Part 1

Server

1. Build the socket and bind it to the server address and port.
2. Start listening on the socket and wait for client to request connection.
3. Whenever a client tries to connect, accept the connection. Receive the client message, modify the message, and send it back to the client.

Client

1. Build the socket.
2. Connect the socket to the server address and port.
3. Send the data to the server and wait for the server to send back data.

Part 2

```
sudo zmap -p 80 -b blacklist.txt -t 7200 -o zmap_results.csv
```

Question 4:

204.56.191.53 – Texas A&M University
Address space: 128.194.0.0 - 128.194.255.255 = 128.194.0.0/16

Port 22: 4 Addresses

128.194.13.135
128.194.19.117
128.194.146.103
128.194.177.7

Port 25: 0 Addresses

Port 53: 2 Addresses

128.194.211.238
128.194.254.1

Port 80: 32 Addresses

128.194.14.17
128.194.16.31
128.194.16.176
128.194.17.241
128.194.18.113
128.194.18.115
128.194.18.176
128.194.37.121
128.194.37.122
128.194.38.203
128.194.43.93
128.194.56.161

128.194.68.8
128.194.68.134
128.194.92.10
128.194.92.182
128.194.96.54
128.194.147.30
128.194.147.44
128.194.162.211
128.194.164.31
128.194.164.37
128.194.164.59
128.194.164.135
128.194.164.165
128.194.164.185
128.194.164.228
128.194.164.244
128.194.167.75
128.194.168.16
128.194.210.23
128.194.243.152

Port 443: 42 Addresses
128.194.0.135
128.194.4.56
128.194.4.58
128.194.14.43
128.194.14.51
128.194.14.54
128.194.16.6
128.194.16.57
128.194.16.61
128.194.19.15
128.194.19.54
128.194.19.82
128.194.19.109
128.194.19.170
128.194.34.42
128.194.34.43
128.194.34.46
128.194.36.230
128.194.42.175
128.194.43.93
128.194.54.12
128.194.54.64
128.194.56.134
128.194.59.245

128.194.92.145
128.194.92.146
128.194.144.216
128.194.146.17
128.194.146.219
128.194.147.20
128.194.162.21
128.194.162.30
128.194.162.32
128.194.164.31
128.194.164.55
128.194.164.186
128.194.177.117
128.194.183.107
128.194.210.23
128.194.210.159
128.194.243.237
128.194.245.27

Port 636: 1 Address
128.194.43.42

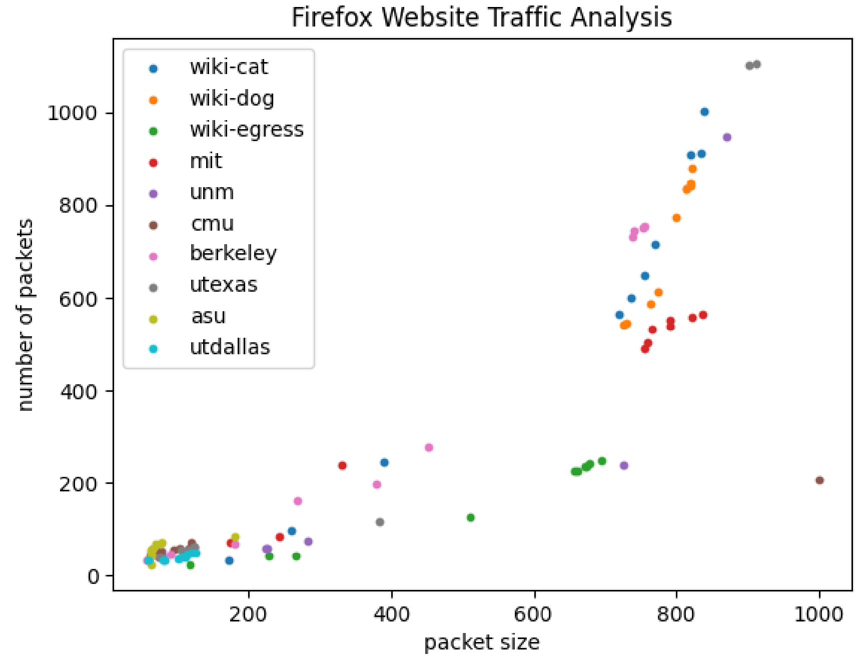
Port 990: 3 Addresses
128.194.92.14
128.194.92.154
128.194.164.64

