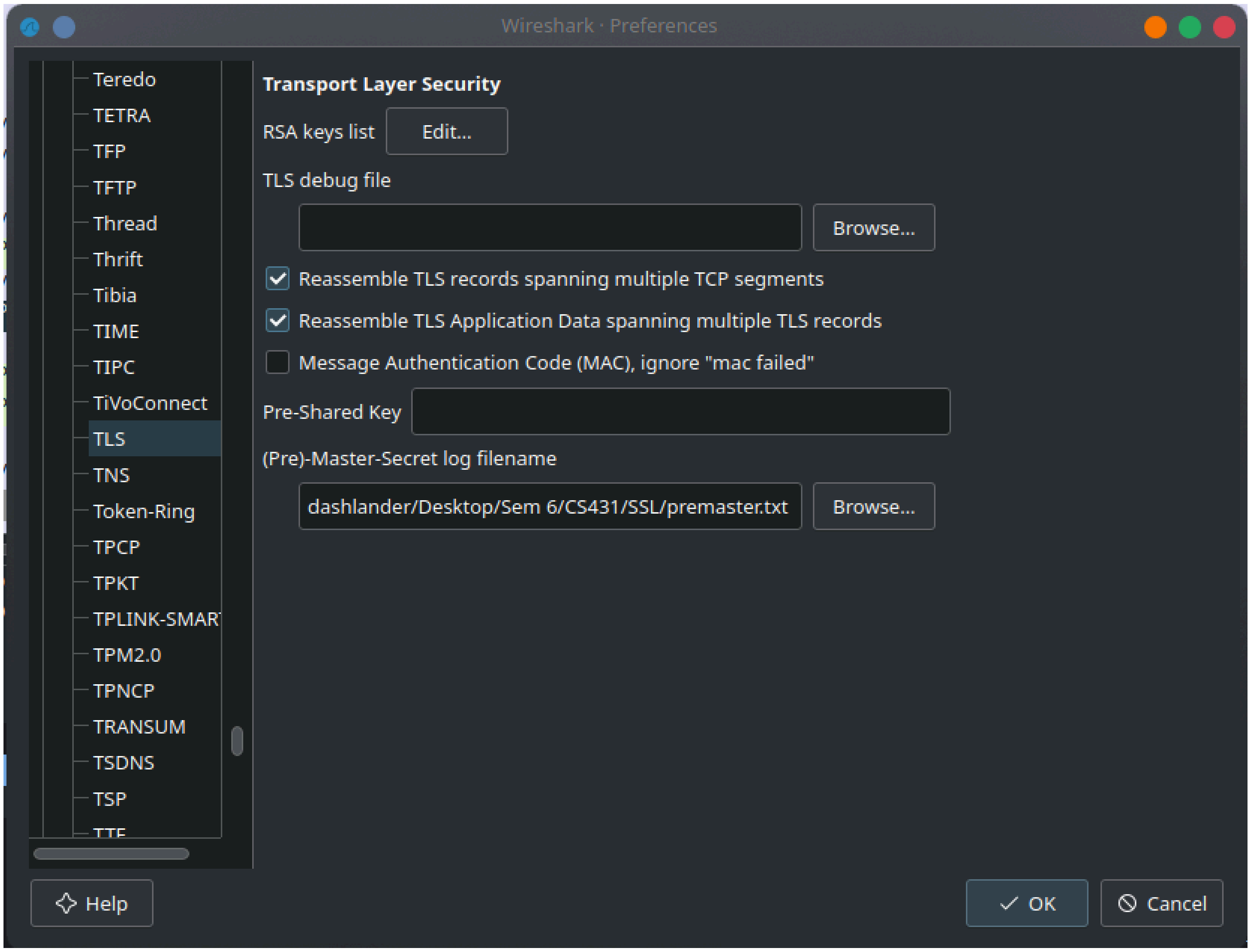
Question 1

The pcapng file is a capture of the encrypted HTTPS traffic between client and server.

Wireshark is used to decrypt the encryption and obtain the HTTPS Flag: The 14741 HTTPS flag is f09ab0834bfa0238cd4b54aa

Steps:

1. Installing Wireshark : yay -S wireshark-qt
2. Opening the pcapng file in Wireshark. However, that is still encrypted traffic.
3. Edit > Preferences > Protocols > TLS > Pre - Master - Secret Log File name: setting that to the premaster.txt.



Transport Layer Security

RSA keys list Edit...

