Lab Notebook 2

Submitted By: Shrikrishna Bhat

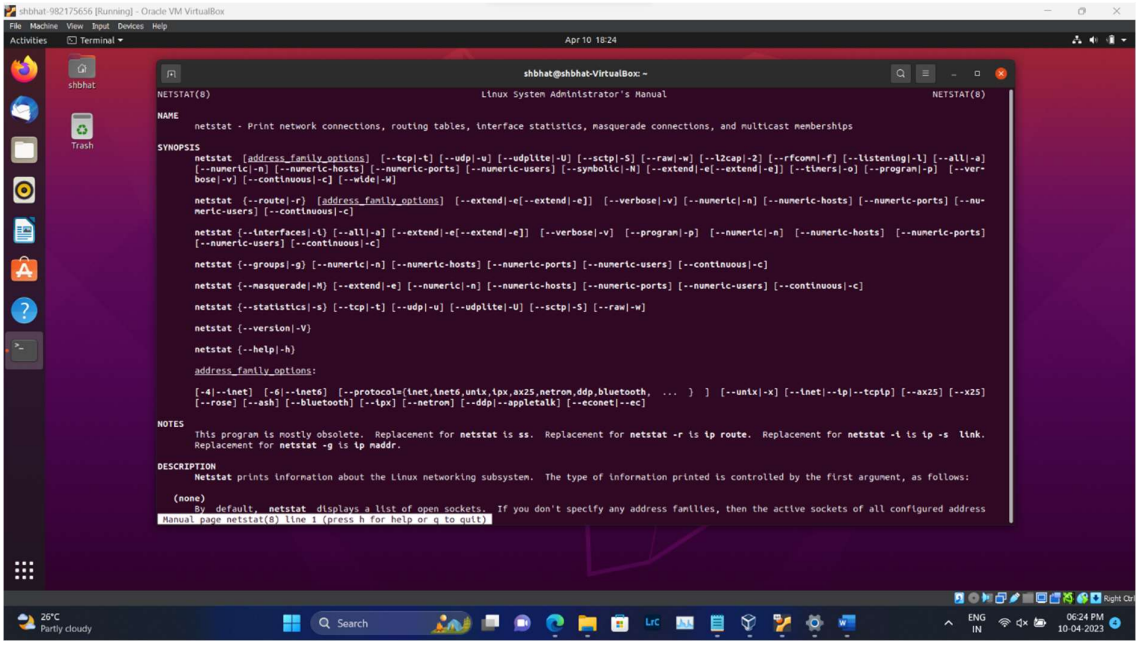
Contents

Section 1

TCP #1

1.1 netstat

1.1.1 man netstat



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

```
# Local services
shbhat@shbhat-VirtualBox:~$ sudo netstat -tlp
[sudo] password for shbhat:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      536/systemd-resolve
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      577/cupsd
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      577/cupsd
```

1.1.3 For port numbers that are named, examine /etc/services and find the port number that corresponds to it. Include this mapping in your lab notebook.

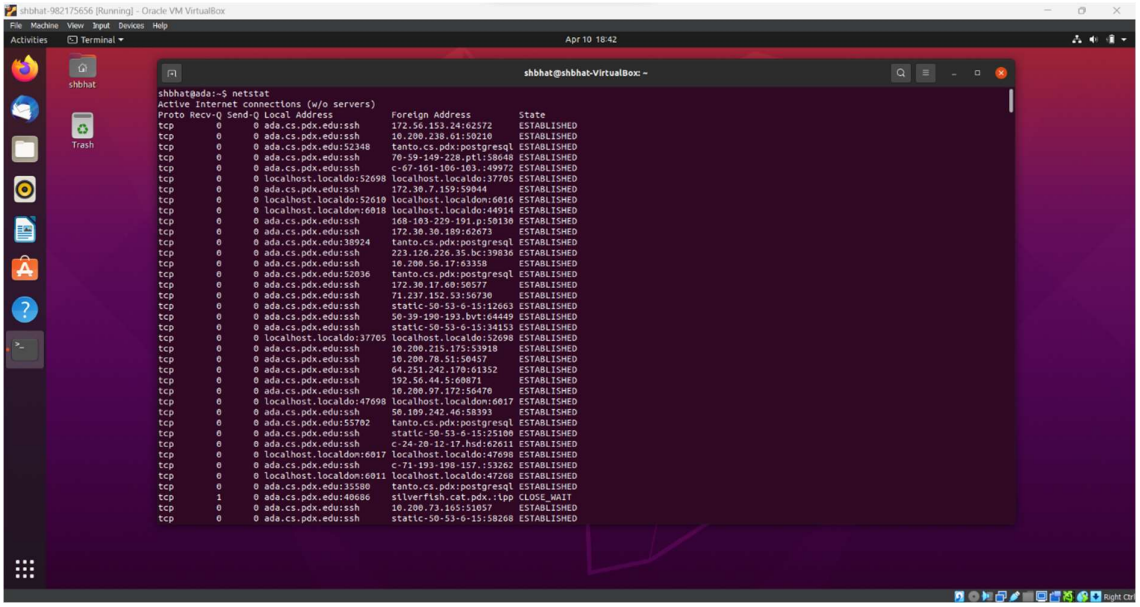
Answer: I got the port number as 631, which corresponds to ipp.

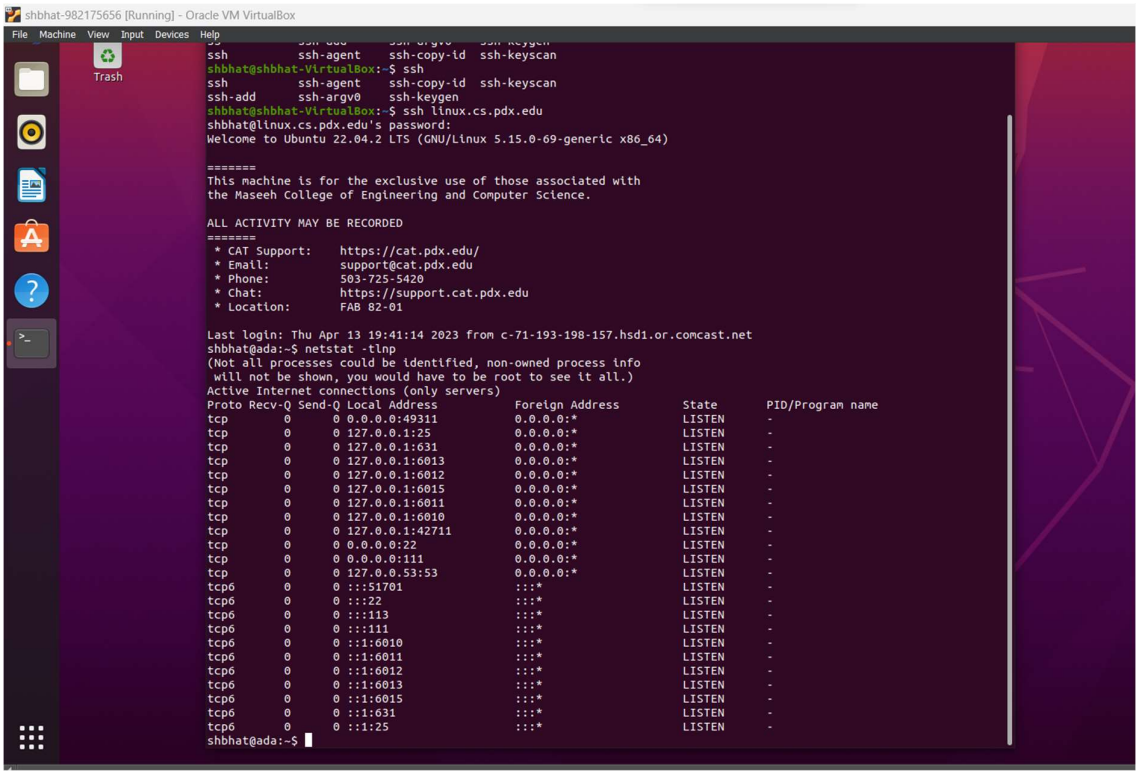
```
shbhat@shbhat-VirtualBox:~$ cat /etc/services | grep ipp
ipp             631/tcp                         # Internet Printing Protocol
```

1.1.4 For ports that only have a number, what service might it be providing based on the name of the program that is being run?

Answer: I did not get any port numbers having only number but on reading about it I found out that it is used to run container services.

1.1.5 Run the netstat command again, but do not use sudo as this is a machine managed by CAT. Include a screenshot of the output.





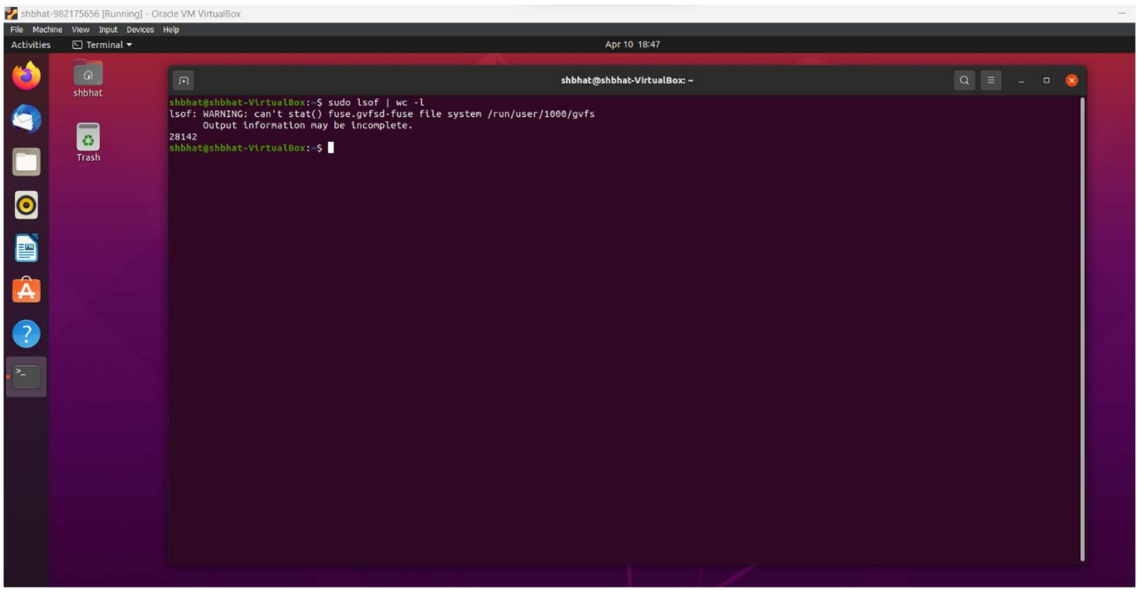
1.1.6 What services does this machine provide for external access?

Answer:

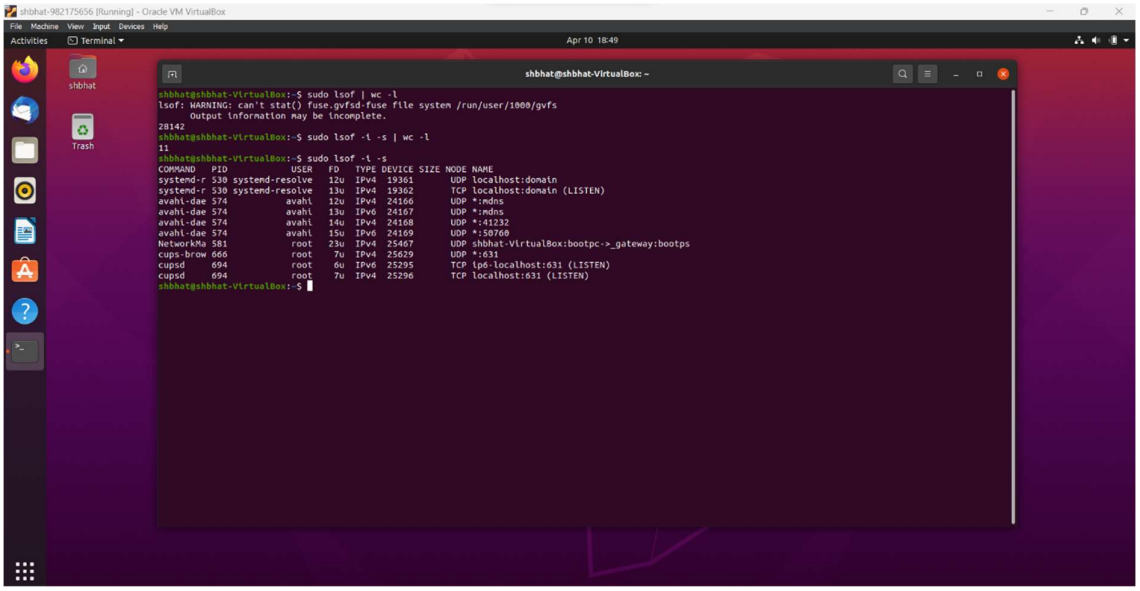
It depends on which port the services are being run, some may provide container service. Some may provide IPP service etc.

1.2 lsof

1.2.1 sudo lsof | wc -l



1.2.2 Use the -i and the -s flag of lsof to generate a listing that is equivalent to the one generated with netstat previously and include it in your lab notebook



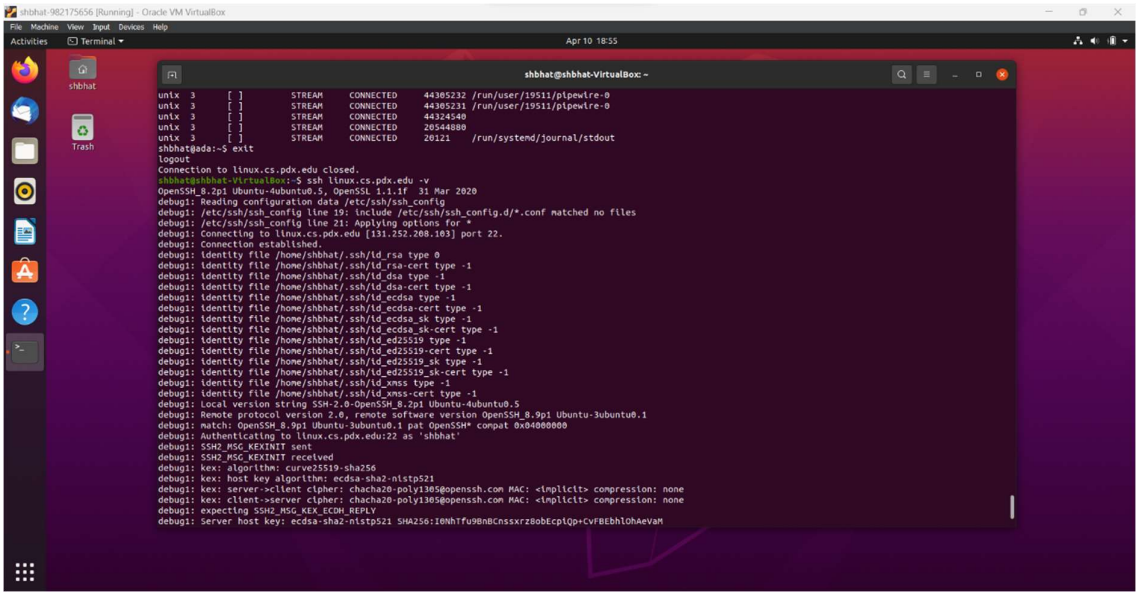
1.3 nc

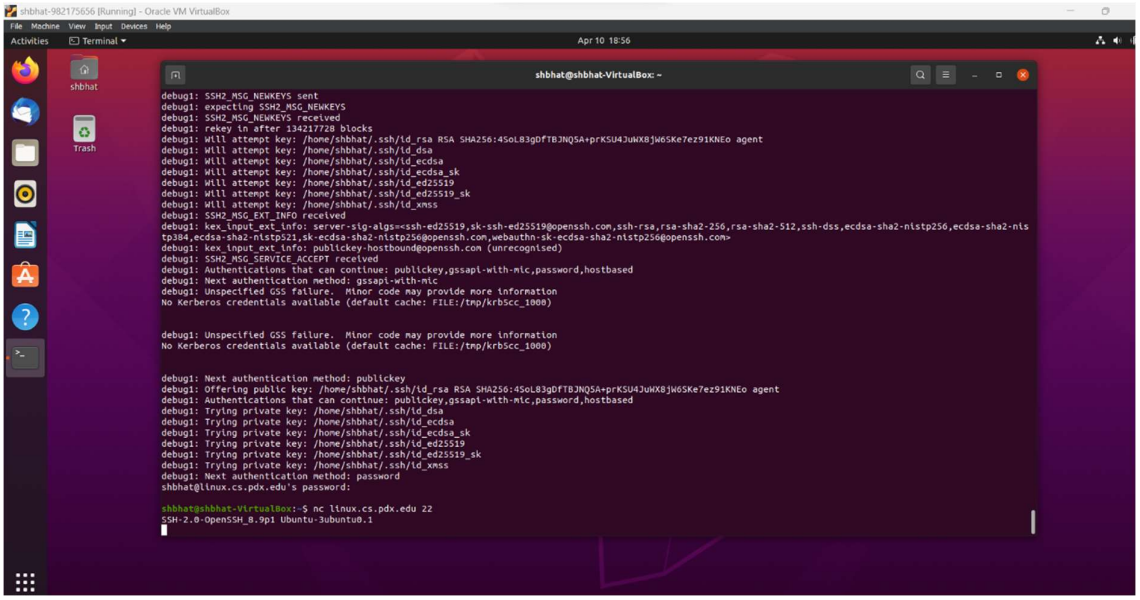
1.3.1 Include for your lab notebook, the version of ssh that is being used. (Type Ctrl+c to exit)

Answer:

Port 22 is being used.

