CS530 F23 Week 2 Lab
Prof. Feng

Amelia Miner
10/8/23

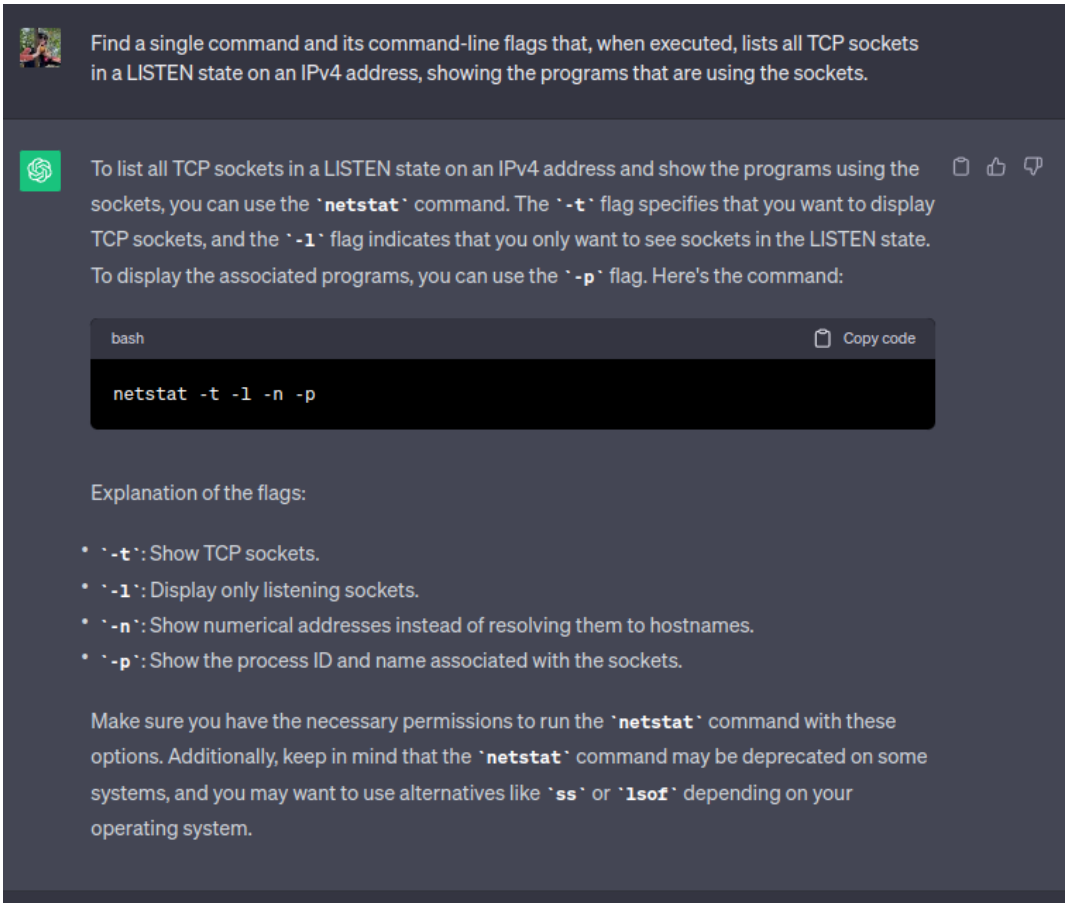
TABLE OF CONTENTS:

Amelia Miner
10/8/23

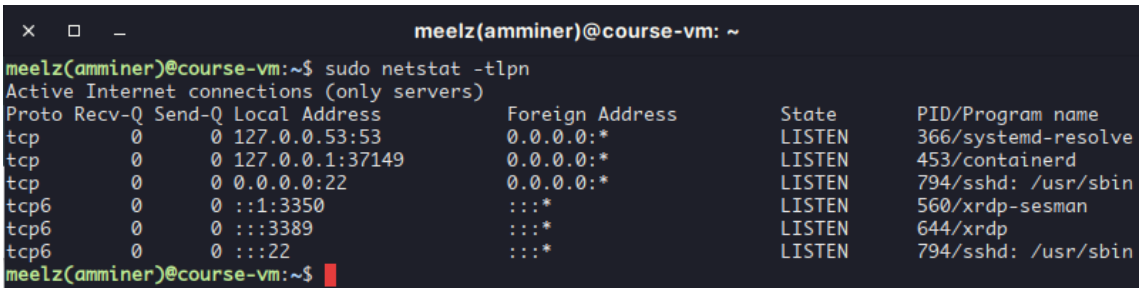
I. Lab 2.1 - TCP, HTTP

1. TCP #1: Sockets

- Using ChatGPT, find a single command and its command-line flags that, when executed, lists all TCP sockets in a LISTEN state on an IPv4 address, showing the program that is using it.
    - Take a screenshot of the prompt and the command that ChatGPT generates



