Lab notebook Week 2

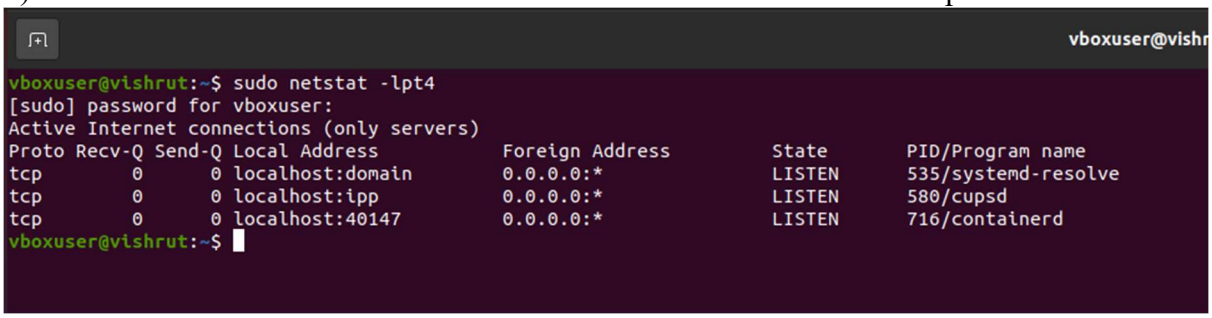
Submitted by: Vishrut Sharma (OdinID: vishrut)

Table of Contents

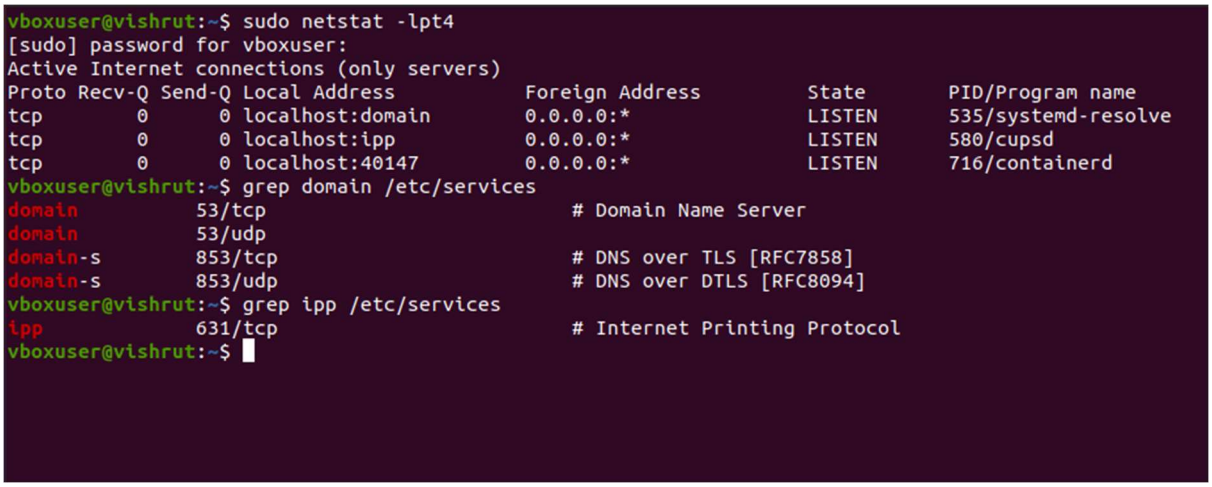
02.1: TCP, HTTP

1. TCP #1 (netstat, lsof, nc)

1) Screenshot below contains the result from the command sudo netstat -lpt4

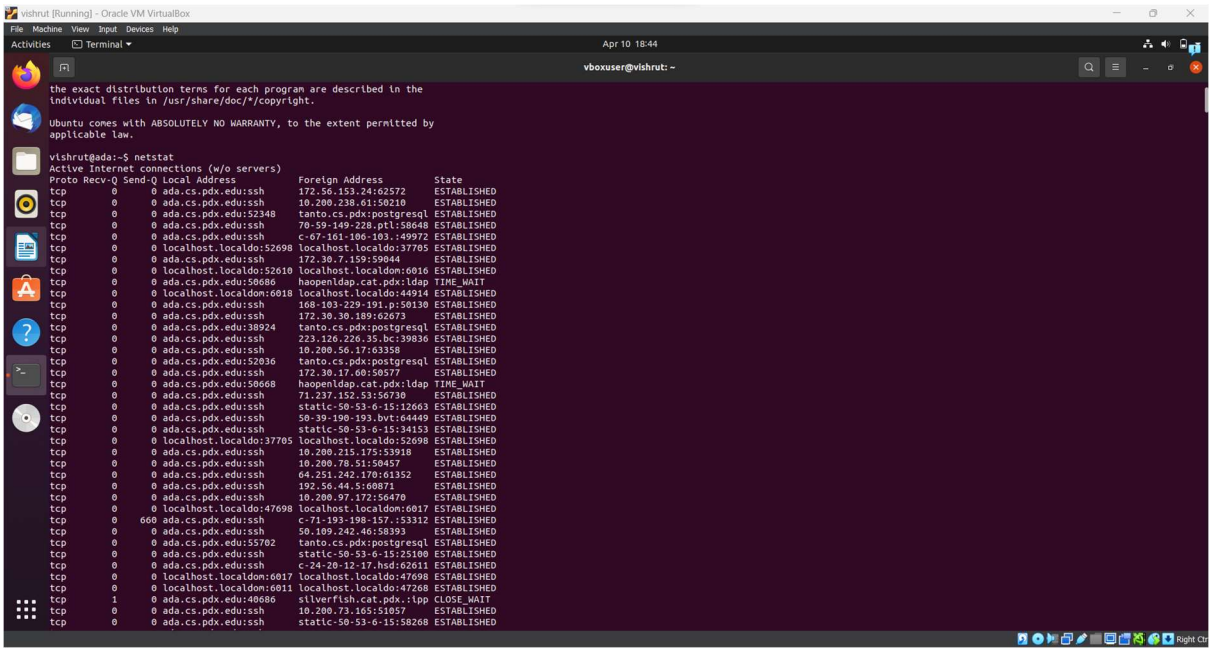


2) The screenshot below contains the port numbers after examining /etc/services

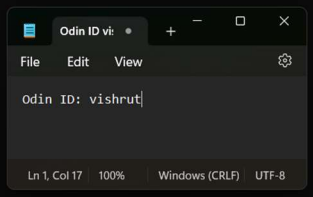


The port that only has a number is running 716/containerd program. It is a daemon that manages the lifecycle of containers in a container runtime environment.

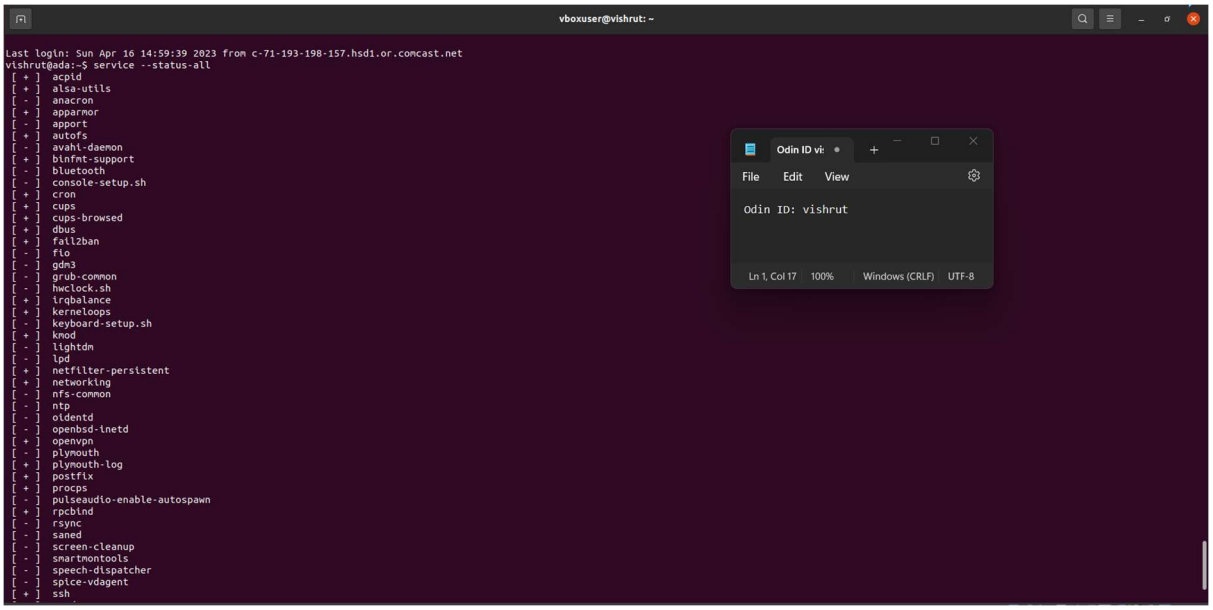
4) The screenshot below contains the result from running the netstat command on linux.cs.pdx.edu.



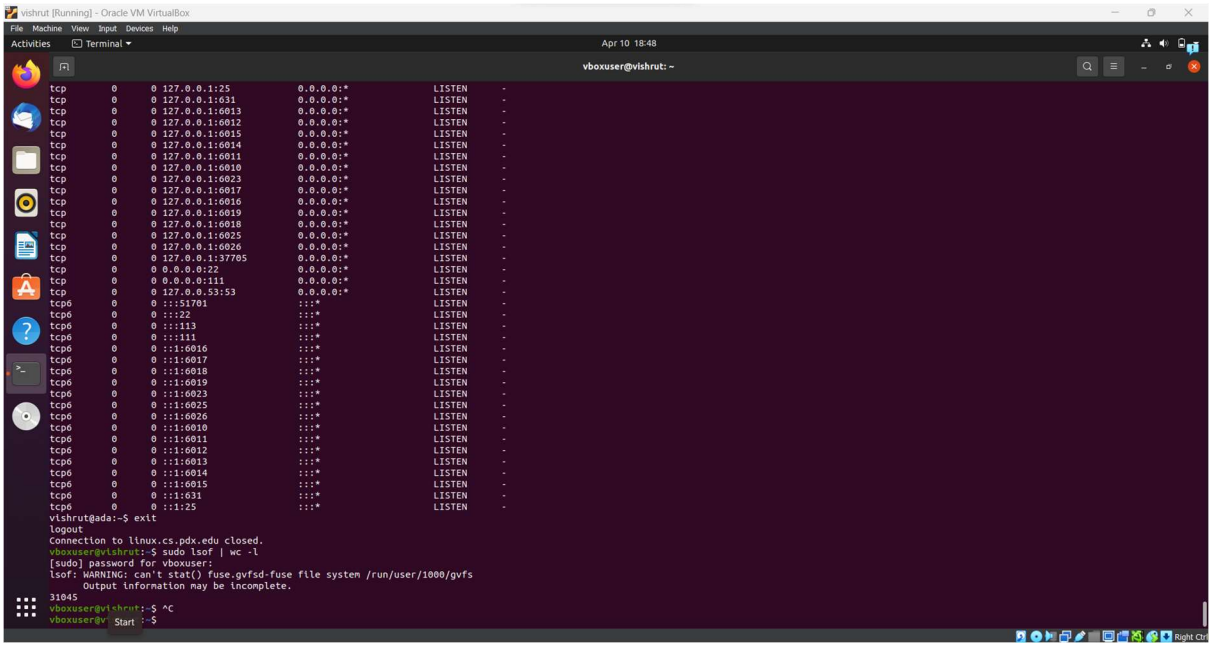

```
Last login: Wed Apr 12 17:31:58 2023 from c-71-193-198-157.hsd1.or.comcast.net
vishrut@ada:~$ netstat -tlnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:49311           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6013          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6012          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6015          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6011          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:42711         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::51701                :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::113                  :::*                    LISTEN      -
tcp6       0      0 :::111                  :::*                    LISTEN      -
tcp6       0      0 ::1:6010                :::*                    LISTEN      -
tcp6       0      0 ::1:6011                :::*                    LISTEN      -
tcp6       0      0 ::1:6012                :::*                    LISTEN      -
tcp6       0      0 ::1:6013                :::*                    LISTEN      -
tcp6       0      0 ::1:6015                :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
vishrut@ada:~$
```



