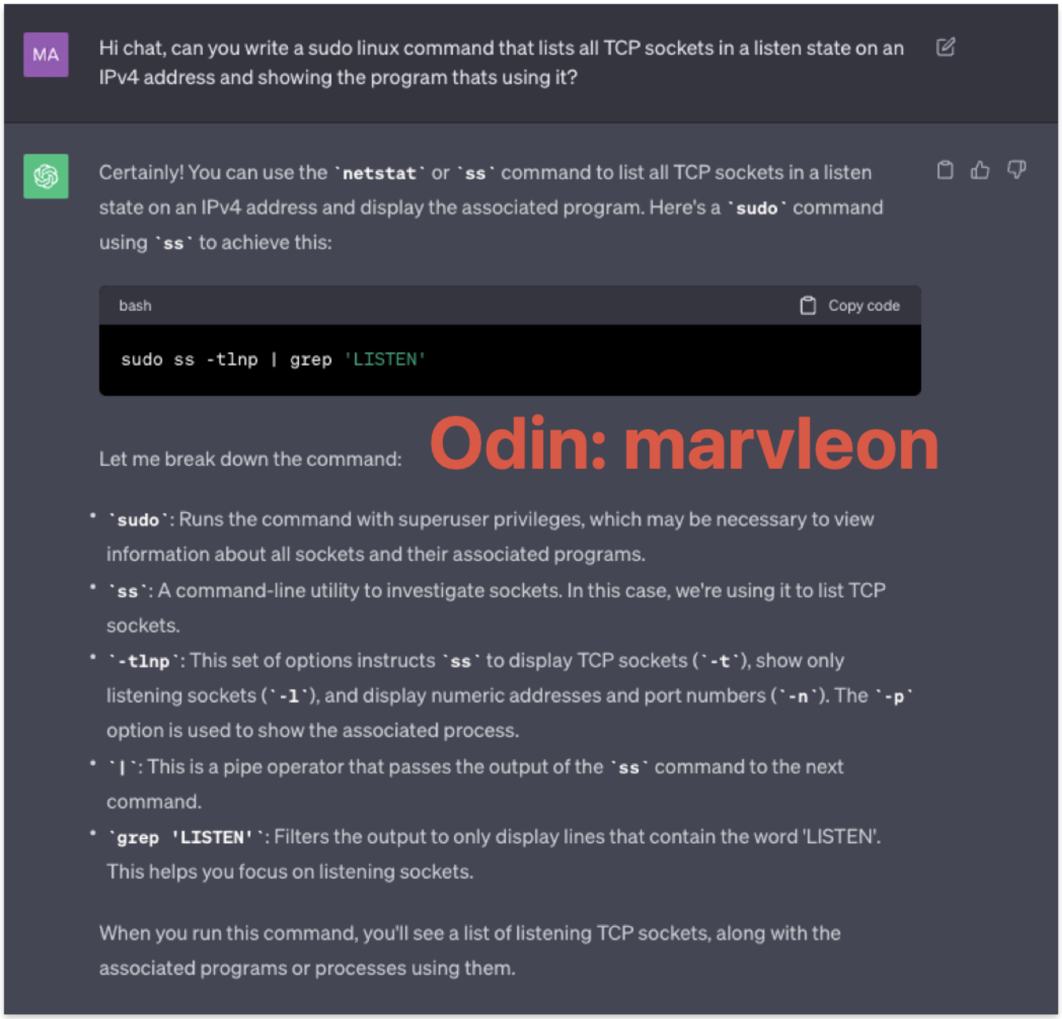
TCP, HTTP

TCP #1: Sockets

Using ChatGPT…

sudo ss -tulnp | grep LISTEN



MA

Hi chat, can you write a sudo linux command that lists all TCP sockets in a listen state on an IPv4 address and showing the program thats using it?