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

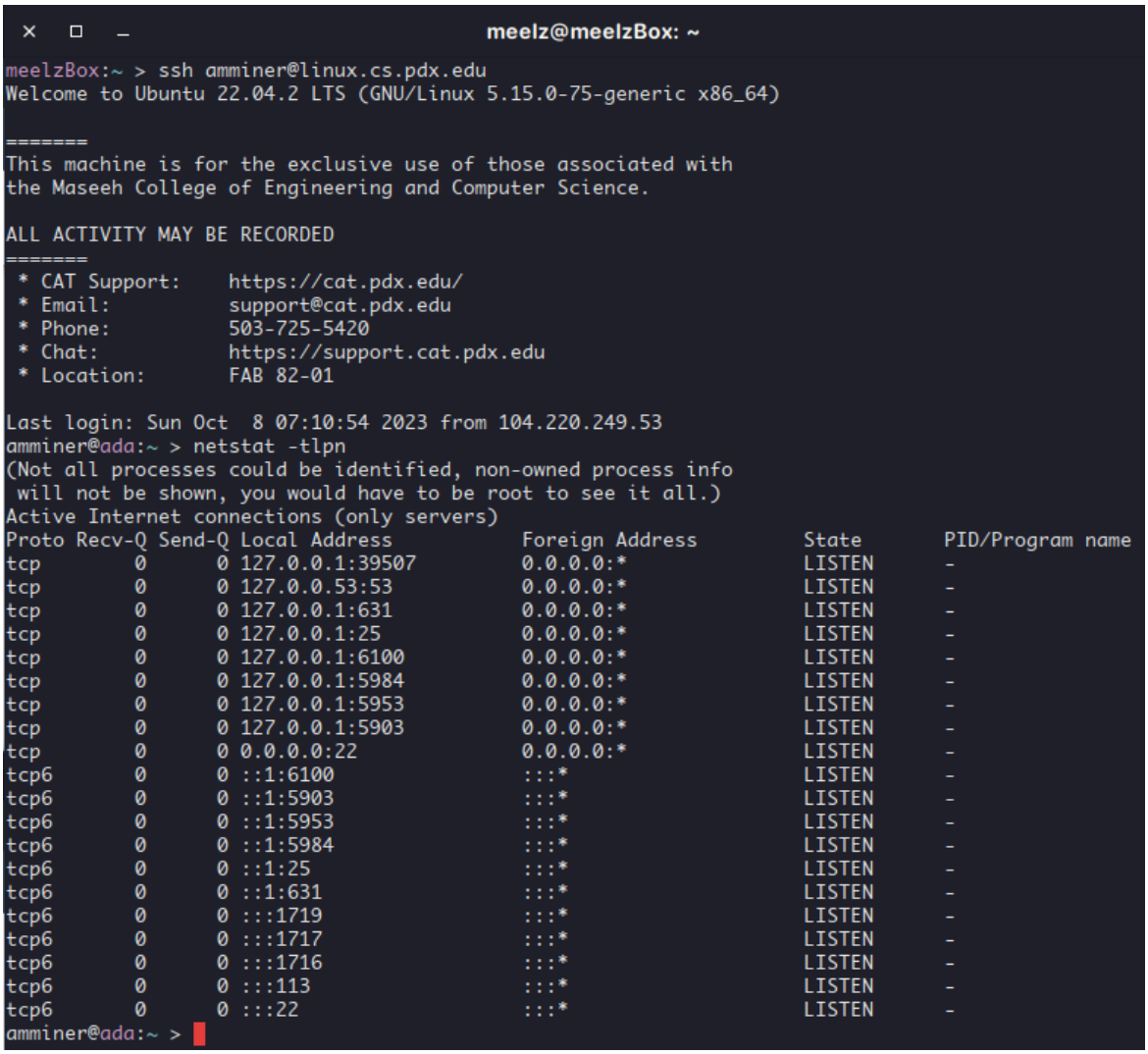


    - List a service that can be contacted from any interface on the machine. List a service that can only be contacted by local processes.

      sshd can be can be contacted from any interface on the machine. containerd can only be contacted by local processes.

Amelia Miner
10/8/23

- **Login to linux.cs.pdx.edu**
  - Run the command again, but do not use sudo as this is a machine managed by CAT. Include a screenshot of the output.



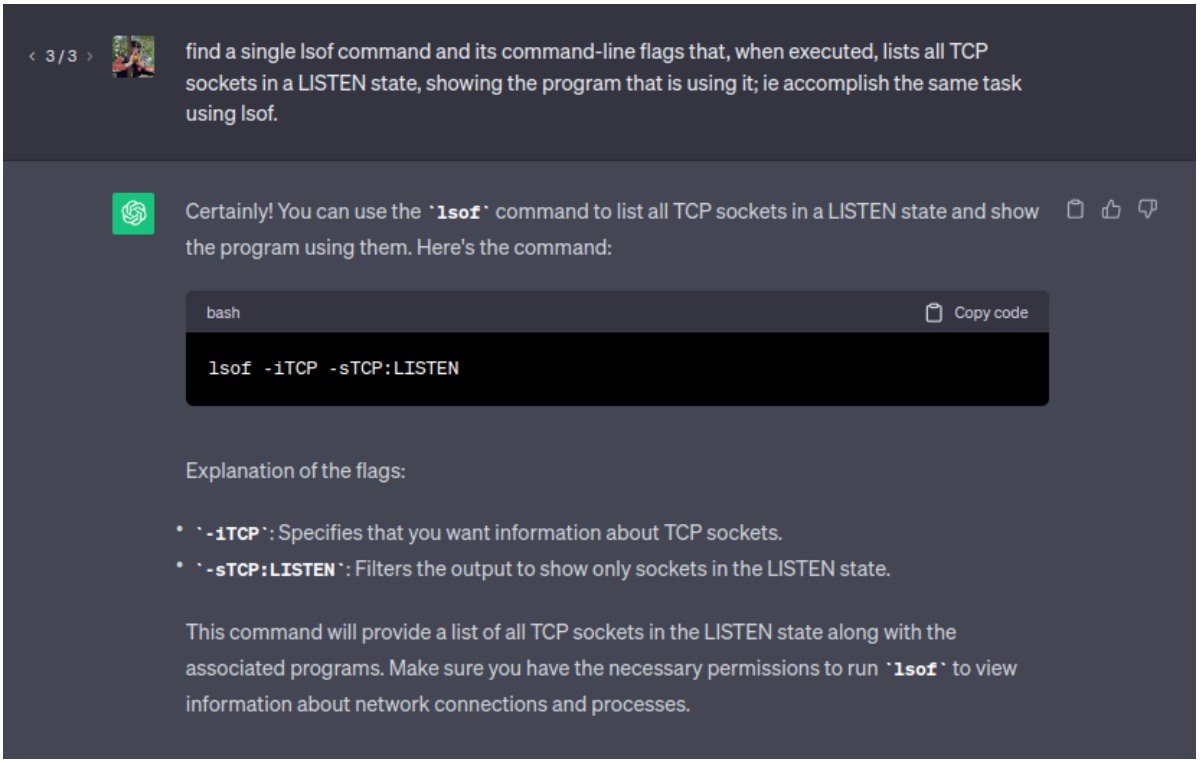
  - List the services this machine provides for external access.