SSh version - SSH-2.0-OpenSSH_8.9p1 is found.





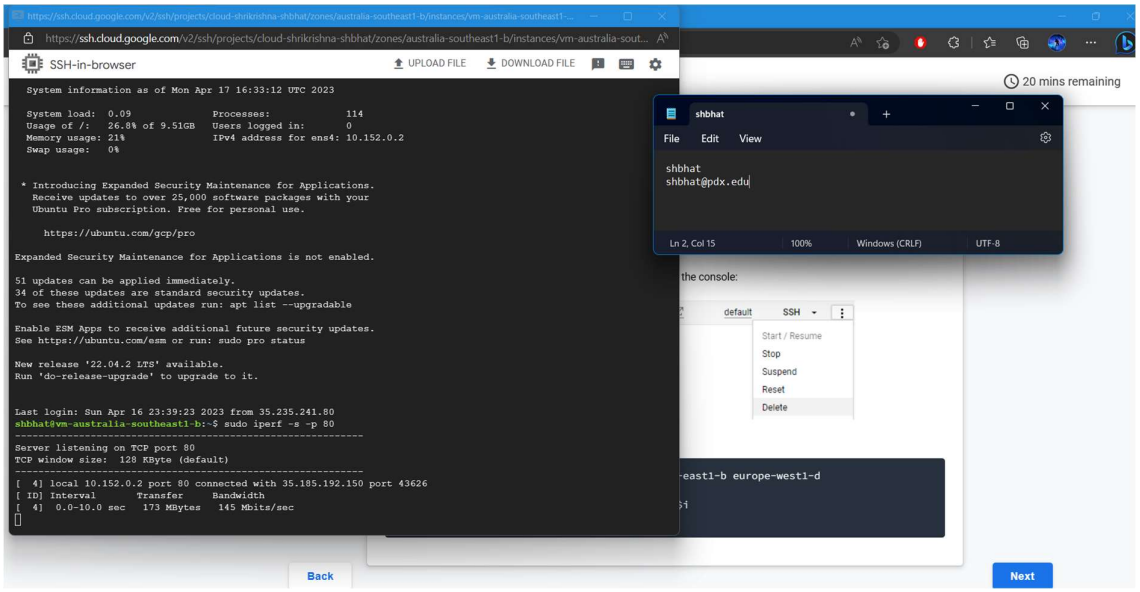
TCP #2

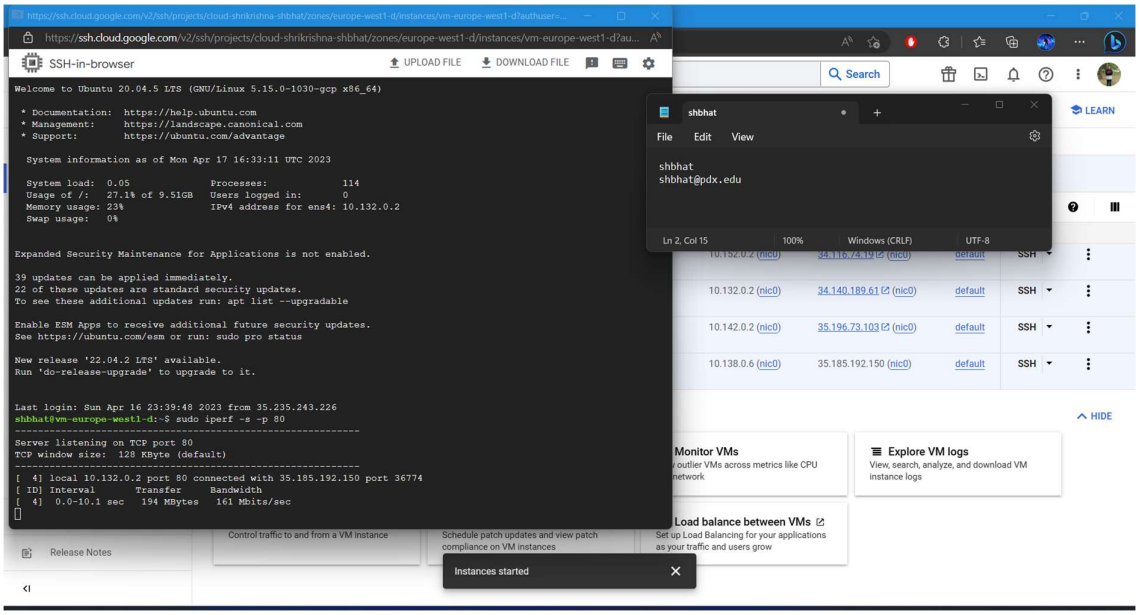
2.1 iperf

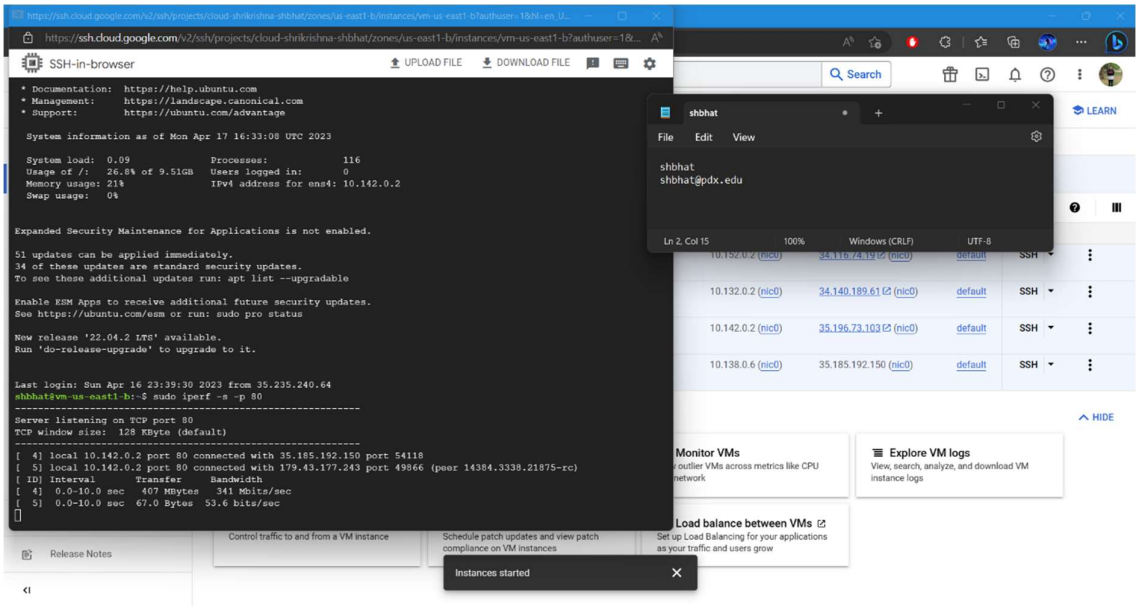
2.1.1 – Install iperf in all cloud instances.

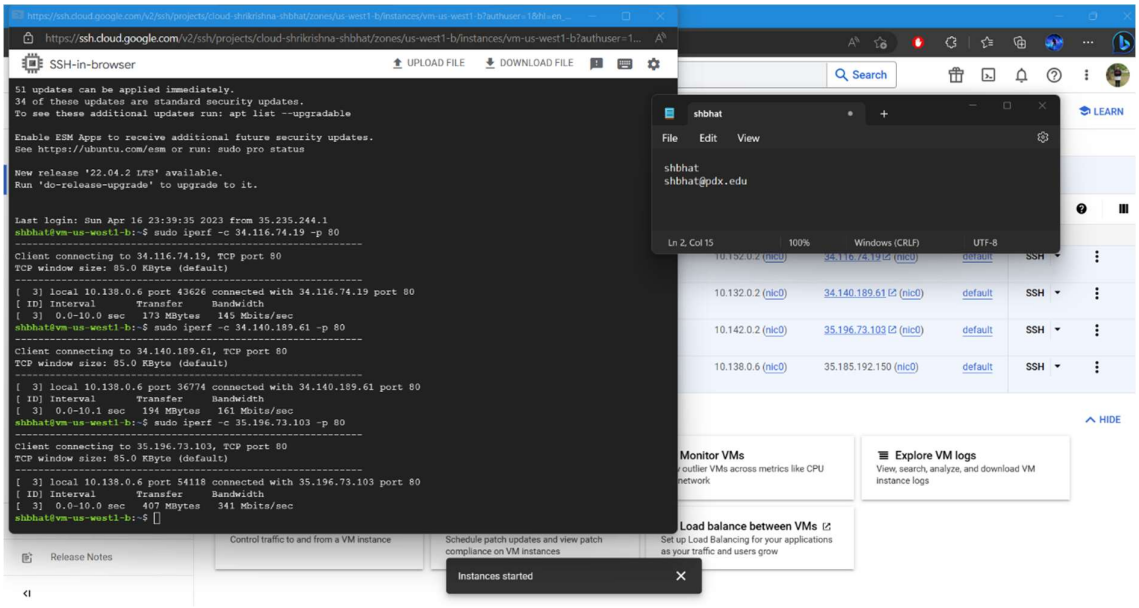
Answer: Installed and checked it.

2.1.2 Show a screenshot of the measured bandwidth available between your us-west1-b VM and each of the other Compute Engine VMs. Explain the relative differences (or lack thereof) in your results.









Why relative differences?

Answer:

There are various causes for differences in bandwidth, it might be due to distance since it might have to fetch from nearby server or distant server. It might also be due to congestion of packets. It might also be due to the quality of the network connection. Networks with higher latency or packet loss rates can result in reduced bandwidth or less consistent bandwidth measurements. It might also be due to not choosing the optimal routing path which can cause more traffic and there might be reduced bandwidth.

HTTP # 3

3.1 HTTP developer tools Part 1

3.1.1 What is the URL being requested?

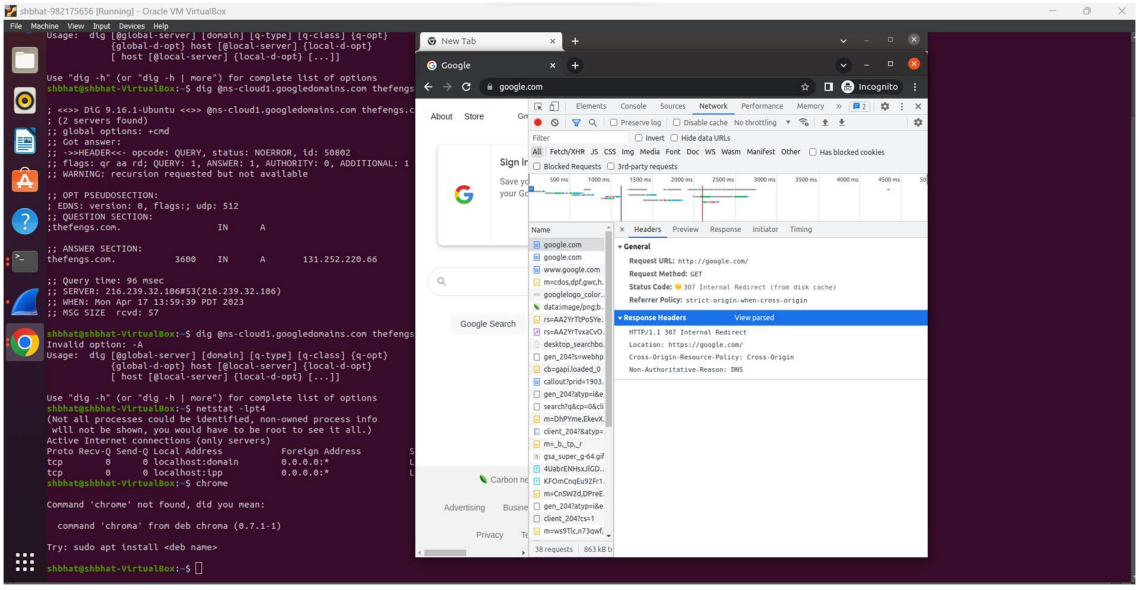
Answer: URL being requested is: http://google.com/

3.1.2 What is the HTTP status code in the response and what does it mean?

Answer: Status code 307 Internal Redirect

3.1.3 Look up the status code. Show the associated HTTP response header that is sent in conjunction with this status code for the request.

Answer:



3.2 HTTP developer tools Part 2

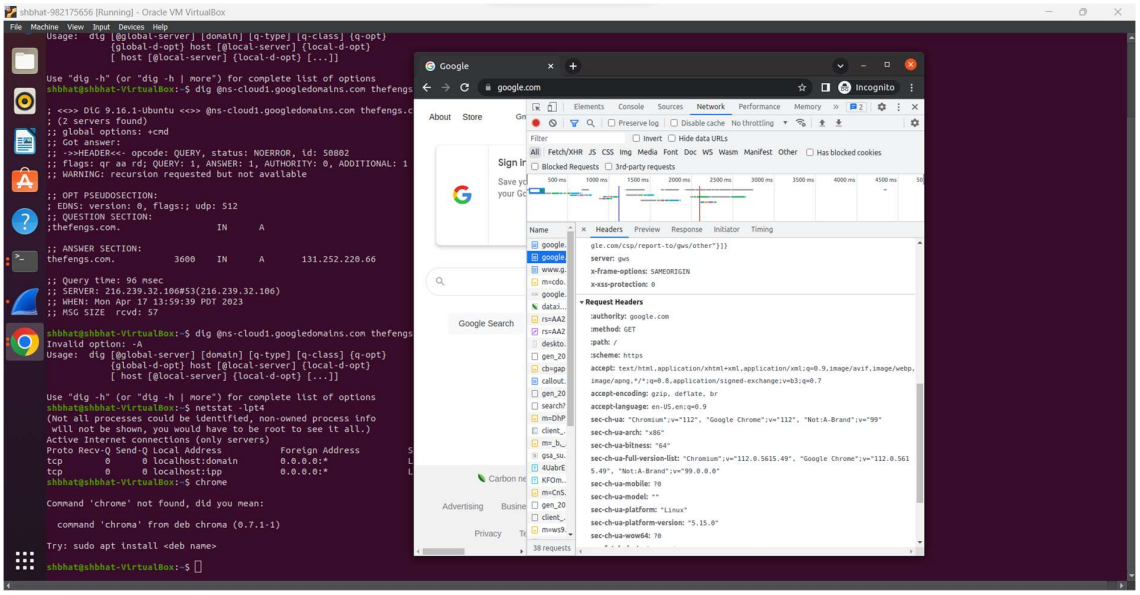
3.2.1 What is the URL being requested? Is it using HTTP or HTTPS?