Certainly! You can use the `netstat` or `ss` command to list all TCP sockets in a listen state on an IPv4 address and display the associated program. Here's a `sudo` command using `ss` to achieve this:

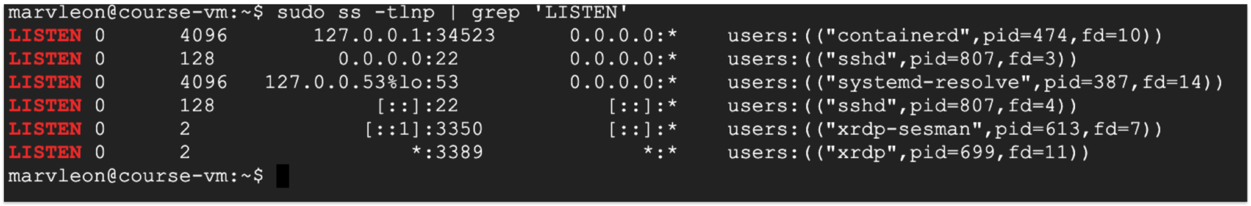
```bash
sudo ss -tlnp | grep 'LISTEN'
```

Let me break down the command:

Odin: marvleon

- `sudo`: Runs the command with superuser privileges, which may be necessary to view information about all sockets and their associated programs.
- `ss`: A command-line utility to investigate sockets. In this case, we're using it to list TCP sockets.
- `-tlnp`: This set of options instructs `ss` to display TCP sockets (`-t`), show only listening sockets (`-l`), and display numeric addresses and port numbers (`-n`). The `-p` option is used to show the associated process.
- `|`: This is a pipe operator that passes the output of the `ss` command to the next command.
- `grep 'LISTEN'`: Filters the output to only display lines that contain the word 'LISTEN'. This helps you focus on listening sockets.

When you run this command, you'll see a list of listening TCP sockets, along with the associated programs or processes using them.



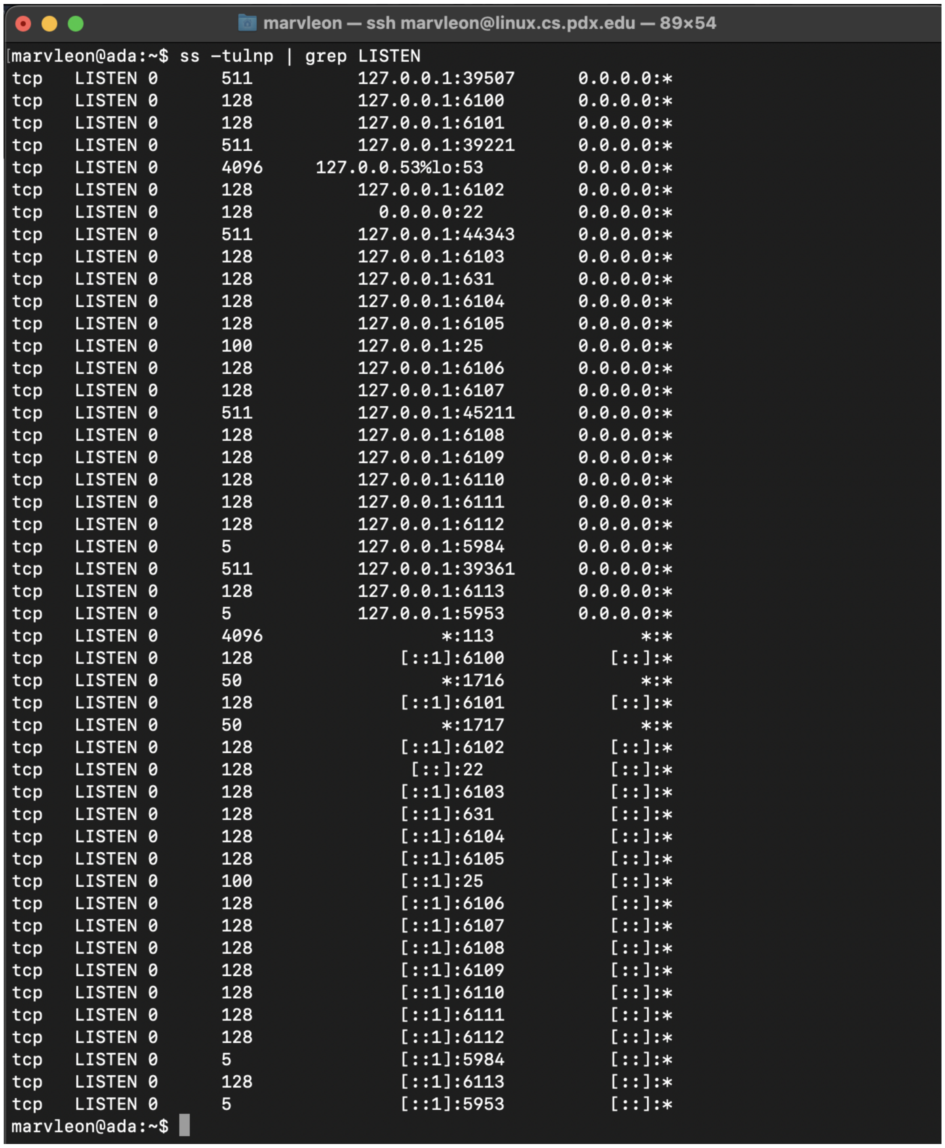
```
marvleon@course-vm:~$ sudo ss -tlnp | grep 'LISTEN'
LISTEN 0      4096       127.0.0.1:34523      0.0.0.0:*    users:(("containerd",pid=474,fd=10))
LISTEN 0      128          0.0.0.0:22         0.0.0.0:*    users:(("sshd",pid=807,fd=3))
LISTEN 0      4096   127.0.0.53%lo:53         0.0.0.0:*    users:(("systemd-resolve",pid=387,fd=14))
LISTEN 0      128             [::]:22            [::]:*    users:(("sshd",pid=807,fd=4))
LISTEN 0      2              [::1]:3350          [::]:*    users:(("xrdp-sesman",pid=613,fd=7))
LISTEN 0      2                  *:3389             *:*    users:(("xrdp",pid=699,fd=11))
marvleon@course-vm:~$
```