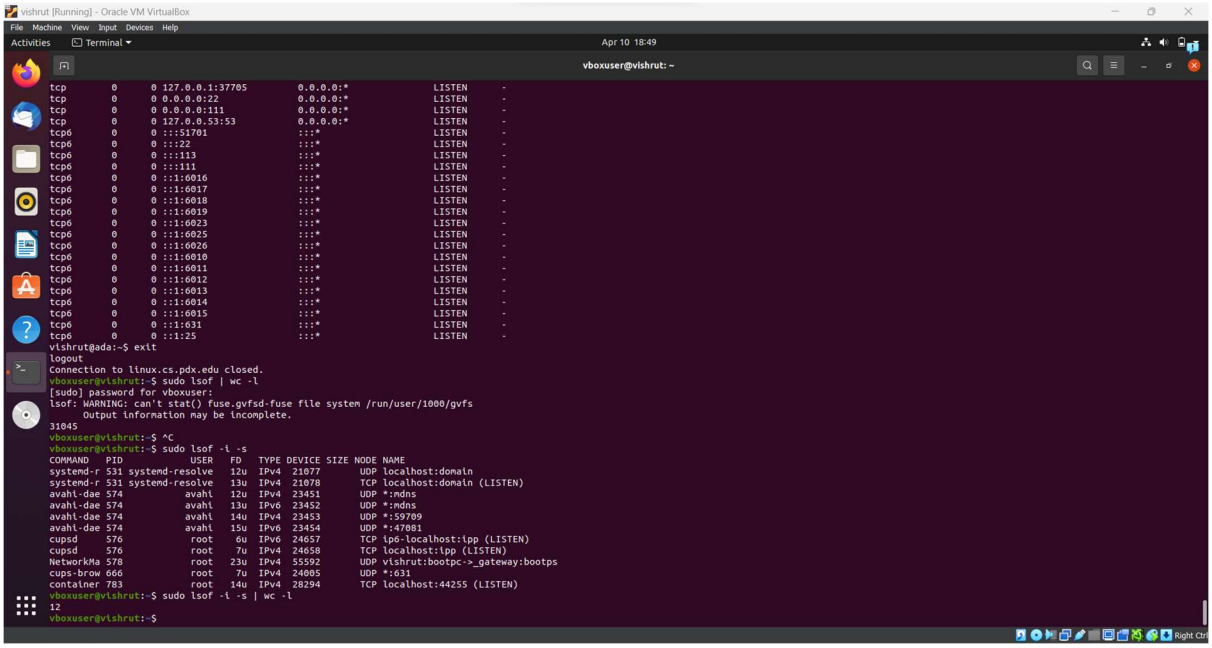
5) The screenshot below shows all the services the machine provides for external access.



6) The screenshot below contains the result from running the lsof command on the Ubuntu VM. The number of open descriptors were 31045.

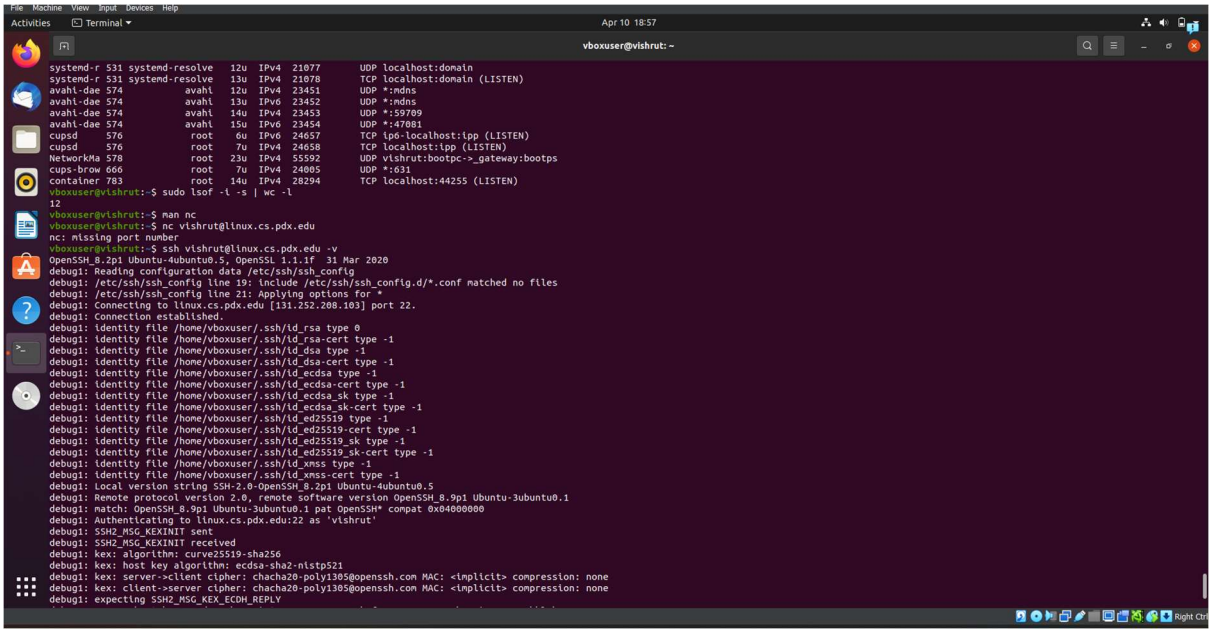


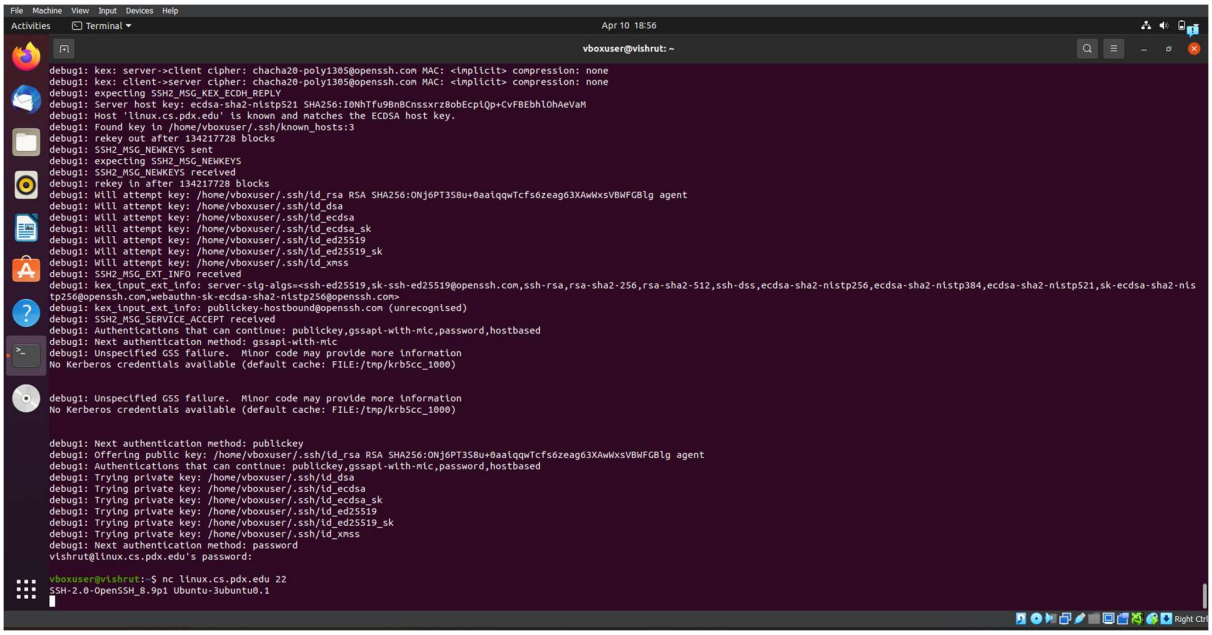
The screenshot below contains the result from running the lsof command but with the -i and the -s flag included. The result was 12.



7) The 2 screenshots below contains the result from netcat command. The first screenshot shows us which port is being used to connect to linux.cs.pdx.edu.

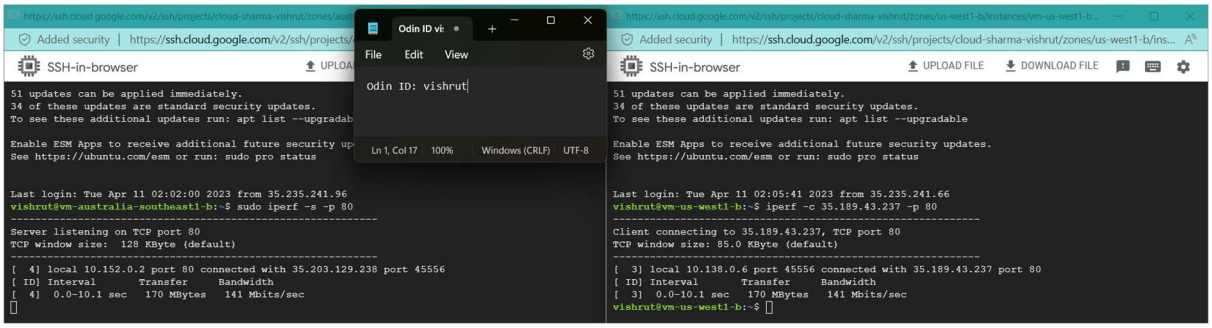
The 2nd screenshot shows the SSH version being used to connect to linux.cs.pdx.edu.



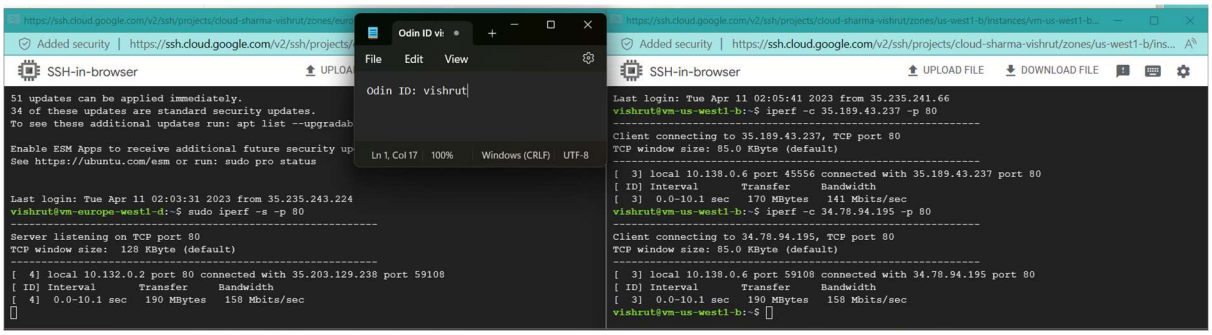


3. Throughput tests

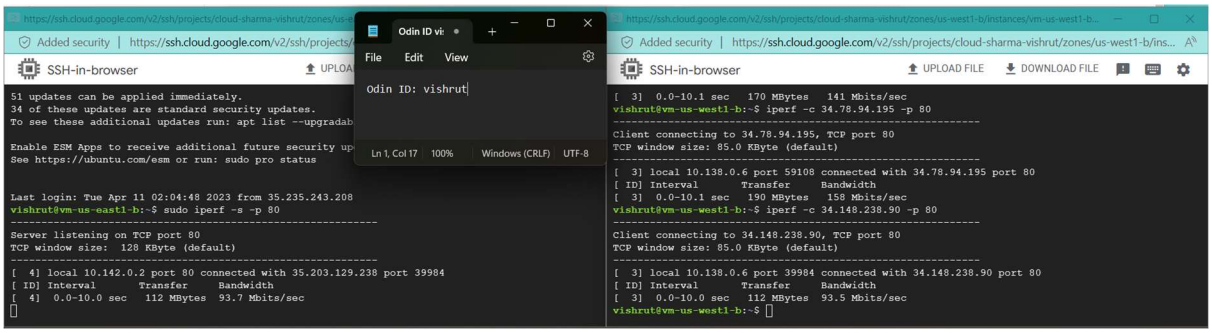
1) The screenshot below shows the measured bandwidth available between us-west1-b (right image) and australia-southeast1-b (left image).



2) The screenshot below shows the measured bandwidth available between us-west1-b (right image) and europe-west1-d (left image).



3) The screenshot below shows the measured bandwidth available between us-west1-b (right image) and us-east1-b (left image).



