

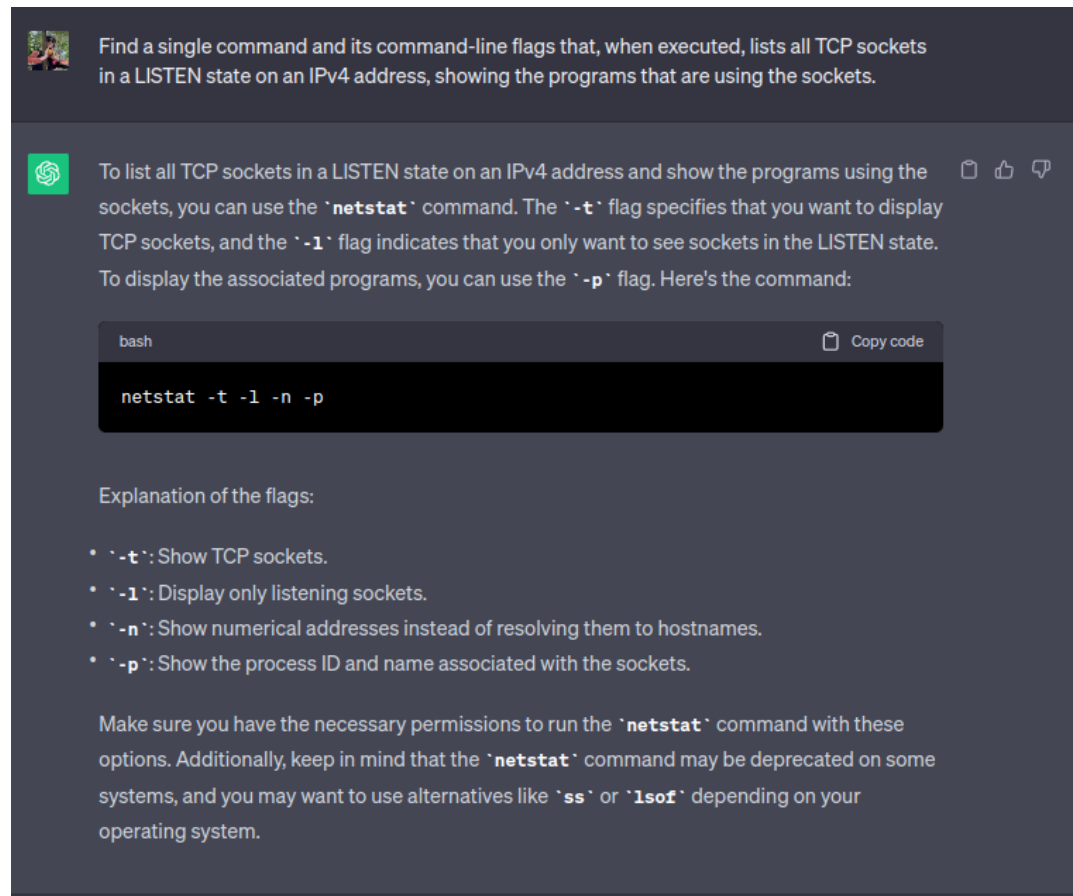
TABLE OF CONTENTS:

I. Lab 2.1 - TCP, HTTP	2
1. TCP #1: Sockets	2
2. LSOF	4
3. TCP #2: Throughput	5
4. - iperf	6
5. HTTP #3: Requests	7
II. Lab 2.2 - TODO	8

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.

```
meelz(amminer)@course-vm: ~
meelz(amminer)@course-vm:~$ sudo netstat -tlpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*                LISTEN      366/systemd-resolve
tcp        0      0 127.0.0.1:37149         0.0.0.0:*                LISTEN      453/containerd
tcp        0      0 0.0.0.0:22              0.0.0.0:*                LISTEN      794/sshd: /usr/sbin
tcp6       0      0 :::1:3350               :::*                    LISTEN      560/xrdp-sesman
tcp6       0      0 :::3389                  :::*                    LISTEN      644/xrdp
tcp6       0      0 :::22                    :::*                    LISTEN      794/sshd: /usr/sbin
```

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

- 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.