TLS debug file

☑ Reassemble TLS records spanning multiple TCP segments

☑ Reassemble TLS Application Data spanning multiple TLS records

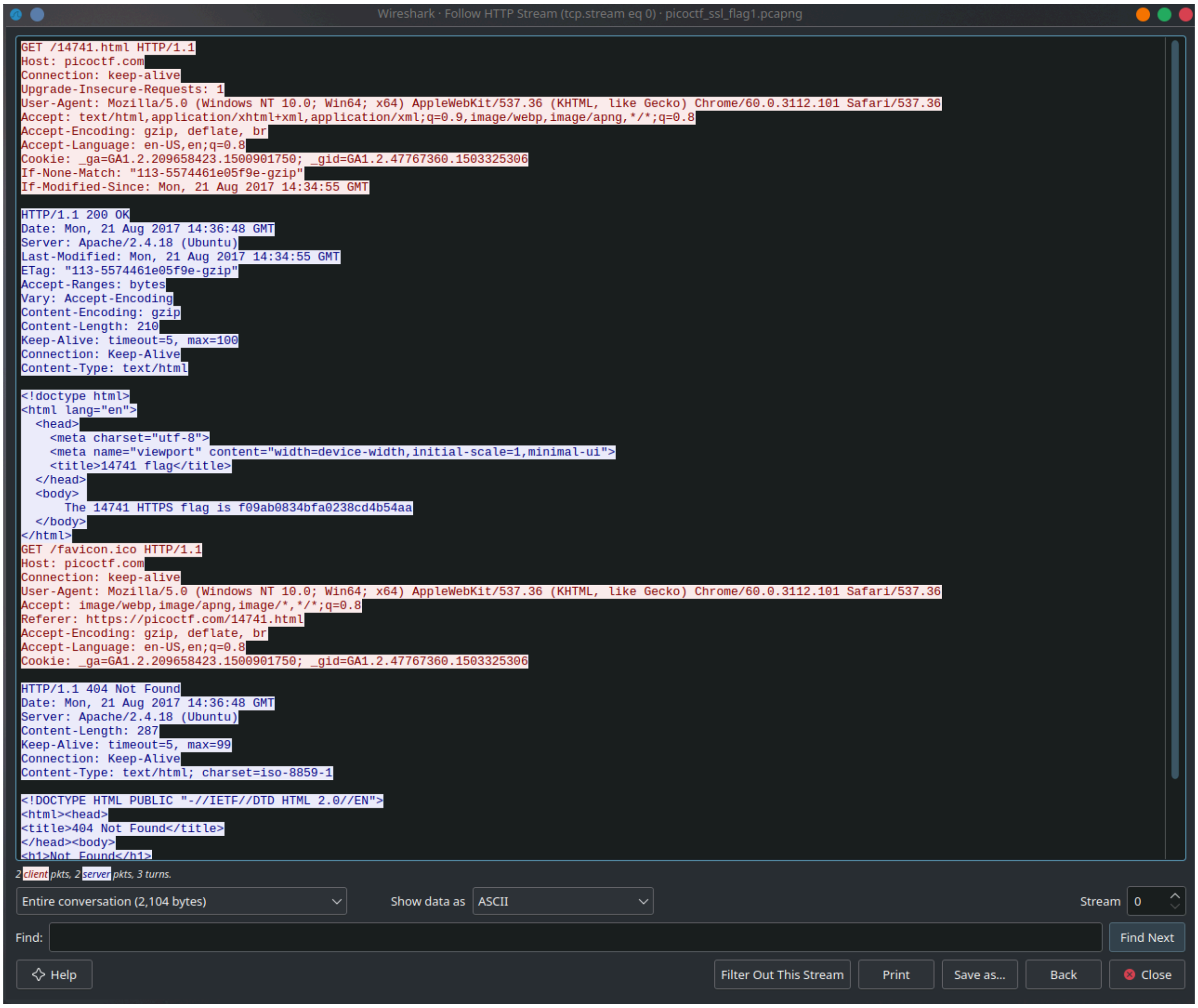
□ Message Authentication Code (MAC), ignore "mac failed"

Pre-Shared Key

(Pre)-Master-Secret log filename

dashlander/Desktop/Sem 6/CS431/SSL/premaster.txt

4. The Traffic is now decrypted. Clicking on an HTTP packet, and then choosing follow and then HTTP Stream will show the window for the following:



Wireshark · Follow HTTP Stream (tcp.stream eq 0) · picoctf_ssl_flag1.pcapng
2 client pkts, 2 server pkts, 3 turns.
Entire conversation (2,104 bytes)
Show data as
ASCII
Stream
0
Find:
Find Next
Help
Filter Out This Stream
Print
Save as…
Back
Close

```
GET /14741.html HTTP/1.1
Host: picoctf.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.8
Cookie: _ga=GA1.2.209658423.1500901750; _gid=GA1.2.47767360.1503325306
If-None-Match: "113-5574461e05f9e-gzip"
If-Modified-Since: Mon, 21 Aug 2017 14:34:55 GMT

HTTP/1.1 200 OK
Date: Mon, 21 Aug 2017 14:36:48 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Mon, 21 Aug 2017 14:34:55 GMT
ETag: "113-5574461e05f9e-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 210
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width,initial-scale=1,minimal-ui">
    <title>14741 flag</title>
  </head>
  <body>
      The 14741 HTTPS flag is f09ab0834bfa0238cd4b54aa
  </body>
</html>
GET /favicon.ico HTTP/1.1
Host: picoctf.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: https://picoctf.com/14741.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.8
Cookie: _ga=GA1.2.209658423.1500901750; _gid=GA1.2.47767360.1503325306

HTTP/1.1 404 Not Found
Date: Mon, 21 Aug 2017 14:36:48 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 287
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
```

The HTTPS flag is given body tags in the HTML Doctype section.

Question 2

The Environment Variable SSLKEYLOGFILE is set in Windows using advanced system settings, and then environment variables and then adding SSLKEYLOGFILE to the Variable and adding a path for the same. It is a Windows client as can be seen from the user agent.

Question 3

The HTTPS traffic file is only decrypted after setting the pre master secret log file. In the absence of this file, wireshark shows no HTTP traffic for the same pcapng file, and is only shown as application data, which is encrypted. Web Browsing with HTTPS is still secure due to the fact that without the keys required for decryption, the contents of the network data is unreadable.