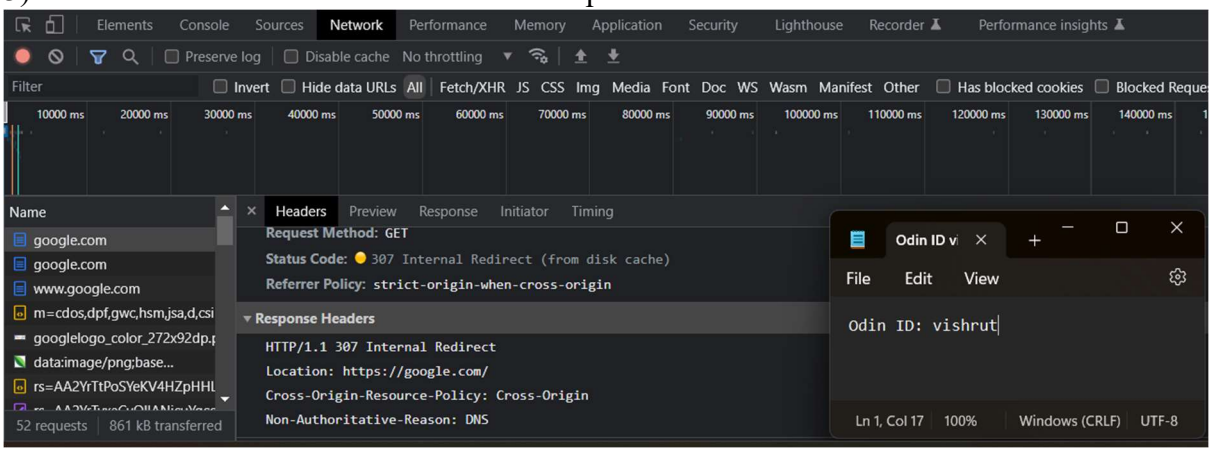
There is a relative difference between the bandwidths between us-west1-b and all the other VMs. Surprisingly the lowest bandwidth (93.5 Mbits/sec) was between us-west1-b and us-east1-b. This might be because of internet traffic and network congestion. The bandwidth between us-west1-b and australia-southeast1-b was 141 Mbits/sec and the highest bandwidth was between us-west1-b and europe-west1-d (158 Mbits/sec).

5. Developer tools

1) URL being requested is http://google.com/

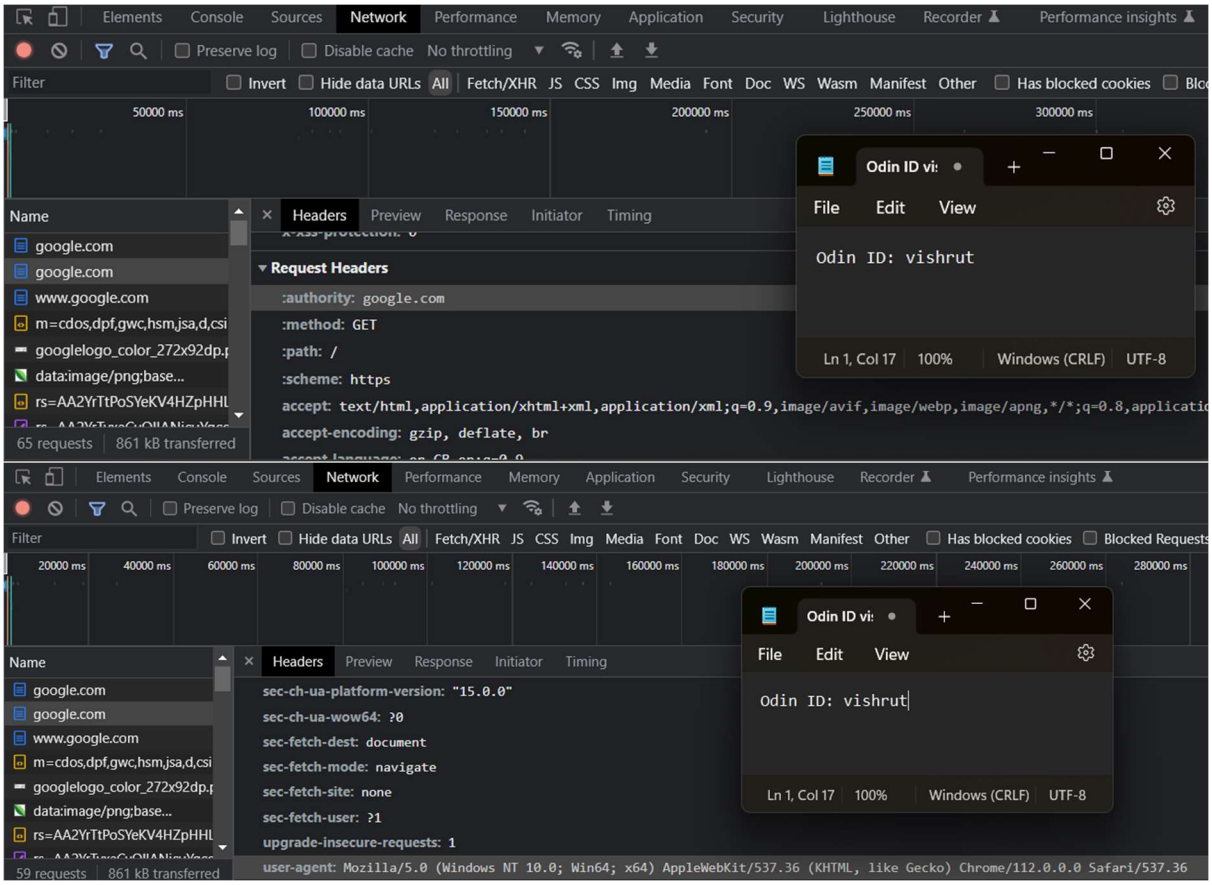
2) The Status code is 307: 'HTTP 307 Temporary Redirect' response code indicates that the resource requested has been temporarily moved to the URL given by the Location headers.

3) The screenshot below shows the HTTP response header.



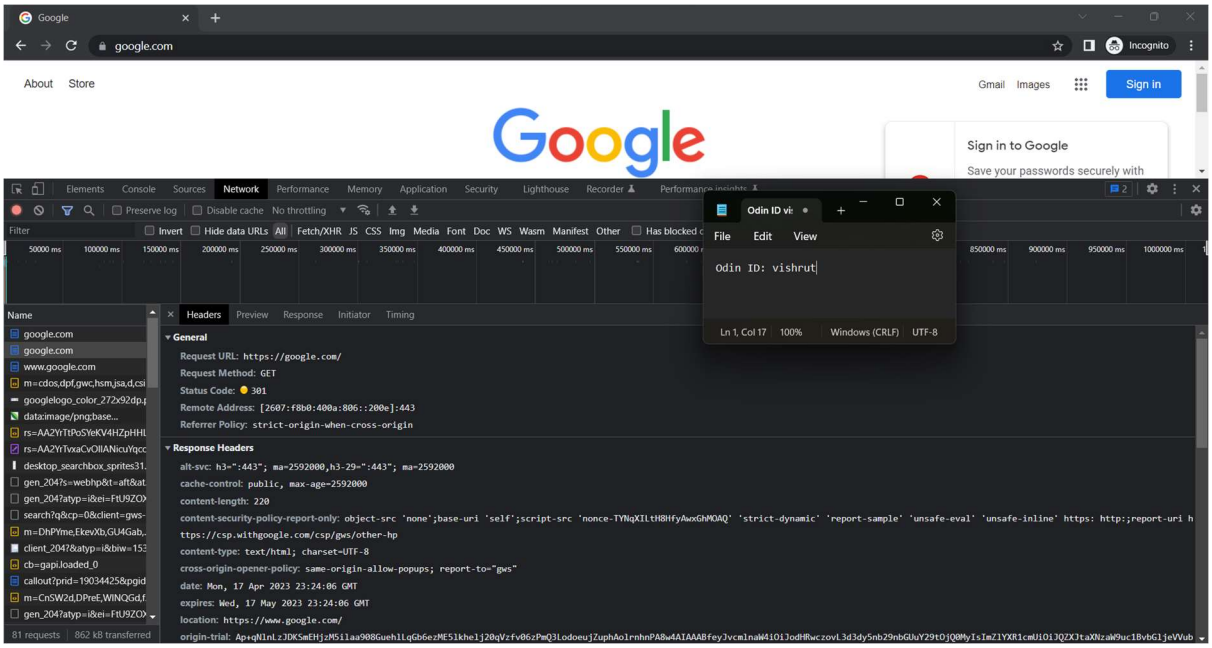
4) URL being requested is https://google.com/. It uses HTTPS.

5) The 2 screenshots below show the authority header and the user-agent field.



6) The Status code is 301: ‘HTTP status code 301’ indicates a permanent redirect, meaning that the requested resource has moved permanently to a new URL. And ‘HTTP 307 Temporary Redirect’ response code indicates that the resource requested has been temporarily moved to the URL given by the Location headers.

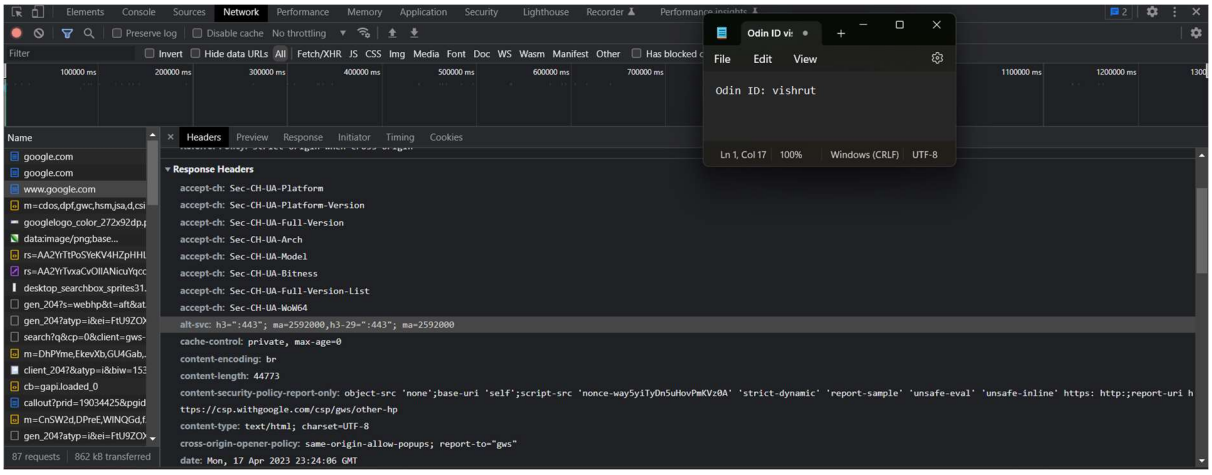
7) The screenshot below shows the associated HTTP response header that is sent in conjunction with this status code for the request.



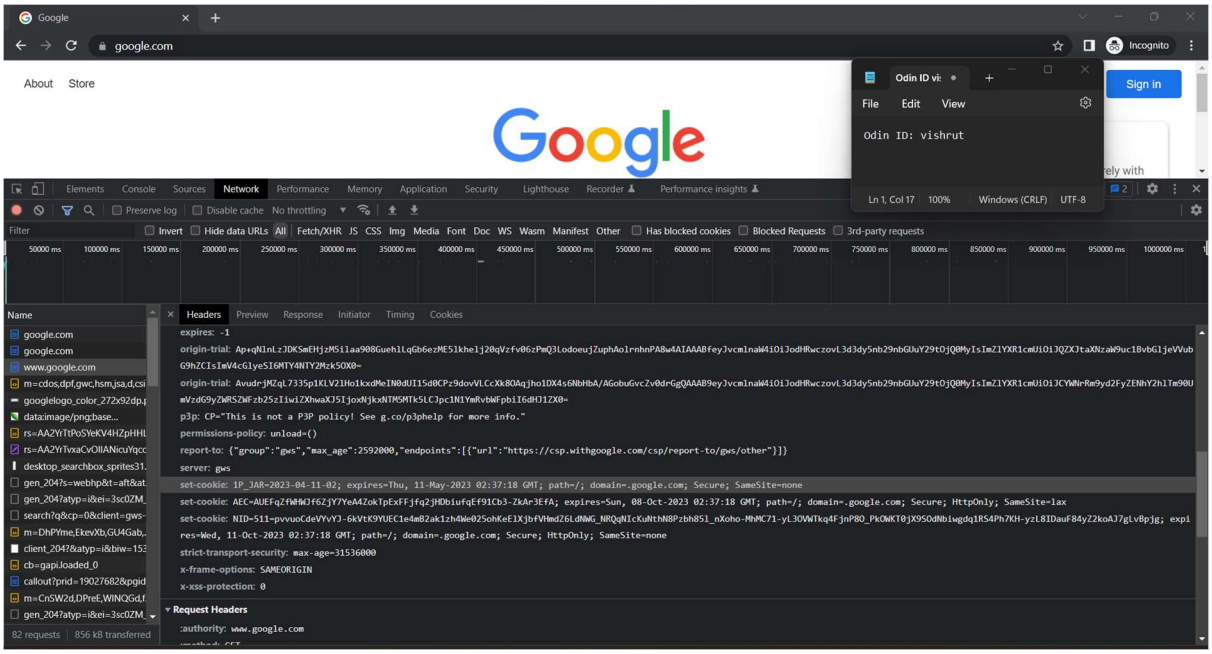
8) URL being requested is https://www.google.com/. It is using HTTPS.