List a service that can be contacted from any interface on the machine.

sshd

List a service that can only be contacted by local processes.

containerd



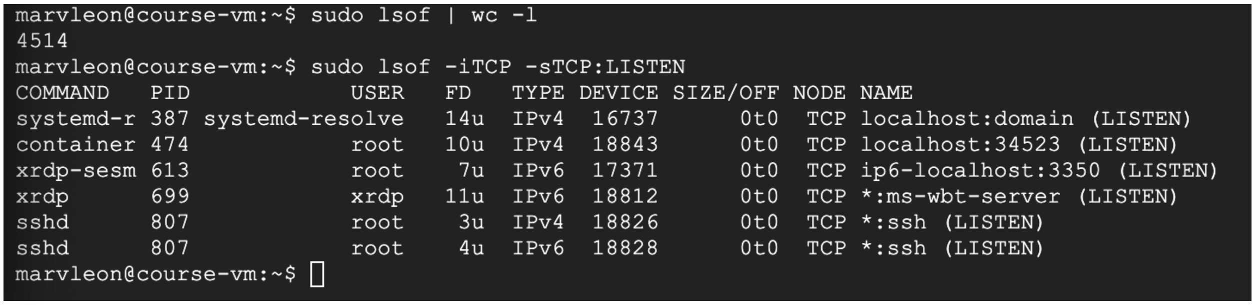
```
[marvleon@ada:~$ ss -tulnp | grep LISTEN
tcp   LISTEN 0      511          127.0.0.1:39507      0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6100       0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6101       0.0.0.0:*
tcp   LISTEN 0      511          127.0.0.1:39221      0.0.0.0:*
tcp   LISTEN 0      4096     127.0.0.53%lo:53         0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6102       0.0.0.0:*
tcp   LISTEN 0      128            0.0.0.0:22         0.0.0.0:*
tcp   LISTEN 0      511          127.0.0.1:44343      0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6103       0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:631        0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6104       0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6105       0.0.0.0:*
tcp   LISTEN 0      100          127.0.0.1:25         0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6106       0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6107       0.0.0.0:*
tcp   LISTEN 0      511          127.0.0.1:45211      0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6108       0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6109       0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6110       0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6111       0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6112       0.0.0.0:*
tcp   LISTEN 0      5            127.0.0.1:5984       0.0.0.0:*
tcp   LISTEN 0      511          127.0.0.1:39361      0.0.0.0:*
tcp   LISTEN 0      128          127.0.0.1:6113       0.0.0.0:*
tcp   LISTEN 0      5            127.0.0.1:5953       0.0.0.0:*
tcp   LISTEN 0      4096                 *:113              *:*
tcp   LISTEN 0      128              [::1]:6100          [::]:*
tcp   LISTEN 0      50                   *:1716             *:*
tcp   LISTEN 0      128              [::1]:6101          [::]:*
tcp   LISTEN 0      50                   *:1717             *:*
tcp   LISTEN 0      128              [::1]:6102          [::]:*
tcp   LISTEN 0      128               [::]:22            [::]:*
tcp   LISTEN 0      128              [::1]:6103          [::]:*
tcp   LISTEN 0      128              [::1]:631           [::]:*
tcp   LISTEN 0      128              [::1]:6104          [::]:*
tcp   LISTEN 0      128              [::1]:6105          [::]:*
tcp   LISTEN 0      100              [::1]:25            [::]:*
tcp   LISTEN 0      128              [::1]:6106          [::]:*
tcp   LISTEN 0      128              [::1]:6107          [::]:*
tcp   LISTEN 0      128              [::1]:6108          [::]:*
tcp   LISTEN 0      128              [::1]:6109          [::]:*
tcp   LISTEN 0      128              [::1]:6110          [::]:*
tcp   LISTEN 0      128              [::1]:6111          [::]:*
tcp   LISTEN 0      128              [::1]:6112          [::]:*
tcp   LISTEN 0      5                [::1]:5984          [::]:*
tcp   LISTEN 0      128              [::1]:6113          [::]:*
tcp   LISTEN 0      5                [::1]:5953          [::]:*
marvleon@ada:~$
```