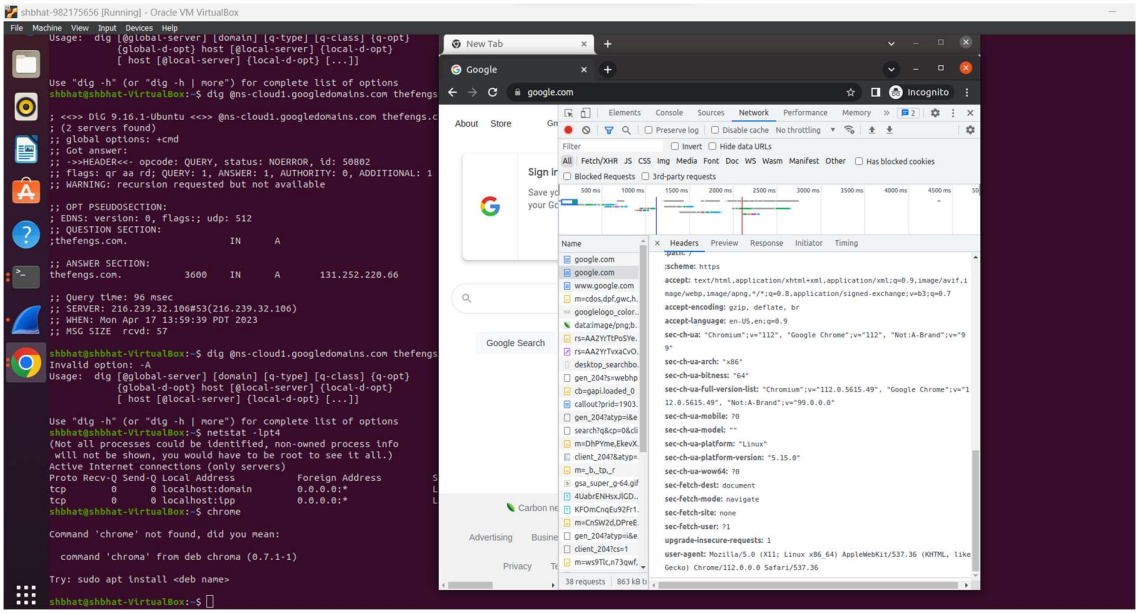
Answer: HTTPS

3.2.2 What are the Host: (HTTP 1.1) or: authority: (HTTP 2.0) headers sent by the browser? What is the User-Agent: HTTP header that is sent?

Answer: User agent is mozilla/5.0

Authority: google.com



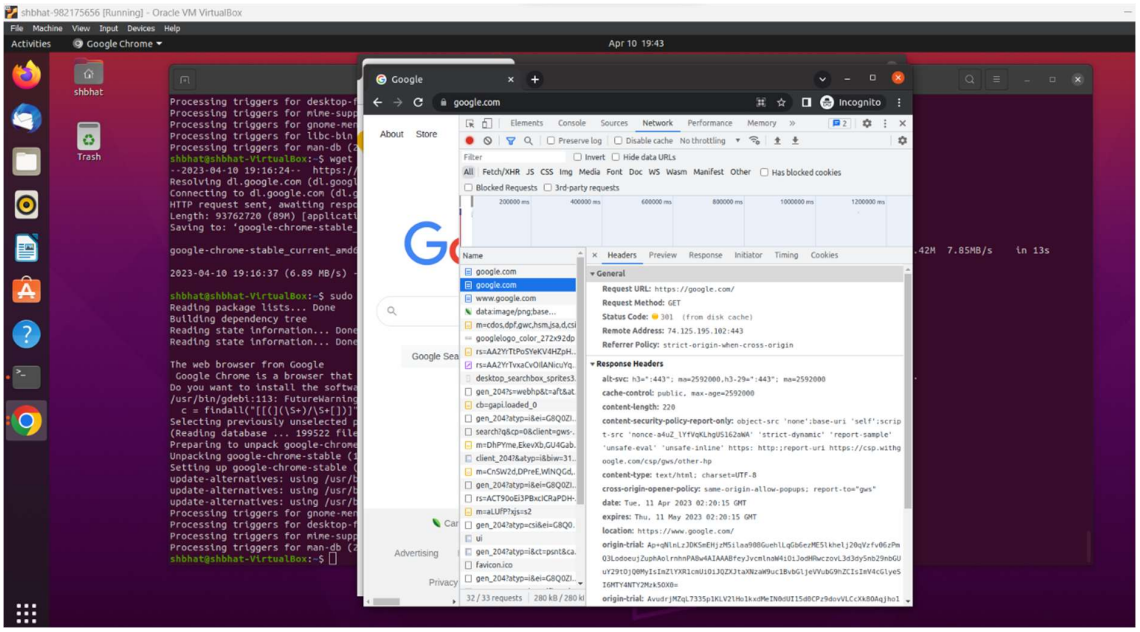


3.2.3 What is the HTTP status code in the response and what does it mean? Is it different from the first status code? If so, what is the semantic difference?

Answer: 301, it is different from first status code.

301 redirect is a permanent redirect, while a 307 redirect is a temporary redirect. If you are permanently moving a page to a new location, use a 301 redirect. If you are temporarily moving a page to a new location, use a 307 redirect.

3.2.4 Show the associated HTTP response header that is sent in conjunction with this status code for the request.



3.3 HTTP developer tools Part 3

3.3.1 What is the URL being requested? Is it using HTTP or HTTPS?

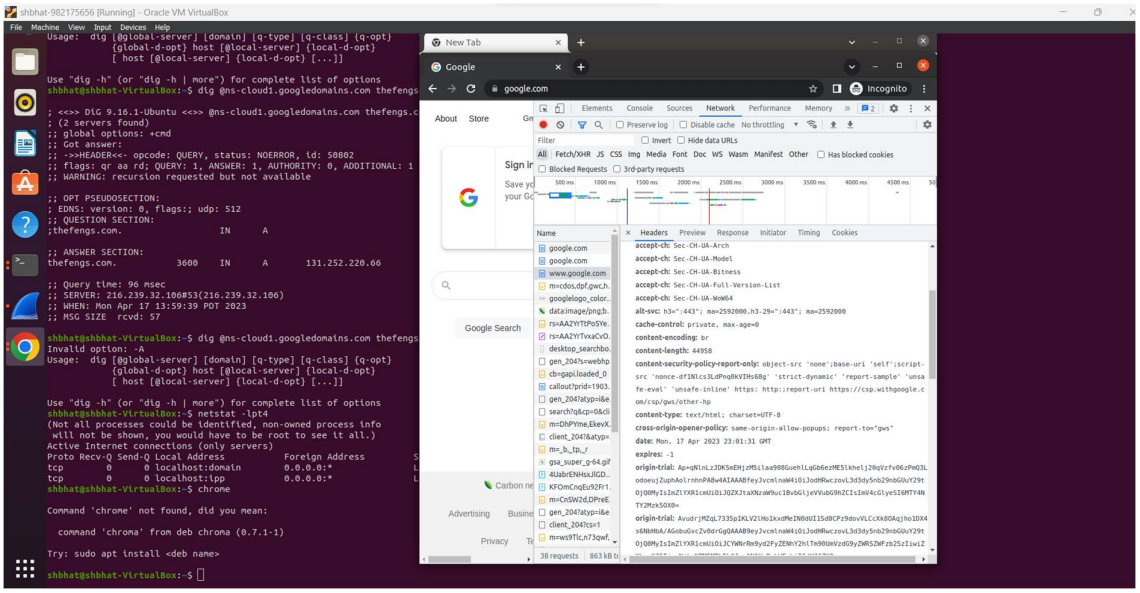
Answer: https://google.com, it is using HTTPS.

3.3.2 What is the HTTP status code in the response?

Answer: Status code 200

3.3.3 Look for an alt-svc: HTTP response header. Does the server believe the client can use HTTP3/QUIC?

Answer: On looking at the alt-svc, we can see that server believes that client can use HTTP3 since we can see the value h3 there.



3.3.4 Examine the HTTP response headers for cookies. Show the cookies that are set and which ones specify that no SameSite restrictions are in place. What does the setting indicate about the cookies that are set?

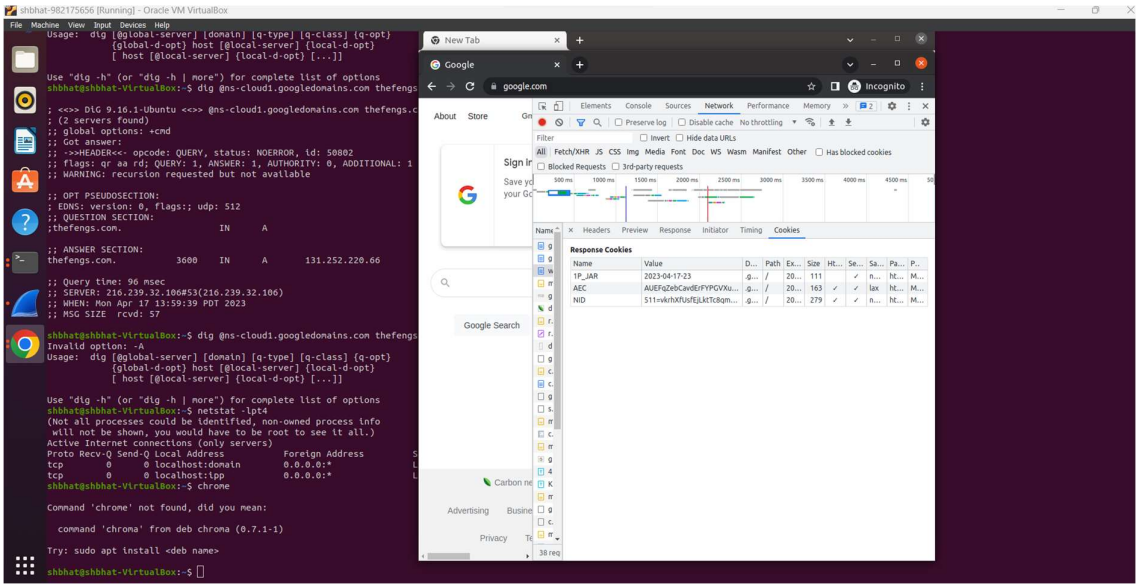
Answer:

On examining the cookies we can see that there are two values ‘lax’ and ‘none’.

Lax - Means that the cookie is not sent on cross-site requests, such as on requests to load images or frames, but is sent when a user is navigating to the origin site from an external site (for example, when following a link). This is the default behaviour if the SameSite attribute is not specified.

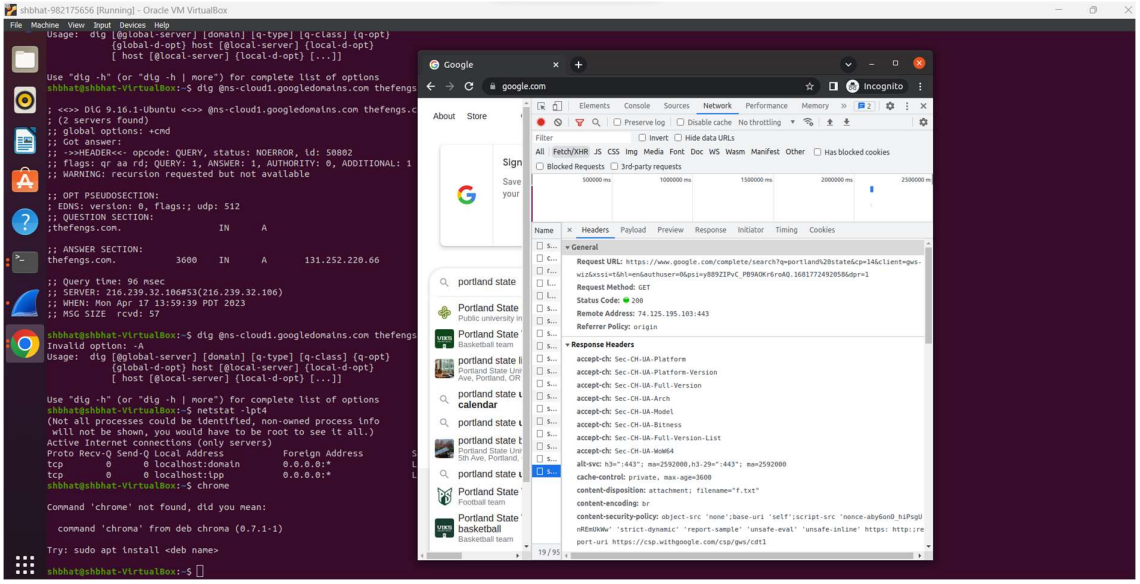
None - means that the browser sends the cookie with both cross-site and same-site requests. The Secure attribute must also be set when setting this value, like so SameSite=None; Secure. If Secure is missing an error will be logged.

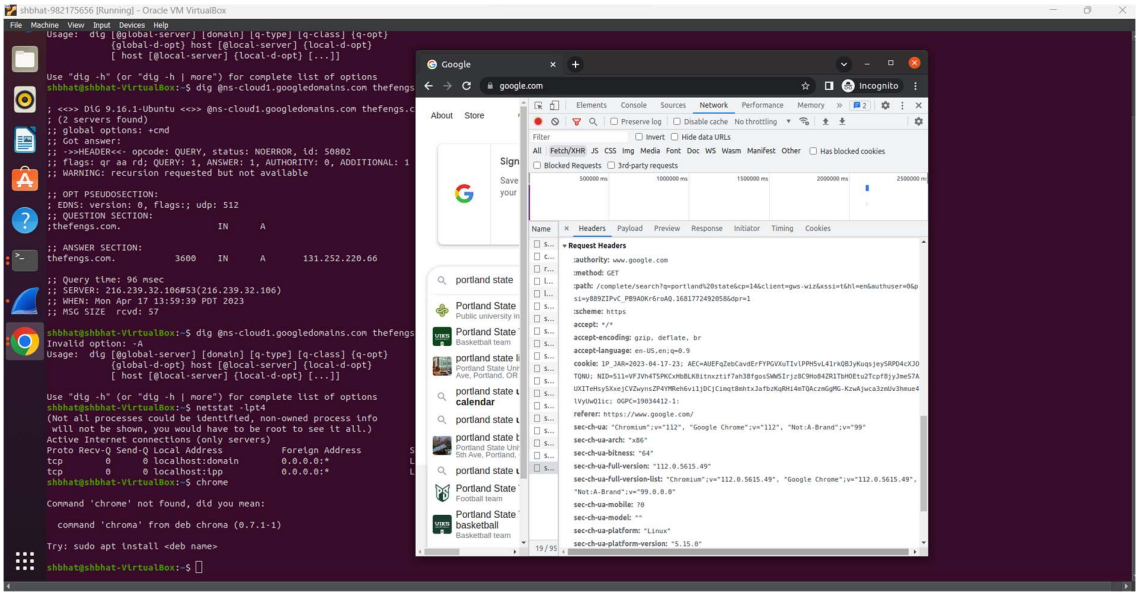
Source : [Set-Cookie - HTTP | MDN (mozilla.org)]

