Angel Ortiz

1. Start Wireshark and Set Filters

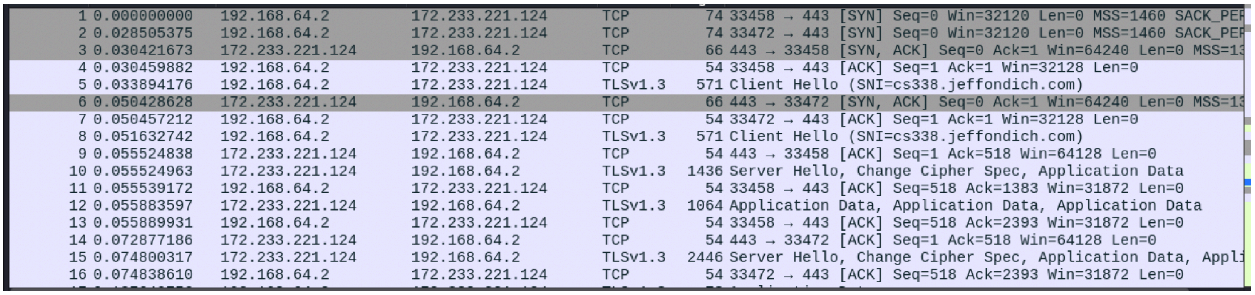
We start by opening Wireshark and we set the capture filter to tcp port 80 and with this we start capturing packets.

2. Initial Website Access With No Authentication

When first accessing the webpage, we open an incognito window in our web browser. Then we navigate to http://cs338.jeffondich.com/basicauth/ without putting in the username of the password. Finally, we observe the initial TCP connection between the browser and the server in Wireshark.

3. TCP Handshake (Three Way Handshake)

The connection starts with us the client (our browser), sending a TCP SYN packet to the server to try and initiate a connection. The server then responds by sending a SYN-ACK packet back to us, accepting the client's request. Finally we the client send back an ACK packet, satisfying the handshake and finally setting up the TCP connection.



```
 1 0.000000000   192.168.64.2       172.233.221.124    TCP        74 33458 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PER
 2 0.028505375   192.168.64.2       172.233.221.124    TCP        74 33472 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PER
 3 0.030421673   172.233.221.124    192.168.64.2       TCP        66 443 → 33458 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=13
 4 0.030459882   192.168.64.2       172.233.221.124    TCP        54 33458 → 443 [ACK] Seq=1 Ack=1 Win=32128 Len=0
 5 0.033894176   192.168.64.2       172.233.221.124    TLSv1.3   571 Client Hello (SNI=cs338.jeffondich.com)
 6 0.050428628   172.233.221.124    192.168.64.2       TCP        66 443 → 33472 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=13
 7 0.050457212   192.168.64.2       172.233.221.124    TCP        54 33472 → 443 [ACK] Seq=1 Ack=1 Win=32128 Len=0
 8 0.051632742   192.168.64.2       172.233.221.124    TLSv1.3   571 Client Hello (SNI=cs338.jeffondich.com)
 9 0.055524838   172.233.221.124    192.168.64.2       TCP        54 443 → 33458 [ACK] Seq=1 Ack=518 Win=64128 Len=0
10 0.055524963   172.233.221.124    192.168.64.2       TLSv1.3  1436 Server Hello, Change Cipher Spec, Application Data
11 0.055539172   192.168.64.2       172.233.221.124    TCP        54 33458 → 443 [ACK] Seq=518 Ack=1383 Win=31872 Len=0
12 0.055883597   172.233.221.124    192.168.64.2       TLSv1.3  1064 Application Data, Application Data, Application Data
13 0.055889931   192.168.64.2       172.233.221.124    TCP        54 33458 → 443 [ACK] Seq=518 Ack=2393 Win=31872 Len=0
14 0.072877186   172.233.221.124    192.168.64.2       TCP        54 443 → 33472 [ACK] Seq=1 Ack=518 Win=64128 Len=0
15 0.074800317   172.233.221.124    192.168.64.2       TLSv1.3  2446 Server Hello, Change Cipher Spec, Application Data, Appli
16 0.074838610   192.168.64.2       172.233.221.124    TCP        54 33472 → 443 [ACK] Seq=518 Ack=2393 Win=31872 Len=0
```