9) The status code is 200.

10) The screenshot below shows the alt-svc section in the response header. The client can use HTTP3/QUIC based on the h3-29 tag in alt-svc.

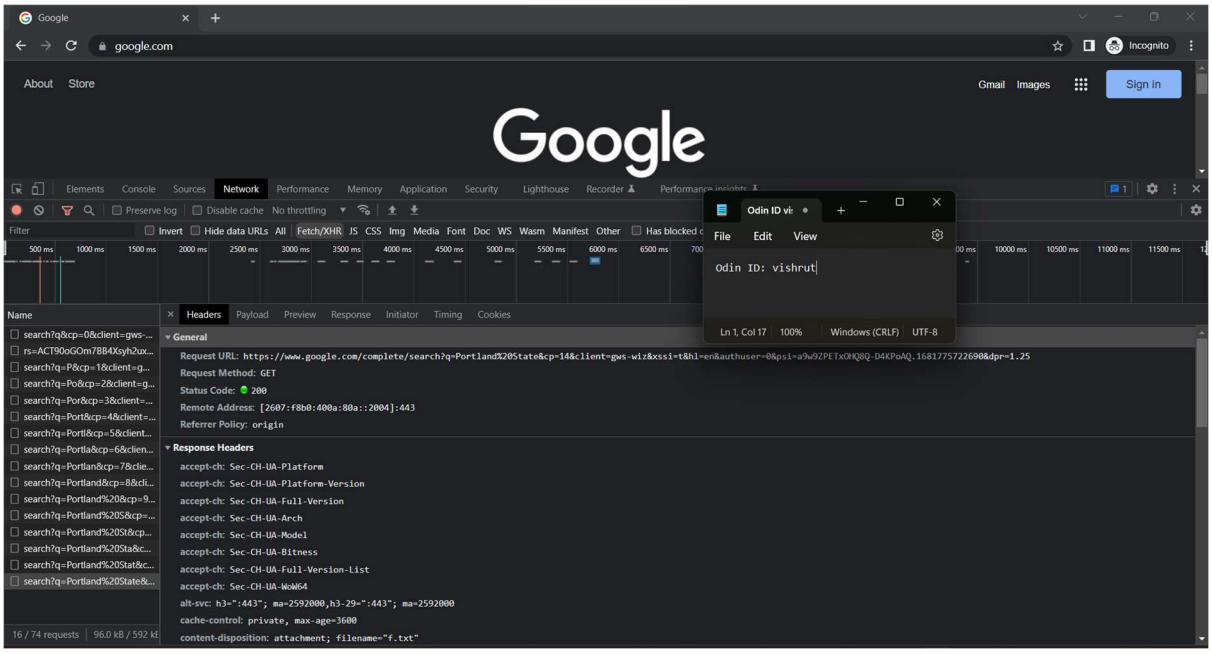


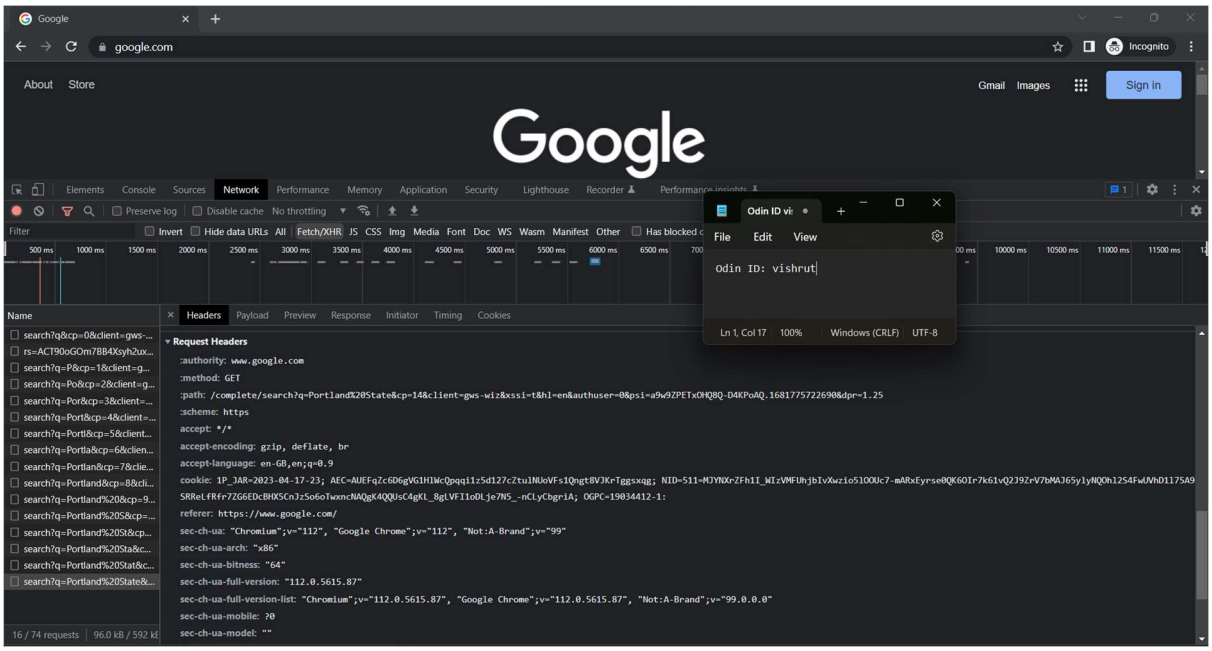
11) The setting of SameSite=None indicates that the cookie can be sent with cross-site requests, including requests from third-party sites.



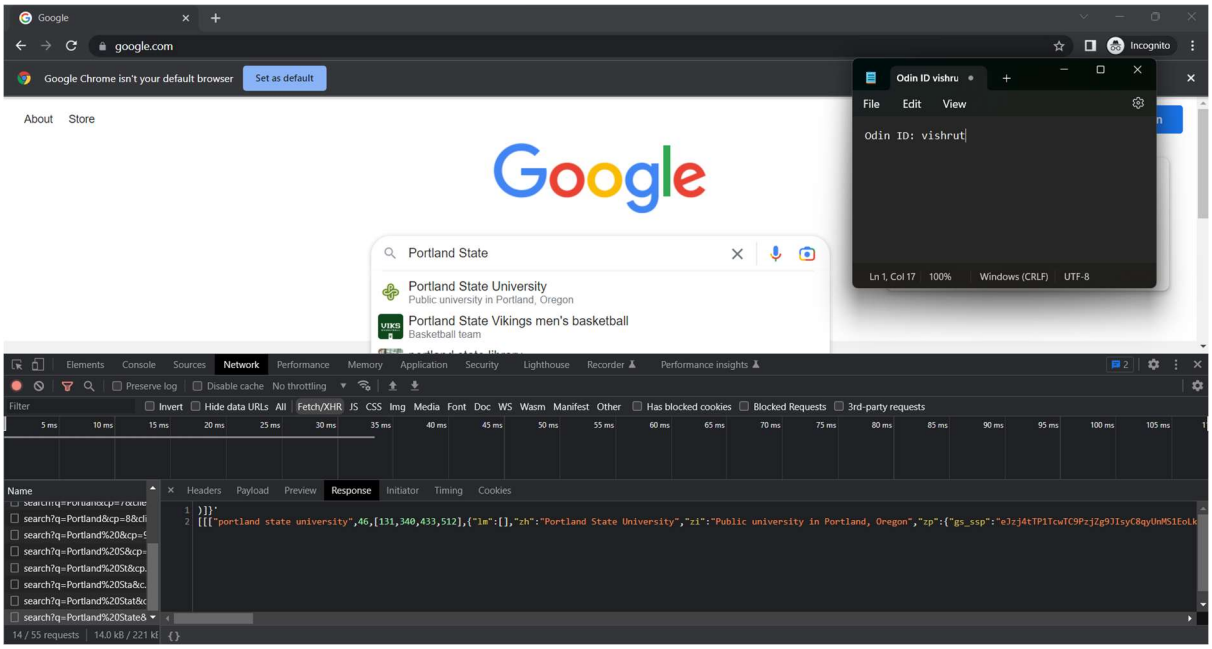
6. Asynchronous HTTP requests

1) The 2 screenshots below show the request and response headers.





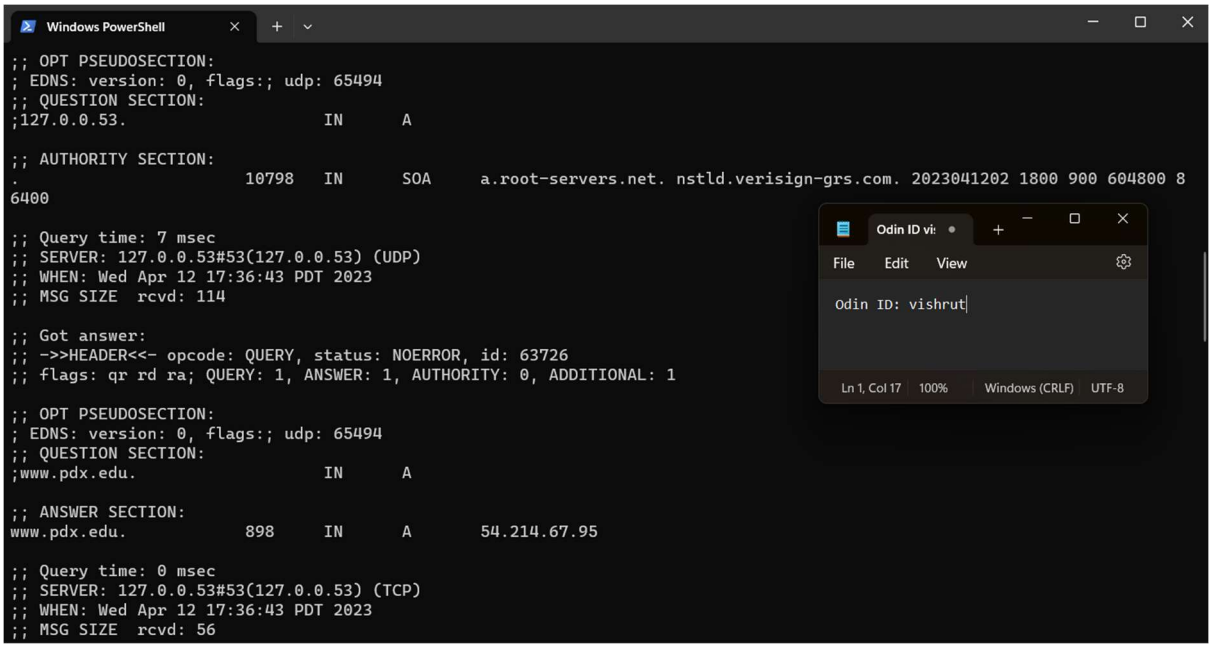
The screenshot below shows that the payload has returned the data that is then rendered on the search page.