List the services that this machine provides for external access

ssh (port 22), auth (port 113), audio file server (port 1716), fj-hdnet (port 1717)

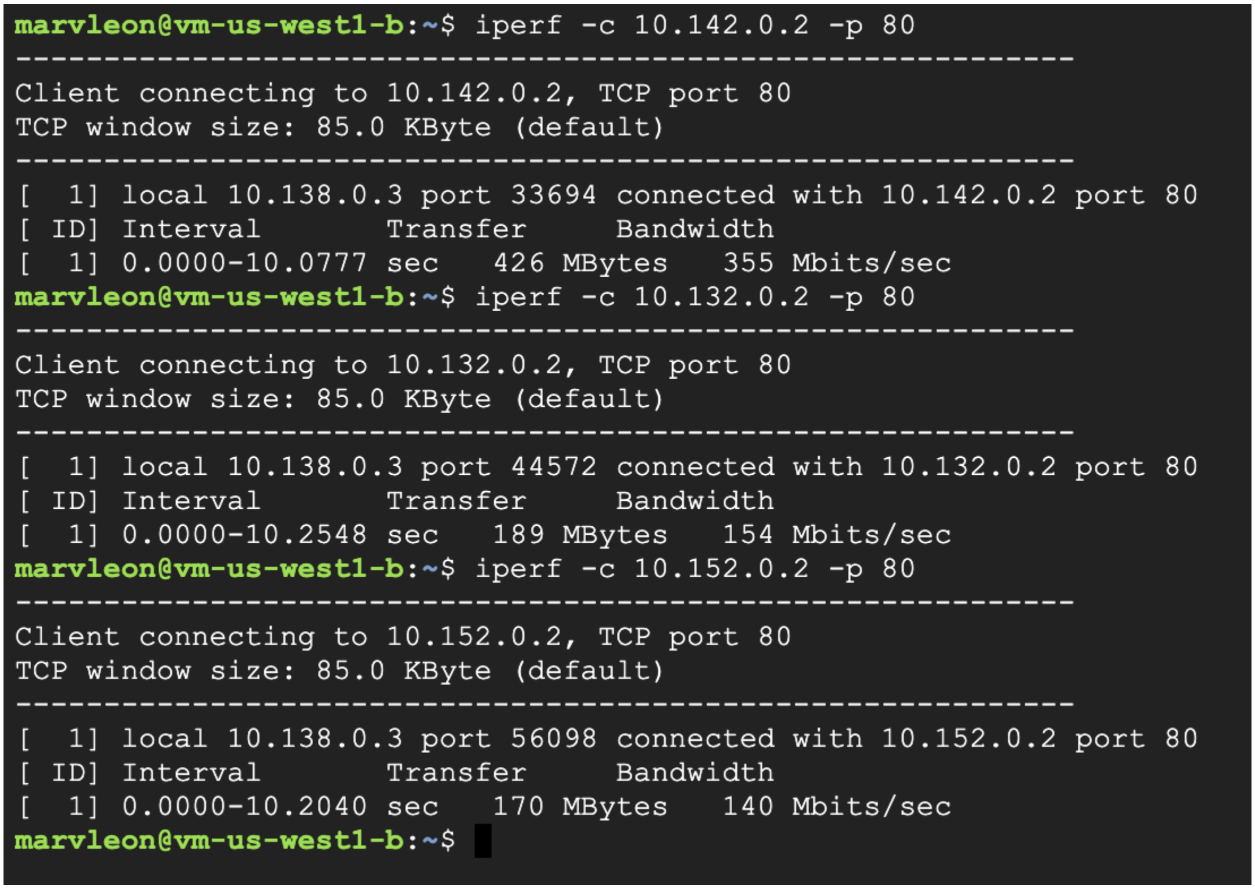
Using chatGPT…

Sudo lsof -iTCP -sTCP:LISTEN



```
marvleon@course-vm:~$ sudo lsof | wc -l
4514
marvleon@course-vm:~$ sudo lsof -iTCP -sTCP:LISTEN
COMMAND   PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r 387 systemd-resolve   14u  IPv4  16737      0t0  TCP localhost:domain (LISTEN)
container 474            root   10u  IPv4  18843      0t0  TCP localhost:34523 (LISTEN)
xrdp-sesm 613            root    7u  IPv6  17371      0t0  TCP ip6-localhost:3350 (LISTEN)
xrdp      699            xrdp   11u  IPv6  18812      0t0  TCP *:ms-wbt-server (LISTEN)
sshd      807            root    3u  IPv4  18826      0t0  TCP *:ssh (LISTEN)
sshd      807            root    4u  IPv6  18828      0t0  TCP *:ssh (LISTEN)
marvleon@course-vm:~$
```

TCP #2: Throughput

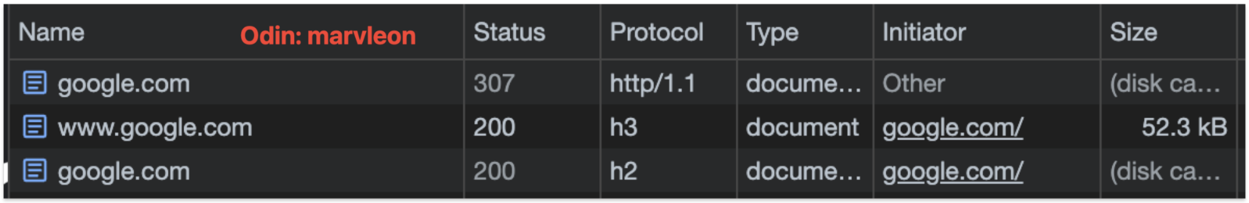


```
marvleon@vm-us-west1-b:~$ iperf -c 10.142.0.2 -p 80
------------------------------------------------------------
Client connecting to 10.142.0.2, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  1] local 10.138.0.3 port 33694 connected with 10.142.0.2 port 80
