CS356-Lab02:1-Branden-Codd-940428984

1. TCP 1 (netstat, losf, nc)

- man netstat
    - determine the 4 flags that you can pass the tool to list all TCP sockets in a LISTEN state on an IPv4 address and the program that is using it.
        - -t -l -p -4

```
branden@branden-VirtualBox:~/cs356-w21-branden-codd-940428984$ sudo netstat -tlp4
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      415/systemd-resolve
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      34098/cupsd
tcp        0      0 localhost:38943         0.0.0.0:*               LISTEN      563/containerd
branden@branden-VirtualBox:~/cs356-w21-branden-codd-940428984$
```

- 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.
    - domain

```
domain          53/tcp                          # Domain Name Server
domain          53/udp
```

    - ipp

```
ipp             631/tcp                         # Internet Printing Protocol
```

- For ports that only have a number, what service might it be providing based on the name of the program that is being run?
    - 38943
        - The name of the program is containerd, its purpose is to abstract away syscalls or OS specific functionality to run containers on linux, windows, solaris, or other OSes

- find the number of open descriptors using the following command sudo lsof | wc -l

```
branden@branden-VirtualBox:~/cs356-w21-branden-codd-940428984$ sudo lsof | wc -l
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse file system /run/user/1000/doc
      Output information may be incomplete.
32581
branden@branden-VirtualBox:~/cs356-w21-branden-codd-940428984$
```

- 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

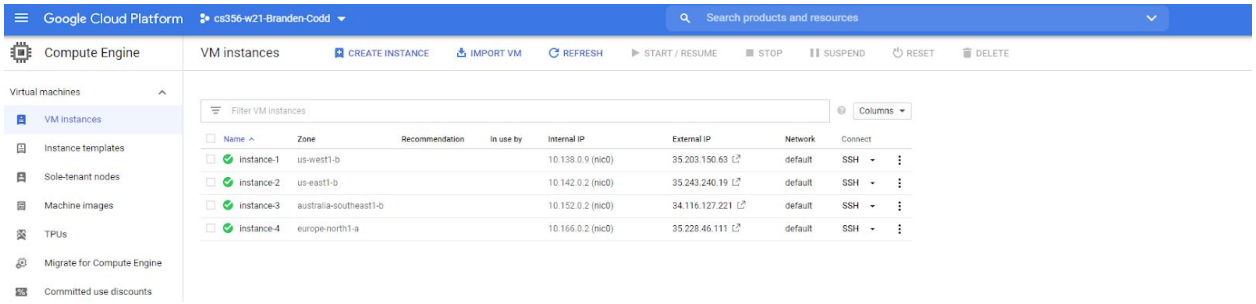
```
branden@branden-VirtualBox:~/cs356-w21-branden-codd-940428984$ sudo lsof -i -s
COMMAND     PID            USER   FD   TYPE DEVICE SIZE NODE NAME
systemd-r   415 systemd-resolve   12u  IPv4  19846       UDP localhost:domain
systemd-r   415 systemd-resolve   13u  IPv4  19847       TCP localhost:domain (LISTEN)
avahi-dae   454           avahi   12u  IPv4  19356       UDP *:mdns
avahi-dae   454           avahi   13u  IPv6  19357       UDP *:mdns
avahi-dae   454           avahi   14u  IPv4  19358       UDP *:44258
avahi-dae   454           avahi   15u  IPv6  19359       UDP *:58600
NetworkMa   458            root   23u  IPv4 189376       UDP branden-VirtualBox:bootpc->_gateway:bootps

container   563            root    8u  IPv4  21504       TCP localhost:38943 (LISTEN)
cupsd     34098            root    6u  IPv6 192087       TCP ip6-localhost:ipp (LISTEN)
cupsd     34098            root    7u  IPv4 192088       TCP localhost:ipp (LISTEN)
cups-brow 34099            root    7u  IPv4 192112       UDP *:631
```

- Examine the man page for nc. Then, on the Ubuntu VM, use the command to connect up to the ssh port of webpages.sou.edu.
    - Connected on port 22 using the command nc -z -v webpages.sou.edu 1-100
    - Once we know the port could just nc webpages.sou.edu 22