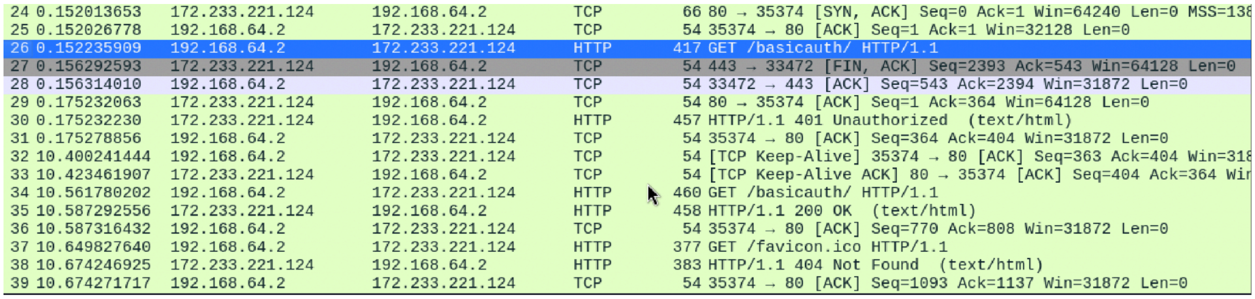
Packet 1 (SYN): The client at IP 192.168.64.2 sends a TCP SYN packet to 172.233.221.124, beginning the connection.

Packet 3 (SYN-ACK): The server at IP 172.233.221.124 responds with a SYN-ACK packet, recognizing the client's request.

Packet 5 (ACK): The client sends an ACK packet back to the server, finishing the handshake.

4. 401 Unauthorized Response

After the handshake is complete we the client send an HTTP GET /basicauth/ request for the website which is protected by a username and password. However since we have not yet inputted the username and password, we cannot access the page and the server responds 'HTTP 401 Unauthorized' status and on the website gives us the place to input our username and password.



```
24 0.152013653   172.233.221.124   192.168.64.2      TCP      66 80 → 35374 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=138
25 0.152026778   192.168.64.2      172.233.221.124   TCP      54 35374 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0
26 0.152235909   192.168.64.2      172.233.221.124   HTTP    417 GET /basicauth/ HTTP/1.1
27 0.156292593   172.233.221.124   192.168.64.2      TCP      54 443 → 33472 [FIN, ACK] Seq=2393 Ack=543 Win=64128 Len=0
28 0.156314010   192.168.64.2      172.233.221.124   TCP      54 33472 → 443 [ACK] Seq=543 Ack=2394 Win=31872 Len=0
29 0.175232063   172.233.221.124   192.168.64.2      TCP      54 80 → 35374 [ACK] Seq=1 Ack=364 Win=64128 Len=0
30 0.175232230   172.233.221.124   192.168.64.2      HTTP    457 HTTP/1.1 401 Unauthorized  (text/html)
31 0.175278856   192.168.64.2      172.233.221.124   TCP      54 35374 → 80 [ACK] Seq=364 Ack=404 Win=31872 Len=0
32 10.400241444  192.168.64.2      172.233.221.124   TCP      54 [TCP Keep-Alive] 35374 → 80 [ACK] Seq=363 Ack=404 Win=318
33 10.423461907  172.233.221.124   192.168.64.2      TCP      54 [TCP Keep-Alive ACK] 80 → 35374 [ACK] Seq=404 Ack=364 Wir
34 10.561780202  192.168.64.2      172.233.221.124   HTTP    460 GET /basicauth/ HTTP/1.1
35 10.587292556  172.233.221.124   192.168.64.2      HTTP    458 HTTP/1.1 200 OK  (text/html)
36 10.587316432  192.168.64.2      172.233.221.124   TCP      54 35374 → 80 [ACK] Seq=770 Ack=808 Win=31872 Len=0
37 10.649827640  192.168.64.2      172.233.221.124   HTTP    377 GET /favicon.ico HTTP/1.1
38 10.674246925  172.233.221.124   192.168.64.2      HTTP    383 HTTP/1.1 404 Not Found  (text/html)
39 10.674271717  192.168.64.2      172.233.221.124   TCP      54 35374 → 80 [ACK] Seq=1093 Ack=1137 Win=31872 Len=0
```