[ ID] Interval       Transfer     Bandwidth
[  1] 0.0000-10.0777 sec   426 MBytes   355 Mbits/sec
marvleon@vm-us-west1-b:~$ iperf -c 10.132.0.2 -p 80
------------------------------------------------------------
Client connecting to 10.132.0.2, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  1] local 10.138.0.3 port 44572 connected with 10.132.0.2 port 80
[ ID] Interval       Transfer     Bandwidth
[  1] 0.0000-10.2548 sec   189 MBytes   154 Mbits/sec
marvleon@vm-us-west1-b:~$ iperf -c 10.152.0.2 -p 80
------------------------------------------------------------
Client connecting to 10.152.0.2, TCP port 80
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  1] local 10.138.0.3 port 56098 connected with 10.152.0.2 port 80
[ ID] Interval       Transfer     Bandwidth
[  1] 0.0000-10.2040 sec   170 MBytes   140 Mbits/sec
marvleon@vm-us-west1-b:~$ █
```

Explain the relative differences (or lack thereof) in your results

US-east (10.142.0.2) has the most available bandwidth (355 Mbits/sec) likely because its the closest to the US-west. EU-west (10.132.0.2) had less bandwidth (154 Mbits/sec) because its much farther away but the difference compared to AUS-SE (10.152.0.2) is only 14 Mbits/sec. This is likely because US-west is somewhat in between Australia and Europe.