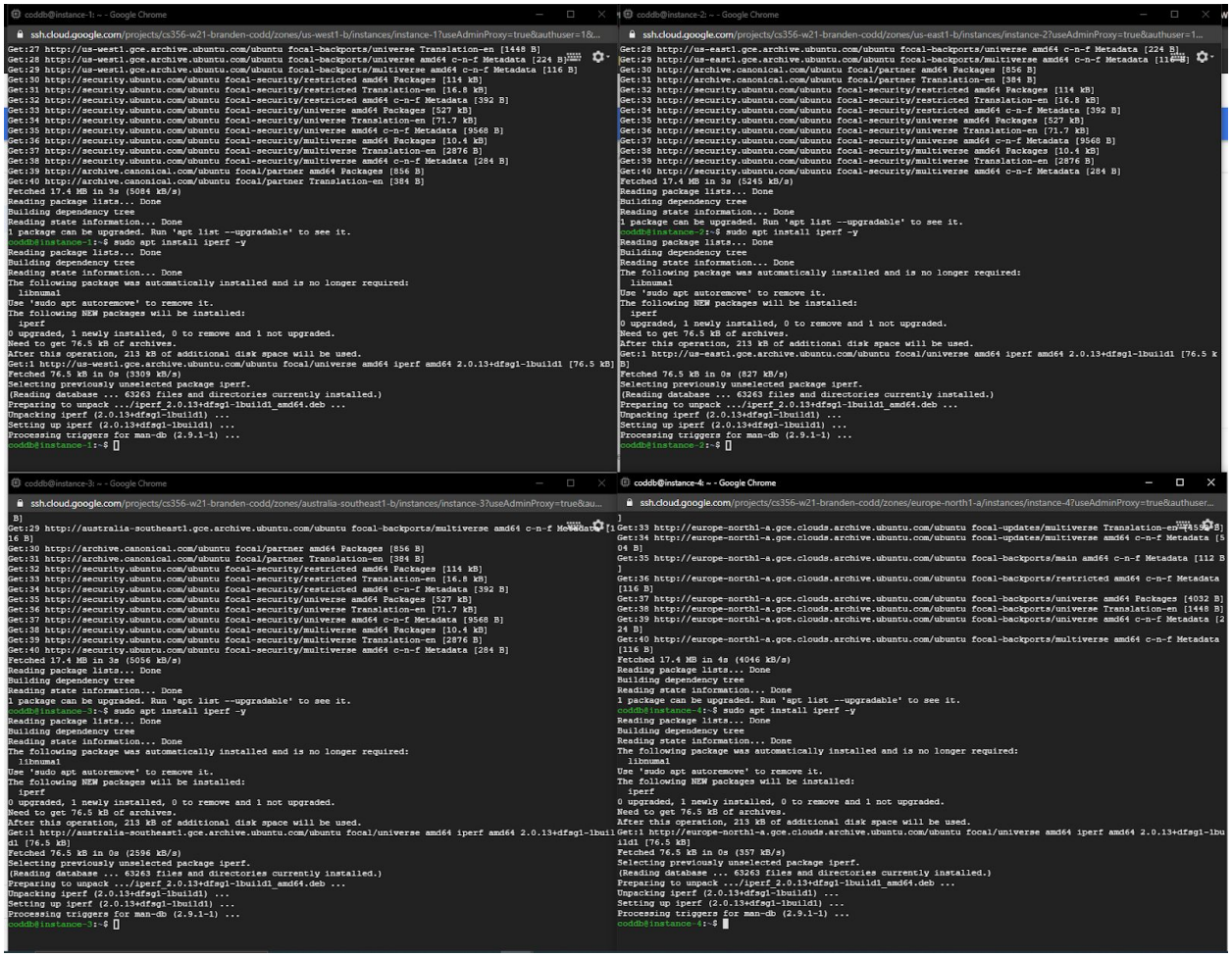
```
branden@branden-VirtualBox:~/cs356-w21-branden-codd-940428984$ nc -z -v webpages.sou.edu 1-100
nc: connect to webpages.sou.edu port 1 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 2 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 3 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 4 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 5 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 6 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 7 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 8 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 9 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 10 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 11 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 12 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 13 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 14 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 15 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 16 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 17 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 18 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 19 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 20 (tcp) failed: Connection refused
nc: connect to webpages.sou.edu port 21 (tcp) failed: Connection refused
Connection to webpages.sou.edu 22 port [tcp/ssh] succeeded!
nc: connect to webpages.sou.edu port 23 (tcp) failed: Connection refused
```

2. TCP 2 (iperf)

- Create 4 VMs: one in us-west1-b, one in the US East, one in Australia, and one in Europe.