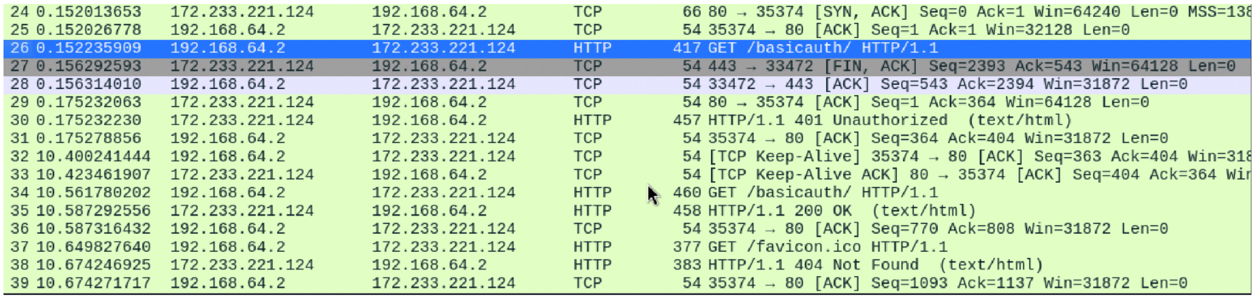
Packet 26: Here the initial request is made by the client before authentication with HTTP GET request where the client 192.168.64.2 sends a request to the server 172.233.221.124 to try and access /basicauth/ using HTTP 1.1.

Packet 29: However with no username or password inputted yet, the server responds with HTTP 401 Unauthorized because the server denied access to /basicauth/.

5. Username and Password and Analyzing them

Now we the user are told to input the username 'cs338' and password 'password in the browser.

Packet 34: The user gives their username and password, and the client sends the HTTP GET request with the Authorization header which holds the the Base64-encoded credentials and in this same packet is analyzes the Base64-encoded information which can be which is decoded into what we typed in.

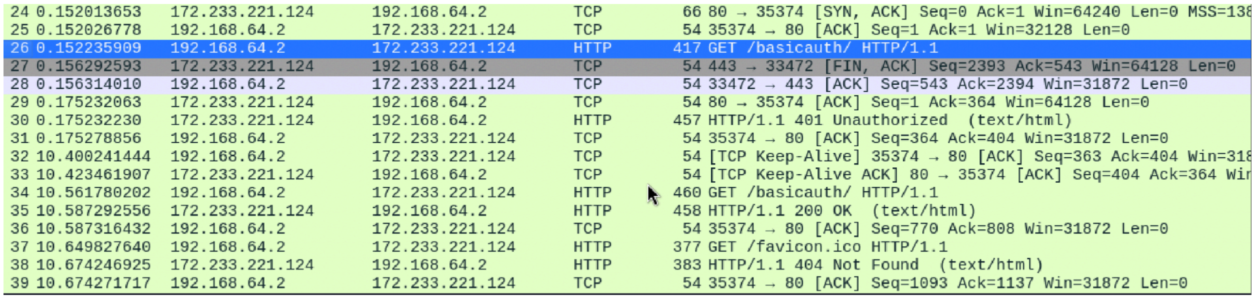


```
24 0.152013653   172.233.221.124   192.168.64.2      TCP        66 80 → 35374 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=138
25 0.152026778   192.168.64.2      172.233.221.124   TCP        54 35374 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0
26 0.152235909   192.168.64.2      172.233.221.124   HTTP      417 GET /basicauth/ HTTP/1.1
27 0.156292593   172.233.221.124   192.168.64.2      TCP        54 443 → 33472 [FIN, ACK] Seq=2393 Ack=543 Win=64128 Len=0
28 0.156314010   192.168.64.2      172.233.221.124   TCP        54 33472 → 443 [ACK] Seq=543 Ack=2394 Win=31872 Len=0
29 0.175232063   172.233.221.124   192.168.64.2      TCP        54 80 → 35374 [ACK] Seq=1 Ack=364 Win=64128 Len=0
30 0.175232230   172.233.221.124   192.168.64.2      HTTP      457 HTTP/1.1 401 Unauthorized  (text/html)
31 0.175278856   192.168.64.2      172.233.221.124   TCP        54 35374 → 80 [ACK] Seq=364 Ack=404 Win=31872 Len=0
32 10.400241444  192.168.64.2      172.233.221.124   TCP        54 [TCP Keep-Alive] 35374 → 80 [ACK] Seq=363 Ack=404 Win=318
33 10.423461907  172.233.221.124   192.168.64.2      TCP        54 [TCP Keep-Alive ACK] 80 → 35374 [ACK] Seq=404 Ack=364 Wir
34 10.561780202  192.168.64.2      172.233.221.124   HTTP      460 GET /basicauth/ HTTP/1.1
35 10.587292556  172.233.221.124   192.168.64.2      HTTP      458 HTTP/1.1 200 OK  (text/html)
36 10.587316432  192.168.64.2      172.233.221.124   TCP        54 35374 → 80 [ACK] Seq=770 Ack=808 Win=31872 Len=0
37 10.649827640  192.168.64.2      172.233.221.124   HTTP      377 GET /favicon.ico HTTP/1.1
38 10.674246925  172.233.221.124   192.168.64.2      HTTP      383 HTTP/1.1 404 Not Found  (text/html)
39 10.674271717  192.168.64.2      172.233.221.124   TCP        54 35374 → 80 [ACK] Seq=1093 Ack=1137 Win=31872 Len=0
```