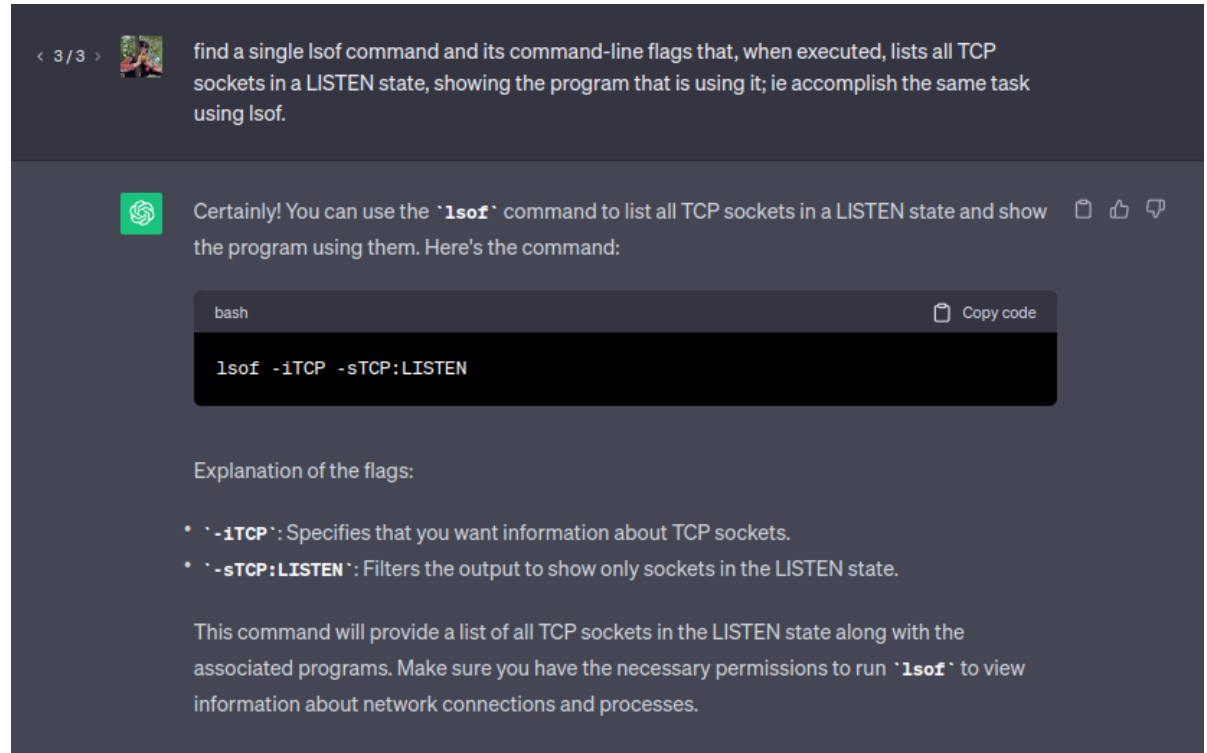
```
meelz@meelzBox: ~  
meelzBox:~ > ssh amminer@linux.cs.pdx.edu  
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-75-generic x86_64)  
  
=====  
This machine is for the exclusive use of those associated with  
the Maseeh College of Engineering and Computer Science.  