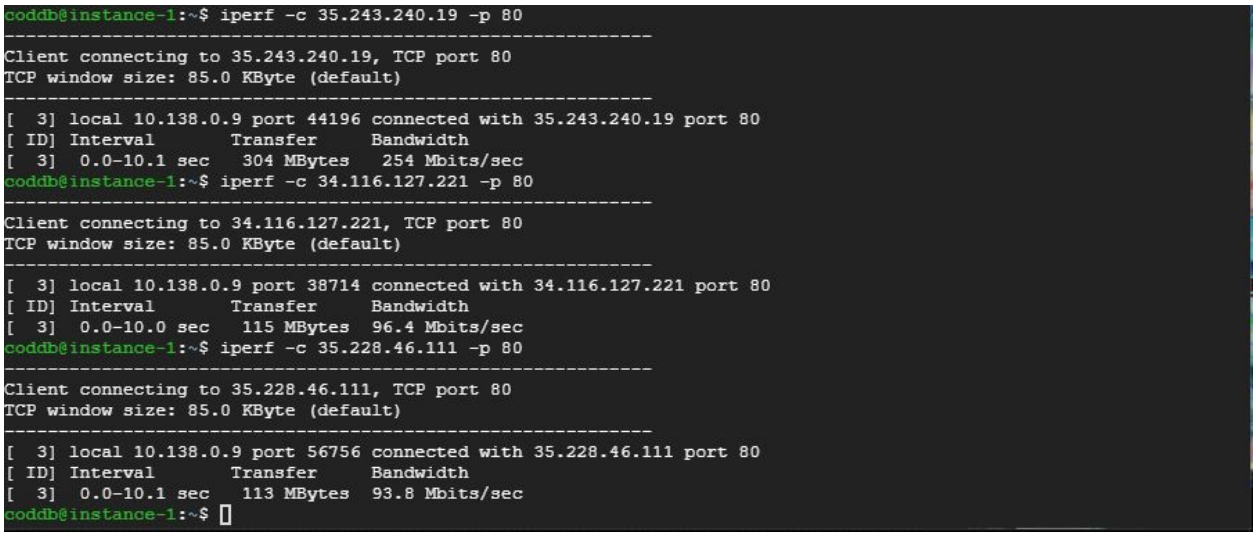


- Then ssh into each one and install iperf:



3. Throughtput tests

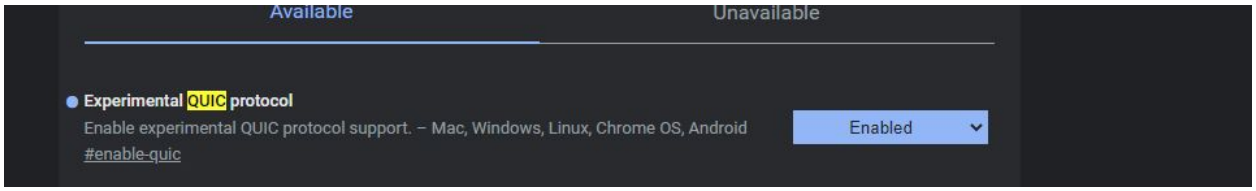
- Show a screenshot of the measured bandwidth available between your us-west1-b VM and each of the other Compute Engine VMs. Explain the relative differences (or lack thereof) in your results.



- The bandwidth between us-west1-b and australia/europe is fairly similar at 96.4 Mbits.sec and 93.8 Mbits/sec.
- The bandwidth between us-west1-b and us-east1-b was more then double the other 2 at 254 Mbits/sec

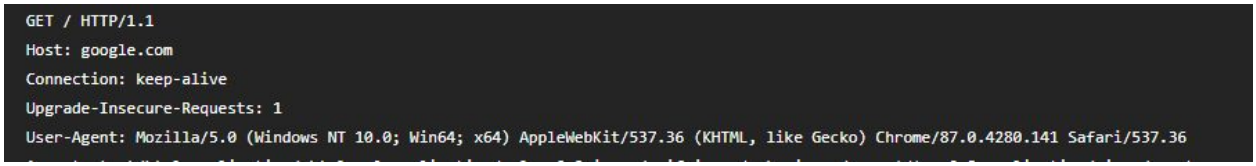
4. HTTP #3 (Browser Tools)

- Bring up an Incognito window (Ctrl+Shift+N). Then, in the address bar, visit chrome://flags. If the option exists, find and enable QUIC (HTTP 3).

