1 Sending emails and SMTP

1. What filter did you use to catch the traffic and explain why you chose that filter?
Tcp.port == 465: we specified port 465 in the command

2. What is the standard port for SMTP and why do we use port 465 in the example above?
The standard port for SMTP is port 25. We used 465 so we can isolate our activity for observation

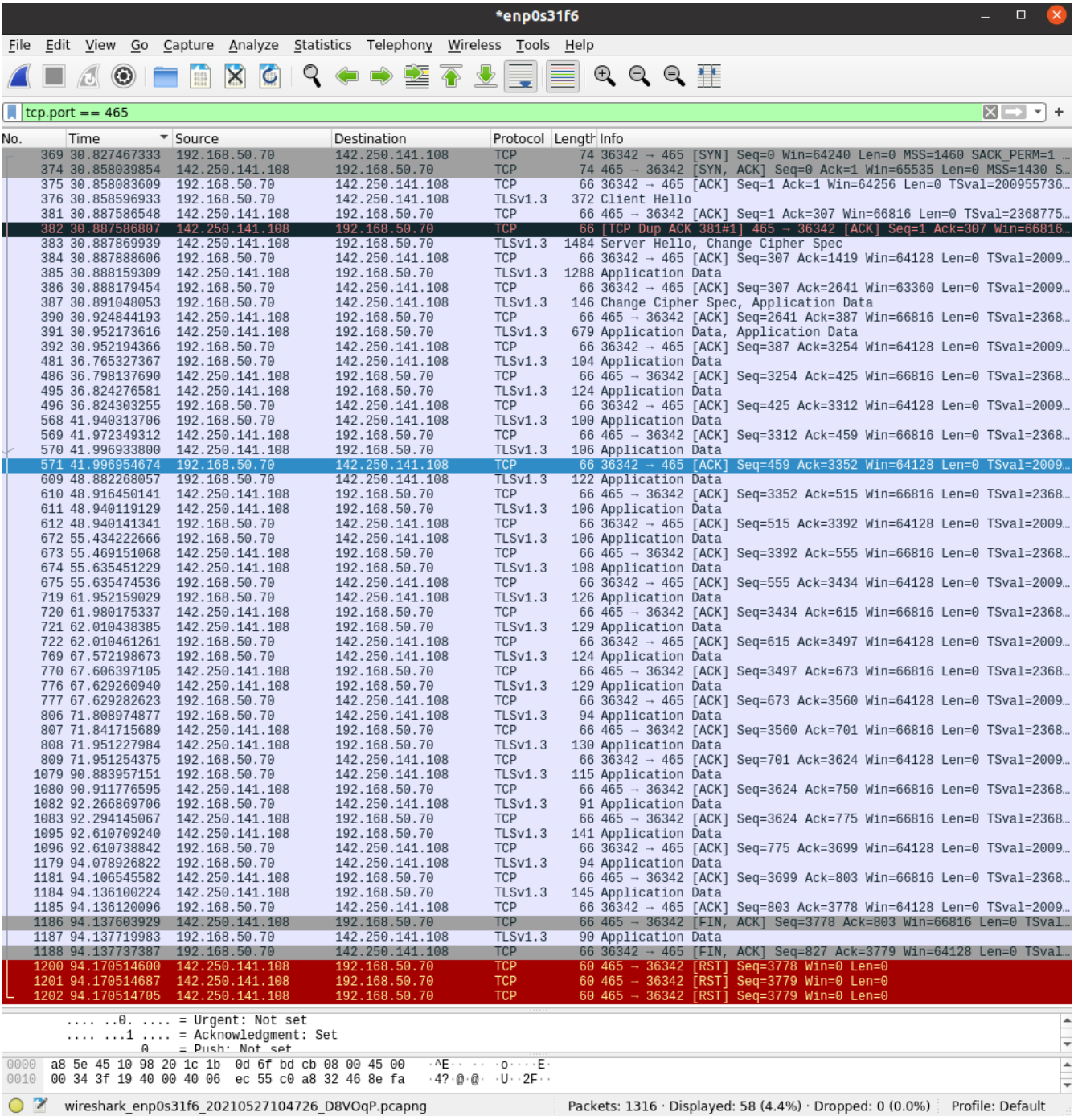
3. Explain each line used in the command line and what it does and why it is needed?
We connect to gmail using SMTP, then “Client hello” then we log into the account. After that we , enter the “from” email followed by the recipient. Then we enter the subject and the email before quitting.