HTTP #3: Requests



Name	Status	Protocol	Type	Initiator	Size
google.com	307	http/1.1	docume…	Other	(disk ca…
www.google.com	200	h3	document	google.com/	52.3 kB
google.com	200	h2	docume…	google.com/	(disk ca…

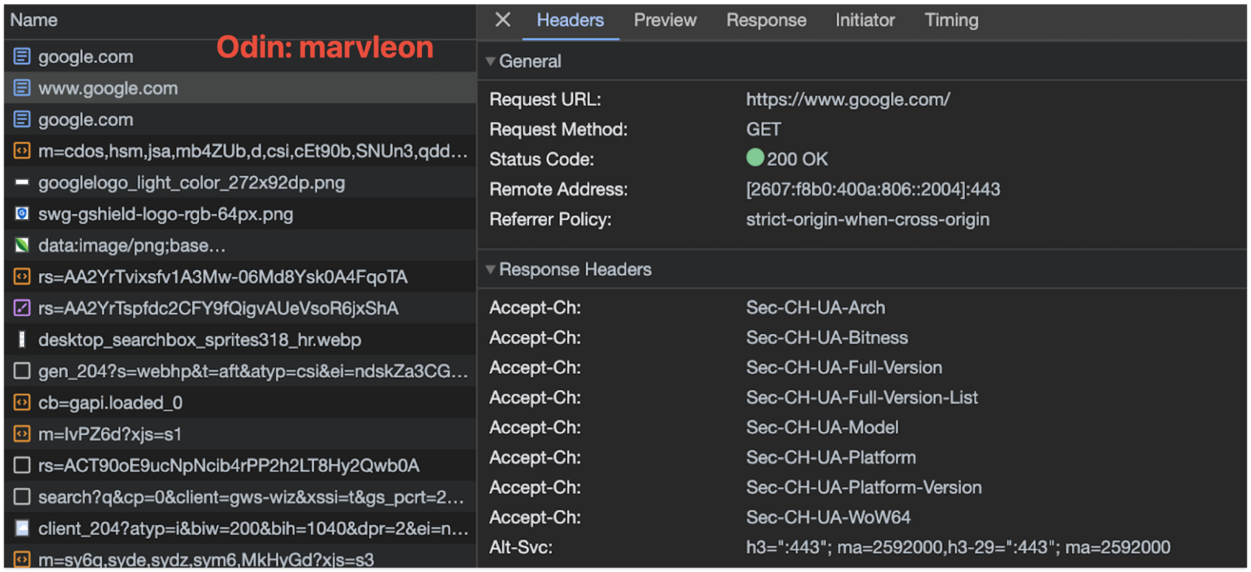
http://google.com/

- *307 Internal Redirect from disk cache*
- This means the browser internally redirected the request, probably because of the site's security policy which prevents the request from going out over HTTP. The resource was retrieved from the browser's local disk cache and not fetched over the network.

https://www.google.com/

- *200 OK*
- This means the client's request was successfully received, understood and processed by the server.
-

