

## picoCTF WebNet1

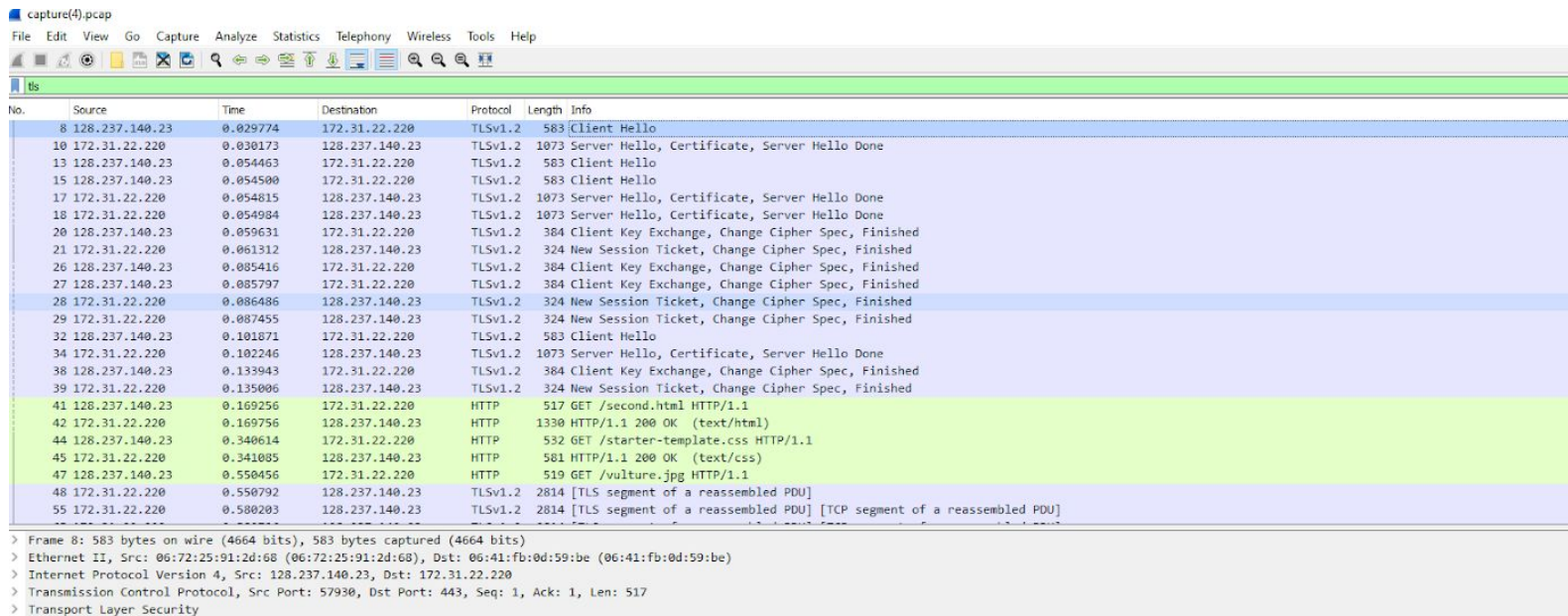
Points: 450.

Description: We found this [packet capture](#) and [key](#). Recover the flag.

Link: <https://play.picoctf.org/practice/challenge/42?category=4&page=2>

Looks like it wants us to decrypt another TLS stream

*edit->Preferences->Protocols->TLS->RSA Keys*



The image shows a Wireshark packet capture of a network session. The top pane shows the packet list with 55 packets. The middle pane shows the packet details for the selected packet (No. 8, a TLSv1.2 Client Hello). The bottom pane shows the packet bytes, which are the raw TLS data. The traffic is between 128.237.140.23 and 172.31.22.220. The TLS stream is from 172.31.22.220 to 128.237.140.23. The HTTP stream is from 128.237.140.23 to 172.31.22.220. The HTTP GET requests are for /second.html, /starter-template.css, and /vulture.jpg. The TLS stream is a Client Hello, followed by several Server Hello, Client Key Exchange, and New Session Ticket messages. The TLS stream is encrypted with RSA.