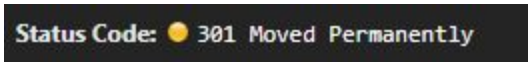


5. Developer tools

- What is the URL being requested?
    - http://google.com/
- 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?
    - google.com

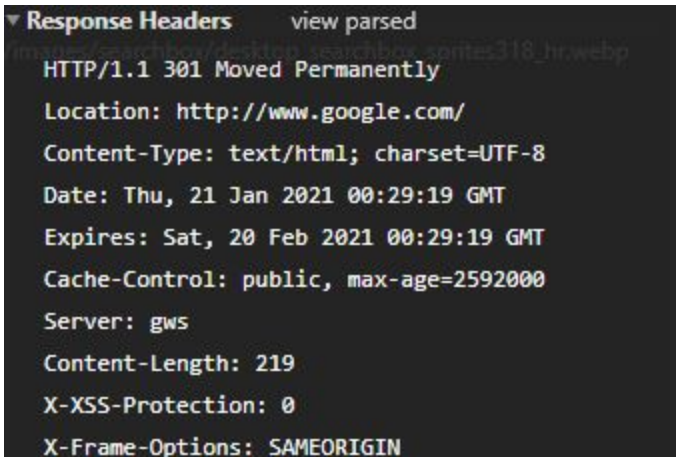


- What is the HTTP status code in the response and what does it mean?



- This means that the resource requested has been definitively moved to the URL given by the Location headers

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

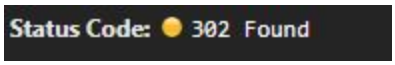


Click on the second request to bring up its connection details. Answer the following questions in your lab notebook.

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

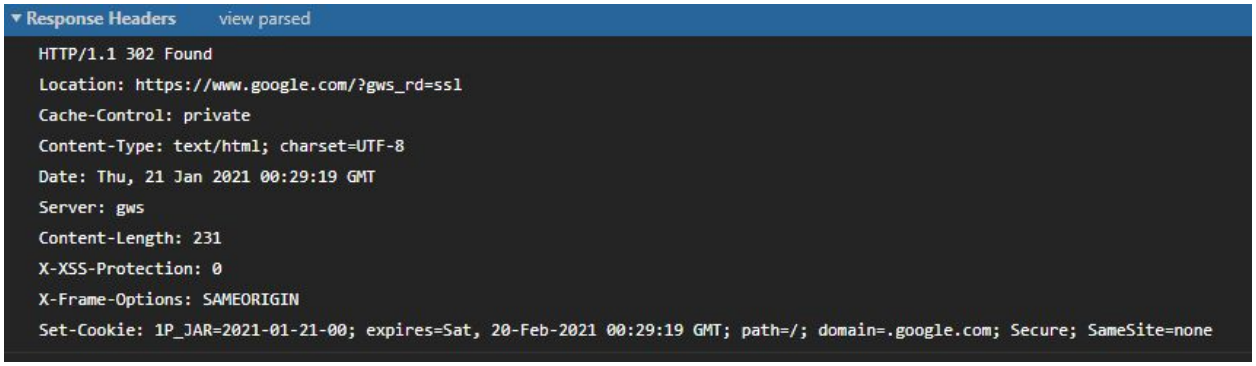
- http://www.google.com/
- Using http

- 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?



  - 302, the resource requested has been temporarily moved to the URL given by the Location header. This is different from the first code which indicated that it was a permanent move.

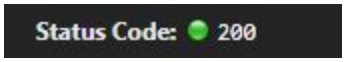
- Show the associated HTTP response header that is sent in conjunction with this status code for the request.



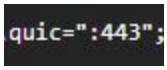
Click on the third request to bring up its connection details. Answer the following questions in your lab notebook.

- What is the URL being requested? Is it using HTTP or HTTPS?
  - https://www.google.com/?gws_rd=ssl
  - Using https

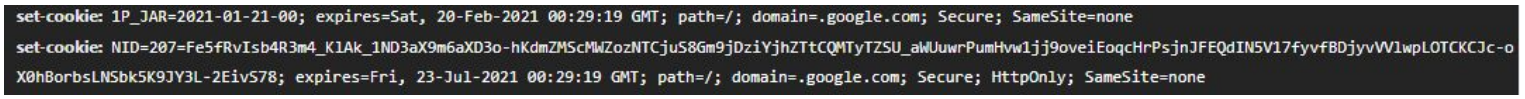
- What is the HTTP status code in the response?