  
ALL ACTIVITY MAY BE RECORDED  
=====  
* 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  
  
Last login: Sun Oct  8 07:10:54 2023 from 104.220.249.53  
amminer@ada:~ > netstat -tln  
(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      0 127.0.0.1:39507         0.0.0.0:*                 LISTEN      -  
tcp        0      0 127.0.0.53:53          0.0.0.0:*                 LISTEN      -  
tcp        0      0 127.0.0.1:631          0.0.0.0:*                 LISTEN      -  
tcp        0      0 127.0.0.1:25           0.0.0.0:*                 LISTEN      -  
tcp        0      0 127.0.0.1:6100         0.0.0.0:*                 LISTEN      -  
tcp        0      0 127.0.0.1:5984         0.0.0.0:*                 LISTEN      -  
tcp        0      0 127.0.0.1:5953         0.0.0.0:*                 LISTEN      -  
tcp        0      0 127.0.0.1:5903         0.0.0.0:*                 LISTEN      -  
tcp        0      0 0.0.0.0:22             0.0.0.0:*                 LISTEN      -  
tcp6       0      0 :::1:6100              :::*                   LISTEN      -  
tcp6       0      0 :::1:5903              :::*                   LISTEN      -  
tcp6       0      0 :::1:5953              :::*                   LISTEN      -  
tcp6       0      0 :::1:5984              :::*                   LISTEN      -  
tcp6       0      0 :::1:25                :::*                   LISTEN      -  
tcp6       0      0 :::1:631               :::*                   LISTEN      -  
tcp6       0      0 :::1:719               :::*                   LISTEN      -  
tcp6       0      0 :::1:717               :::*                   LISTEN      -  
tcp6       0      0 :::1:716               :::*                   LISTEN      -  
tcp6       0      0 :::1:113               :::*                   LISTEN      -  
tcp6       0      0 :::22                  :::*                   LISTEN      -  
amminer@ada:~ >
```

- List the services this machine provides for external access.

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

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.

```
meelz(amminer)@course-vm:~$ sudo lsof -iTCP -sTCP:LISTEN
COMMAND  PID   USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r 366 systemd-resolve 14u  IPv4 16321      0t0  TCP localhost:domain (LISTEN)
container 453    root     8u  IPv4 17389      0t0  TCP localhost:37149 (LISTEN)
xrdp-sesm 560    root     7u  IPv6 17910      0t0  TCP ip6-localhost:3350 (LISTEN)
xrdp      644    xrdp    11u  IPv6 17166      0t0  TCP *:ms-wbt-server (LISTEN)
sshd      794    root     3u  IPv4 17368      0t0  TCP *:ssh (LISTEN)
sshd      794    root     4u  IPv6 17370      0t0  TCP *:ssh (LISTEN)
meelz(amminer)@course-vm:~$
```

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

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 $addr | wc -l; done
2
2
2
amminer@vm-us-west1-b:~$ 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 $addr | wc -l; done
2
2
2
amminer@vm-us-west1-b:~$
```

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:

The screenshot shows the Chrome DevTools Network tab with the 'All' filter selected. The first three requests are highlighted in blue. The table below summarizes the data for these requests:

Name	Status	Type	Initiator	Size	Time	Waterfall
google.com	307	docum...	Other	0 B	Pending	
google.com	301	docum...	(index)	0 B	Pending	
google.com	200	docum...	(index)	(disk ca...)	Pending	

The waterfall chart shows the timing of these requests, with the first two being pending and the third starting around 1000ms.

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

<http://google.com>,

<https://google.com>,

and <http://google.com>

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

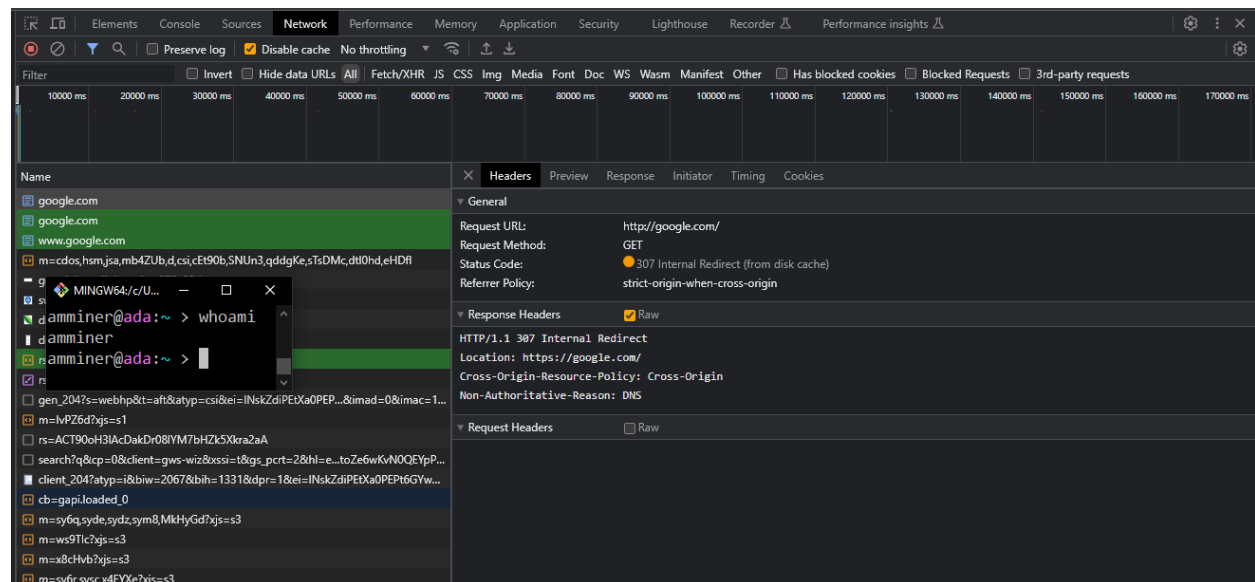
307-temporary redirect. The response includes a new address to which the resource has been “temporarily” moved.