4. How much back and forth communication do you see for establishing the connection?
Establishing a connection sent 8 packets back and forth.

5. What is the port your local machine is using between sending the two emails when communicating with the SMTP server?
Port 465

6. Explain who sends the first FIN flag and how the quitting process works.
The server sends the first FIN flag and the client responds with their own

7. Add a screenshot of your Wireshark output and add it to your document.



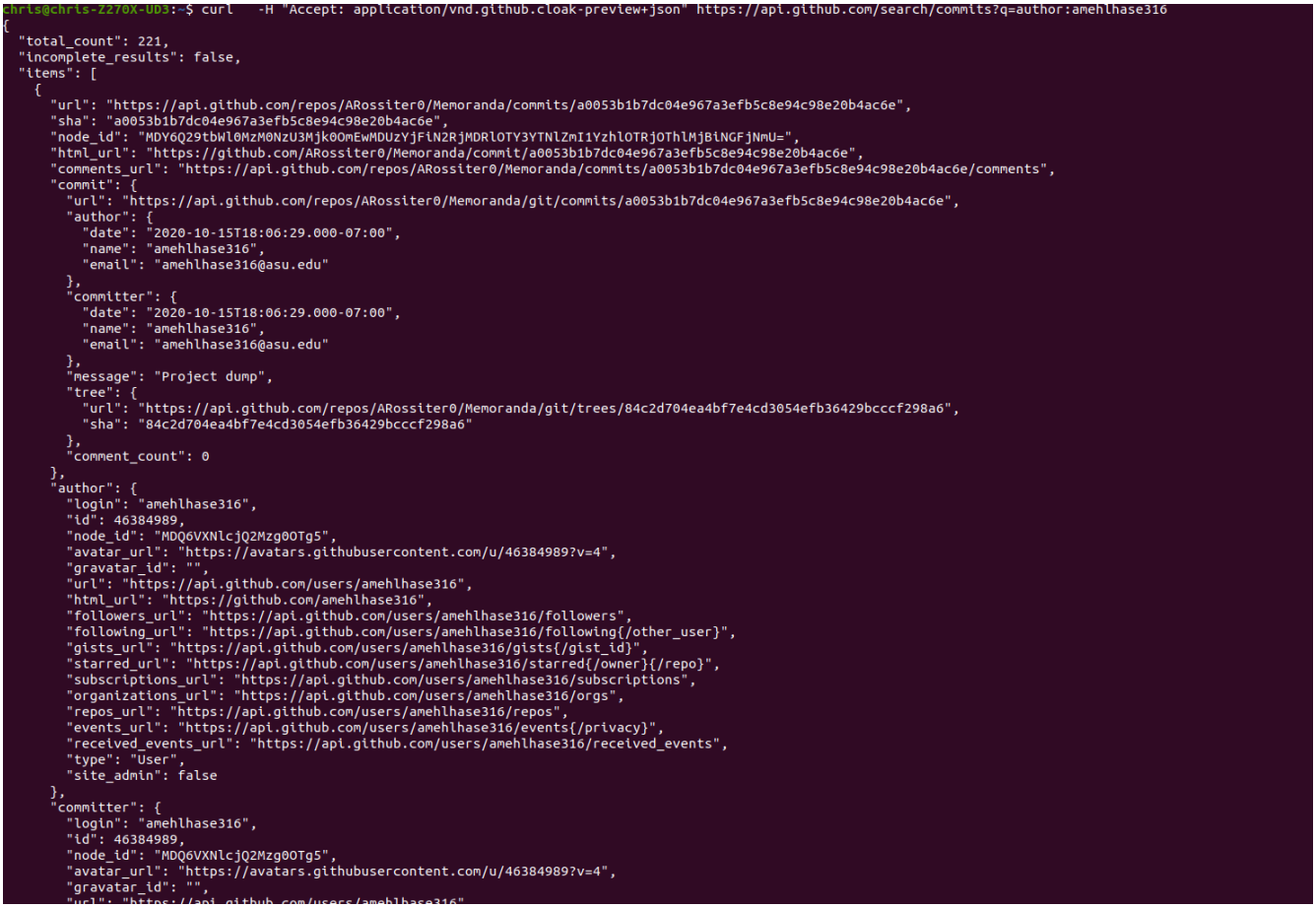
2 Understanding HTTP

1. Explain the specific API calls you used.

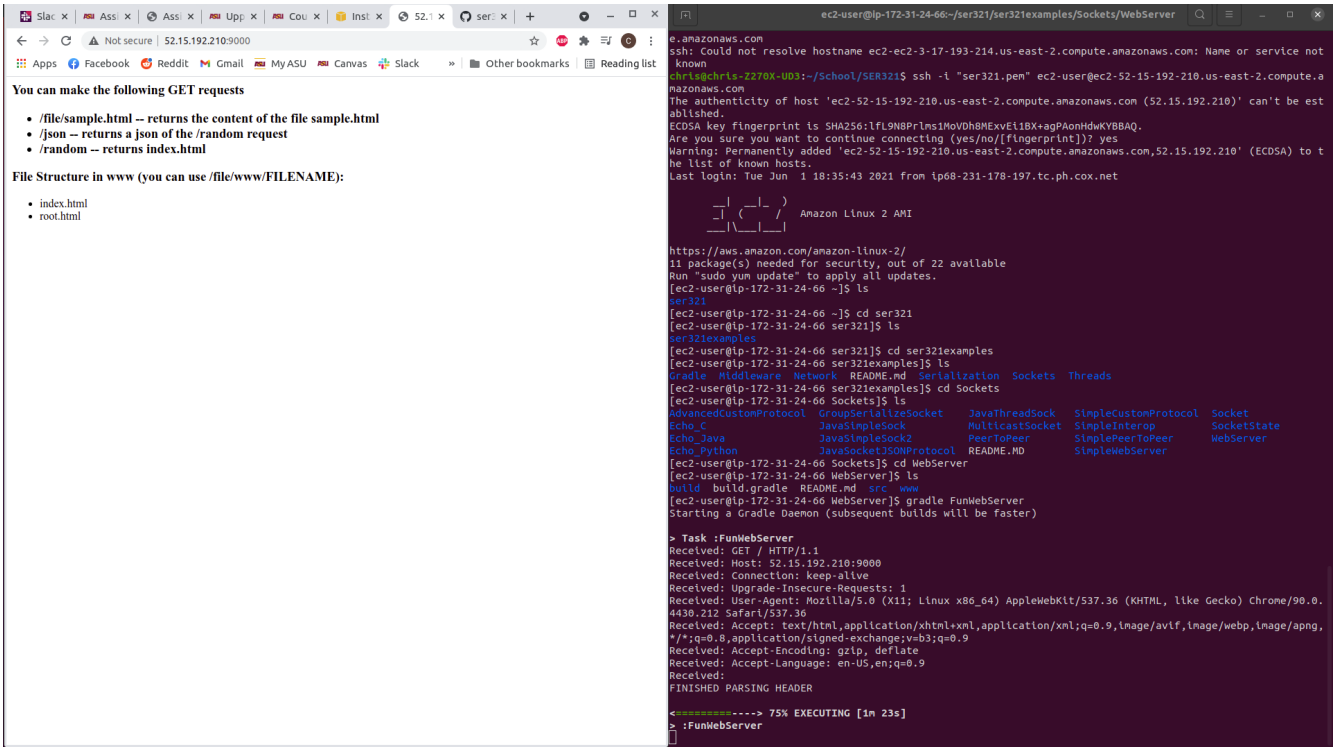
curl -H "Accept: application/vnd.github.cloak-preview+json" https://api.github.com/search/commits?q=author:amehlhase316

2. Explain the difference between stateless and a state-full communication.

In stateless communication, the client sends a request to the server and the server replies back depending on the state. In state-full communication the client sends a request to the server and if the server does not respond, the client continues to resend the request.



3 Setup your second system and run Server on it



1. What filter did you use? Explain why you chose that filter.

ip.addr == 52.15.192.210 && http

2. What happens when you are on /random and click the refresh button compared to the browser refresh (you can also use the command line output that the WebServer generates to answer this)?

Hitting refresh in the browser produces 2 GET requests
Hitting random button produces 1 get request

3. What kinds of response codes are you able to get through different requests to your server?
200 OK
400 Bad requests
404 Not Found

4. Explain the response codes you get and why you get them?
200: When there were no issues the code was OK.
400: Entering wrong URL
404: Trying to access something that does not exists on the site

5. When you do a ipOfSecondMachine:9000 take a look what Wireshark generates as a server response. Are you able to find the data that the server sends back to you?
Yes, we can see everything in plain text

6. Based on the above question explain why HTTPs is now more common than HTTP.

HTTPs encrypts what is sent and received so it is much more difficult to see what is being sent.

