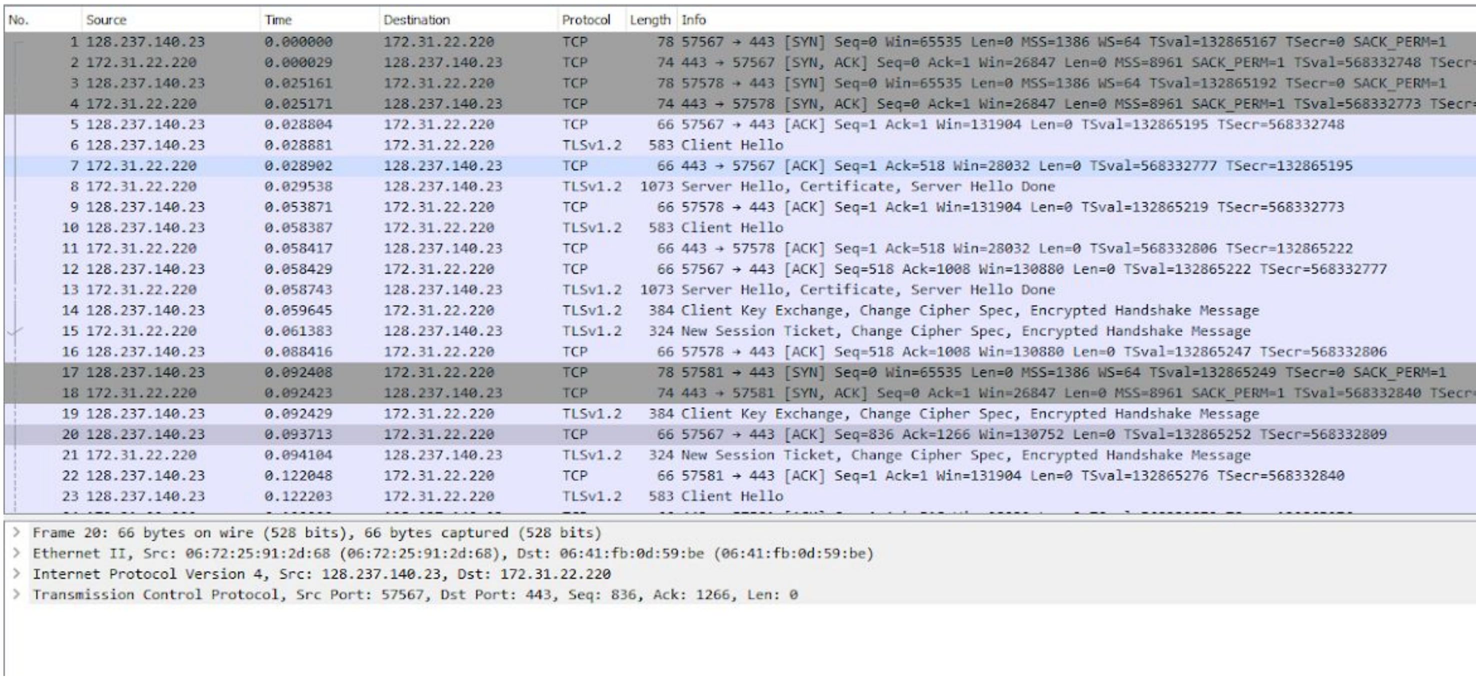
picoCTF WebNet0

Points: 350.

Description: We found this packet capture and key. Recover the flag.
Link: https://play.picoctf.org/practice/challenge/32?category=4&page=2

When opening the file in Wireshark I saw the Protocol "TLSv1.2" since the challenge provided a key I am assuming I have to decrypt the TLS stream.