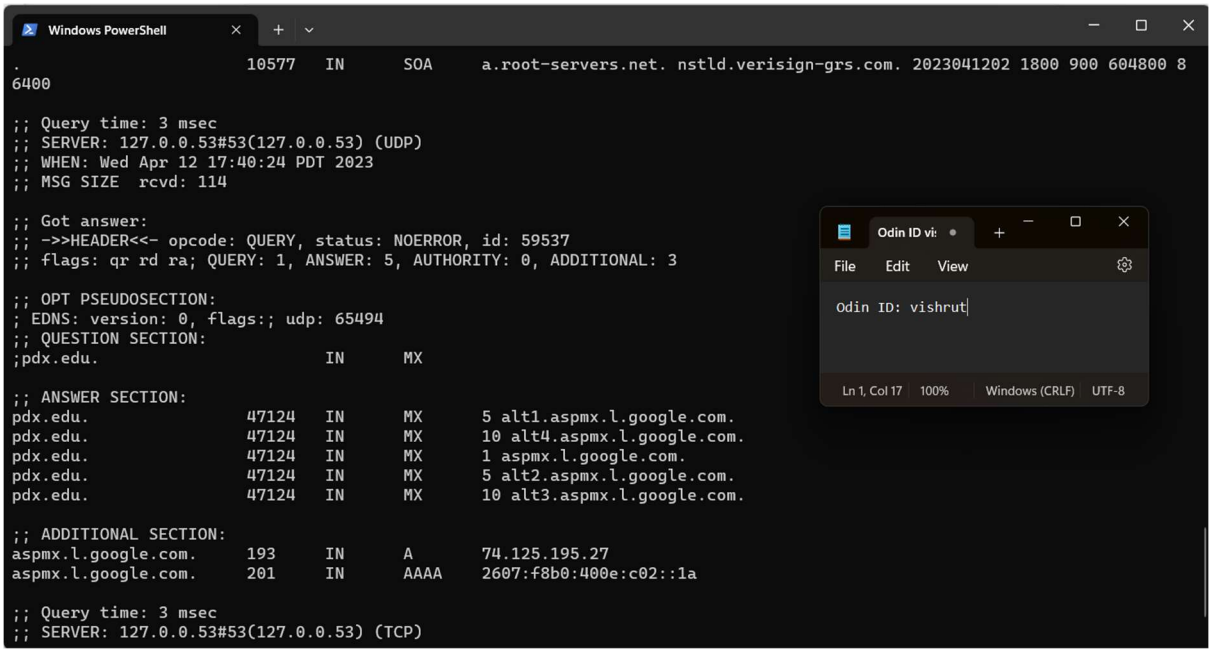


02.2: DNS, Recap

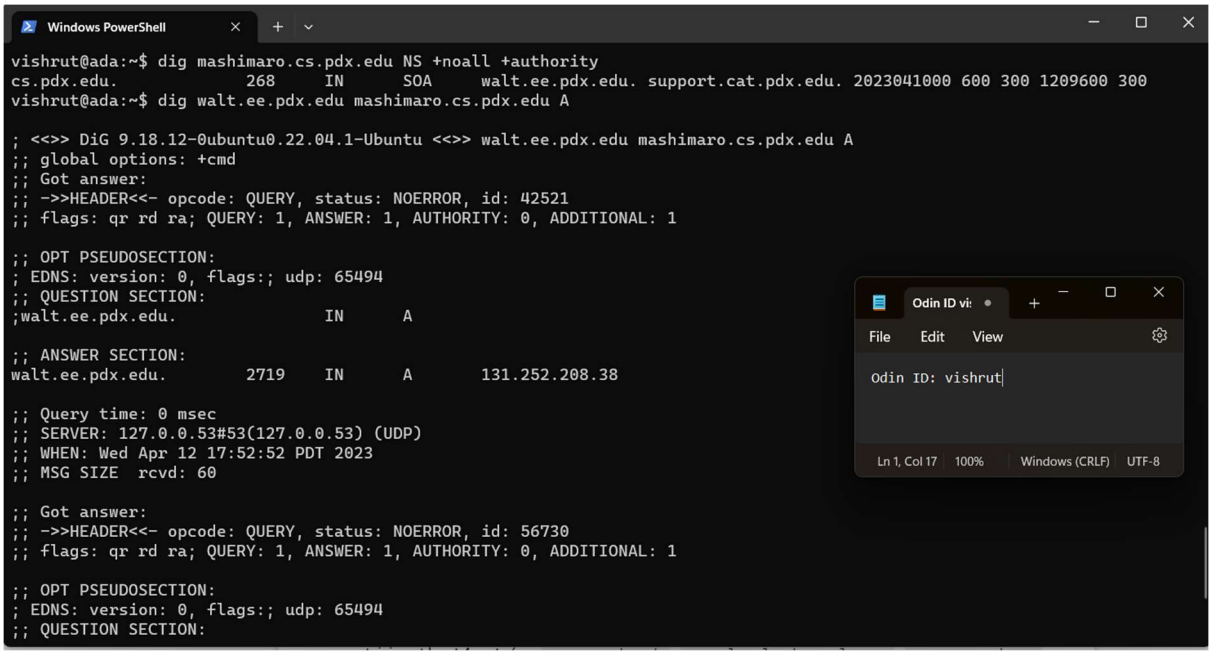
1. DNS #1 (dig)

1) The ANSWER section of the A record for www.pdx.edu indicates the IP address where PSU's web services are hosted. The ANSWER section of the MX record for pdx.edu indicates the hostnames of the mail servers where PSU's email services are hosted.

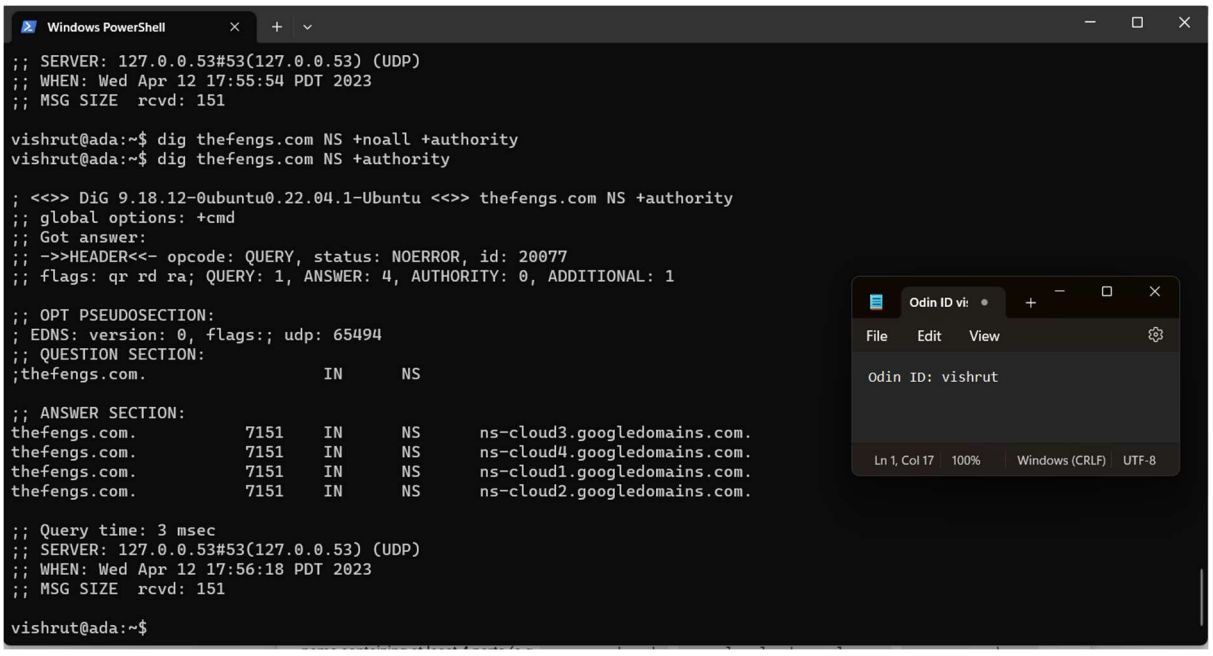


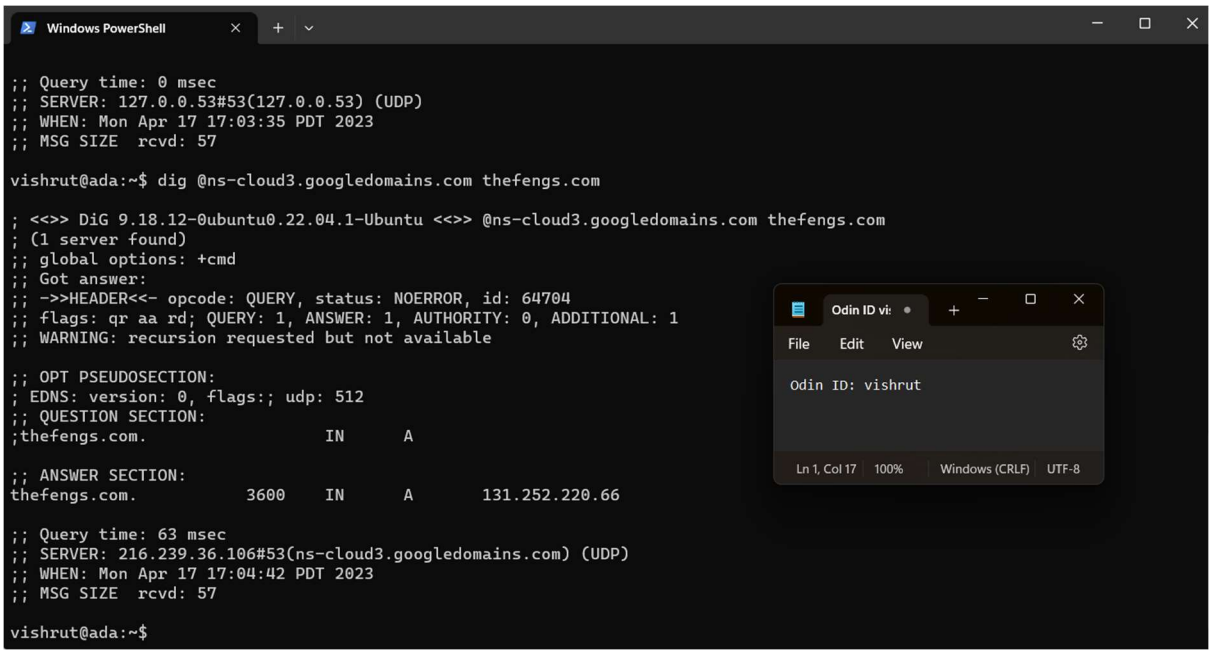


2) The screenshot below shows the authoritative server of mashimaro.cs.pdx.edu and also the result after querying walt.ee.pdx.edu for the A record of mashimaro.cs.pdx.edu.



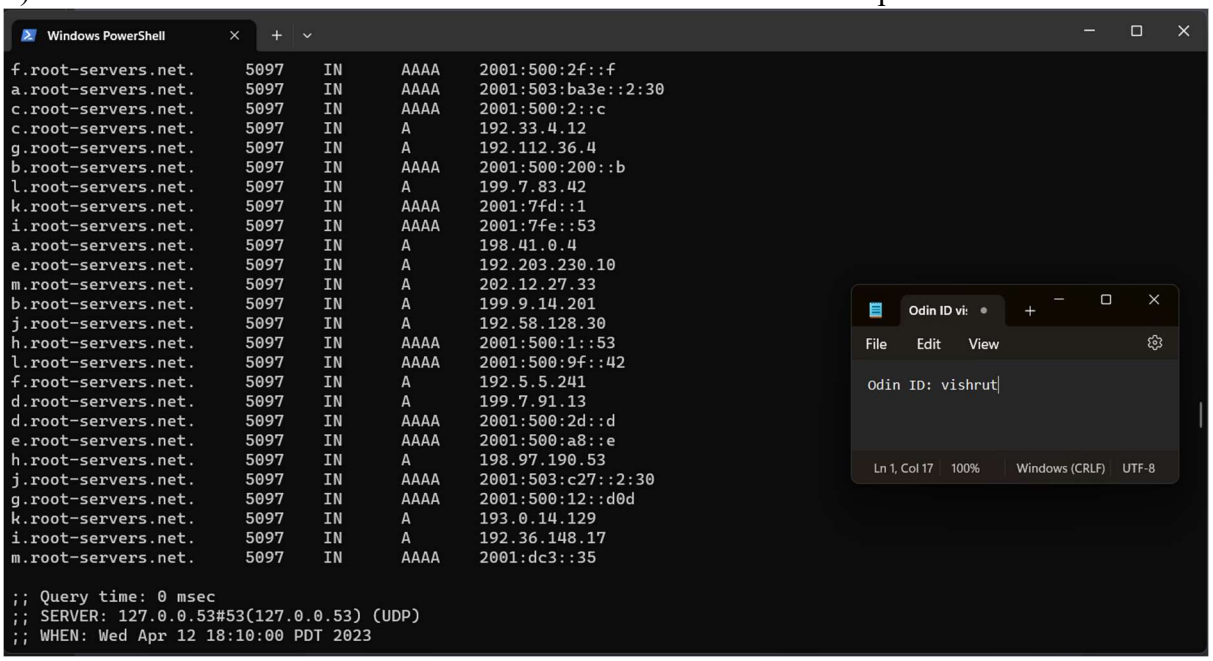
3) The screenshots below show the authoritative server for thefengs.com and the result after querying that server for the A record of thefengs.com.