6. Successful Server Response

After the user inputs the correct username and password and the server receives them, the server sends an HTTP 200 OK response and gives the user access to /basicauth/.

Packet 35: 'HTTP 200 OK' confirms that the authentication process was successful and the user now has access to /basicauth/.



```
24 0.152013653   172.233.221.124   192.168.64.2      TCP        66 80 → 35374 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=138
25 0.152026778   192.168.64.2      172.233.221.124   TCP        54 35374 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0
26 0.152235909   192.168.64.2      172.233.221.124   HTTP      417 GET /basicauth/ HTTP/1.1
27 0.156292593   172.233.221.124   192.168.64.2      TCP        54 443 → 33472 [FIN, ACK] Seq=2393 Ack=543 Win=64128 Len=0
28 0.156314010   192.168.64.2      172.233.221.124   TCP        54 33472 → 443 [ACK] Seq=543 Ack=2394 Win=31872 Len=0
29 0.175232063   172.233.221.124   192.168.64.2      TCP        54 80 → 35374 [ACK] Seq=1 Ack=364 Win=64128 Len=0
30 0.175232230   172.233.221.124   192.168.64.2      HTTP      457 HTTP/1.1 401 Unauthorized  (text/html)
31 0.175278856   192.168.64.2      172.233.221.124   TCP        54 35374 → 80 [ACK] Seq=364 Ack=404 Win=31872 Len=0
32 10.400241444  192.168.64.2      172.233.221.124   TCP        54 [TCP Keep-Alive] 35374 → 80 [ACK] Seq=363 Ack=404 Win=318
33 10.423461907  172.233.221.124   192.168.64.2      TCP        54 [TCP Keep-Alive ACK] 80 → 35374 [ACK] Seq=404 Ack=364 Wir
34 10.561780202  192.168.64.2      172.233.221.124   HTTP      460 GET /basicauth/ HTTP/1.1
35 10.587292556  172.233.221.124   192.168.64.2      HTTP      458 HTTP/1.1 200 OK  (text/html)
36 10.587316432  192.168.64.2      172.233.221.124   TCP        54 35374 → 80 [ACK] Seq=770 Ack=808 Win=31872 Len=0
37 10.649827640  192.168.64.2      172.233.221.124   HTTP      377 GET /favicon.ico HTTP/1.1
38 10.674246925  172.233.221.124   192.168.64.2      HTTP      383 HTTP/1.1 404 Not Found  (text/html)
39 10.674271717  192.168.64.2      172.233.221.124   TCP        54 35374 → 80 [ACK] Seq=1093 Ack=1137 Win=31872 Len=0
```