    It looks like only ssh is available to external connections on linux.cs.pdx.edu.

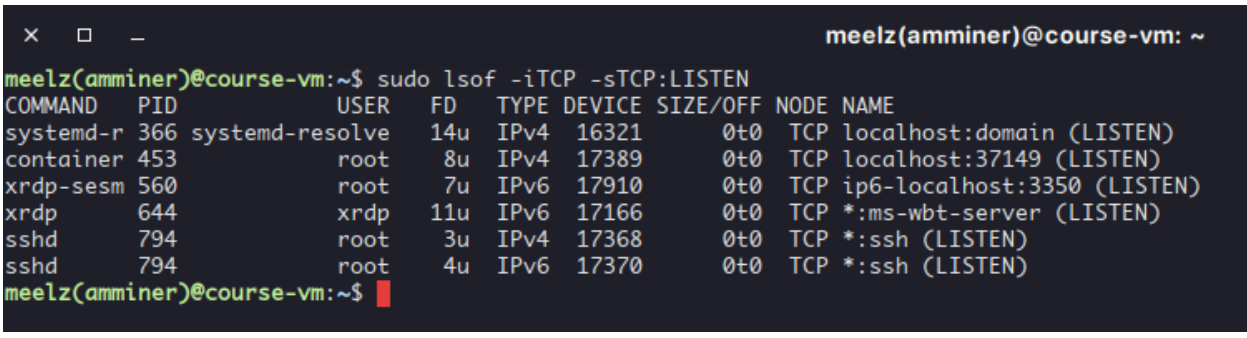
Amelia Miner
10/8/23

2. LSOF

- Using ChatGPT, find a single lsof command and its command-line flags that, when executed, lists all TCP sockets in a LISTEN state on an IPv4 address, showing the program that is using it. Note that you can leverage the conversation in the previous step and simply ask ChatGPT to repeat the task using lsof.
    - Take a screenshot of the prompt and the command that ChatGPT generates.



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



Amelia Miner

3. TCP #2: Throughput

- VMs instantiated:

  NAME: vm-europe-west1-d
  INTERNAL_IP: 10.132.0.2
  EXTERNAL_IP: 35.195.100.133

  NAME: vm-us-west1-b
  INTERNAL_IP: 10.138.0.6
  EXTERNAL_IP: 34.168.52.191

  NAME: vm-us-east1-b
  INTERNAL_IP: 10.142.0.3
  EXTERNAL_IP: 34.74.3.81

  NAME: vm-australia-southeast1-b
  INTERNAL_IP: 10.152.0.2
  EXTERNAL_IP: 35.189.16.39

Amelia Miner
10/8/23

4. - iperf

- On each foreign machine, run `sudo iperf -s -p 80`.
- On the local machine, run `iperf -c <IP address> -p 80` for each foreign machine's internal IP.
- 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.

```
amminer@vm-us-west1-b:~$ for addr in 10.132.0.2 10.142.0.3 10.152.0.2
> do
> iperf -c $addr -p 80 | tee $addr.txt
> done
------------------------------------------------------------
Client connecting to 10.132.0.2, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  1] local 10.138.0.6 port 46862 connected with 10.132.0.2 port 80
[ ID] Interval       Transfer     Bandwidth
[  1] 0.0000-10.2068 sec   185 MBytes   152 Mbits/sec
------------------------------------------------------------
Client connecting to 10.142.0.3, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  1] local 10.138.0.6 port 47144 connected with 10.142.0.3 port 80
[ ID] Interval       Transfer     Bandwidth
[  1] 0.0000-10.0767 sec   435 MBytes   362 Mbits/sec
------------------------------------------------------------
Client connecting to 10.152.0.2, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  1] local 10.138.0.6 port 38712 connected with 10.152.0.2 port 80
[ ID] Interval       Transfer     Bandwidth
[  1] 0.0000-10.2228 sec   173 MBytes   142 Mbits/sec
amminer@vm-us-west1-b:~$ ls
10.132.0.2.txt  10.142.0.3.txt  10.152.0.2.txt
amminer@vm-us-west1-b:~$
```

(in the same order as above: eu-west, us-east, aus-southeast).