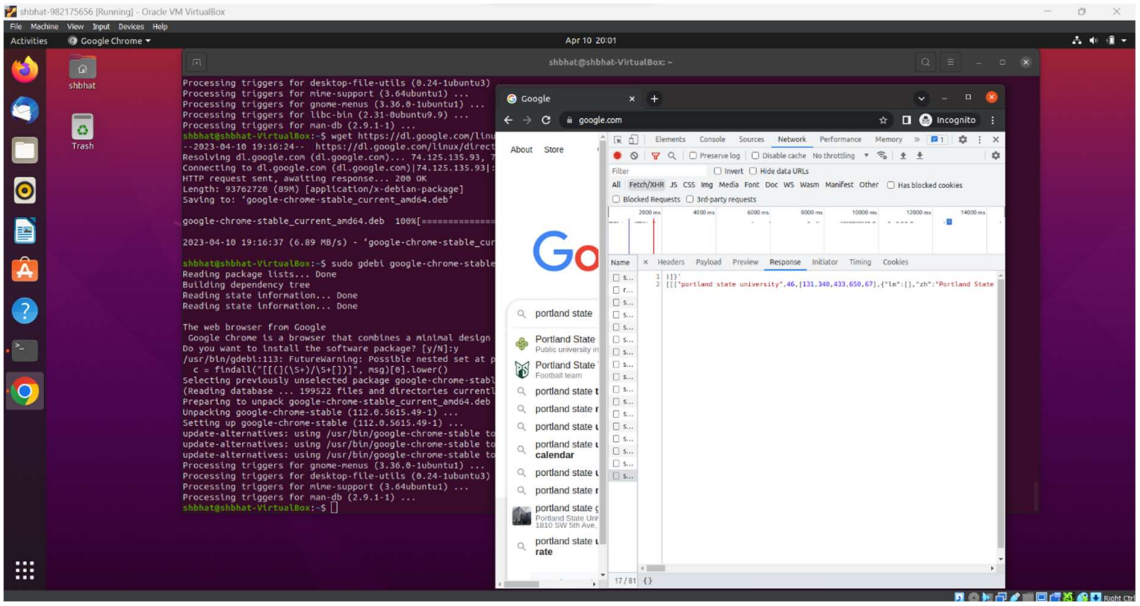


3.4 Asynchronous HTTP requests

3.4.1 Show the requests and responses in the listing. Click on the last request sent, then click on the response to see that its payload has returned the data that is then rendered on the search page similar to what is shown below for “rabbid”.




shbhat-982175656 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Usage: dig [@global-server] [domain] [q-type] [q-class] {q-opt}
{global-d-opt} host [@local-server] {local-d-opt}
[host [@local-server] {local-d-opt} [...]]
Use "dig -h" (or "dig -h | more") for complete list of options
shbhat@shbhat-VirtualBox:~$ dig @ns-cloud1.googledomains.com thefengs
; <<>> DiG 9.16.1-Ubuntu <<>> @ns-cloud1.googledomains.com thefengs.c
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50802
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;thefengs.com. IN A
;; ANSWER SECTION:
thefengs.com. 3600 IN A 131.252.220.66
;; Query time: 96 msec
;; SERVER: 216.239.32.106#53(216.239.32.106)
;; WHEN: Mon Apr 17 13:59:39 PDT 2023
;; MSG SIZE rcvd: 57
shbhat@shbhat-VirtualBox:~$ dig @ns-cloud1.googledomains.com thefengs
Invalid option: -A
Usage: dig [@global-server] [domain] [q-type] [q-class] {q-opt}
{global-d-opt} host [@local-server] {local-d-opt}
[host [@local-server] {local-d-opt} [...]]
Use "dig -h" (or "dig -h | more") for complete list of options
shbhat@shbhat-VirtualBox:~$ netstat -lpt4
(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
tcp 0 0 localhost:domain 0.0.0.0:*
tcp 0 0 localhost:ipp 0.0.0.0:*
shbhat@shbhat-VirtualBox:~$ chrome
Command 'chrome' not found, did you mean:
command 'chroma' from deb chroma (0.7.1-1)
Try: sudo apt install <deb name>
shbhat@shbhat-VirtualBox:~$
Google
google.com
About Store
portland state
Portland State
Public university in
Portland State
Basketball team
portland state
calendar
Portland State
Football team
Portland State
basketball
Basketball team
Elements Console Sources Network Performance Memory
Request Headers
:authority: www.google.com
:method: GET
:path: /complete/search?q=portland%20state&cp=14&client=gws-wiz&xssi=t&hl=en&authuser=0&psi=y809ZIPvC_PB9AOKr6roAQ.1681772492058&dpr=1
:scheme: https
accept: */*
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="112", "Google Chrome";v="112", "Not:A-Brand";v="99"
sec-ch-ua-arch: "x86"
sec-ch-ua-bitness: "64"
sec-ch-ua-full-version: "112.0.5615.49"
sec-ch-ua-full-version-list: "Chromium";v="112.0.5615.49", "Google Chrome";v="112.0.5615.49", "Not:A-Brand";v="99.0.0.0"
sec-ch-ua-mobile: ?0
sec-ch-ua-model: ""
sec-ch-ua-platform: "Linux"
sec-ch-ua-platform-version: "5.15.0"

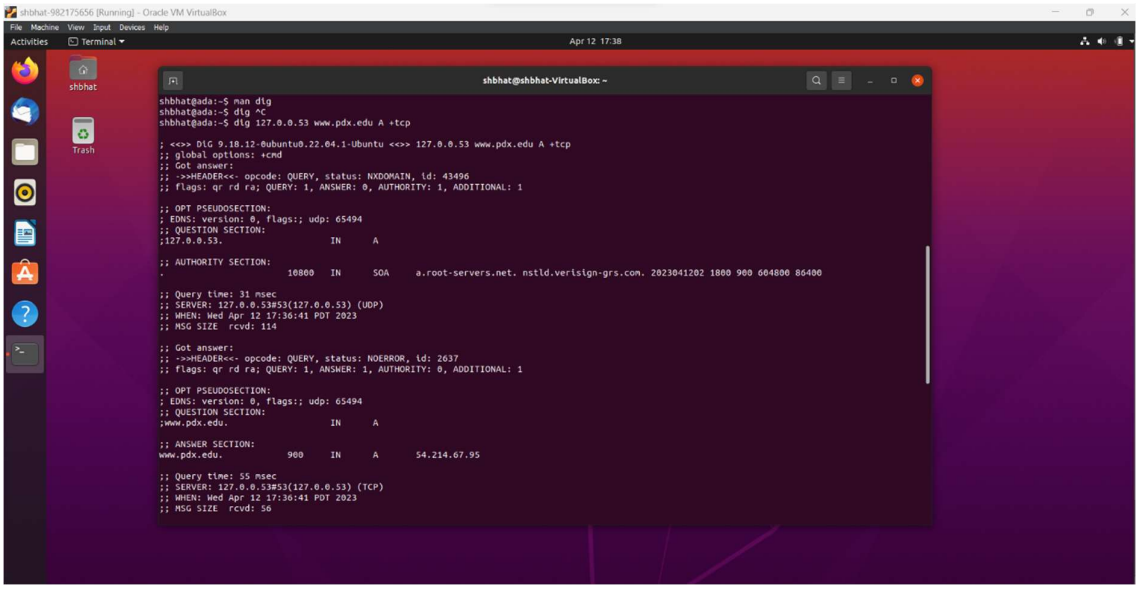

shbhat-982175656 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Google Chrome Apr 10 20:01
shbhat@shbhat-VirtualBox: ~
shbhat
Trash
Processing triggers for desktop-file-utils (0.24-1ubuntu3)
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.9) ...
Processing triggers for man-db (2.9.1-1) ...
shbhat@shbhat-VirtualBox:~$ wget https://dl.google.com/linux/direct
--2023-04-10 19:16:24-- https://dl.google.com/linux/direct
Resolving dl.google.com (dl.google.com)... 74.125.135.93, 7
Connecting to dl.google.com (dl.google.com)|74.125.135.93|:
HTTP request sent, awaiting response... 200 OK
Length: 93762720 (89M) [application/x-debian-package]
Saving to: 'google-chrome-stable_current_amd64.deb'
google-chrome-stable_current_amd64.deb 100%[
2023-04-10 19:16:37 (6.89 MB/s) - 'google-chrome-stable_cur
shbhat@shbhat-VirtualBox:~$ sudo gdebi google-chrome-stable
Reading package lists... Done
Building dependency tree
Reading state information... Done
Reading state information... Done
The web browser from Google
Google Chrome is a browser that combines a minimal design
Do you want to install the software package? [y/N]:y
/usr/bin/gdebi:113: FutureWarning: Possible nested set at p
c = findall("[[(]\S+)/\S+[])]", msg)[0].lower()
Selecting previously unselected package google-chrome-stabl
(Reading database ... 199522 files and directories current
Preparing to unpack google-chrome-stable_current_amd64.deb
Unpacking google-chrome-stable (112.0.5615.49-1) ...
Setting up google-chrome-stable (112.0.5615.49-1) ...
update-alternatives: using /usr/bin/google-chrome-stable to
update-alternatives: using /usr/bin/google-chrome-stable to
update-alternatives: using /usr/bin/google-chrome-stable to
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3)
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
shbhat@shbhat-VirtualBox:~$
Google
google.com
Incognito
About Store
portland state
Portland State
Public university in
Portland State
Football team
portland state
calendar
rate
Elements Console Sources Network Performance Memory
Response
["portland state university",46,[131,340,433,650,67],{"lm":[],"zh":"Portland State

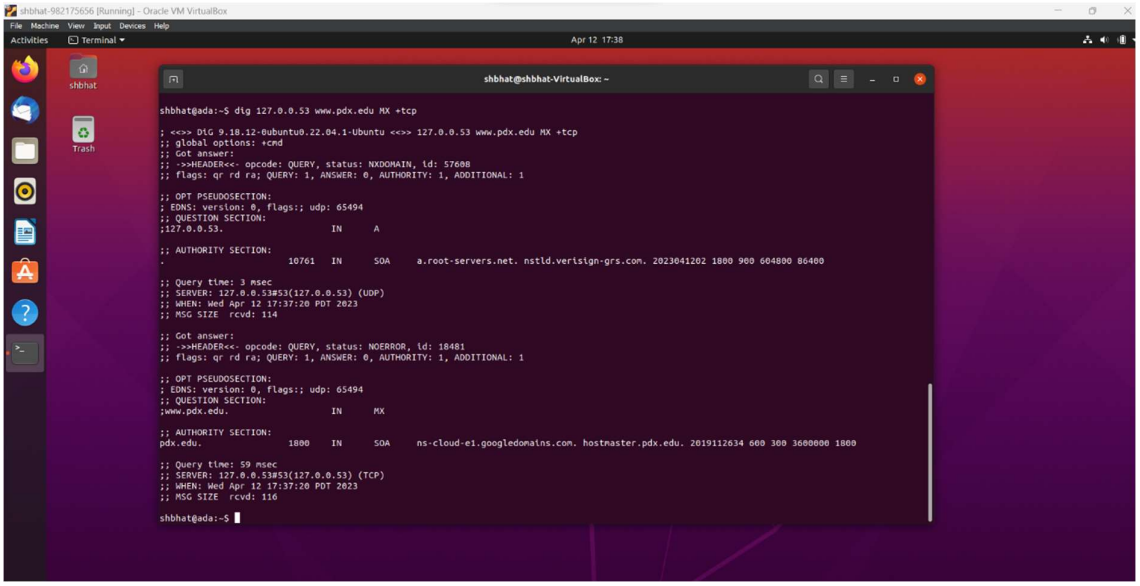
Section 2

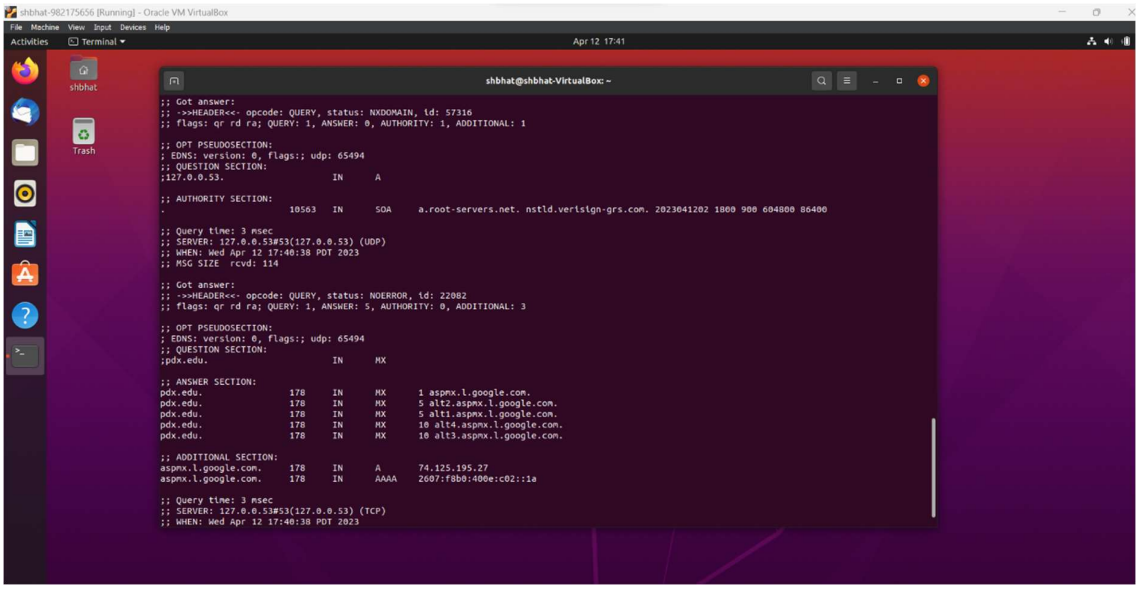
DNS #1

1.1 dig

1.1.1 Use dig to query the PSU's local DNS server at 131.252.208.53 for the A record of www.pdx.edu using TCP. Then, use dig to do the same for the MX record of pdx.edu. What do the ANSWER sections explain about where PSU's web/mail services are run from?







The ANSWER section of the first query should provide an IP address, which is where the web server for www.pdx.edu is hosted. The ANSWER section of the second query should provide one or more mail server names, along with their priority values, which are used for handling email traffic for pdx.edu.

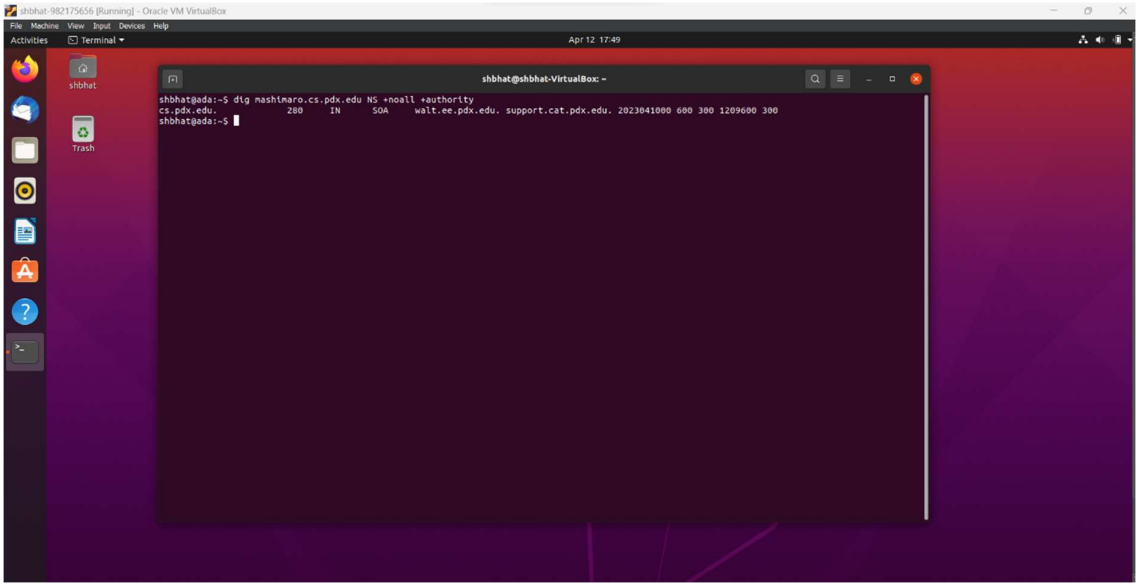
54.214.67.95 – Web services are hosted

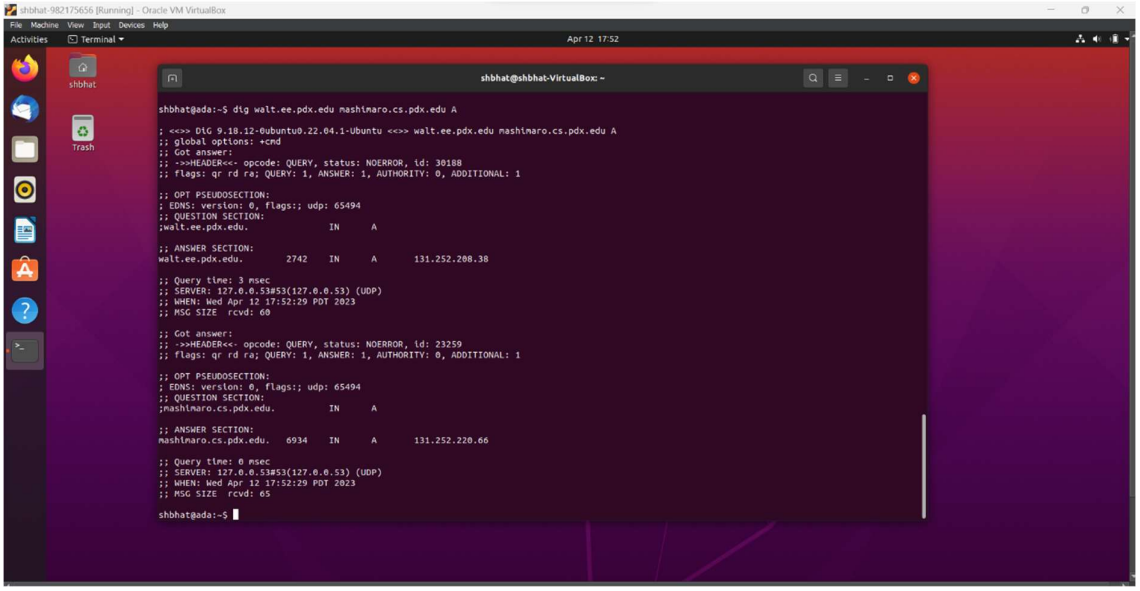
;; ANSWER SECTION:

pdx.edu.	178	IN	MX	1 aspmx.l.google.com.
pdx.edu.	178	IN	MX	5 alt2.aspmx.l.google.com.
pdx.edu.	178	IN	MX	5 alt1.aspmx.l.google.com.
pdx.edu.	178	IN	MX	10 alt4.aspmx.l.google.com.
pdx.edu.	178	IN	MX	10 alt3.aspmx.l.google.com.