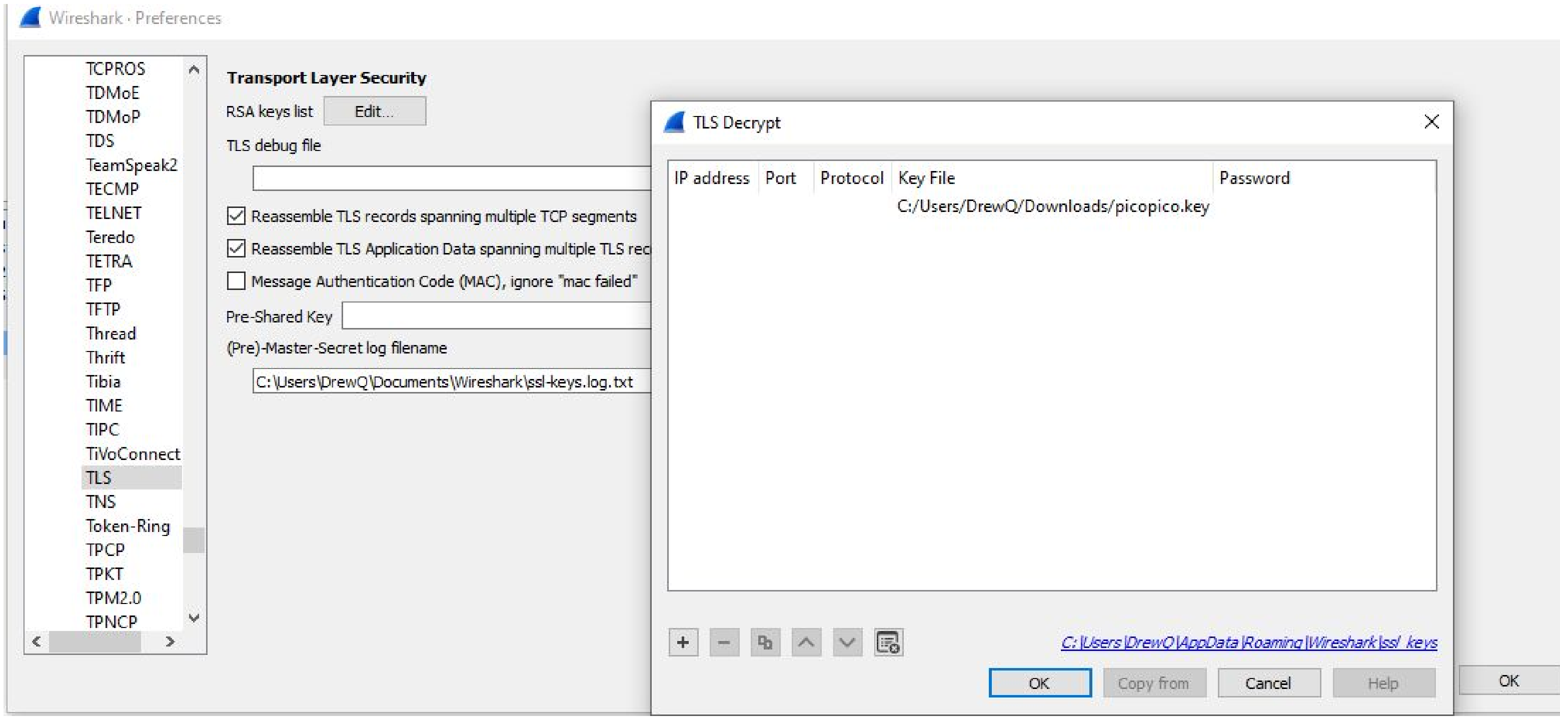
No.	Source	Time	Destination	Protocol	Length	Info
1	128.237.140.23	0.000000	172.31.22.220	TCP	78	57567 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1386 WS=64 TSval=132865167 TSecr=0 SACK_PERM=1
2	172.31.22.220	0.000029	128.237.140.23	TCP	74	443 → 57567 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=8961 SACK_PERM=1 TSval=568332748 TSecr
3	128.237.140.23	0.025161	172.31.22.220	TCP	78	57578 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1386 WS=64 TSval=132865192 TSecr=0 SACK_PERM=1
4	172.31.22.220	0.025171	128.237.140.23	TCP	74	443 → 57578 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=8961 SACK_PERM=1 TSval=568332773 TSecr
5	128.237.140.23	0.028804	172.31.22.220	TCP	66	57567 → 443 [ACK] Seq=1 Ack=1 Win=131904 Len=0 TSval=132865195 TSecr=568332748
6	128.237.140.23	0.028881	172.31.22.220	TLSv1.2	583	Client Hello
7	172.31.22.220	0.028902	128.237.140.23	TCP	66	443 → 57567 [ACK] Seq=1 Ack=518 Win=28032 Len=0 TSval=568332777 TSecr=132865195
8	172.31.22.220	0.029538	128.237.140.23	TLSv1.2	1073	Server Hello, Certificate, Server Hello Done
9	128.237.140.23	0.053871	172.31.22.220	TCP	66	57578 → 443 [ACK] Seq=1 Ack=1 Win=131904 Len=0 TSval=132865219 TSecr=568332773
10	128.237.140.23	0.058387	172.31.22.220	TLSv1.2	583	Client Hello
11	172.31.22.220	0.058417	128.237.140.23	TCP	66	443 → 57578 [ACK] Seq=1 Ack=518 Win=28032 Len=0 TSval=568332806 TSecr=132865222
12	128.237.140.23	0.058429	172.31.22.220	TCP	66	57567 → 443 [ACK] Seq=518 Ack=1008 Win=130880 Len=0 TSval=132865222 TSecr=568332777