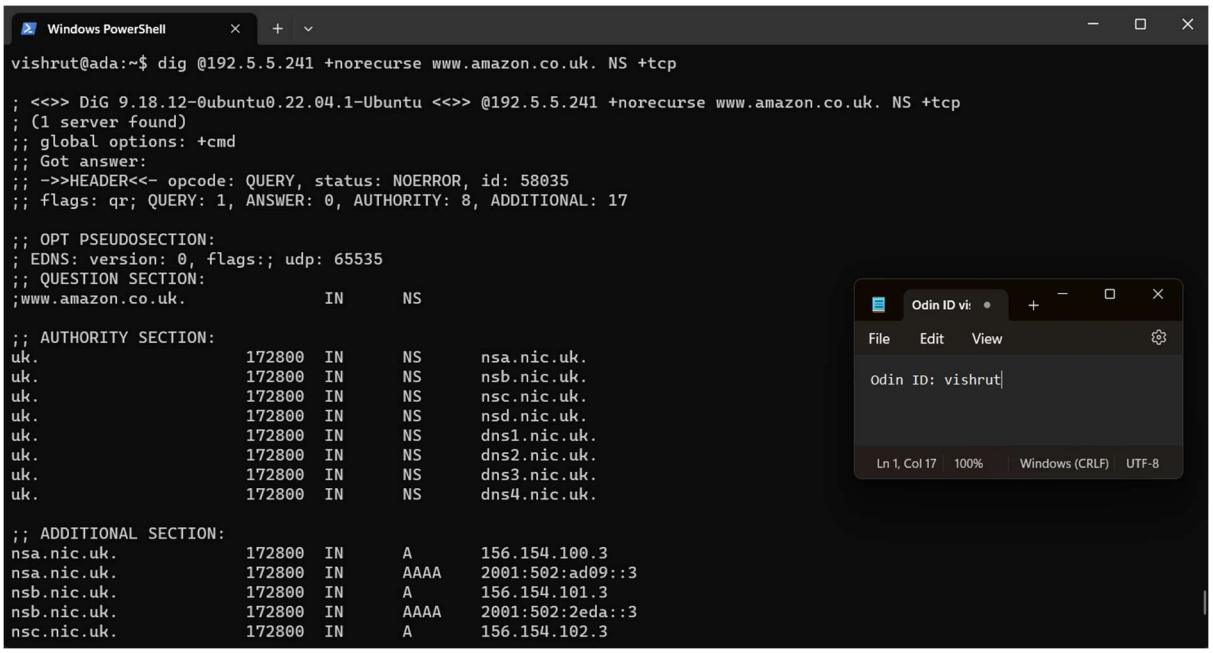


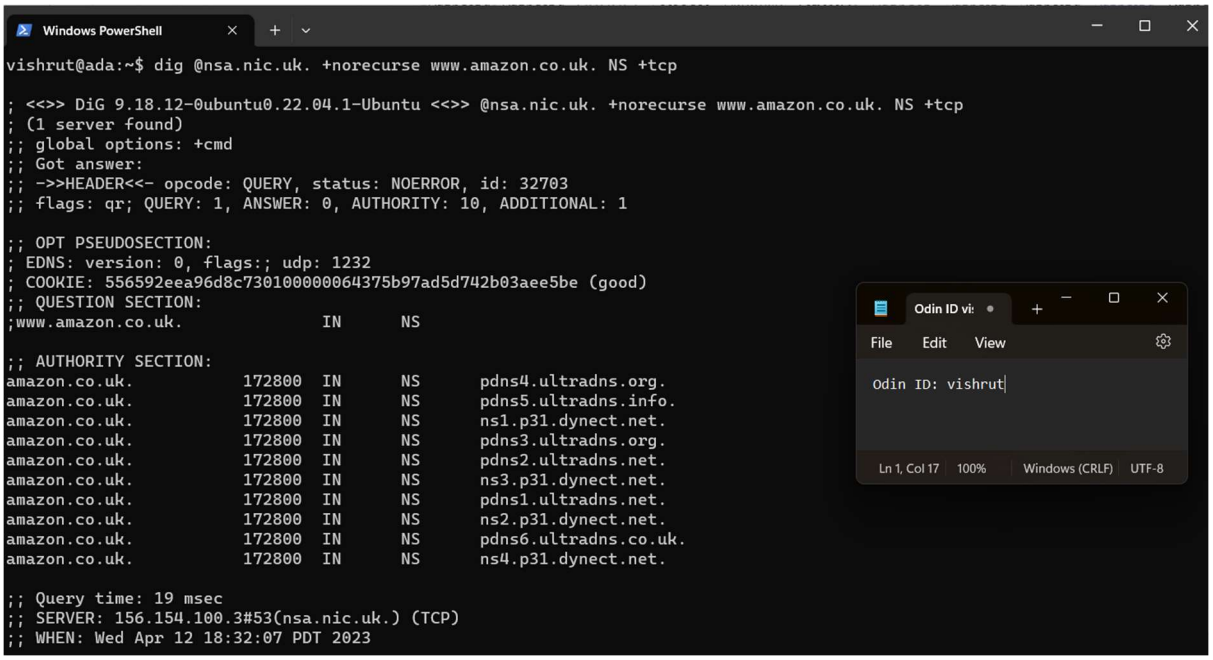


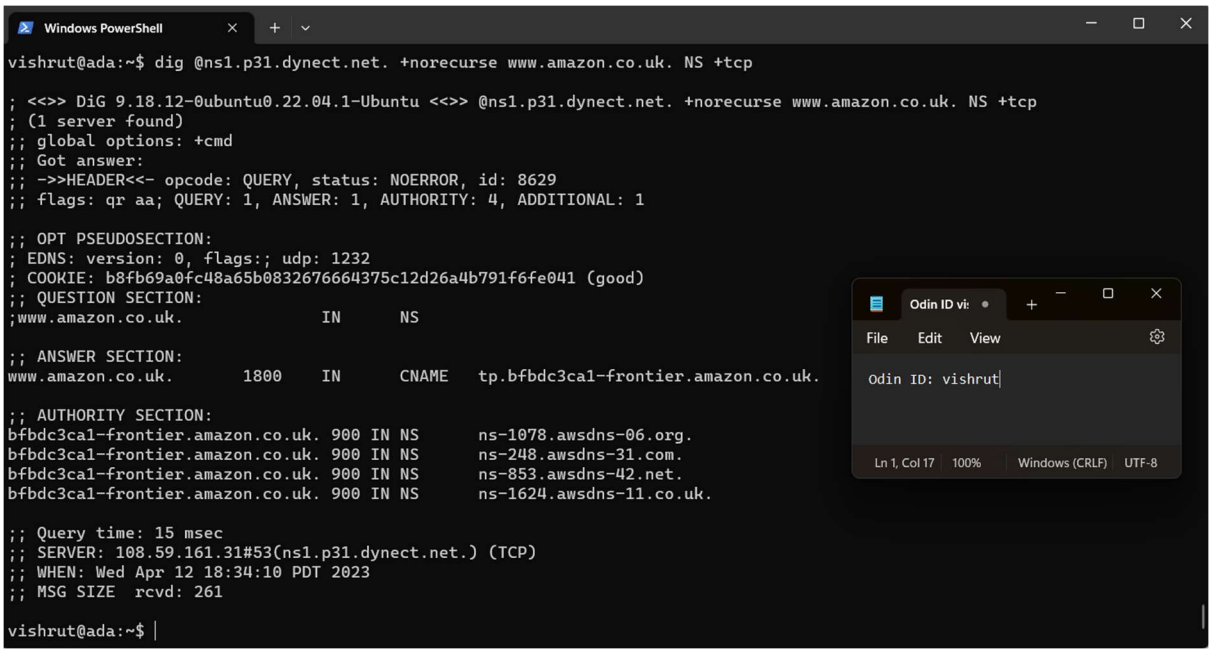
4) When a web request hits port 80 of 131.252.220.66, the server uses the HTTP protocol to determine which site to serve from. Specifically, the HTTP protocol uses the ‘Host’ header in the HTTP request to determine which site to serve.

5) The screenshots below show the result of the DNS iterative lookup of www.amazon.co.uk




Windows PowerShell
vishrut@ada:~$ dig @192.5.5.241 +norecurse www.amazon.co.uk. NS +tcp
; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> @192.5.5.241 +norecurse www.amazon.co.uk. NS +tcp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58035
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 17
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65535
;; QUESTION SECTION:
;www.amazon.co.uk. IN NS
;; AUTHORITY SECTION:
uk. 172800 IN NS nsa.nic.uk.
uk. 172800 IN NS nsb.nic.uk.
uk. 172800 IN NS nsc.nic.uk.
uk. 172800 IN NS nsd.nic.uk.
uk. 172800 IN NS dns1.nic.uk.
uk. 172800 IN NS dns2.nic.uk.
uk. 172800 IN NS dns3.nic.uk.
uk. 172800 IN NS dns4.nic.uk.
;; ADDITIONAL SECTION:
nsa.nic.uk. 172800 IN A 156.154.100.3
nsa.nic.uk. 172800 IN AAAA 2001:502:ad09::3
nsb.nic.uk. 172800 IN A 156.154.101.3
nsb.nic.uk. 172800 IN AAAA 2001:502:2eda::3
nsc.nic.uk. 172800 IN A 156.154.102.3
Odin ID vi:
File Edit View
Odin ID: vishrut
Ln 1, Col 17 100% Windows (CRLF) UTF-8

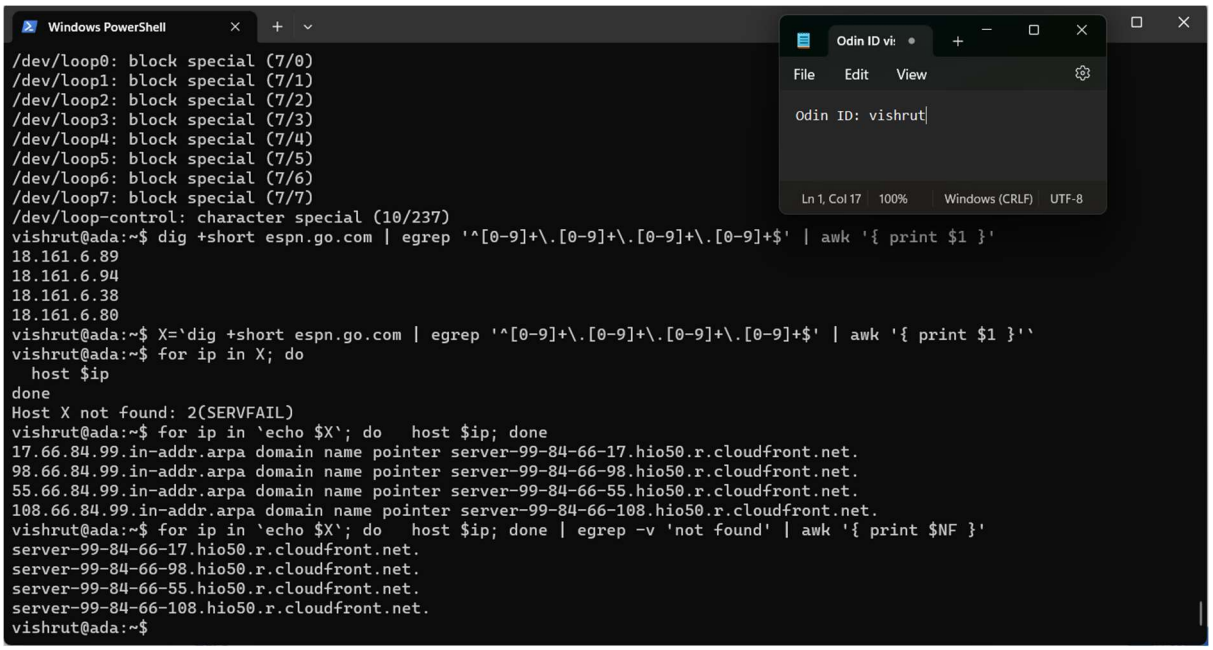

Windows PowerShell
vishrut@ada:~$ dig @nsa.nic.uk. +norecurse www.amazon.co.uk. NS +tcp
; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> @nsa.nic.uk. +norecurse www.amazon.co.uk. NS +tcp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32703
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 556592eea96d8c730100000064375b97ad5d742b03aee5be (good)
;; QUESTION SECTION:
;www.amazon.co.uk. IN NS
;; AUTHORITY SECTION:
amazon.co.uk. 172800 IN NS pdns4.ultradns.org.
amazon.co.uk. 172800 IN NS pdns5.ultradns.info.
amazon.co.uk. 172800 IN NS ns1.p31.dynect.net.
amazon.co.uk. 172800 IN NS pdns3.ultradns.org.
amazon.co.uk. 172800 IN NS pdns2.ultradns.net.
amazon.co.uk. 172800 IN NS ns3.p31.dynect.net.
amazon.co.uk. 172800 IN NS pdns1.ultradns.net.
amazon.co.uk. 172800 IN NS ns2.p31.dynect.net.
amazon.co.uk. 172800 IN NS pdns6.ultradns.co.uk.
amazon.co.uk. 172800 IN NS ns4.p31.dynect.net.
;; Query time: 19 msec
;; SERVER: 156.154.100.3#53(nsa.nic.uk.) (TCP)
;; WHEN: Wed Apr 12 18:32:07 PDT 2023
Odin ID vi:
File Edit View
Odin ID: vishrut
Ln 1, Col 17 100% Windows (CRLF) UTF-8



