10.138.0.2      35.233.233.233  TCP       66 35726 → 80 [ACK] Seq=1 Ack=1 Win=65408 Len=0 TSval=955201896 TSecr=664367728
6271 249.480387 10.138.0.2      35.233.233.233  HTTP     203 GET / HTTP/1.1
6272 249.480895 35.233.233.233  10.138.0.2      TCP       66 80 → 35726 [ACK] Seq=1 Ack=138 Win=64640 Len=0 TSval=664367729 TSecr=955201896
6273 249.481296 35.233.233.233  10.138.0.2      TCP     7106 80 → 35726 [PSH, ACK] Seq=1 Ack=138 Win=64640 Len=7040 TSval=664367729 TSecr=955201896 [TCP segment of a reass
6274 249.481322 10.138.0.2      35.233.233.233  TCP       66 35726 → 80 [ACK] Seq=138 Ack=7041 Win=79488 Len=0 TSval=955201897 TSecr=664367729
6275 249.481455 35.233.233.233  10.138.0.2      HTTP     799 HTTP/1.1 200 OK  (text/html)
6276 249.481463 10.138.0.2      35.233.233.233  TCP       66 35726 → 80 [ACK] Seq=138 Ack=7774 Win=82304 Len=0 TSval=955201897 TSecr=664367729
6277 249.482554 10.138.0.2      35.233.233.233  TCP       66 35726 → 80 [FIN, ACK] Seq=138 Ack=7774 Win=82304 Len=0 TSval=955201898 TSecr=664367729
6278 249.483184 35.233.233.233  10.138.0.2      TCP       66 80 → 35726 [FIN, ACK] Seq=7774 Ack=139 Win=64640 Len=0 TSval=664367731 TSecr=955201898
6279 249.483373 10.138.0.2      35.233.233.233  TCP       66 35726 → 80 [ACK] Seq=139 Ack=7775 Win=82304 Len=0 TSval=955201899 TSecr=664367731
```

```
▸ Frame 6279: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 35.233.233.233
▸ Transmission Control Protocol, Src Port: 35726, Dst Port: 80, Seq: 139, Ack: 7775, Len: 0
```

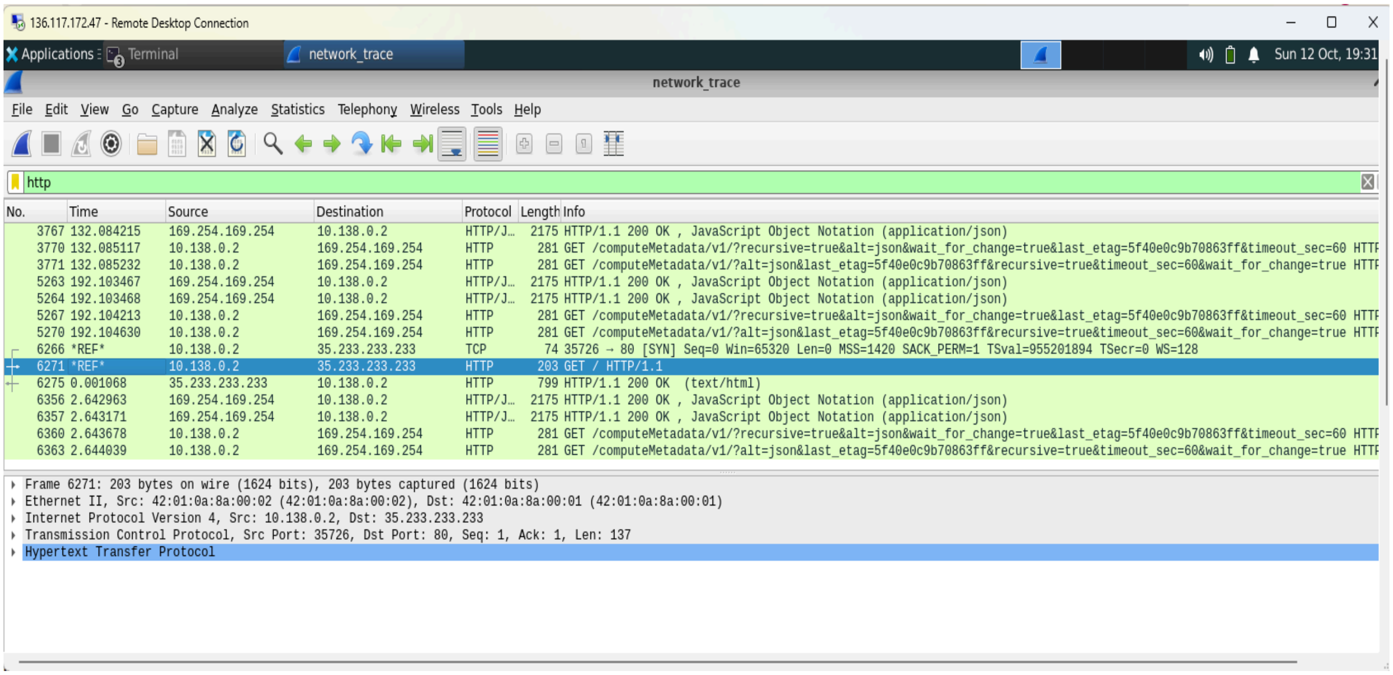
```
0000  42 01 0a 8a 00 01 42 01  0a 8a 00 02 08 00 45 00   B·····B· ······E·
0010  00 34 e6 62 40 00 40 06  3c 03 0a 8a 00 02 23 e9   ·4·b@·@· <·····#·
0020  e9 e9 8b 8e 00 50 fa 83  da f6 15 e7 70 e6 80 10   ·····P·· ····p···
```