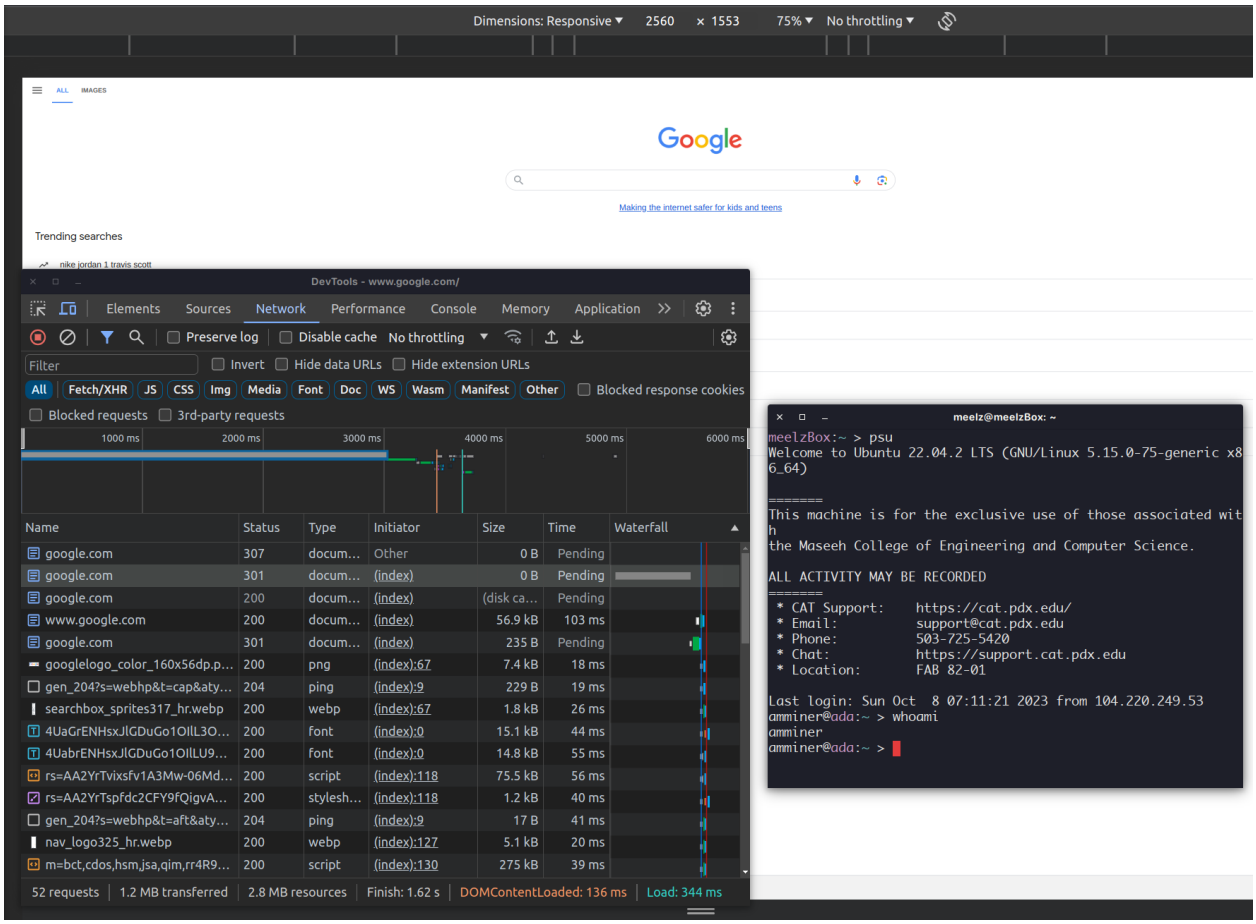
Bandwidth values correspond roughly with discrepancies I would expect based on physical distances between the machines. Interestingly, when I run traceroute to these machines, discrepancies in the number of hops are minimal, presumably because I'm routing over gcloud's internal network which creates a sort of virtual data link over the actual routers that underlie it, like what we were talking about last week in lecture?

```
amminer@vm-us-west1-b:~$ for addr in 10.132.0.2 10.142.0.3 10.152.0.2; do traceroute $addr | wc -l; done
2
2
2
amminer@vm-us-west1-b:~$ for addr in 10.132.0.2 10.142.0.3 10.152.0.2; do traceroute $addr; done
traceroute to 10.132.0.2 (10.132.0.2), 30 hops max, 60 byte packets
 1  vm-europe-west1-d.europe-west1-d.c.cloud-miner-amminer.internal (10.132.0.2)  135.685 ms  135.638 ms *
traceroute to 10.142.0.3 (10.142.0.3), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  vm-us-east1-b.us-east1-b.c.cloud-miner-amminer.internal (10.142.0.3)  65.189 ms * *
traceroute to 10.152.0.2 (10.152.0.2), 30 hops max, 60 byte packets
 1  vm-australia-southeast1-b.australia-southeast1-b.c.cloud-miner-amminer.internal (10.152.0.2)  149.845 ms *  149.791
amminer@vm-us-west1-b:~$ for addr in 10.132.0.2 10.142.0.3 10.152.0.2; do traceroute $addr | wc -l; done
2
3
2
amminer@vm-us-west1-b:~$ for addr in 10.132.0.2 10.142.0.3 10.152.0.2; do traceroute $addr | wc -l; done
2
2
2
amminer@vm-us-west1-b:~$ for addr in 10.132.0.2 10.142.0.3 10.152.0.2; do traceroute $addr | wc -l; done
2
2
2
amminer@vm-us-west1-b:~$ for addr in 10.132.0.2 10.142.0.3 10.152.0.2; do traceroute $addr | wc -l; done
2
2
2
amminer@vm-us-west1-b:~$ for addr in 10.132.0.2 10.142.0.3 10.152.0.2; do traceroute $addr | wc -l; done
2
3
2
amminer@vm-us-west1-b:~$
```

Amelia Miner
10/8/23

5. HTTP #3: Requests

- Using chrome,visit http://google.com in incognito mode with quic/http3 enabled. Take a screenshot of the initial 3 requests that the browser makes:



- For each of the initial 3 requests:
  - What is the URL being requested?