2. Reverse DNS lookups

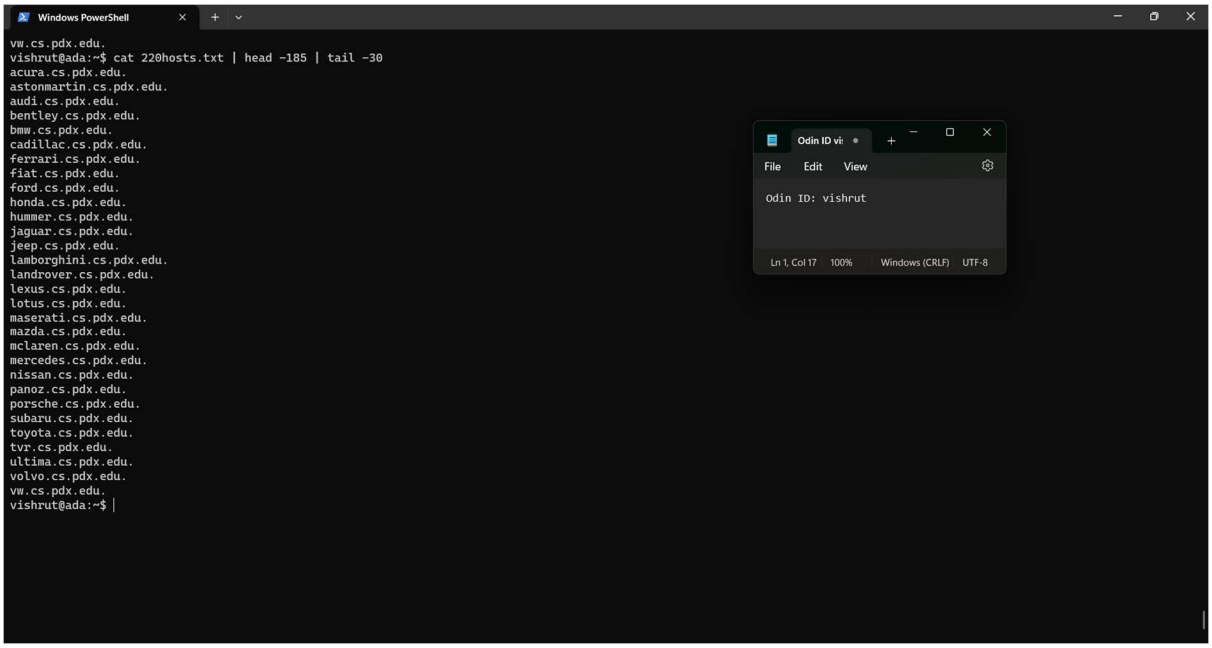
The screenshot below shows the result of running a single command line with commands dig, egrep, and awk, to list all IPv4 addresses that espn.go.com points to.

And also the result of looping over the IPv4 addresses and performing reverse lookups to get the DNS server names.



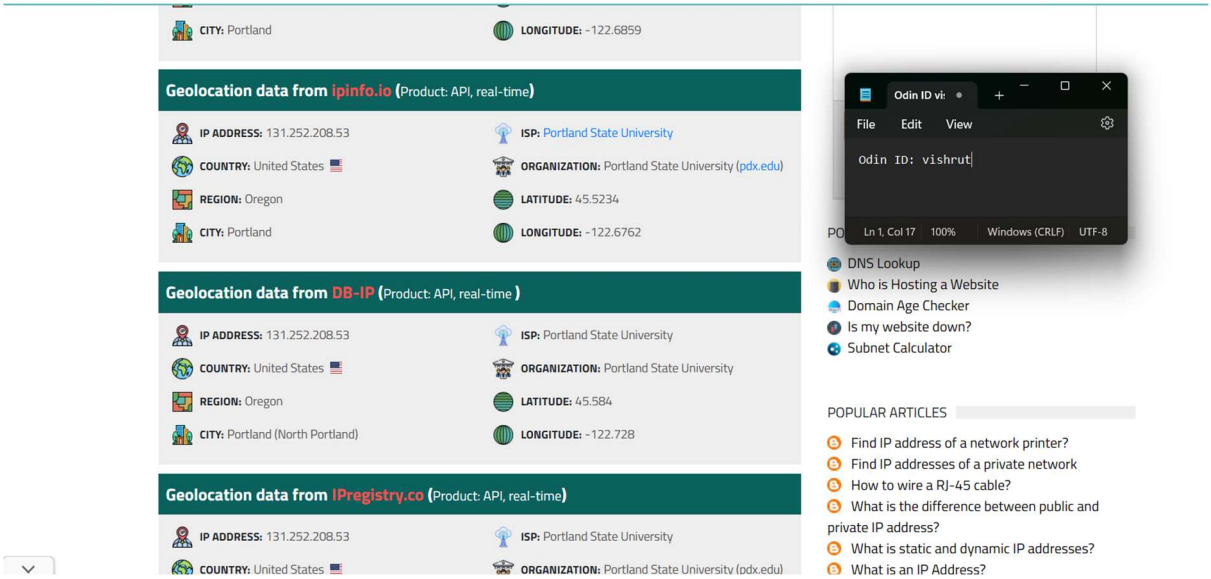
3. Host enumeration

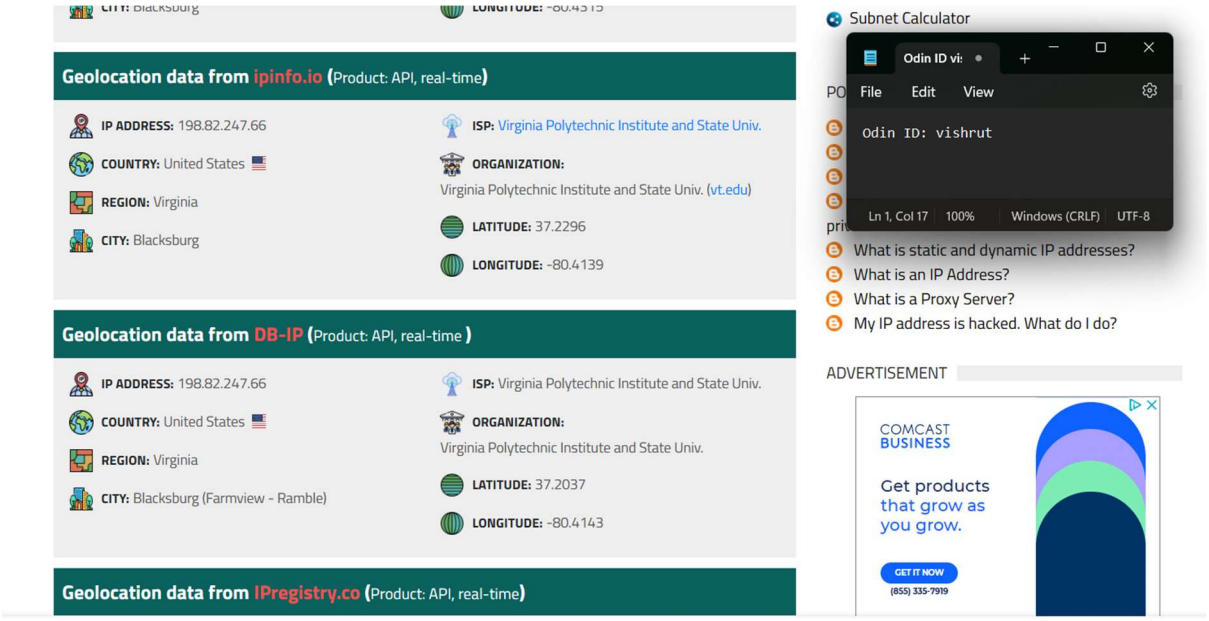
The screenshot below shows the set of car manufacturers names.



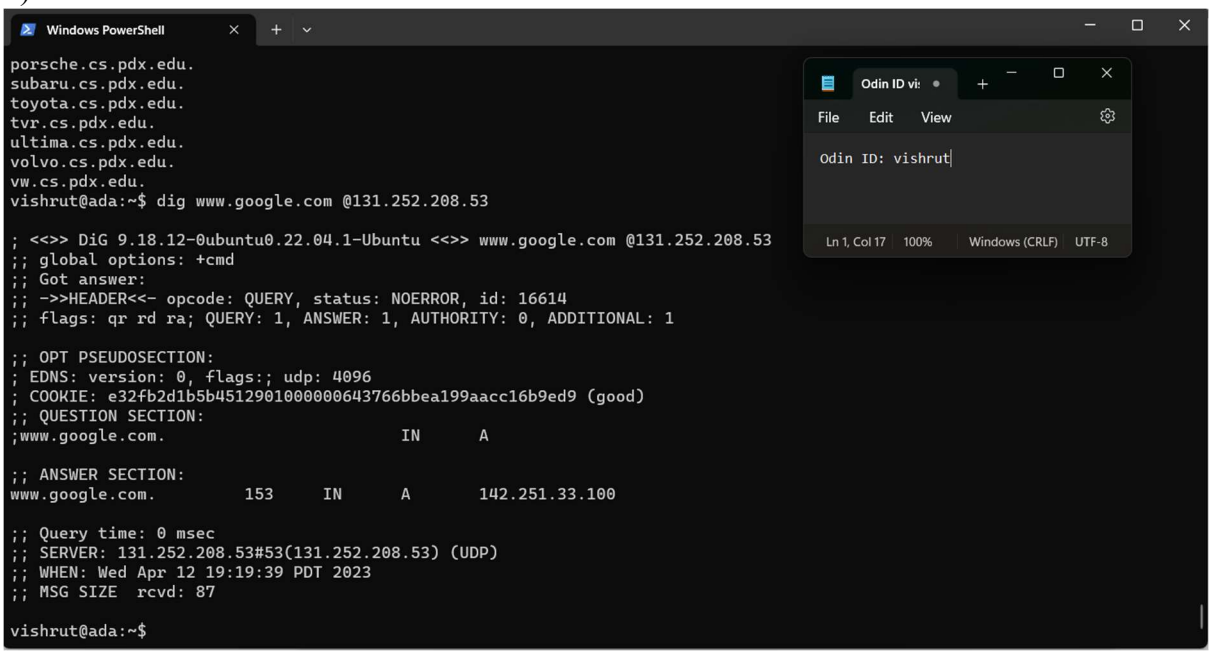
4. DNS #2 (Geographic DNS)