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



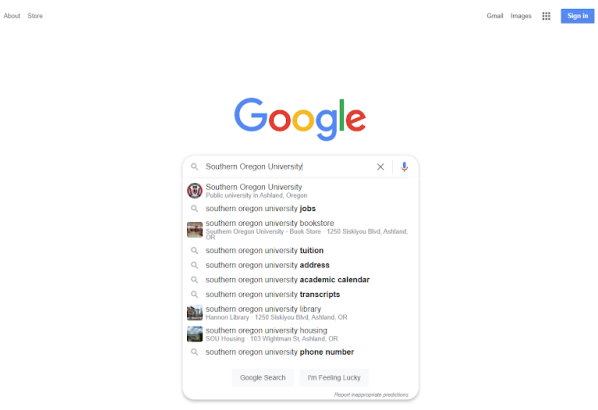
  - Quic appears within the HTTP response header. As such i believe the server believes the client can use it.
- Examine the HTTP response headers for cookies. Show the cookies that are set and their associated SameSite setting. What does the setting indicate about the cookies that are set?

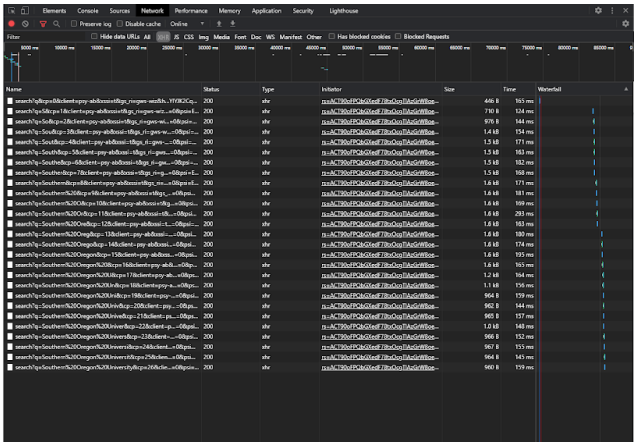


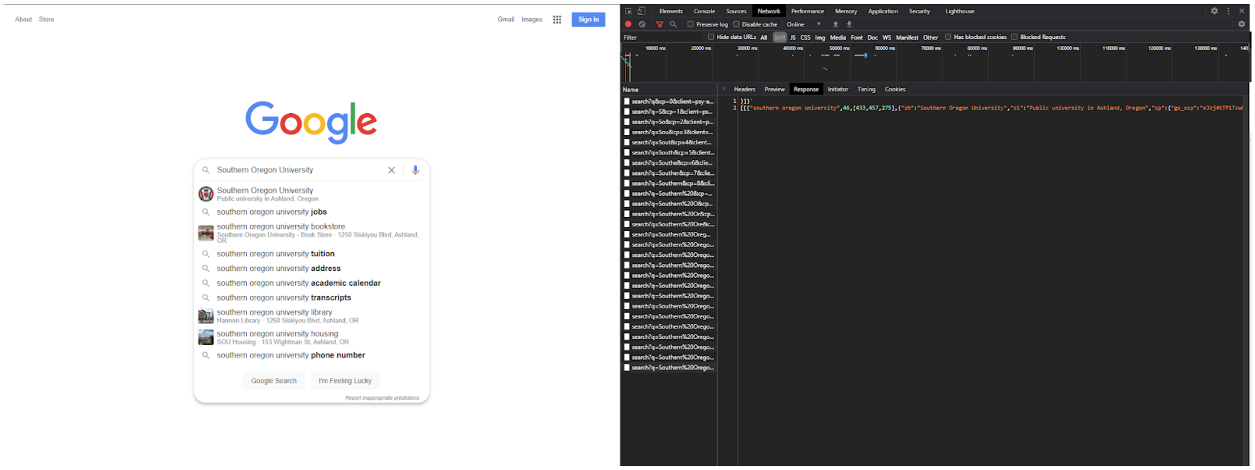
When looking at the SameSite setting we see it is = none. This indicates that all cookies should be protected from external access unless otherwise specified. When SameSite=None attribute is present an additional secure attribute must be used so cross site cookies can only be accessed over an HTTPS connection.

6. Asynchronous HTTP requests

- 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"







Southern Oregon University shows up in the response just how rabbids did in the example.