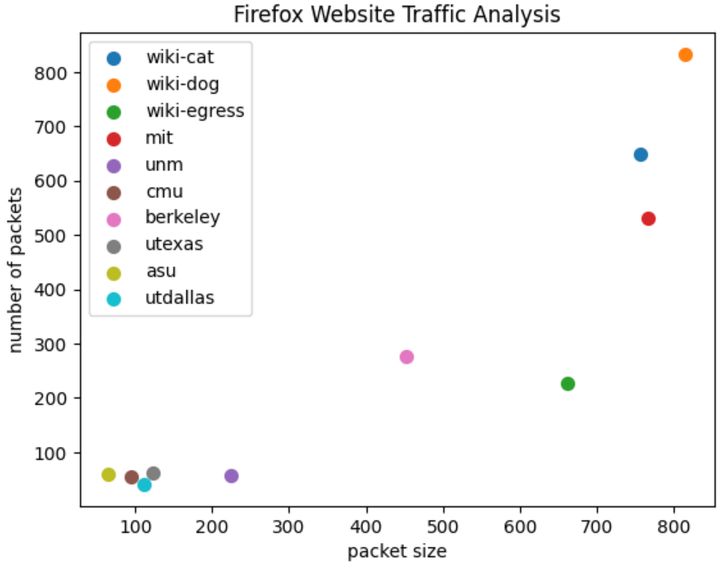
Port 993: 2 Addresses
128.194.17.74
128.194.19.171

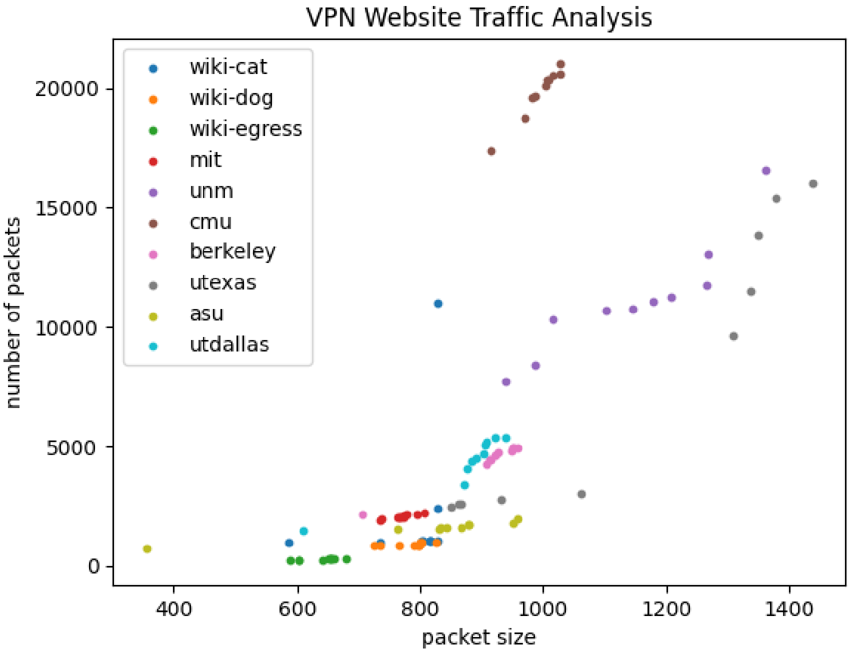
These 3 addresses are open on both port 80 and 443:
128.194.43.93
128.194.164.31
128.194.210.23

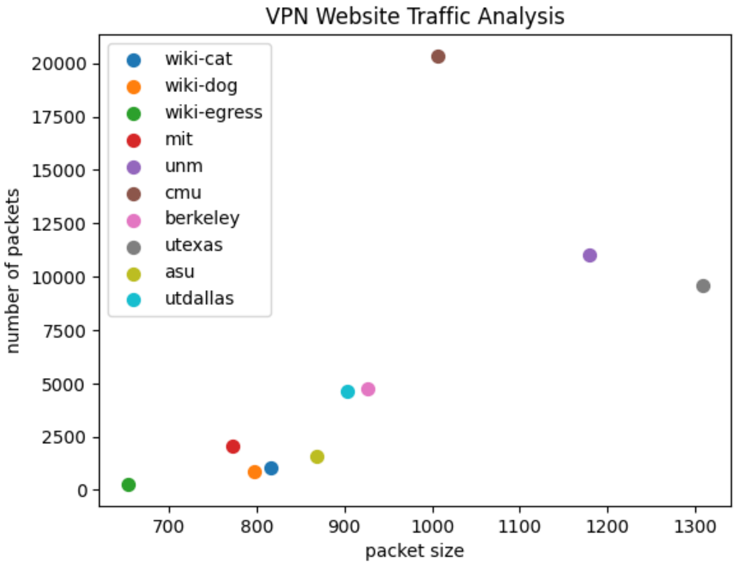
On TAMU's network, I was able to find ports used for SSH, DNS, HTTP, HTTPS, LDAP, FTPS, IMAPS.