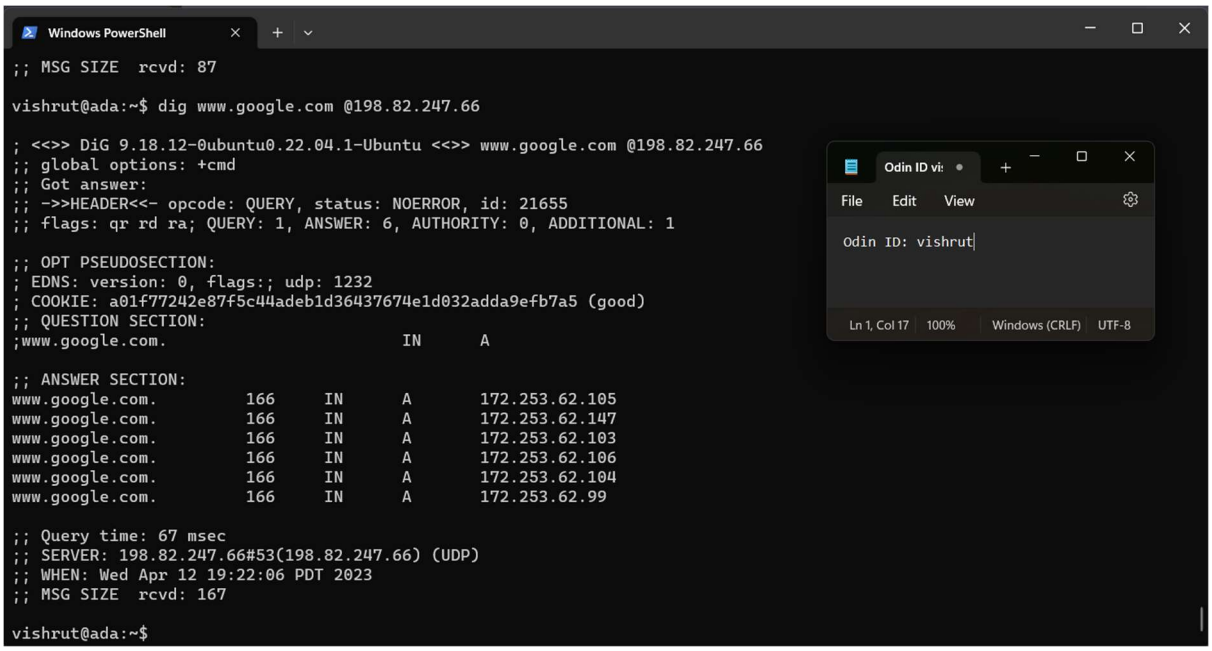
1) Result of ipinfo.io and DB-IP




Geolocation data from ipinfo.io (Product: API, real-time)
IP ADDRESS: 198.82.247.66
COUNTRY: United States
REGION: Virginia
CITY: Blacksburg
ISP: Virginia Polytechnic Institute and State Univ.
ORGANIZATION:
Virginia Polytechnic Institute and State Univ. (vt.edu)
LATITUDE: 37.2296
LONGITUDE: -80.4139
Geolocation data from DB-IP (Product: API, real-time)
IP ADDRESS: 198.82.247.66
COUNTRY: United States
REGION: Virginia
CITY: Blacksburg (Farmview - Ramble)
ISP: Virginia Polytechnic Institute and State Univ.
ORGANIZATION:
Virginia Polytechnic Institute and State Univ.
LATITUDE: 37.2037
LONGITUDE: -80.4143
Geolocation data from IPregistry.co (Product: API, real-time)
Subnet Calculator
Odin ID vi:
File
Edit
View
Odin ID: vishrut
Ln 1, Col 17
100%
Windows (CRLF)
UTF-8
What is static and dynamic IP addresses?
What is an IP Address?
What is a Proxy Server?
My IP address is hacked. What do I do?
ADVERTISEMENT
COMCAST BUSINESS
Get products that grow as you grow.
GET IT NOW
(855) 335-7919

2)


Windows PowerShell
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.
vishrut@ada:~$ dig www.google.com @131.252.208.53
; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> www.google.com @131.252.208.53
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16614
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e32fb2d1b5b4512901000006437766bbea199aacc16b9ed9 (good)
;; QUESTION SECTION:
;www.google.com. IN A
;; ANSWER SECTION:
www.google.com. 153 IN A 142.251.33.100
;; Query time: 0 msec
;; SERVER: 131.252.208.53#53(131.252.208.53) (UDP)
;; WHEN: Wed Apr 12 19:19:39 PDT 2023
;; MSG SIZE rcvd: 87
vishrut@ada:~$
Odin ID vi:
File
Edit
View
Odin ID: vishrut
Ln 1, Col 17
100%
Windows (CRLF)
UTF-8



3) Below are the distances between each DNS server and the IP address

142.251.33.100 to 172.253.62.105 -> 2016 n mi, 3734 km

142.251.33.100 to 172.253.62.103 -> 2016 n mi, 3734 km

142.251.33.100 to 172.253.62.147 -> 611 n mi, 1132 km

142.251.33.100 to 172.253.62.104 -> 2016 n mi, 3734 km

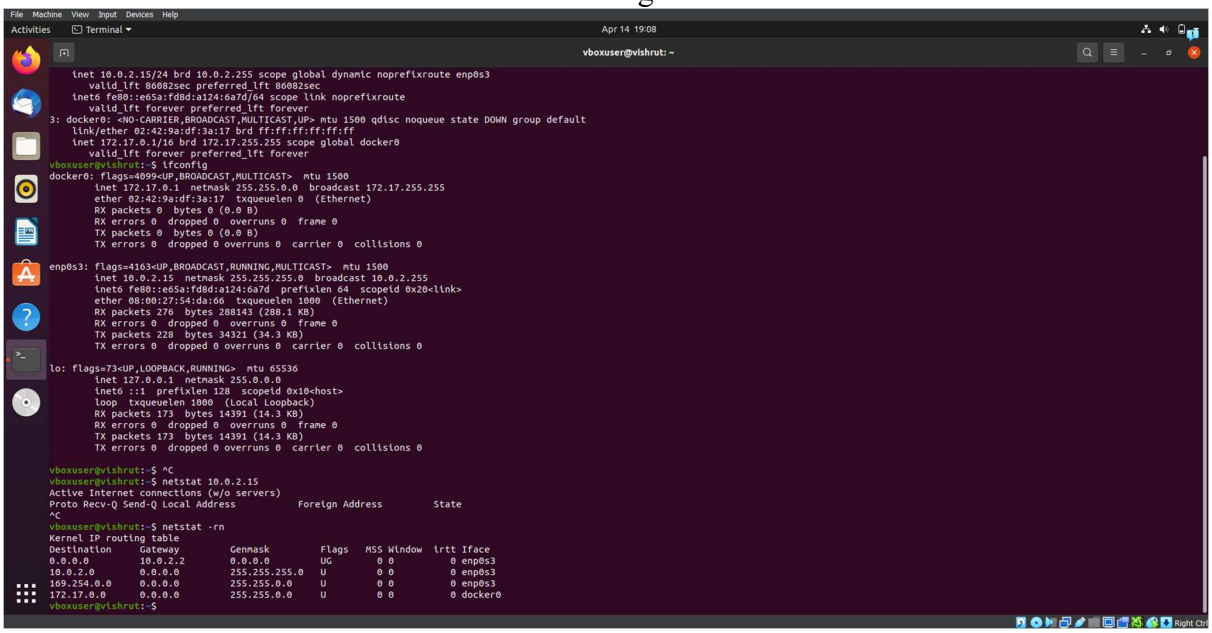
142.251.33.100 to 172.253.62.106 -> 2016 n mi, 3734 km

142.251.33.100 to 172.253.62.99 -> 2016 n mi, 3734 km

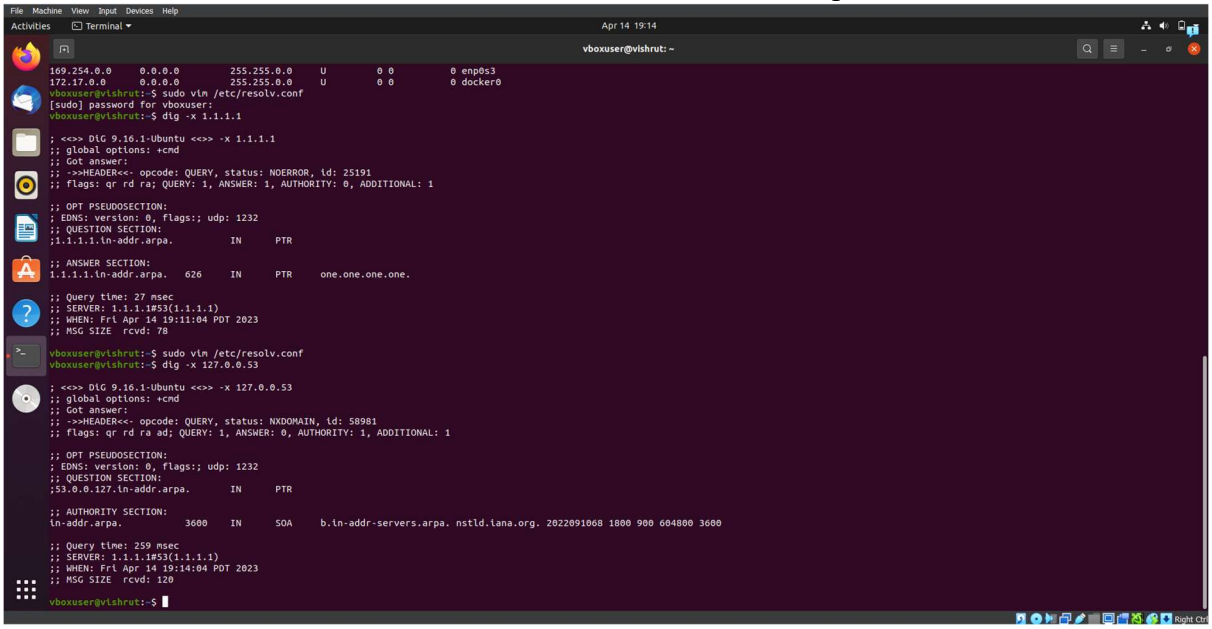
4) No, there is no clear indication of the geographic location of the servers in the traceroute.

5. Network Recap Lab #3

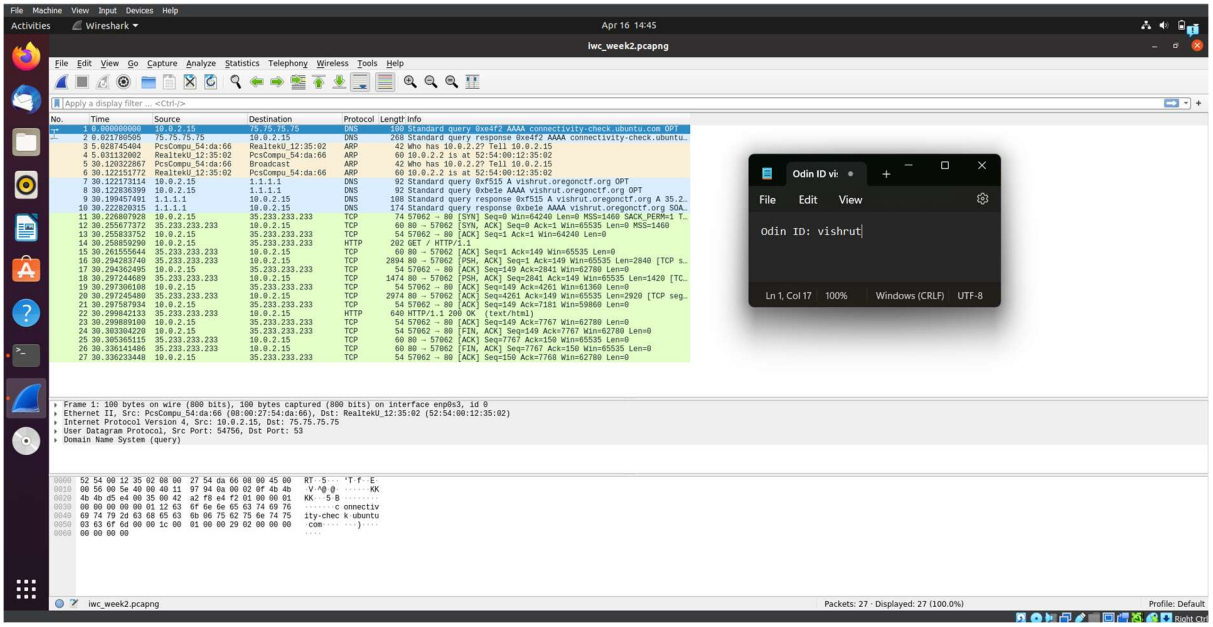
The screenshot below shows the results of ifconfig and the netstat commands.



The screenshot below shows the result of the reverse DNS lookup on the DNS server.



6. Collect and analyze the network trace of a connection



1) There are 3 DNS requests

2) There are 7 TCP connections initiated by the browser simultaneously to the site.

3) There is 1 HTTP GET request for the embedded object.