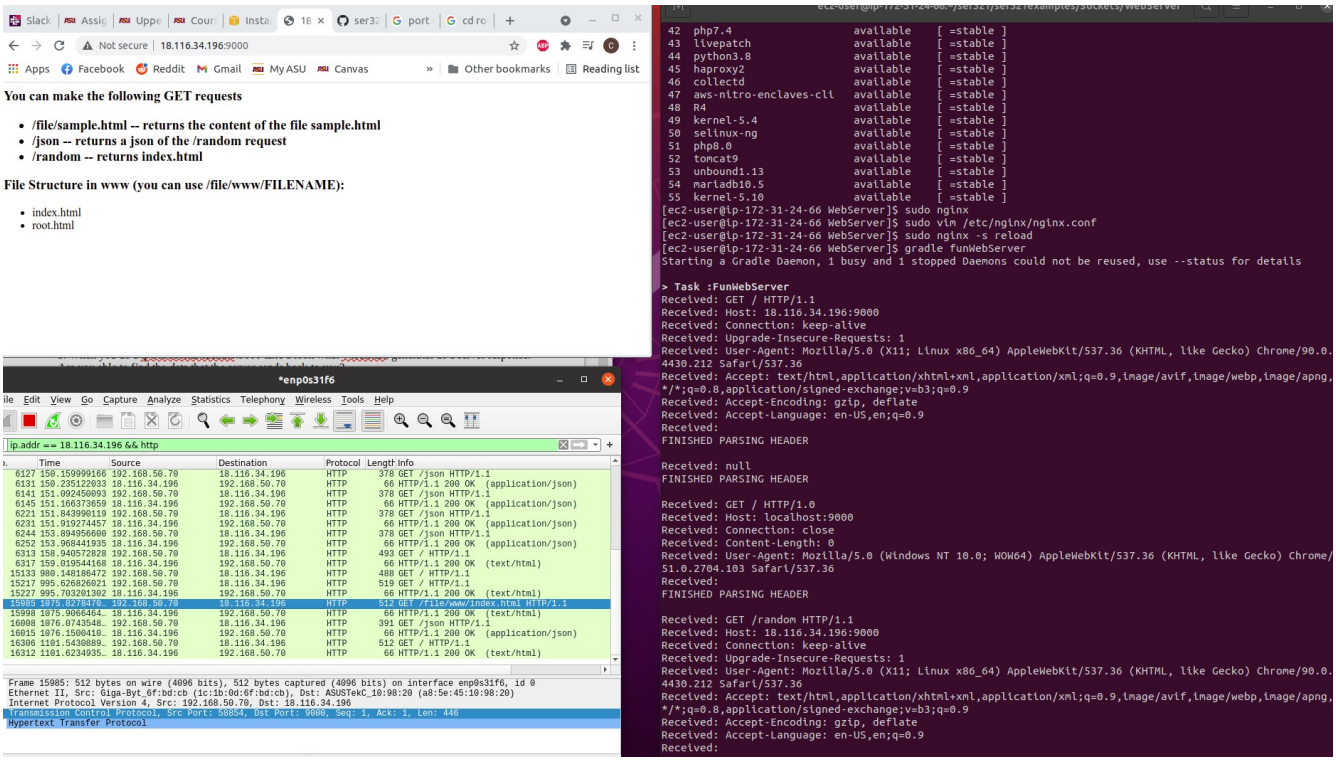
7. What port does the server listen to for HTTP requests in our case and is that the most common port for HTTP?
22

8. What local port is used when sending different requests to the WebServer? How does it differ to the traffic to your SMTP server from part 1?
TCP: 37934
HTTP: 42266

3.4 Setting up a "real" Web server

1. Check your traffic to your Webserver now. What port is the traffic going to now? Is it the same as previously used or is it and should it be different?
The ports are the same as before.

2. Is it still HTTP or is it now HTTPs? Why?
It is still HTTP. I did not set up HTTPs



3.6.1 Multiply
If there is one input, the result is multiplied by one. If there are two inputs, the result is the product of the two inputs. If there are more than two inputs, A message is shown to the client explaining that there was more than two inputs received.