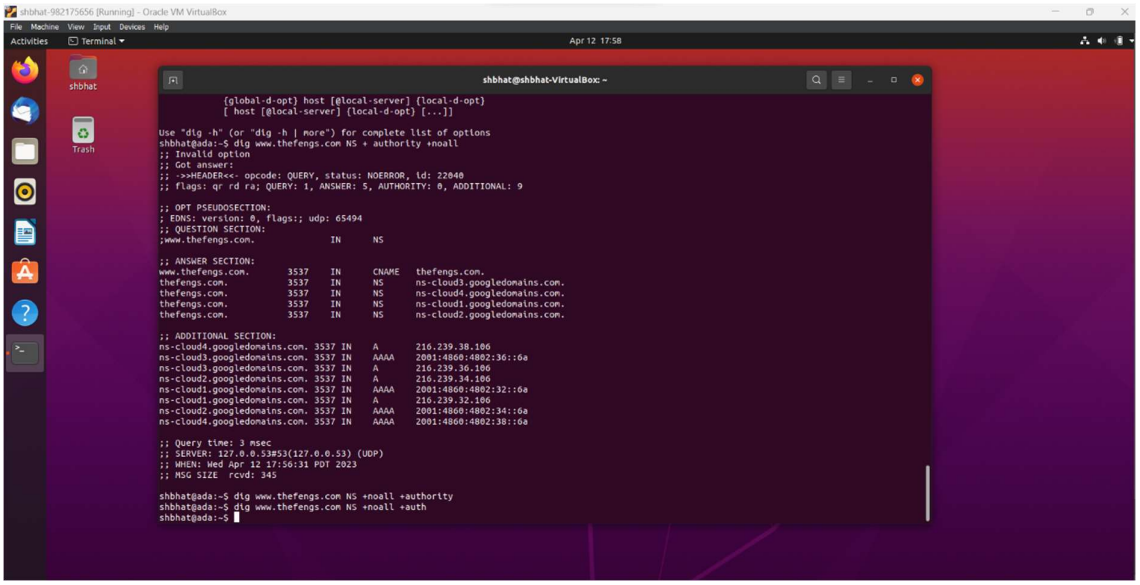
Mail services are hosted

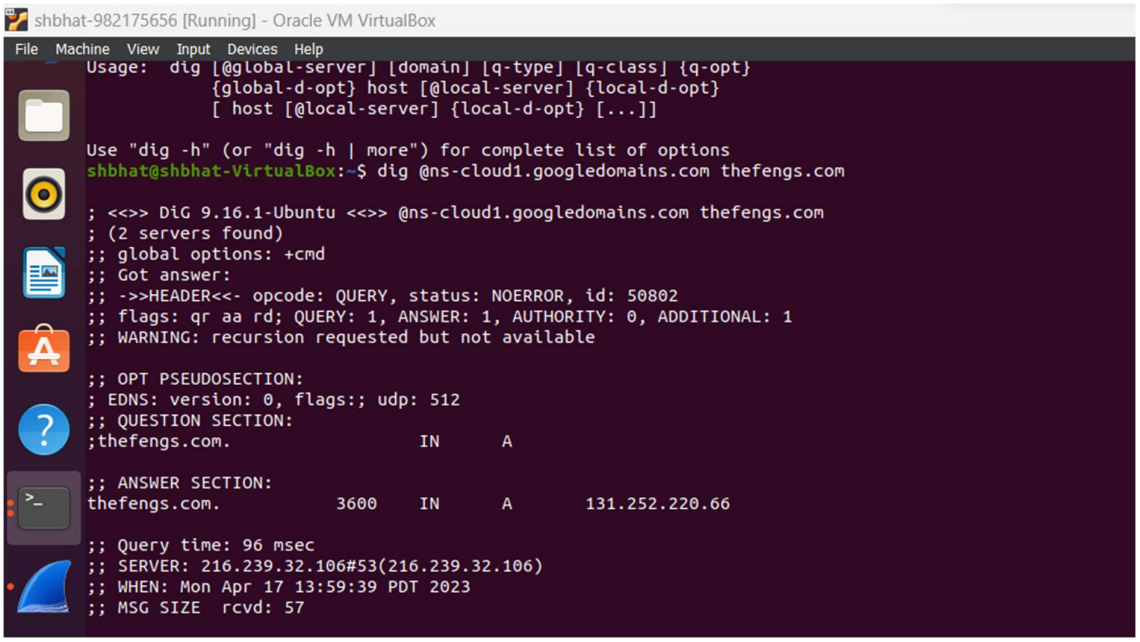
1.1.2 Find the authoritative server (NS record type, AUTHORITY section response) for mashimaro.cs.pdx.edu and then query that server for the A record of mashimaro.cs.pdx.edu. Show both.





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





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

Answer:

When a web request hits port 80 of an IP address, the server relies on the HTTP protocol header to determine which site to serve from. The HTTP protocol header is a part of the HTTP request that a client sends to a server when making an HTTP request. This header

contains several fields, including the "Host" field, which specifies the domain name of the website being requested.

For example, if a client sends an HTTP request to 131.252.220.66 with the following header:

GET / HTTP/1.1

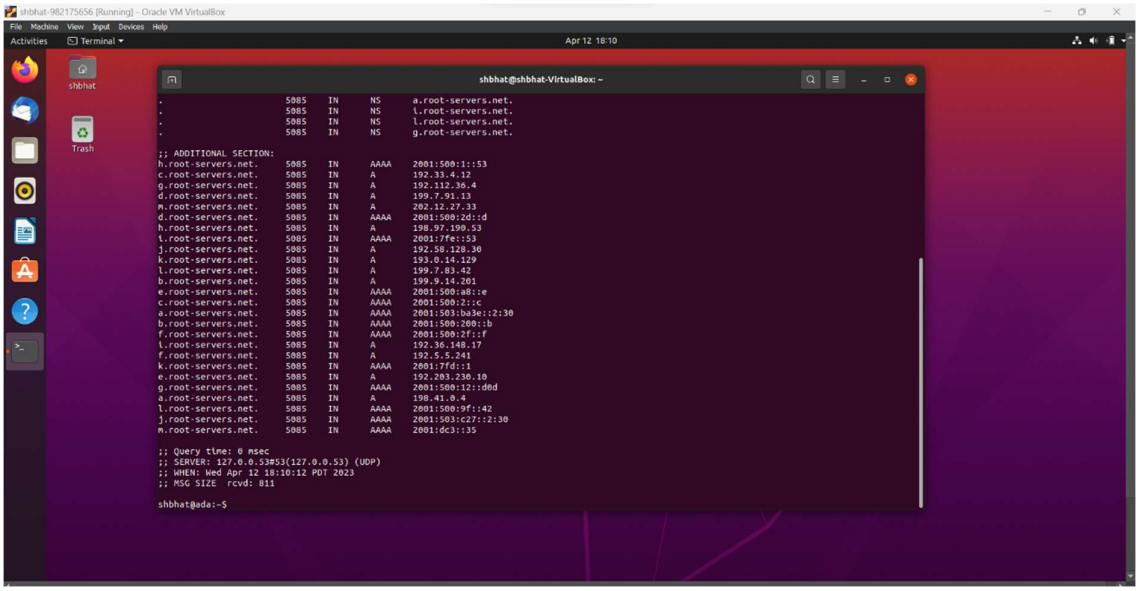
Host: example.com

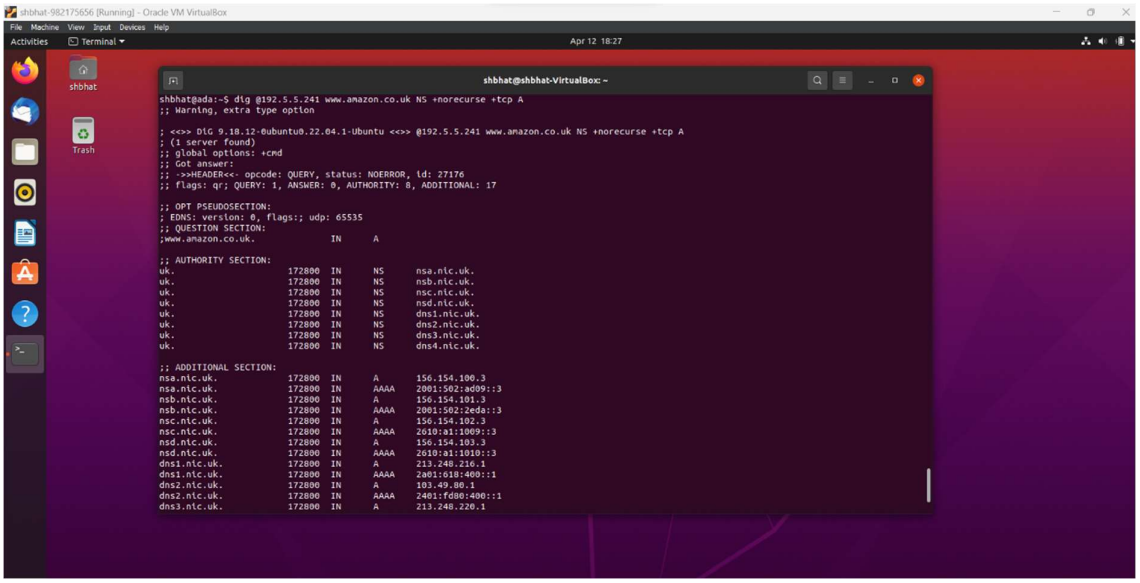
The server at 131.252.220.66 will check the "Host" field in the HTTP header to determine which site the request is intended for. In this case, the server will recognize that the request is intended for the "example.com" website and will serve the appropriate content.

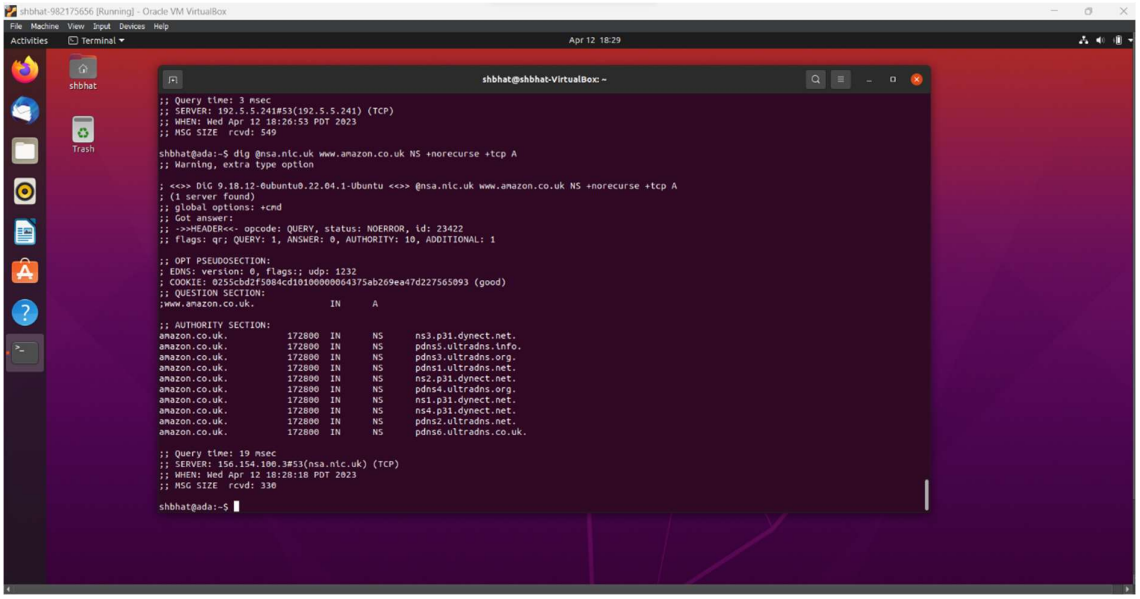
If the "Host" field is missing or contains an unrecognized domain name, the server will typically serve a default website or return an error message.