No.	Source	Time	Destination	Protocol	Length	Info
8	128.237.140.23	0.029774	172.31.22.220	TLSv1.2	583	Client Hello
10	172.31.22.220	0.030173	128.237.140.23	TLSv1.2	1073	Server Hello, Certificate, Server Hello Done
13	128.237.140.23	0.054463	172.31.22.220	TLSv1.2	583	Client Hello
15	128.237.140.23	0.054500	172.31.22.220	TLSv1.2	583	Client Hello
17	172.31.22.220	0.054815	128.237.140.23	TLSv1.2	1073	Server Hello, Certificate, Server Hello Done
18	172.31.22.220	0.054984	128.237.140.23	TLSv1.2	1073	Server Hello, Certificate, Server Hello Done
20	128.237.140.23	0.059631	172.31.22.220	TLSv1.2	384	Client Key Exchange, Change Cipher Spec, Finished
21	172.31.22.220	0.061312	128.237.140.23	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Finished
26	128.237.140.23	0.085416	172.31.22.220	TLSv1.2	384	Client Key Exchange, Change Cipher Spec, Finished
27	128.237.140.23	0.085797	172.31.22.220	TLSv1.2	384	Client Key Exchange, Change Cipher Spec, Finished
28	172.31.22.220	0.086486	128.237.140.23	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Finished
29	172.31.22.220	0.087455	128.237.140.23	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Finished
32	128.237.140.23	0.101871	172.31.22.220	TLSv1.2	583	Client Hello
34	172.31.22.220	0.102246	128.237.140.23	TLSv1.2	1073	Server Hello, Certificate, Server Hello Done
38	128.237.140.23	0.133943	172.31.22.220	TLSv1.2	384	Client Key Exchange, Change Cipher Spec, Finished
39	172.31.22.220	0.135006	128.237.140.23	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Finished
41	128.237.140.23	0.169256	172.31.22.220	HTTP	517	GET /second.html HTTP/1.1
42	172.31.22.220	0.169756	128.237.140.23	HTTP	1330	HTTP/1.1 200 OK (text/html)
44	128.237.140.23	0.340614	172.31.22.220	HTTP	532	GET /starter-template.css HTTP/1.1
45	172.31.22.220	0.341085	128.237.140.23	HTTP	581	HTTP/1.1 200 OK (text/css)
47	128.237.140.23	0.550456	172.31.22.220	HTTP	519	GET /vulture.jpg HTTP/1.1
48	172.31.22.220	0.550792	128.237.140.23	TLSv1.2	2814	[TLS segment of a reassembled PDU]
55	172.31.22.220	0.580203	128.237.140.23	TLSv1.2	2814	[TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]

> Frame 8: 583 bytes on wire (4664 bits), 583 bytes captured (4664 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: 57930, Dst Port: 443, Seq: 1, Ack: 1, Len: 517  
> Transport Layer Security

I am going to follow the TLS stream to inspect the data.

HTTP/1.1 200 OK

Date: Fri, 23 Aug 2019 16:27:04 GMT

Server: Apache/2.4.29 (Ubuntu)

Last-Modified: Fri, 23 Aug 2019 16:26:33 GMT

ETag: "112fb-590cb44f2cbe6"

Accept-Ranges: bytes

Content-Length: 70395

Pico-Flag: **picoCTF{this.is.not.your.flag.anymore}**

Keep-Alive: timeout=5, max=99

Connection: Keep-Alive

Content-Type: image/jpeg

.....JFIF.....Exif..MM.\*.....J.....R.(.....;.....Z.....picoCTF{h  
oney.roasted.peanuts}.....ICC\_PROFILE.....lcms.....mnrRGB XYZ .....

The data provided two flags `picoCTF{this.is.not.your.flag.anymore}` and `picoCTF{honey.roasted.peanuts}`. Trying the first flag the data provided did not work, but the second did work and I received points.

WebNet1 450 