    http://google.com,

    https://google.com,

    and http://google.com

Amelia Miner
10/8/23

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

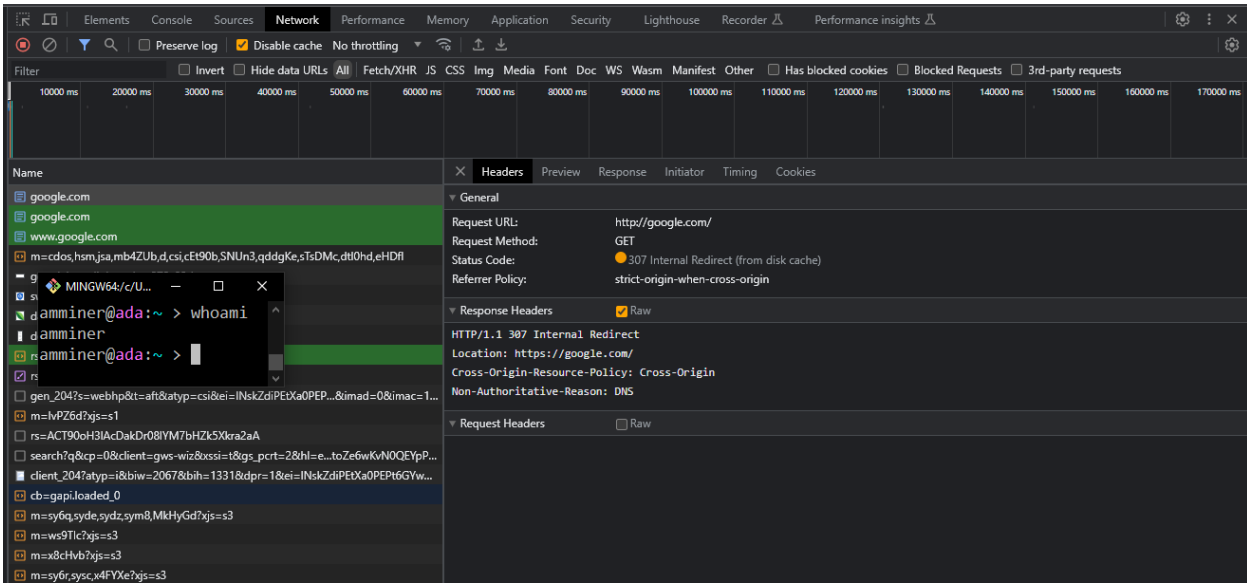
  307-temporary redirect. The response includes a new address to which the resource has been “temporarily” moved.

  301-moved permanently. The response includes a new address to which the resource has been “permanently” moved.

  200-ok. The request was successful - here’s those bits you asked for.

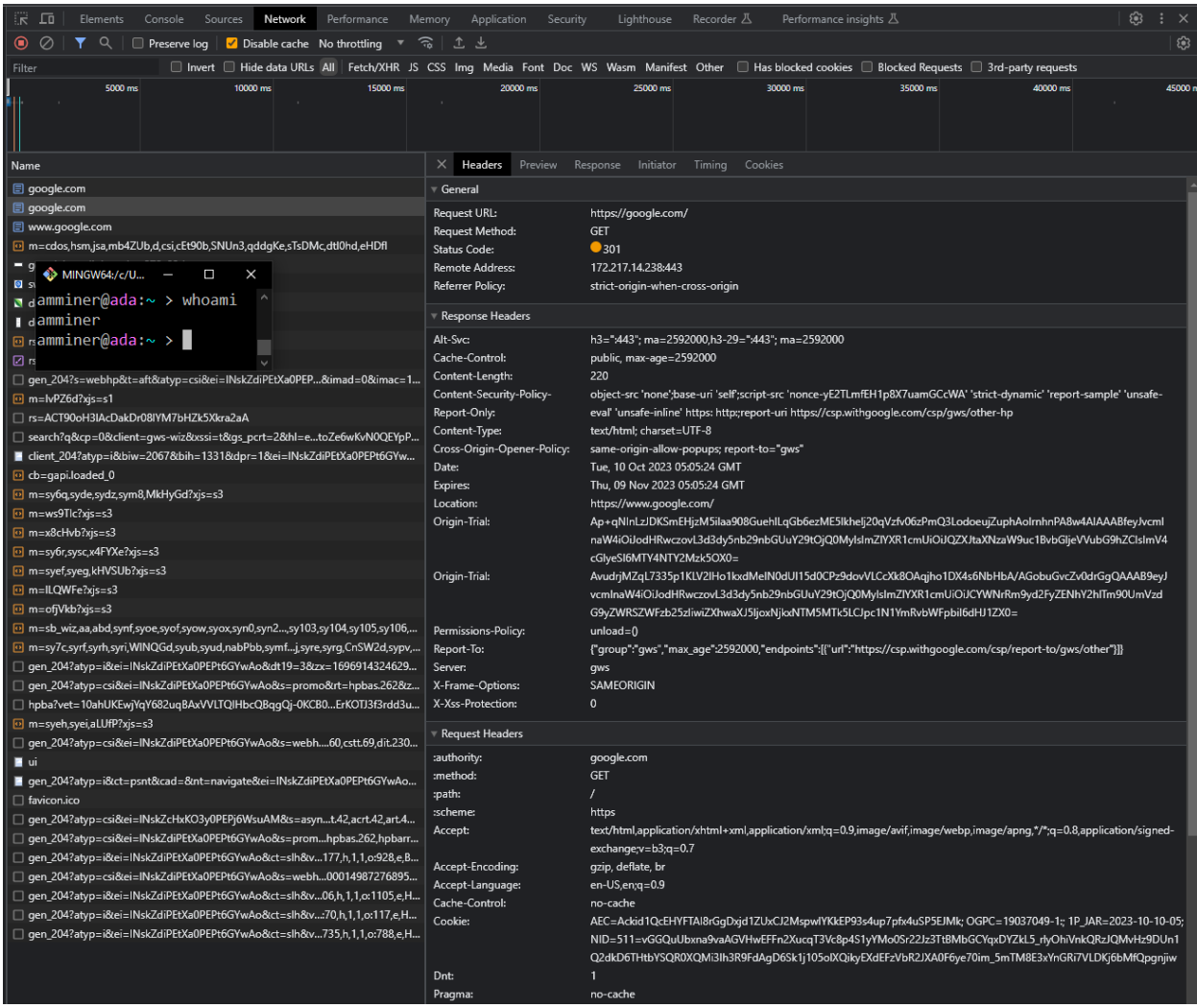
- Take a screenshot indicating the version of the HTTP protocol that is used for each request. (Hint: look at the response status line and alt-svc: HTTP response headers indicating HTTP/2 or HTTP/3).