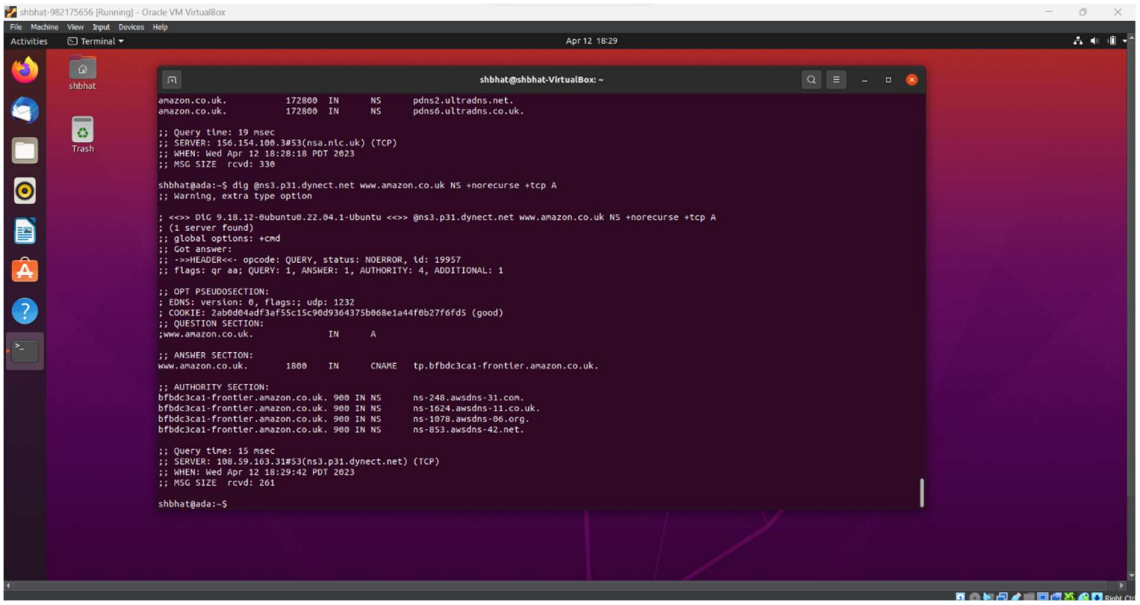
1.2 DNS iterative lookup

1.2.1 Include the results of each query for your lab notebook.



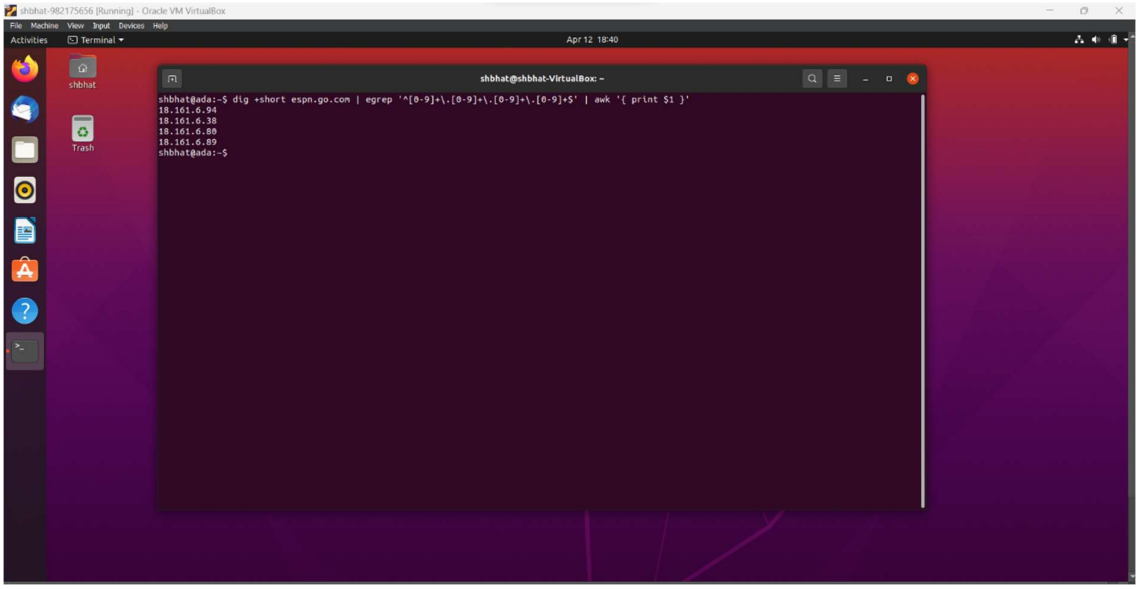

shbhat-982175656 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Apr 12 18:27
shbhat
Trash
shbhat@shbhat-VirtualBox: ~
shbhat@ada:~$ dig @192.5.5.241 www.amazon.co.uk NS +norecurse +tcp A
;; Warning, extra type option
; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> @192.5.5.241 www.amazon.co.uk NS +norecurse +tcp A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27176
;; 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 A
;; 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
nsc.nic.uk. 172800 IN AAAA 2610:a1:1009::3
nsd.nic.uk. 172800 IN A 156.154.103.3
nsd.nic.uk. 172800 IN AAAA 2610:a1:1010::3
dns1.nic.uk. 172800 IN A 213.248.216.1
dns1.nic.uk. 172800 IN AAAA 2a01:618:400::1
dns2.nic.uk. 172800 IN A 103.49.80.1
dns2.nic.uk. 172800 IN AAAA 2401:fd80:400::1
dns3.nic.uk. 172800 IN A 213.248.220.1


shbhat-982175656 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Apr 12 18:29
shbhat
Trash
shbhat@shbhat-VirtualBox: ~
;; Query time: 3 msec
;; SERVER: 192.5.5.241#53(192.5.5.241) (TCP)
;; WHEN: Wed Apr 12 18:26:53 PDT 2023
;; MSG SIZE rcvd: 549
shbhat@ada:~$ dig @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
;; Warning, extra type option
; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23422
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0255cbd2f5084cd10100000064375ab269ea47d227565093 (good)
;; QUESTION SECTION:
;www.amazon.co.uk. IN A
;; AUTHORITY SECTION:
amazon.co.uk. 172800 IN NS ns3.p31.dynect.net.
amazon.co.uk. 172800 IN NS pdns5.ultradns.info.
amazon.co.uk. 172800 IN NS pdns3.ultradns.org.
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 pdns4.ultradns.org.
amazon.co.uk. 172800 IN NS ns1.p31.dynect.net.
amazon.co.uk. 172800 IN NS ns4.p31.dynect.net.
amazon.co.uk. 172800 IN NS pdns2.ultradns.net.
amazon.co.uk. 172800 IN NS pdns6.ultradns.co.uk.
;; Query time: 19 msec
;; SERVER: 156.154.100.3#53(nsa.nic.uk) (TCP)
;; WHEN: Wed Apr 12 18:28:18 PDT 2023
;; MSG SIZE rcvd: 330
shbhat@ada:~$

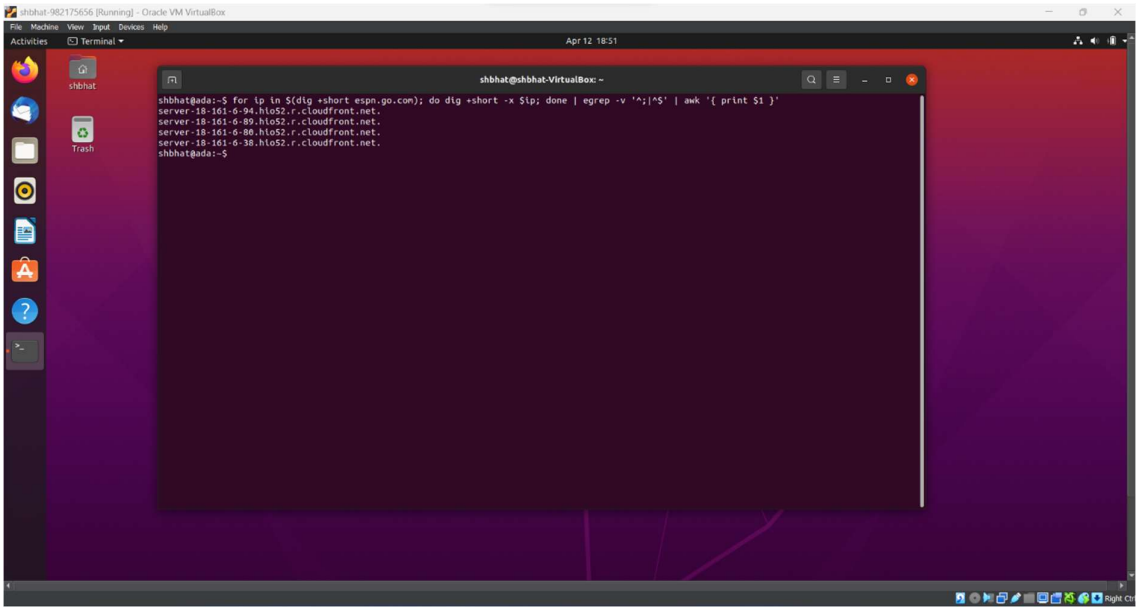


1.3 Reverse DNS Lookup

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



1.3.2 Take that list and create a single for loop in the shell that iterates over the list and performs a reverse lookup of each IP address to find each address's associated DNS name. As with the previous step, pipe the output of the for loop to egrep and awk so that the output consists only of the DNS names.

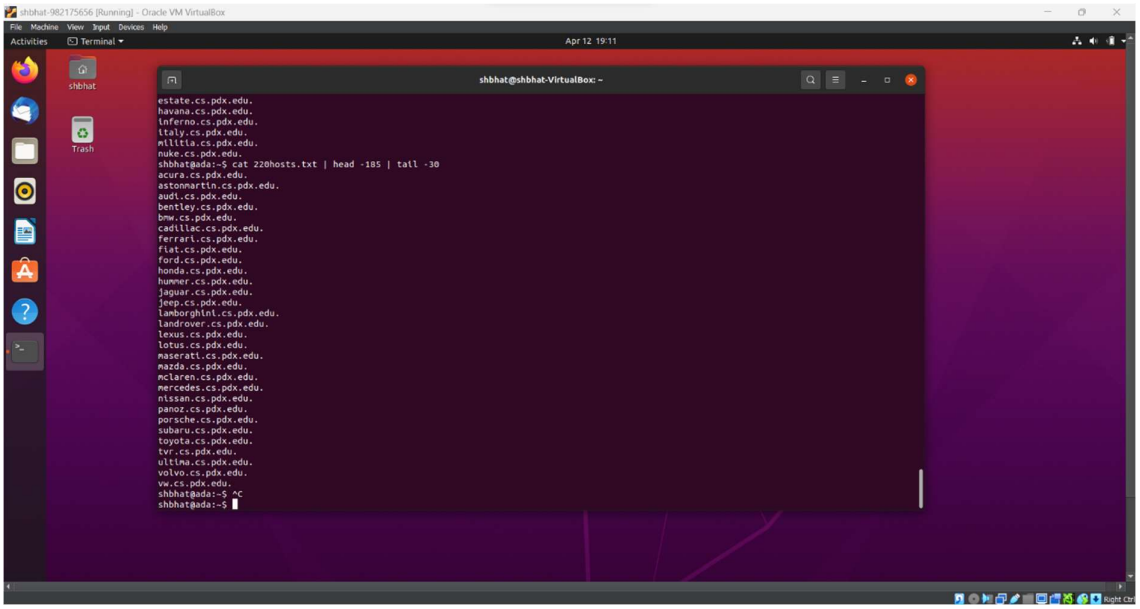


1.4 Hosts Enumeration

1.4.1 Show the results in your lab notebook.

Answer:

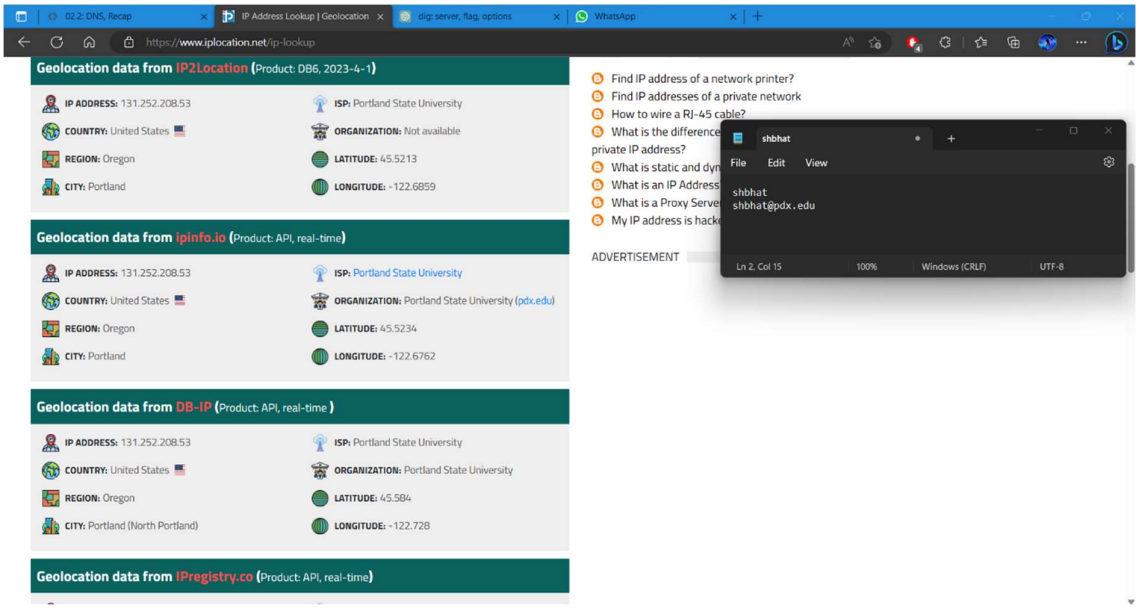
cat 220hosts.txt | head -185 | tail -30

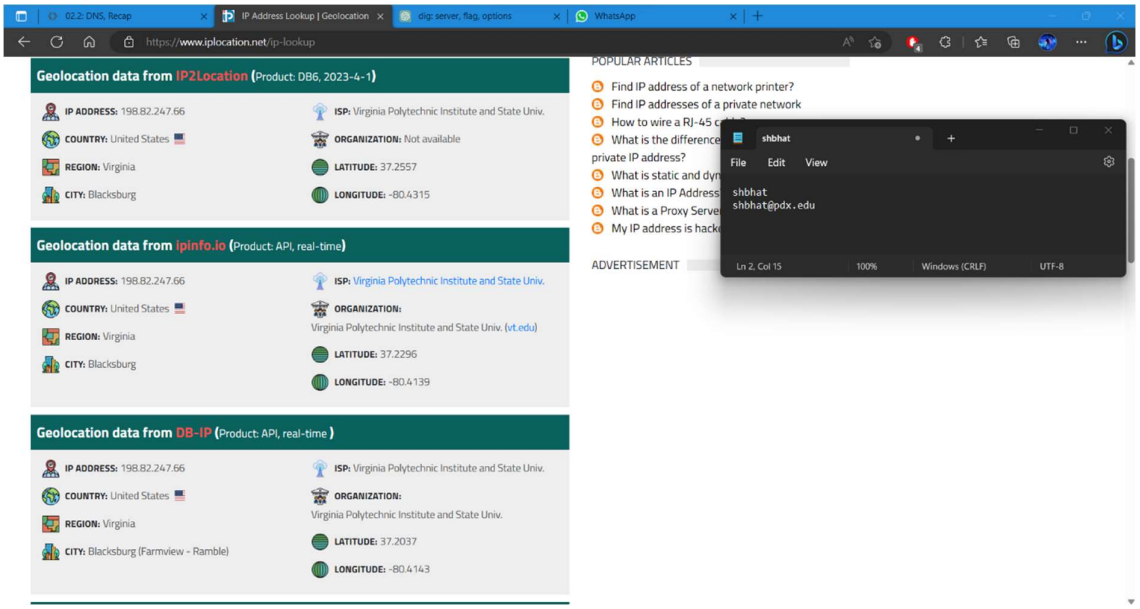


DNS #2

2.1 Geographic DNS

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

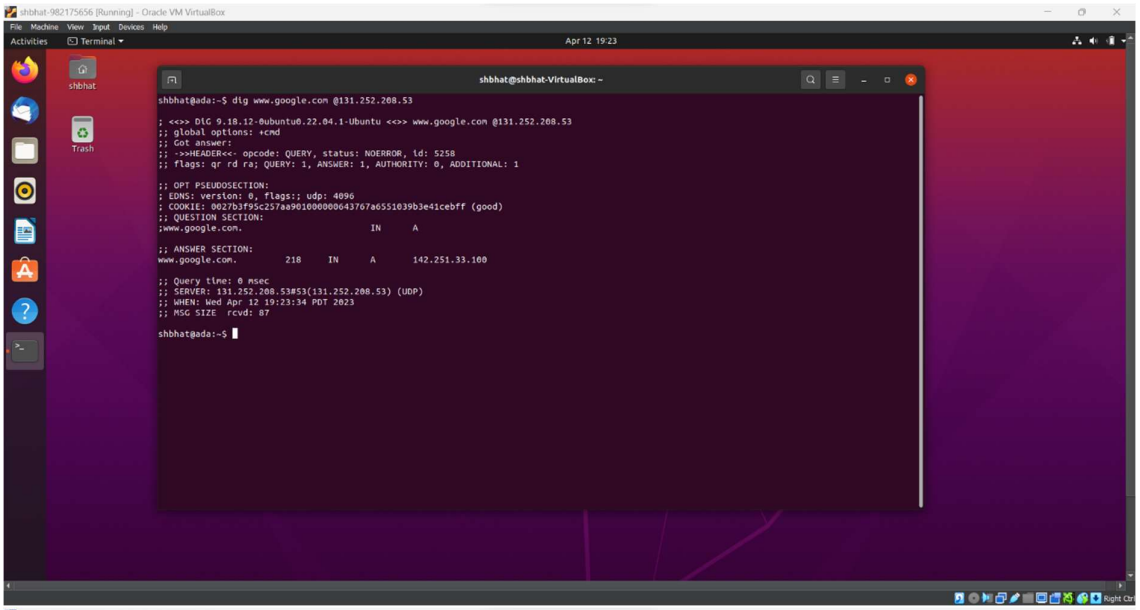


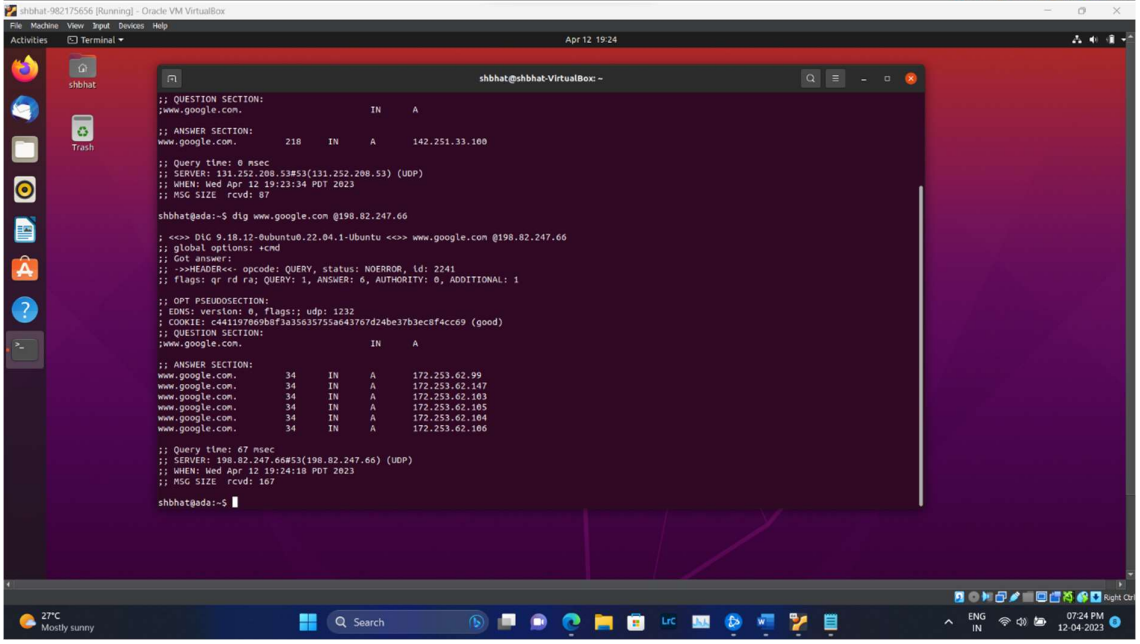


2.1.2 Record one address for www.google.com from each result for your lab notebook.

Answer:

Web server: 142.251.33.100


shbhat-982175656 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Apr 12 19:23
shbhat
Trash
shbhat@shbhat-VirtualBox: ~
shbhat@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: 5258
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 0027b3f95c257aa9010000006437 67a6551039b3e41cebff (good)
;; QUESTION SECTION:
;www.google.com. IN A
;; ANSWER SECTION:
www.google.com. 218 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 19:23:34 PDT 2023
;; MSG SIZE rcvd: 87
shbhat@ada:~$


shbhat-982175656 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Apr 12 19:24
shbhat
Trash
shbhat@shbhat-VirtualBox: ~
;; QUESTION SECTION:
;www.google.com. IN A
;; ANSWER SECTION:
www.google.com. 218 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 19:23:34 PDT 2023
;; MSG SIZE rcvd: 87
shbhat@ada:~$ dig www.google.com @198.82.247.66
; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> www.google.com @198.82.247.66
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2241
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c44119706 9bbf3a35635755a643767d24be37b3ec8f4cc69 (good)
;; QUESTION SECTION:
;www.google.com. IN A
;; ANSWER SECTION:
www.google.com. 34 IN A 172.253.62.99
www.google.com. 34 IN A 172.253.62.147
www.google.com. 34 IN A 172.253.62.103
www.google.com. 34 IN A 172.253.62.105
www.google.com. 34 IN A 172.253.62.104
www.google.com. 34 IN A 172.253.62.106
;; Query time: 67 msec
;; SERVER: 198.82.247.66#53(198.82.247.66) (UDP)
;; WHEN: Wed Apr 12 19:24:18 PDT 2023
;; MSG SIZE rcvd: 167
shbhat@ada:~$
27°C
Mostly sunny
Search
ENG
IN
07:24 PM
12-04-2023

2.1.3 What is the geographic distance between each DNS server and the IP address it resolves for www.google.com?

Answer:

DNS Servers:

172.253.62.105 -> 2016 n mi, 3734 km

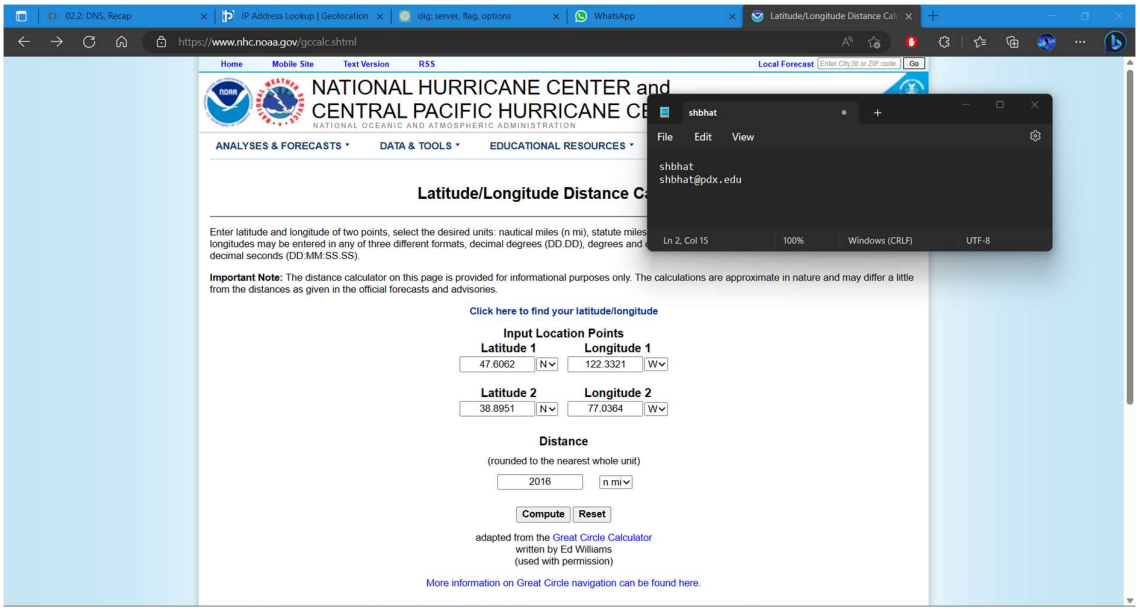
172.253.62.103 -> 2016 n mi, 3734 km

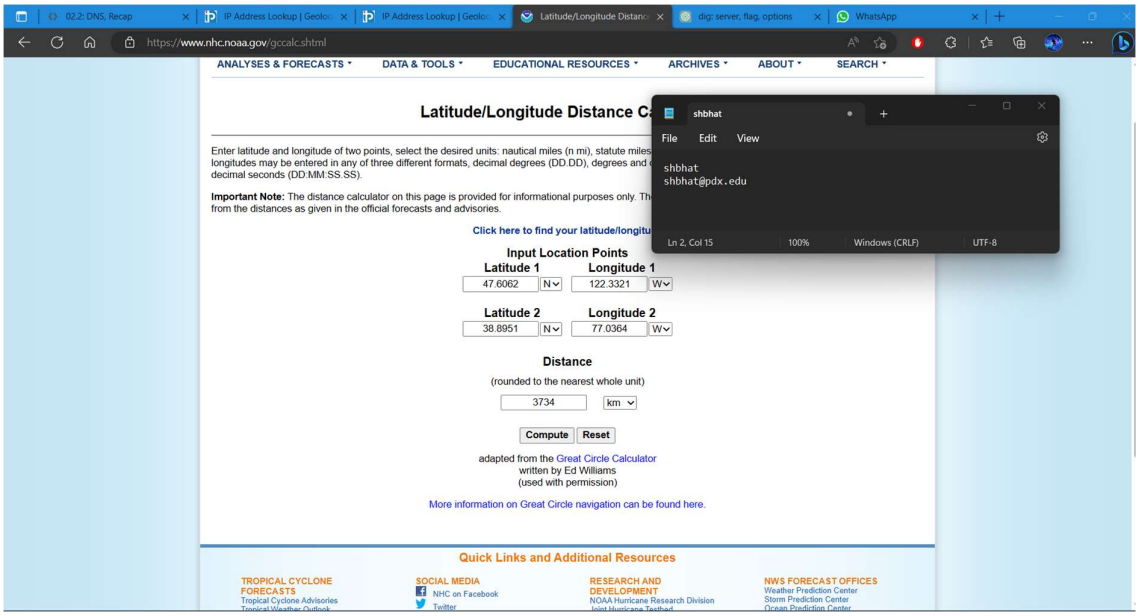
172.253.62.147 -> 611 n mi, 1132 km

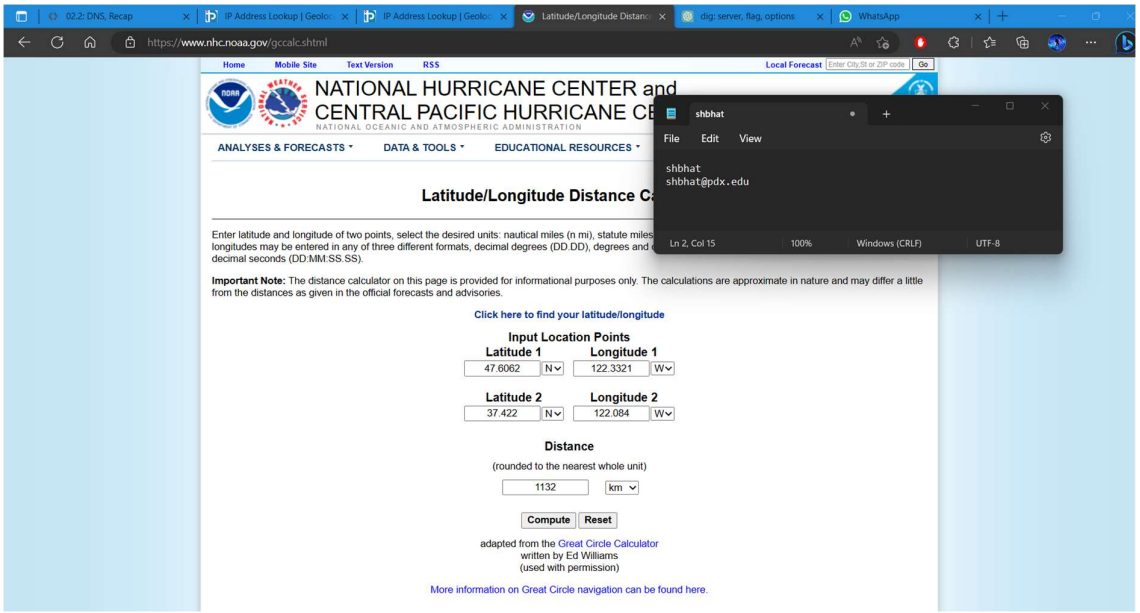
172.253.62.104 -> 2016 n mi, 3734 km

172.253.62.106 -> 2016 n mi, 3734 km

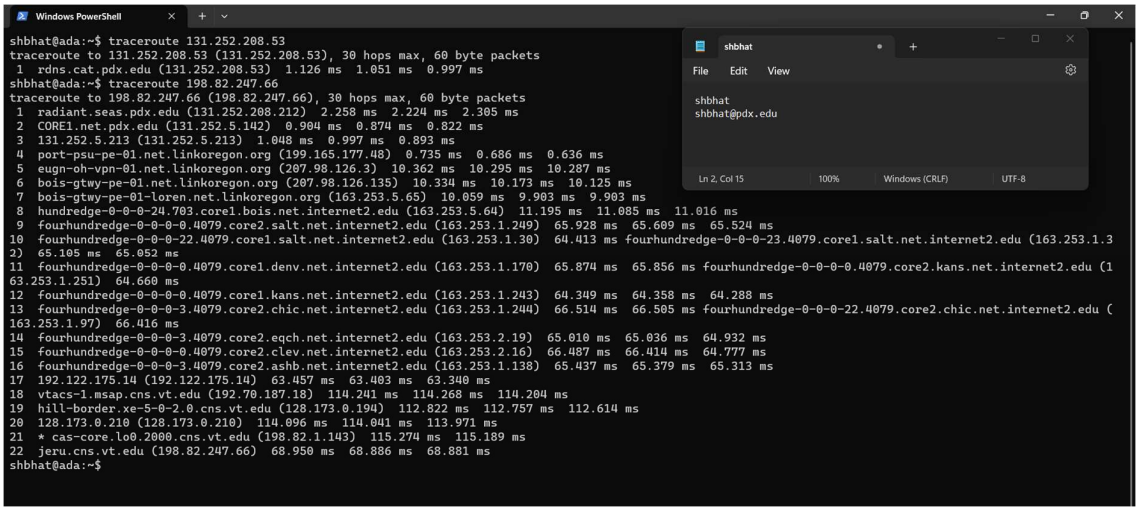
172.253.62.99 -> 2016 n mi, 3734 km




02.2: DNS, Recap
IP Address Lookup | Geoloc
IP Address Lookup | Geoloc
Latitude/Longitude Distanc
dig: server, flag, options
WhatsApp
https://www.nhc.noaa.gov/gccalc.shtml
ANALYSES & FORECASTS
DATA & TOOLS
EDUCATIONAL RESOURCES
ARCHIVES
ABOUT
SEARCH
Latitude/Longitude Distance C
Enter latitude and longitude of two points, select the desired units: nautical miles (n mi), statute miles
longitudes may be entered in any of three different formats, decimal degrees (DD.DD), degrees and
decimal seconds (DD:MM:SS.SS).
Important Note: The distance calculator on this page is provided for informational purposes only. Th
from the distances as given in the official forecasts and advisories.
Click here to find your latitude/longitu
Input Location Points
Latitude 1
Longitude 1
47.6062
N
122.3321
W
Latitude 2
Longitude 2
38.8951
N
77.0364
W
Distance
(rounded to the nearest whole unit)
3734
km
Compute
Reset
adapted from the Great Circle Calculator
written by Ed Williams
(used with permission)
More information on Great Circle navigation can be found here.
Quick Links and Additional Resources
TROPICAL CYCLONE FORECASTS
Tropical Cyclone Advisories
SOCIAL MEDIA
NHC on Facebook
Twitter
RESEARCH AND DEVELOPMENT
NOAA Hurricane Research Division
NWS FORECAST OFFICES
Weather Prediction Center
Storm Prediction Center
shbhat
File
Edit
View
shbhat
shbhat@pdx.edu
Ln 2, Col 15
100%
Windows (CRLF)
UTF-8