```
No.  Time     Source          Destination     Protocol Length Info
6266 *REF*    10.138.0.2      35.233.233.233  TCP        74 35726 → 80 [SYN] Seq=0 Win=653
6269 0.001560 35.233.233.233  10.138.0.2      TCP        74 80 → 35726 [SYN, ACK] Seq=0 Ac
6270 0.001599 10.138.0.2      35.233.233.233  TCP        66 35726 → 80 [ACK] Seq=1 Ack=1 W
6271 0.001795 10.138.0.2      35.233.233.233  HTTP      203 GET / HTTP/1.1
6272 0.002303 35.233.233.233  10.138.0.2      TCP        66 80 → 35726 [ACK] Seq=1 Ack=138
6273 0.002704 35.233.233.233  10.138.0.2      TCP      7106 80 → 35726 [PSH, ACK] Seq=1 Ac
6274 0.002730 10.138.0.2      35.233.233.233  TCP        66 35726 → 80 [ACK] Seq=138 Ack=7
6275 0.002863 35.233.233.233  10.138.0.2      HTTP      799 HTTP/1.1 200 OK  (text/html)
6276 0.002871 10.138.0.2      35.233.233.233  TCP        66 35726 → 80 [ACK] Seq=138 Ack=7
6277 0.003962 10.138.0.2      35.233.233.233  TCP        66 35726 → 80 [FIN, ACK] Seq=138
6278 0.004592 35.233.233.233  10.138.0.2      TCP        66 80 → 35726 [FIN, ACK] Seq=7774
6279 0.004781 10.138.0.2      35.233.233.233  TCP        66 35726 → 80 [ACK] Seq=139 Ack=7
```

- What packet numbers in the trace correspond to the initial TCP handshake for the web request?6266 (SYN), 6269 (SYN-ACK), 6270 (ACK)
- How long does it take to perform the initial TCP handshake? Handshake duration ≈ 0.001599 seconds ≈ 1.6 milliseconds

HTTP


136.117.172.47 - Remote Desktop Connection
Applications
Terminal
network_trace
Sun 12 Oct, 19:31
network_trace
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.  Time       Source          Destination     Protocol Length Info
3767 132.084215 169.254.169.254 10.138.0.2      HTTP/J…  2175 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
3770 132.085117 10.138.0.2      169.254.169.254 HTTP      281 GET /computeMetadata/v1/?recursive=true&alt=json&wait_for_change=true&last_etag=5f40e0c9b70863ff&timeout_sec=60 HTTP
3771 132.085232 10.138.0.2      169.254.169.254 HTTP      281 GET /computeMetadata/v1/?alt=json&last_etag=5f40e0c9b70863ff&recursive=true&timeout_sec=60&wait_for_change=true HTTP
5263 192.103467 169.254.169.254 10.138.0.2      HTTP/J…  2175 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
5264 192.103468 169.254.169.254 10.138.0.2      HTTP/J…  2175 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
5267 192.104213 10.138.0.2      169.254.169.254 HTTP      281 GET /computeMetadata/v1/?recursive=true&alt=json&wait_for_change=true&last_etag=5f40e0c9b70863ff&timeout_sec=60 HTTP
5270 192.104630 10.138.0.2      169.254.169.254 HTTP      281 GET /computeMetadata/v1/?alt=json&last_etag=5f40e0c9b70863ff&recursive=true&timeout_sec=60&wait_for_change=true HTTP
6266 *REF*      10.138.0.2      35.233.233.233  TCP        74 35726 → 80 [SYN] Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM=1 TSval=955201894 TSecr=0 WS=128
6271 *REF*      10.138.0.2      35.233.233.233  HTTP      203 GET / HTTP/1.1
6275 0.001068   35.233.233.233  10.138.0.2      HTTP      799 HTTP/1.1 200 OK  (text/html)
6356 2.642963   169.254.169.254 10.138.0.2      HTTP/J…  2175 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
6357 2.643171   169.254.169.254 10.138.0.2      HTTP/J…  2175 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
6360 2.643678   10.138.0.2      169.254.169.254 HTTP      281 GET /computeMetadata/v1/?recursive=true&alt=json&wait_for_change=true&last_etag=5f40e0c9b70863ff&timeout_sec=60 HTTP
6363 2.644039   10.138.0.2      169.254.169.254 HTTP      281 GET /computeMetadata/v1/?alt=json&last_etag=5f40e0c9b70863ff&recursive=true&timeout_sec=60&wait_for_change=true HTTP
```

```
Frame 6271: 203 bytes on wire (1624 bits), 203 bytes captured (1624 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: 35.233.233.233
Transmission Control Protocol, Src Port: 35726, Dst Port: 80, Seq: 1, Ack: 1, Len: 137
Hypertext Transfer Protocol
```

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

  Http request is 6271 and http response is 6275

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

  It takes 0.001068 seconds