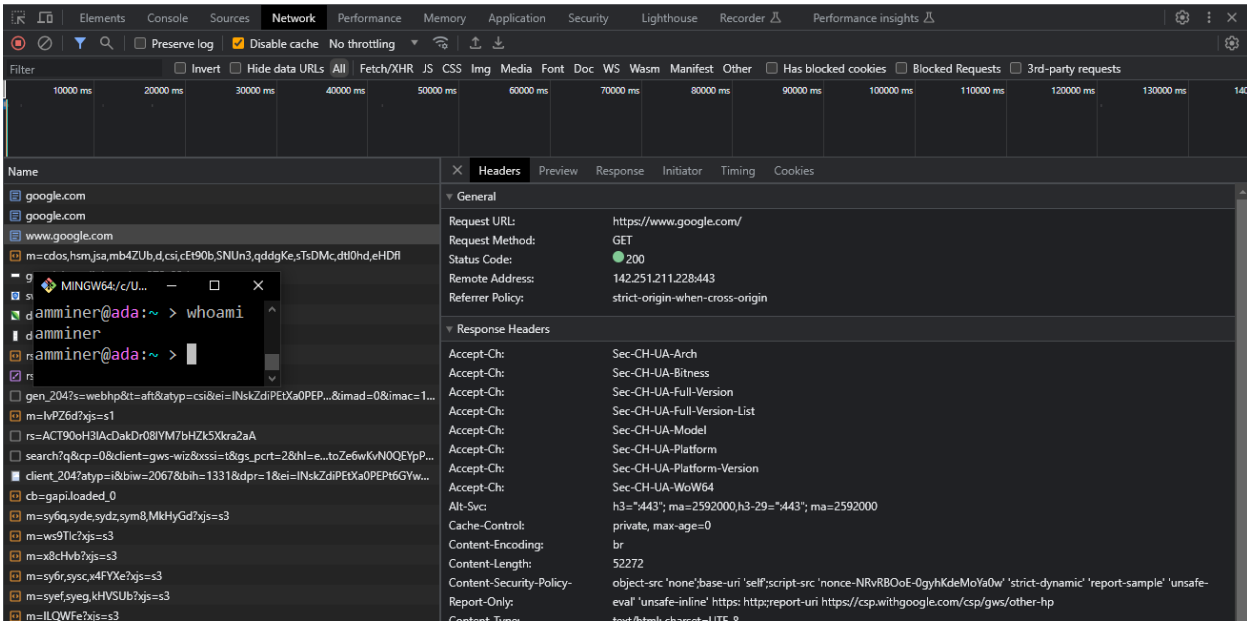
  My first request shows http/1.1. The other requests aren’t showing any version info in their headers. alt-svc in the responses doesn’t mean anything to me - what’s wrong with my setup? Chrome also occasionally mixes up the wrong status code/name combinations, like 200-internal redirect, etc.