13	172.31.22.220	0.058743	128.237.140.23	TLSv1.2	1073	Server Hello, Certificate, Server Hello Done
14	128.237.140.23	0.059645	172.31.22.220	TLSv1.2	384	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
15	172.31.22.220	0.061383	128.237.140.23	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
16	128.237.140.23	0.088416	172.31.22.220	TCP	66	57578 → 443 [ACK] Seq=518 Ack=1008 Win=130880 Len=0 TSval=132865247 TSecr=568332806
17	128.237.140.23	0.092408	172.31.22.220	TCP	78	57581 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1386 WS=64 TSval=132865249 TSecr=0 SACK_PERM=1
18	172.31.22.220	0.092423	128.237.140.23	TCP	74	443 → 57581 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=8961 SACK_PERM=1 TSval=568332840 TSecr
19	128.237.140.23	0.092429	172.31.22.220	TLSv1.2	384	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
20	128.237.140.23	0.093713	172.31.22.220	TCP	66	57567 → 443 [ACK] Seq=836 Ack=1266 Win=130752 Len=0 TSval=132865252 TSecr=568332809
21	172.31.22.220	0.094104	128.237.140.23	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
22	128.237.140.23	0.122048	172.31.22.220	TCP	66	57581 → 443 [ACK] Seq=1 Ack=1 Win=131904 Len=0 TSval=132865276 TSecr=568332840
23	128.237.140.23	0.122203	172.31.22.220	TLSv1.2	583	Client Hello

```
> Frame 20: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: 06:72:25:91:2d:68 (06:72:25:91:2d:68), Dst: 06:41:fb:0d:59:be (06:41:fb:0d:59:be)
> Internet Protocol Version 4, Src: 128.237.140.23, Dst: 172.31.22.220
> Transmission Control Protocol, Src Port: 57567, Dst Port: 443, Seq: 836, Ack: 1266, Len: 0
```