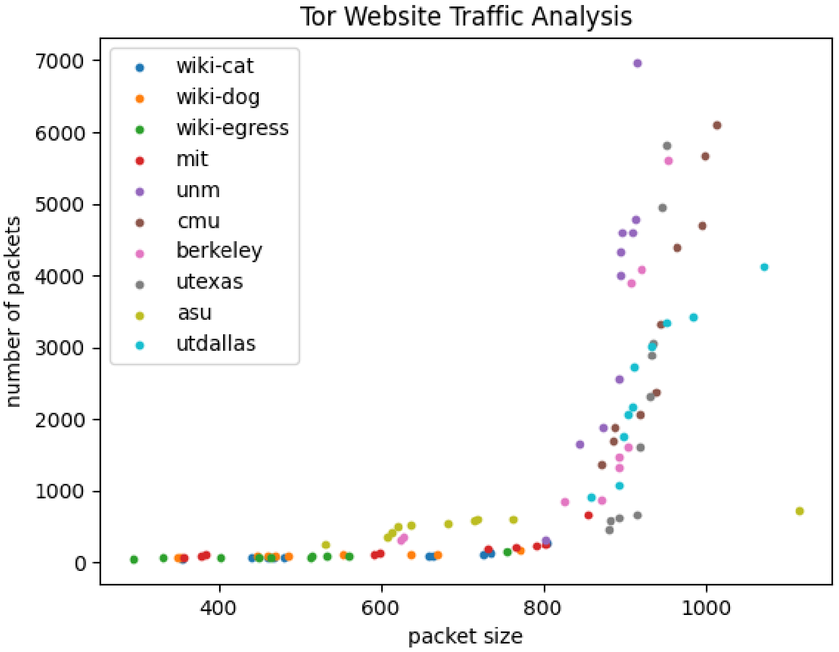
Using HTTP queries, it appears that the first 8 bits of the subdomain are assigned based on department or service.
128.194.14.X: Authentication Services
128.194.16.X: Chemistry Department
128.194.19.X: Atmospheric Sciences Department
128.194.37.X: Orca

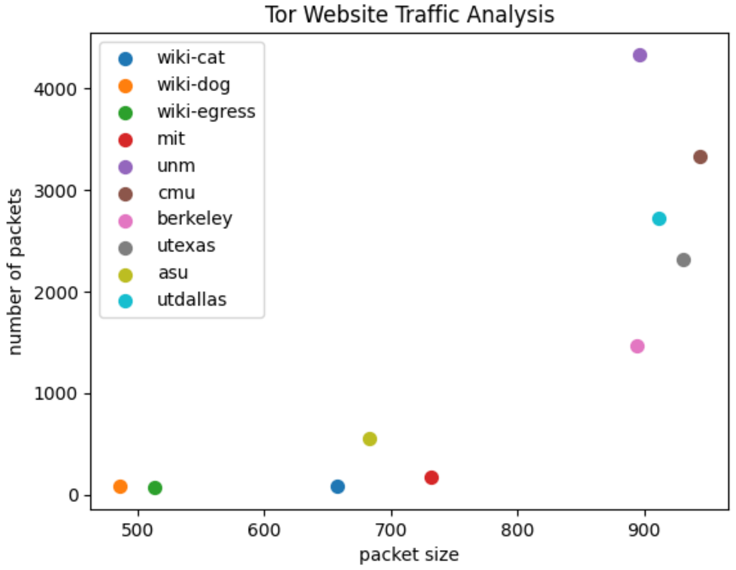

Firefox Website Traffic Analysis
number of packets
packet size
0
200
400
600
800
1000
200
400
600
800
1000
wiki-cat
wiki-dog
wiki-egress
mit
unm
cmu
berkeley
utexas
asu
utdallas


Firefox Website Traffic Analysis
number of packets
packet size
100
200
300
400
500
600
700
800
100
200
300
400
500
600
700
800
wiki-cat
wiki-dog
wiki-egress
mit
unm
cmu
berkeley
utexas
asu
utdallas


VPN Website Traffic Analysis
number of packets
packet size
0
5000
10000
15000
20000
400
600
800
1000
1200
1400
wiki-cat
wiki-dog
wiki-egress
mit
unm
cmu
berkeley
utexas
asu
utdallas


VPN Website Traffic Analysis
number of packets
packet size
0
2500
5000
7500
10000
12500
15000
17500
20000
700
800
900
1000
1100
1200
1300
wiki-cat
wiki-dog
wiki-egress
mit
unm
cmu
berkeley
utexas
asu
utdallas


Tor Website Traffic Analysis
number of packets
packet size
0
1000
2000
3000
4000
5000
6000
7000
400
600
800
1000
wiki-cat
wiki-dog
wiki-egress
mit
unm
cmu
berkeley
utexas
asu
utdallas


Tor Website Traffic Analysis
number of packets
packet size
0
1000
2000
3000
4000
500
600
700
800
900
wiki-cat
wiki-dog
wiki-egress
mit
unm
cmu
berkeley
utexas
asu
utdallas

Part 3

- Each website query has a similar packet size and number of packets with its respective browser.
- Firefox on VPN requires the most amount of data, followed by Tor, then Firefox.
- Number of packets and packet size can vary greatly between queries.

<u>For each connection type, what is visible to a passive device on the network?</u>

- Firefox
  - Source/Destination IP
  - Source/Destination ports
  - Unencrypted Payload data (for HTTP)
  - Packet protocol / type
- VPN
  - VPN Server
  - Encrypted Payload Data
- Tor
  - Encrypted Source/Destination
  - Encrypted data

<u>Can you use the connection statistics to determine which of the 10 websites was visited?</u>

Yes, to a certain extent. Each website query has a large variance of packet size and number of packets between each query, even when using the same platform. It would take multiple queries to the same website to determine what website is being visited with confidence. The user querying the same website multiple times in a row is plausible since they may be navigating between pages on the same website.