CS530 F23 Week 2 Lab
Prof. Feng

Amelia Miner
10/8/23





CS530 F23 Week 2 Lab
Prof. Feng

Amelia Miner
10/8/23

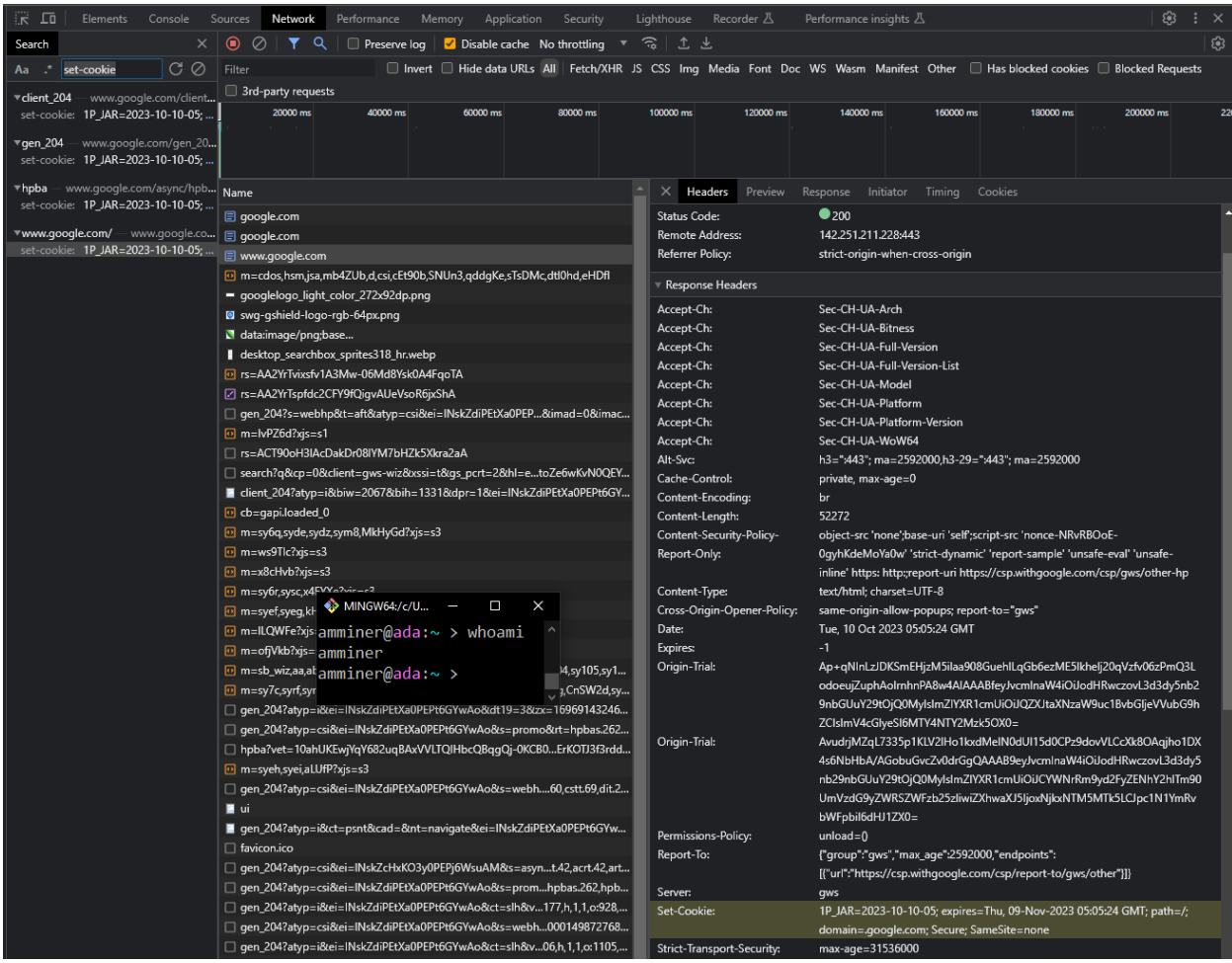
- Find the Location: response header for the two redirections.
    - What URL does the first redirection send the browser to?

      https://google.com

    - What URL does the second redirection send the browser to?

      https://www.google.com/

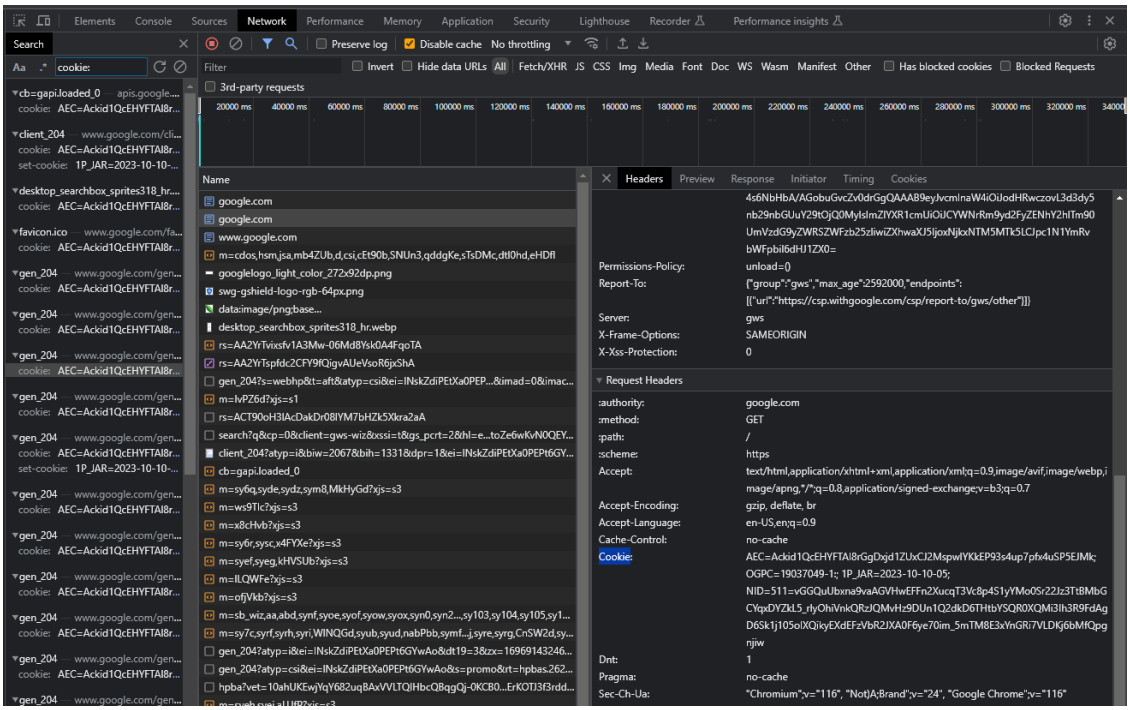
- Examine the HTTP request and response headers for cookies throughout the requests.
    - Take a screenshot of when cookies are set via Set-Cookie:
      In the third request:

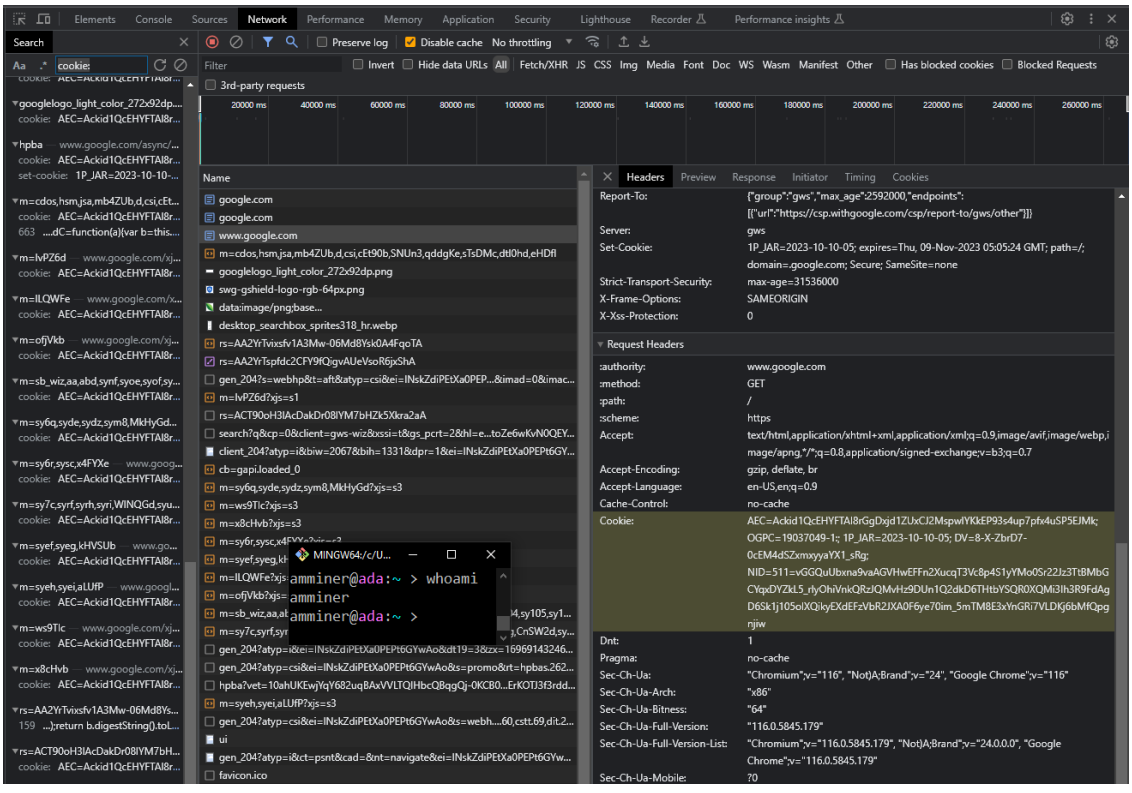


CS530 F23 Week 2 Lab
Prof. Feng

Amelia Miner
10/8/23

- Take a screenshot of when cookies are attached via Cookie:
  In the second and third requests:



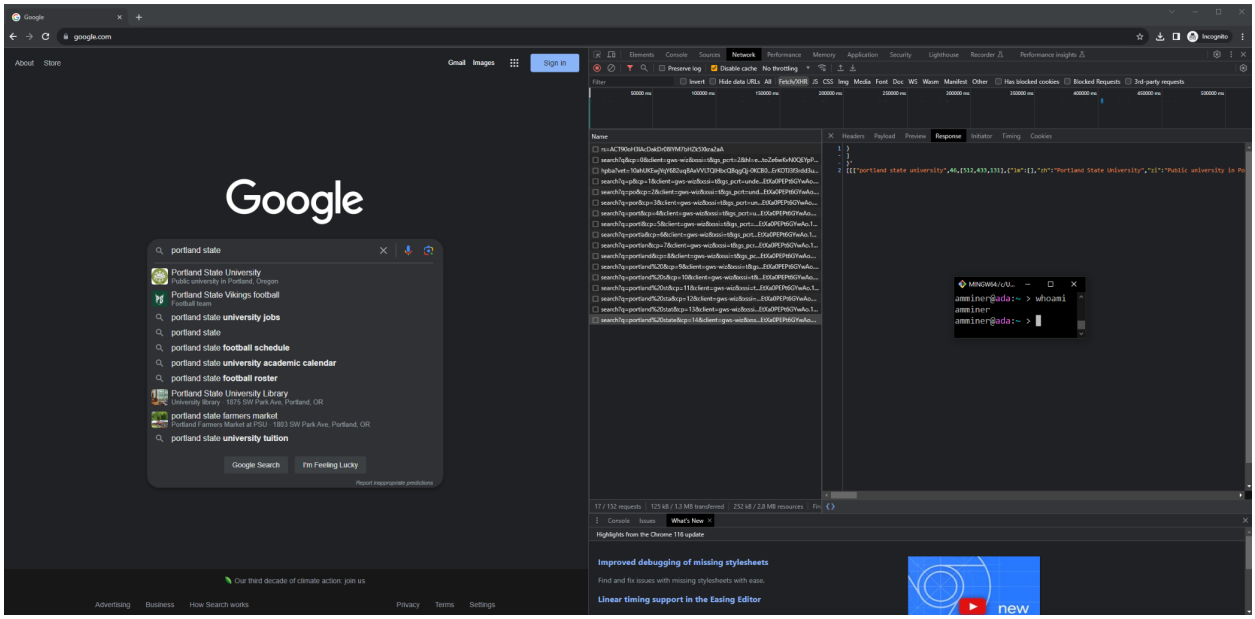


CS530 F23 Week 2 Lab
Prof. Feng

Amelia Miner
10/8/23

6. - Asynchronous HTTP requests

- Show the asynchronous HTTP requests made by typing in the search bar:



Amelia Miner
10/8/23

II. Lab 2.2 - TODO

…