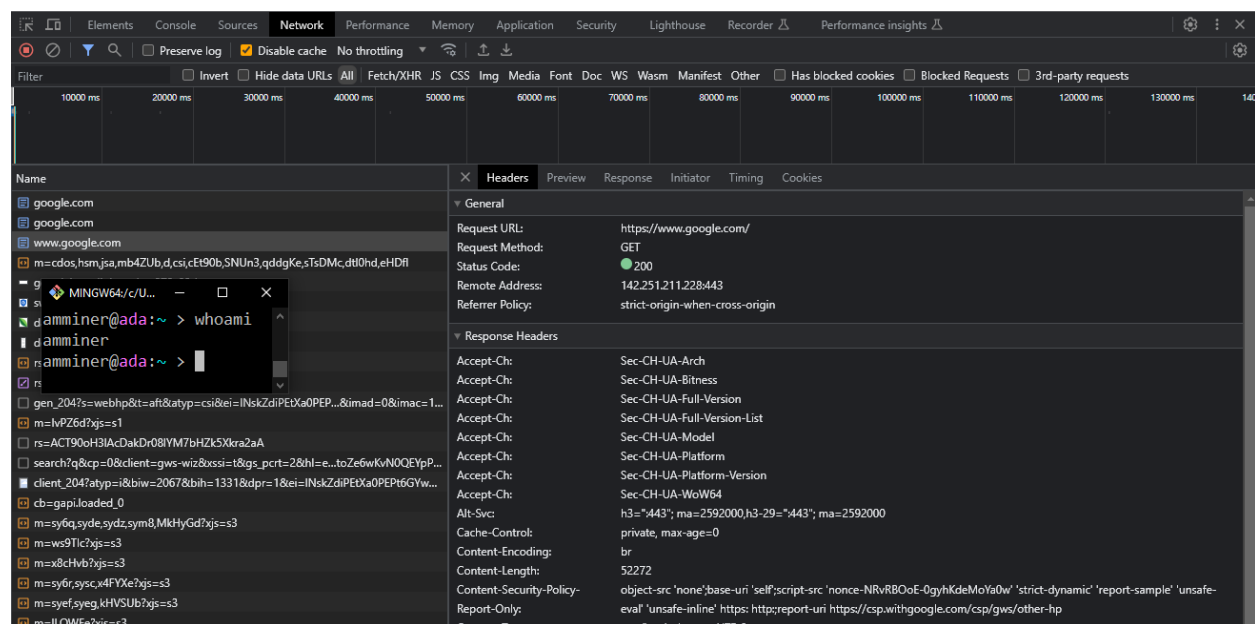
301-moved permanently. The response includes a new address to which the resource has been “permanently” moved.

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).