I followed the Wireshark wiki page to decrypt the data (https://wiki.wireshark.org/TLS).

"Go to *Edit -> Preferences*. Open the *Protocols* tree and select *TLS*."

I added the key the challenge provided to the RSA key list.



Transport Layer Security

RSA keys list

TLS debug file

☑ Reassemble TLS records spanning multiple TCP segments

☑ Reassemble TLS Application Data spanning multiple TLS rec

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

Pre-Shared Key

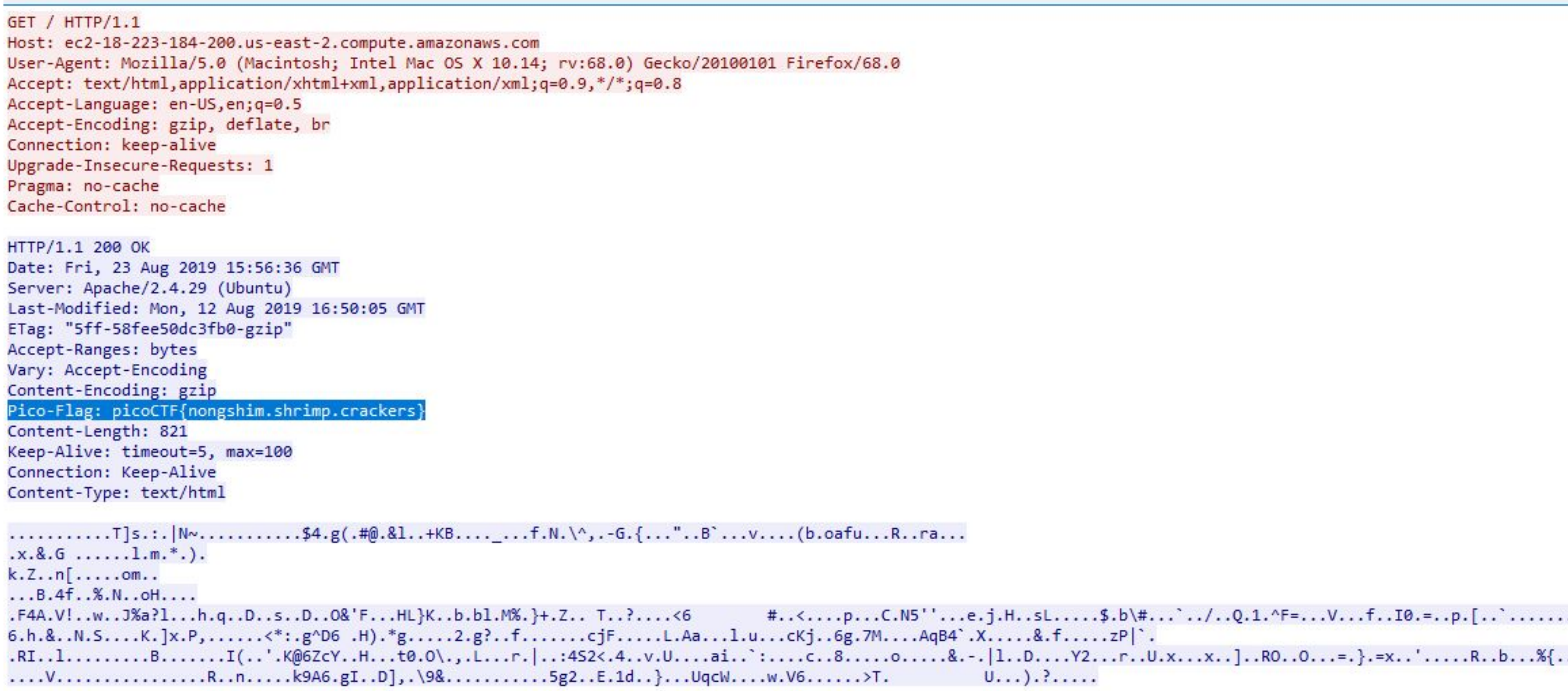
(Pre)-Master-Secret log filename

C:\Users\DrewQ\Documents\Wireshark\ssl-keys.log.txt

IP address	Port	Protocol	Key File	Password
			C:/Users/DrewQ/Downloads/picopico.key	

C:\Users\DrewQ\AppData\Roaming\Wireshark\ssl_keys

Then I filtered the Wireshark traffic for just TLS and checked the data.



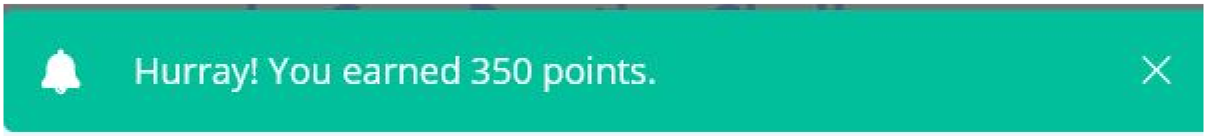
```
GET / HTTP/1.1
Host: ec2-18-223-184-200.us-east-2.compute.amazonaws.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Fri, 23 Aug 2019 15:56:36 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Mon, 12 Aug 2019 16:50:05 GMT
ETag: "5ff-58fee50dc3fb0-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Pico-Flag: picoCTF{nongshim.shrimp.crackers}
Content-Length: 821
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

..........T]s.:.|N~..........$4.g(.#@.&l..+KB...._...f.N.\^,.-G.{..."..B`...v....(b.oafu...R..ra...
.x.&.G ......l.m.*.).
k.Z..n[.....om..
...B.4f..%.N..oH....
.F4A.V!..w..J%a?l...h.q..D..s..D..O&'F...HL}K..b.bl.M%.}+.Z.. T..?....<6        #..<....p...C.N5''...e.j.H..sL.....$.b\#...`../..Q.1.^F=...V...f..I0.=..p.[..`......
6.h.&..N.S....K.]x.P,......<*:.g^D6 .H).*g.....2.g?..f.......cjF.....L.Aa...l.u...cKj..6g.7M....AqB4`.X.....&.f.....zP|`.
.RI..l........B.......I(..'.K@6ZcY..H...t0.O\.,.L...r.|..:4S2<.4..v.U....ai..`:....c..8.....o.....&.-.|l..D....Y2...r..U.x...x..]..RO..O...=.}.=x..'.....R..b...%{.
....V...............R..n.....k9A6.gI..D],.\9&..........5g2..E.1d..}...UqcW....w.V6......>T.          U...).?.....
```

This looks like a web request. In the plaintext it states: Pico-Flag: picoCTF{nongshim.shrimp.crackers}

I then submitted the flag I found in the TLS stream and it was correct!



Hurray! You earned 350 points.