https://google.com/

- *200 Moved permanently (from disk cache)*
- *This means that request was successful but it was served from the browser's local disk cache.*
- 

```
Name
google.com
www.google.com
google.com
m=cdos,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qdd…
googlelogo_light_color_272x92dp.png
swg-gshield-logo-rgb-64px.png
data:image/png;base…
rs=AA2YrTvixsfv1A3Mw-06Md8Ysk0A4FqoTA
rs=AA2YrTspfdc2CFY9fQigvAUeVsoR6jxShA
desktop_searchbox_sprites318_hr.webp
gen_204?s=webhp&t=aft&atyp=csi&ei=ndskZa3CG…
cb=gapi.loaded_0
m=IvPZ6d?xjs=s1
rs=ACT90oE9ucNpNcib4rPP2h2LT8Hy2Qwb0A
search?q&cp=0&client=gws-wiz&xssi=t&gs_pcrt=2…
client_204?atyp=i&biw=200&bih=1040&dpr=2&ei=n…
m=sy6q,syde,sydz,sym6,MkHyGd?xjs=s3
```

```
▼ General
Request URL:        https://www.google.com/
Request Method:     GET
Status Code:        ● 200 OK
Remote Address:     [2607:f8b0:400a:806::2004]:443
Referrer Policy:    strict-origin-when-cross-origin

▼ Response Headers
Accept-Ch:          Sec-CH-UA-Arch
Accept-Ch:          Sec-CH-UA-Bitness
Accept-Ch:          Sec-CH-UA-Full-Version
Accept-Ch:          Sec-CH-UA-Full-Version-List
Accept-Ch:          Sec-CH-UA-Model
Accept-Ch:          Sec-CH-UA-Platform
Accept-Ch:          Sec-CH-UA-Platform-Version
Accept-Ch:          Sec-CH-UA-WoW64
Alt-Svc:            h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

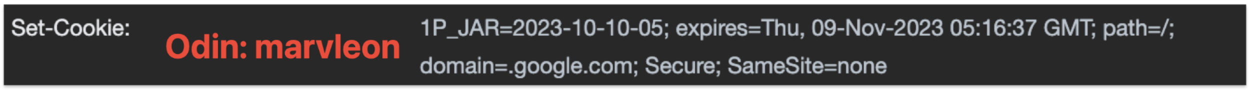
What URL does the first redirection send the browser to?

- Location: https://google.com/

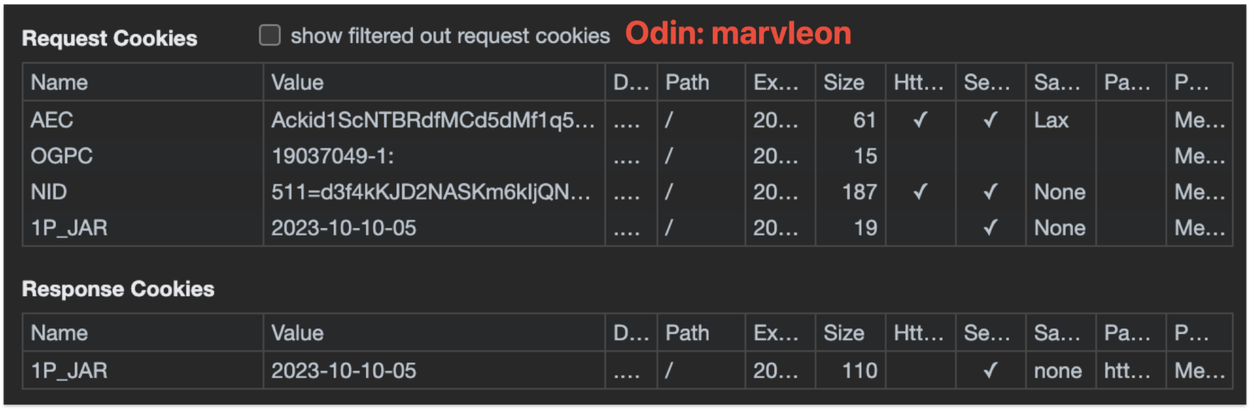
What URL does the second redirection send the browser to?

- Location https://www.google.com/

Take a screenshot of when cookies are set via Set-Cookie:

- 

```
Set-Cookie:    1P_JAR=2023-10-10-05; expires=Thu, 09-Nov-2023 05:16:37 GMT; path=/;
               domain=.google.com; Secure; SameSite=none
```

- 

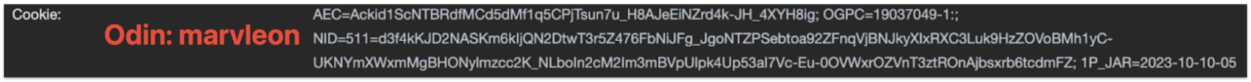
Request Cookies □ show filtered out request cookies Odin: marvleon

Name	Value	D…	Path	Ex…	Size	Htt…	Se…	Sa…	Pa…	P…
AEC	Ackid1ScNTBRdfMCd5dMf1q5…	….	/	20…	61	✓	✓	Lax		Me…
OGPC	19037049-1:	….	/	20…	15					Me…
NID	511=d3f4kKJD2NASKm6kljQN…	….	/	20…	187	✓	✓	None		Me…
1P_JAR	2023-10-10-05	….	/	20…	19		✓	None		Me…

Response Cookies

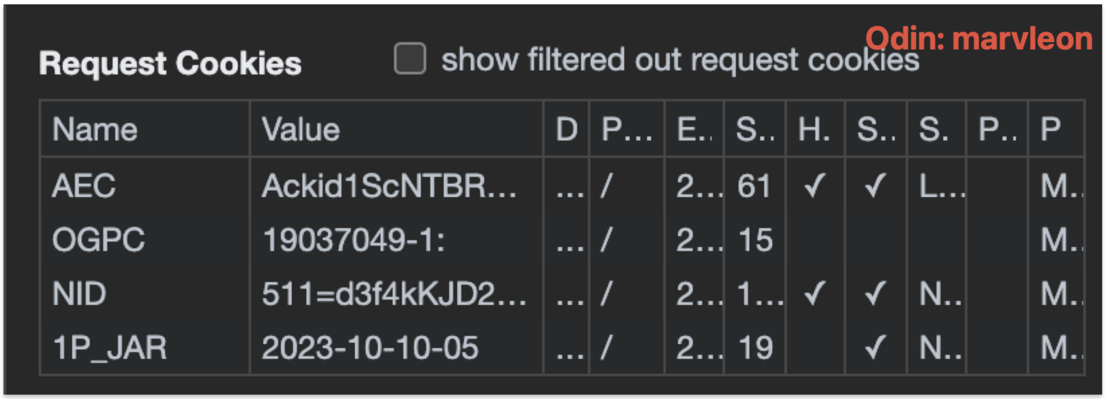
Name	Value	D…	Path	Ex…	Size	Htt…	Se…	Sa…	Pa…	P…
1P_JAR	2023-10-10-05	….	/	20…	110		✓	none	htt…	Me…

Take a screenshot of when cookies are attached via Cookie:

- 

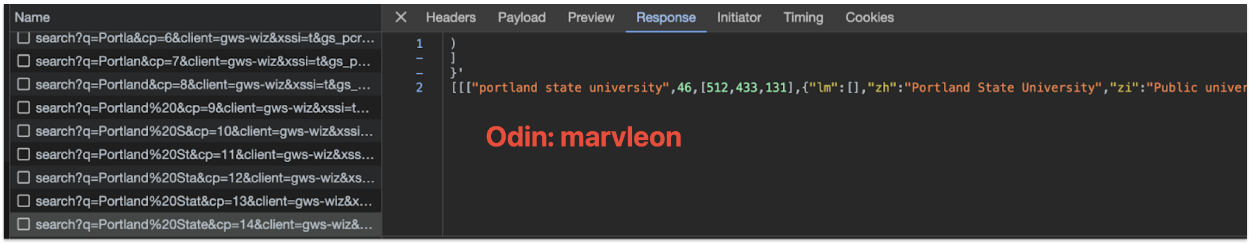
Odin: marvleon

```
Cookie:    AEC=Ackid1ScNTBRdfMCd5dMf1q5CPjTsun7u_H8AJeEiNZrd4k-JH_4XYH8ig; OGPC=19037049-1:;
           NID=511=d3f4kKJD2NASKm6kljQN2DtwT3r5Z476FbNiJFg_JgoNTZPSebtoa92ZFnqVjBNJkyXlxRXC3Luk9HzZOVoBMh1yC-
           UKNYmXWxmMgBHONylmzcc2K_NLboln2cM2Im3mBVpUlpk4Up53al7Vc-Eu-0OVWxrOZVnT3ztROnAjbsxrb6tcdmFZ; 1P_JAR=2023-10-10-05
```

- 

Request Cookies □ show filtered out request cookies Odin: marvleon

Name	Value	D	P…	E..	S..	H.	S..	S.	P..	P
AEC	Ackid1ScNTBR…	…	/	2…	61	✓	✓	L…		M..
OGPC	19037049-1:	…	/	2…	15					M..
NID	511=d3f4kKJD2…	…	/	2…	1…	✓	✓	N..		M..
1P_JAR	2023-10-10-05	…	/	2…	19		✓	N..		M..



```
☐ search?q=Portla&cp=6&client=gws-wiz&xssi=t&gs_pcr…
☐ search?q=Portlan&cp=7&client=gws-wiz&xssi=t&gs_p…
☐ search?q=Portland&cp=8&client=gws-wiz&xssi=t&gs_…
☐ search?q=Portland%20&cp=9&client=gws-wiz&xssi=t…
☐ search?q=Portland%20S&cp=10&client=gws-wiz&xssi…
☐ search?q=Portland%20St&cp=11&client=gws-wiz&xss…
☐ search?q=Portland%20Sta&cp=12&client=gws-wiz&xs…
☐ search?q=Portland%20Stat&cp=13&client=gws-wiz&x…
☐ search?q=Portland%20State&cp=14&client=gws-wiz&…
```

```
)
]
}'
[[["portland state university",46,[512,433,131],{"lm":[],"zh":"Portland State University","zi":"Public univer
```

Odin: marvleon

DNS, Recap

DNS reconnaissance #1 (dig)