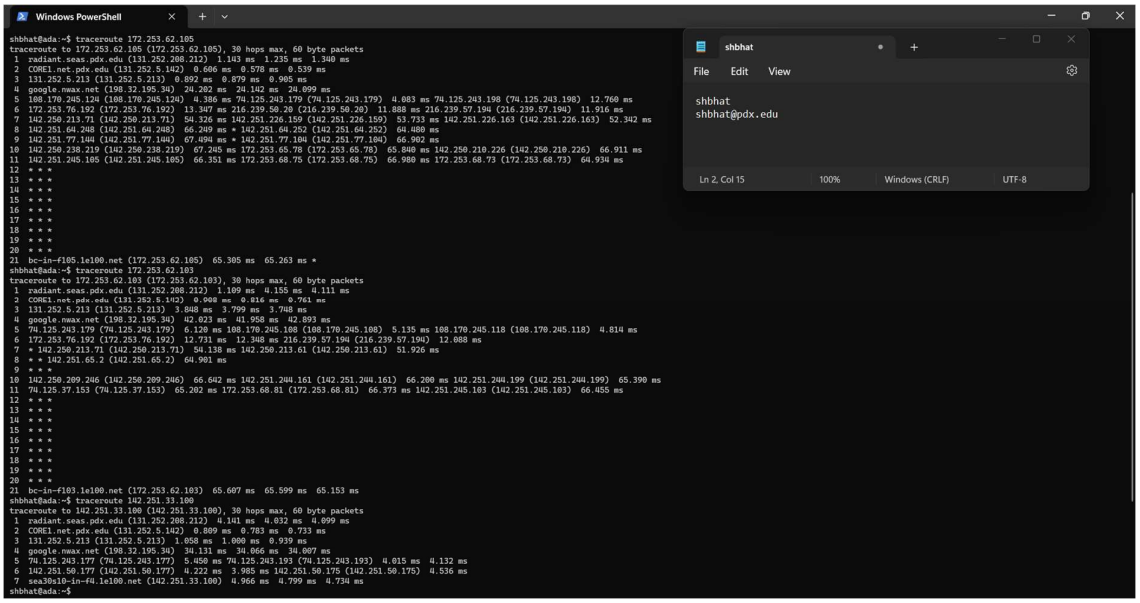

02.2: DNS, Recap
IP Address Lookup | Geoloc
IP Address Lookup | Geoloc
Latitude/Longitude Distanc
dig: server, flag, options
WhatsApp
https://www.nhc.noaa.gov/gccalc.shtml
Home
Mobile Site
Text Version
RSS
Local Forecast
Enter City,St or ZIP code
Go
NATIONAL HURRICANE CENTER and
CENTRAL PACIFIC HURRICANE CE
NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION
ANALYSES & FORECASTS
DATA & TOOLS
EDUCATIONAL RESOURCES
Latitude/Longitude Distance C
Enter latitude and longitude of two points, select the desired units: nautical miles (n mi), statute miles
longitudes may be entered in any of three different formats, decimal degrees (DD.DD), degrees and
decimal seconds (DD:MM:SS.SS).
Important Note: The distance calculator on this page is provided for informational purposes only. The calculations are approximate in nature and may differ a little from the distances as given in the official forecasts and advisories.
Click here to find your latitude/longitude
Input Location Points
Latitude 1
Longitude 1
47.6062
N
122.3321
W
Latitude 2
Longitude 2
37.422
N
122.084
W
Distance
(rounded to the nearest whole unit)
1132
km
Compute
Reset
adapted from the Great Circle Calculator
written by Ed Williams
(used with permission)
More information on Great Circle navigation can be found here.
shbhat
File
Edit
View
shbhat
shbhat@pdx.edu
Ln 2, Col 15
100%
Windows (CRLF)
UTF-8

2.1.4 Traceroute - Do the routes reveal any information on the accuracy of the geographic locations given? (Answer might be no)



Yes they do reveal the location details, For first 2 IP addresses, we got the traceroute and it describes the accuracy of location.

When traceroute is done to 2 of the google servers it times out after reaching some point, but when we do traceroute to main webserver of google it points to a location in Seattle.



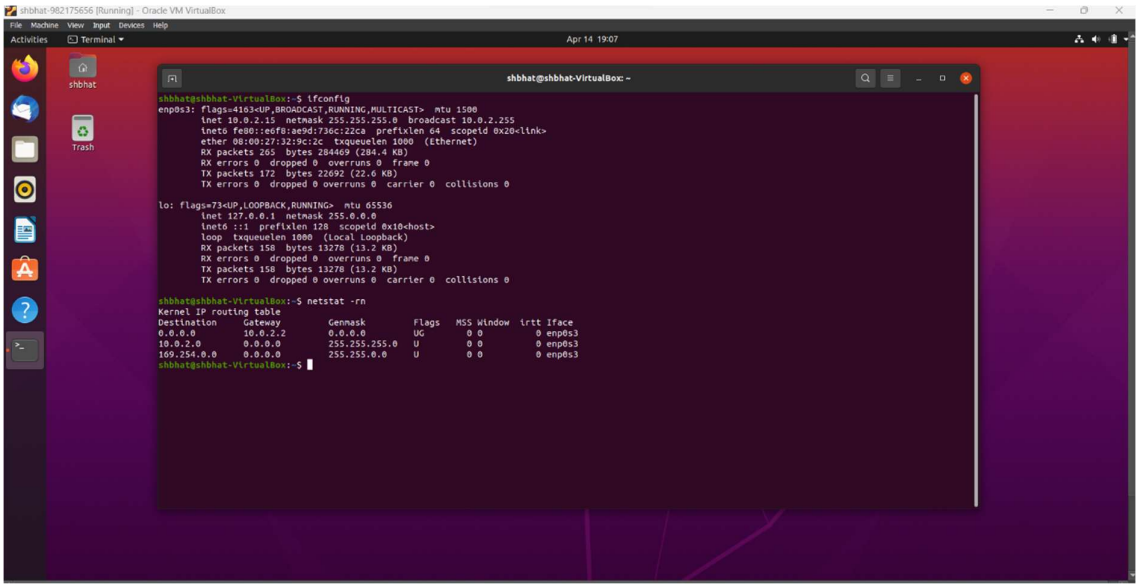
Network Recap Lab #3

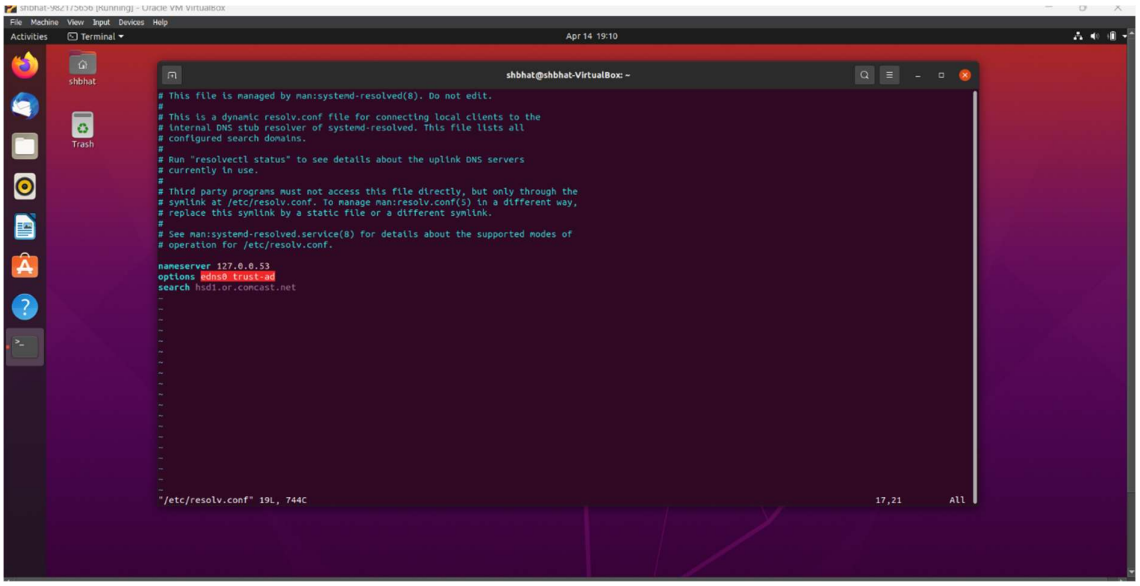
3.1 REVERSE DNS

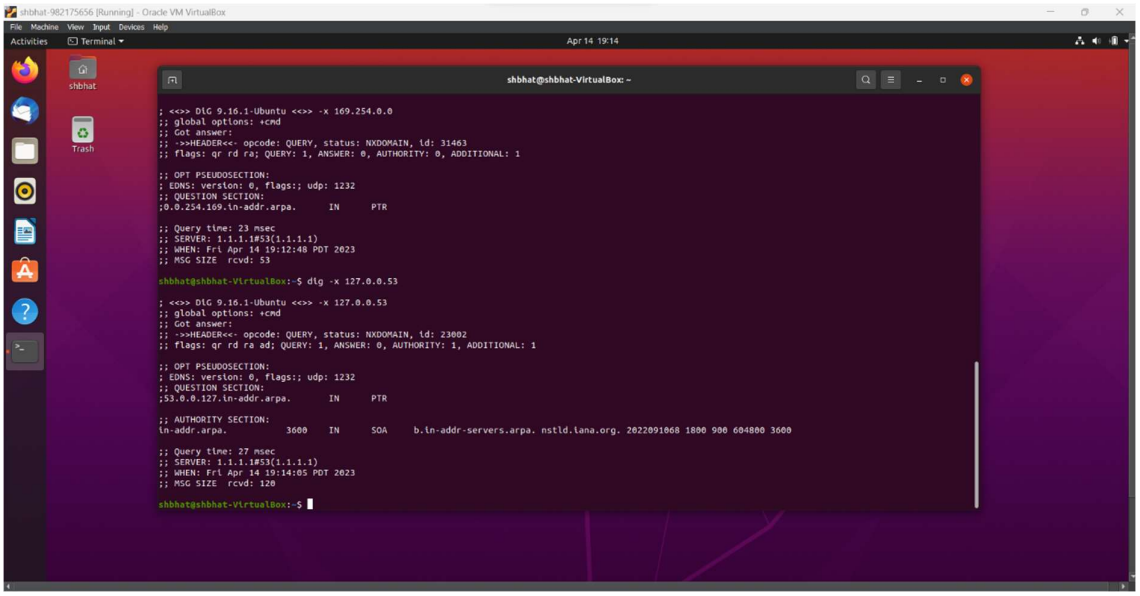
3.1.1 Perform a reverse DNS lookup on the DNS server to find its name.

Include it in your lab notebook.

Answer:

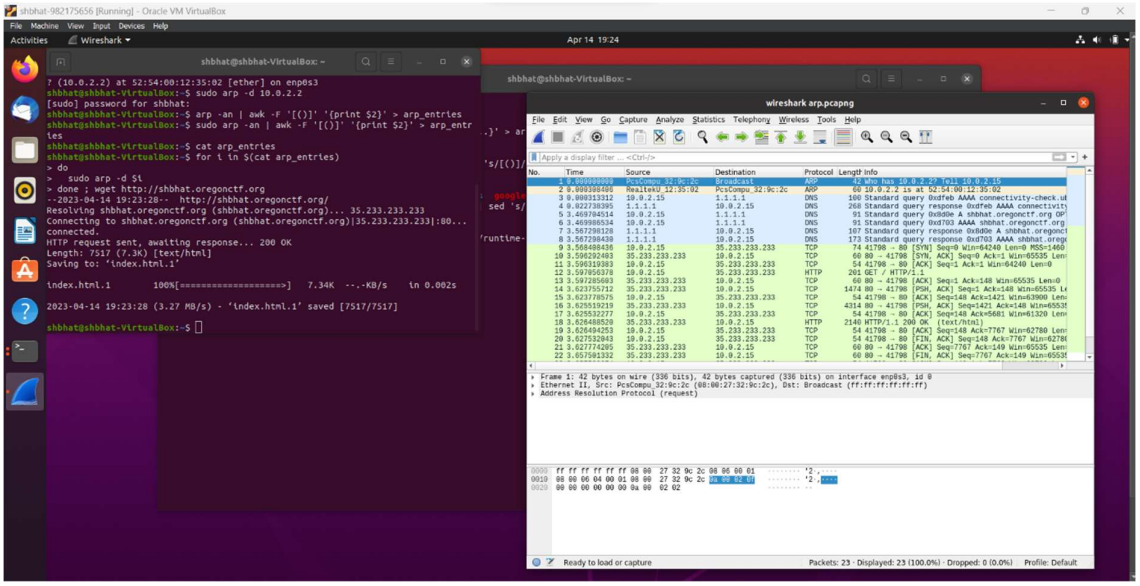





shbhat-982175656 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Apr 14 19:14
shbhat
Trash
shbhat@shbhat-VirtualBox: ~
; <<>> DiG 9.16.1-Ubuntu <<>> -x 169.254.0.0
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 31463
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;0.0.254.169.in-addr.arpa. IN PTR
;; Query time: 23 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Fri Apr 14 19:12:48 PDT 2023
;; MSG SIZE rcvd: 53
shbhat@shbhat-VirtualBox:~$ dig -x 127.0.0.53
; <<>> DiG 9.16.1-Ubuntu <<>> -x 127.0.0.53
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 23002
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;53.0.0.127.in-addr.arpa. IN PTR
;; AUTHORITY SECTION:
in-addr.arpa. 3600 IN SOA b.in-addr-servers.arpa. nstld.iana.org. 2022091068 1800 900 604800 3600
;; Query time: 27 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Fri Apr 14 19:14:05 PDT 2023
;; MSG SIZE rcvd: 120
shbhat@shbhat-VirtualBox:~$

3.2 ARP and Wireshark

3.2.1 Take a screenshot of the trace within Wireshark and include an annotation of the packets in the trace to explain the purpose of each of the packets being exchanged.



Brief annotation of packets and explanation.

1) ARP The client sends an ARP request first to determine the MAC address of the DNS server and sends appropriate response.
2) DNS is then initiated to DNS server to get specific IP address of specific domain name and we get DNS response with IP address.
3) Next is TCP connection and connection is initiated via 3-way handshake and we get SYN and ACK.
4) Finally, HTTP request is sent which is mainly GET in our case and we get HTTP response with status code usually 200 that connection is successfully established.

3.2.2 How many DNS requests are made?

Answer:

3 DNS requests are made and 3 DNS responses.

3.2.3 How many TCP connections does the browser initiate simultaneously to the site?

Answer:

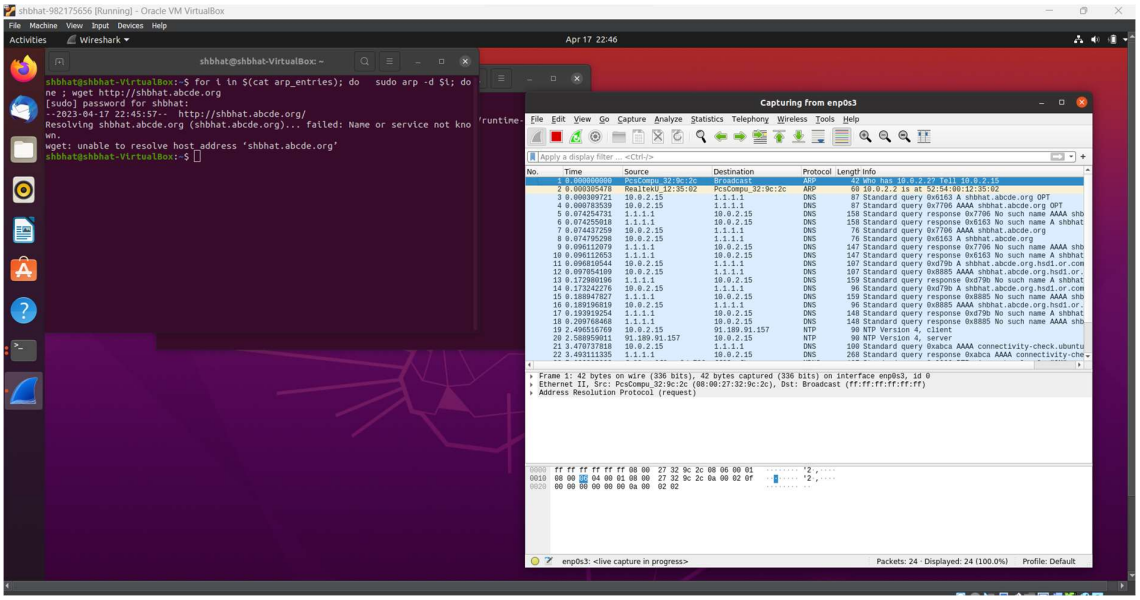
Total 14 TCP requests and if we divide it by 2 we will get 7 which is the request initiated simultaneously to the site.

3.2.4 How many HTTP GET requests are there for embedded objects?

Answer:

1 HTTP Get

3.2.5 Run the lab again using random characters after the <OdinID> in the DNS name you are fetching.



3.2.6 How many DNS requests are made?

Answer:

Total of 16 DNS requests, 8 requests and 8 responses.

3.2.7 How many TCP connections does the browser initiate simultaneously to the site?

Answer:

0 TCP since the site is invalid.

3.2.8 How many HTTP GET requests are there for embedded objects?

Answer:

0 HTTP requests because this site does not exist.