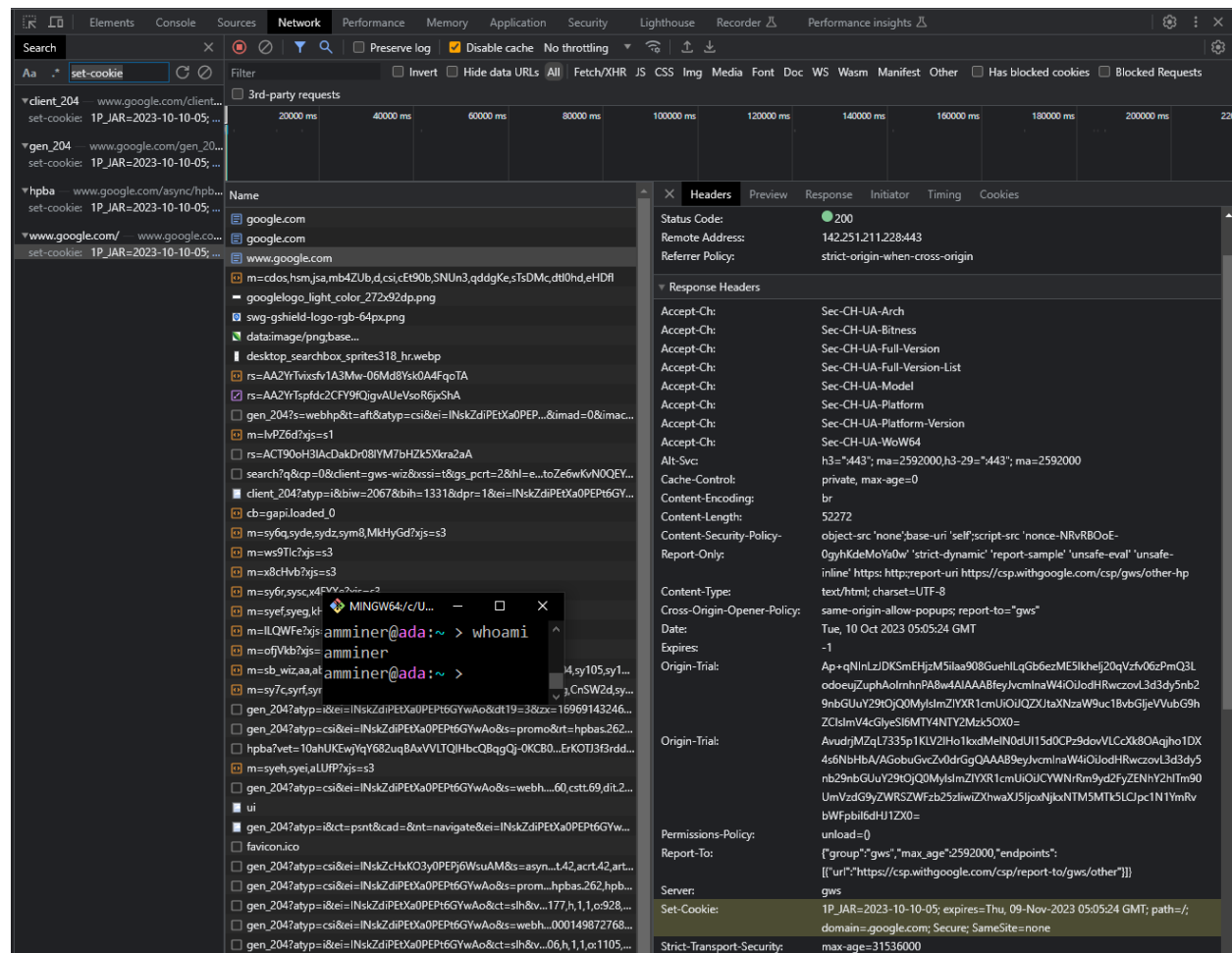
My first request shows http/1.1. The other requests aren’t showing any version info in their headers. `alt-svc` in the responses doesn’t mean anything to me - what’s wrong with my setup? Chrome also occasionally mixes up the wrong status code/name combinations, like 200-internal redirect, etc.



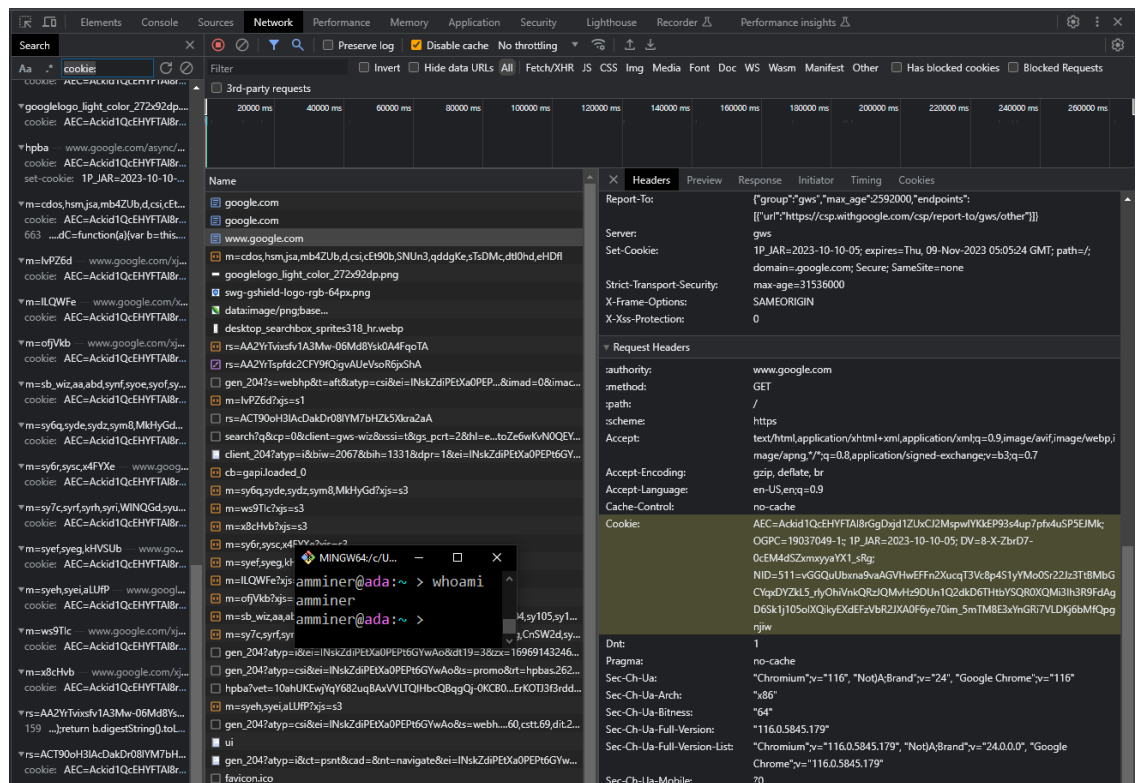
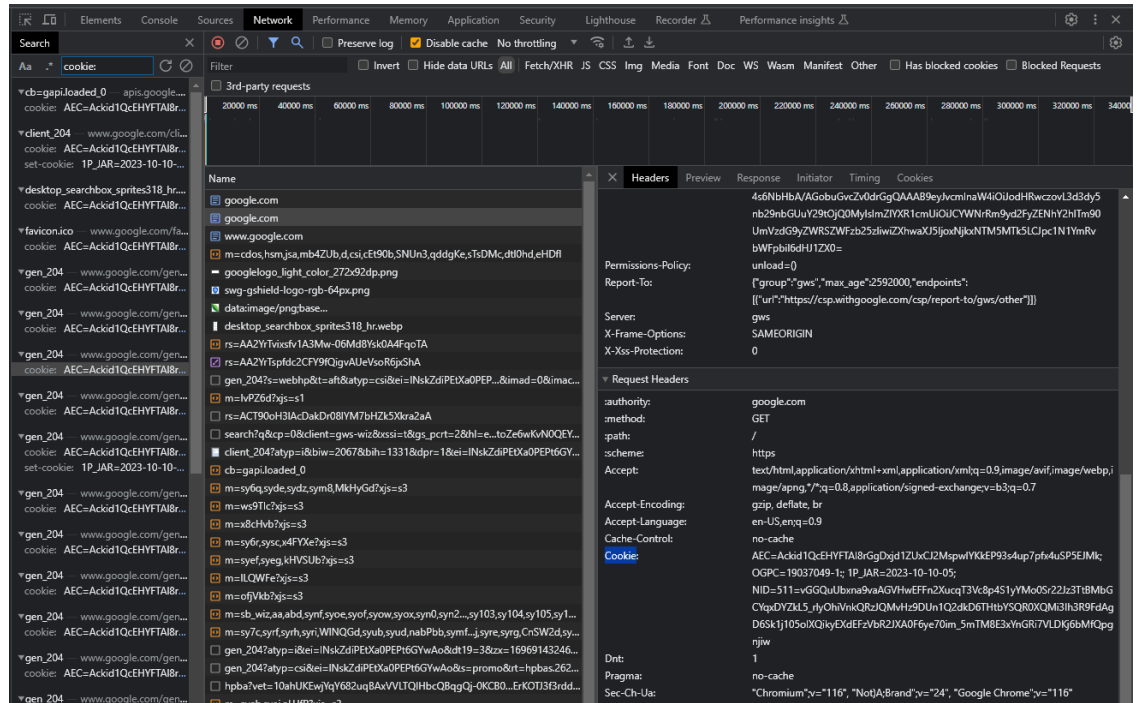


- <https://www.google.com/>

- In the third request:

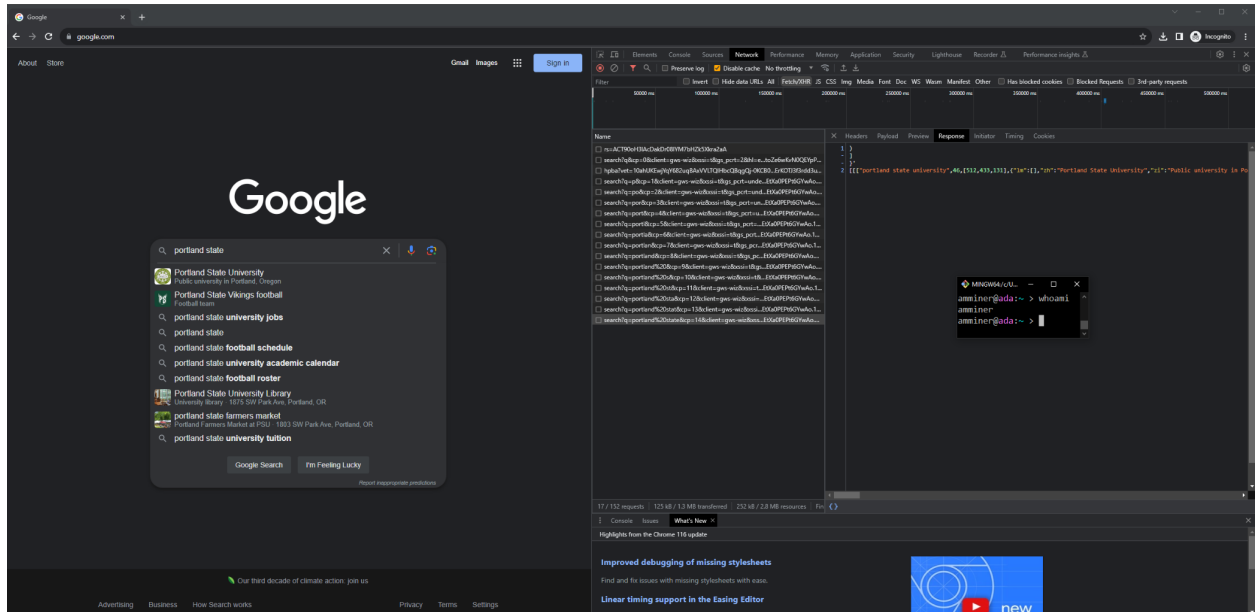


- Take a screenshot of when cookies are attached via Cookie:
In the second and third requests:



6. - Asynchronous HTTP requests

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



II. Lab 2.2 - TODO

...