

Contact Us

CSAW 2021 CTF

OreoByte

Contact Us

329

Veronica sent a message to her client via their website's Contact Us page. Can you find the message?

Author: **moat**, Pacific Northwest National Laboratory

[View Hint](#)

[ContactUs.pc...](#)[sslkeyfile.txt](#)

2021-09-10

Contents

Contact Us	3
Using Wireshark Decrypt The SSL Traffic	3
Using Tshark	4
Victory	5

Contact Us

Writeup by: Oreobyte

Team: OnlyFeet

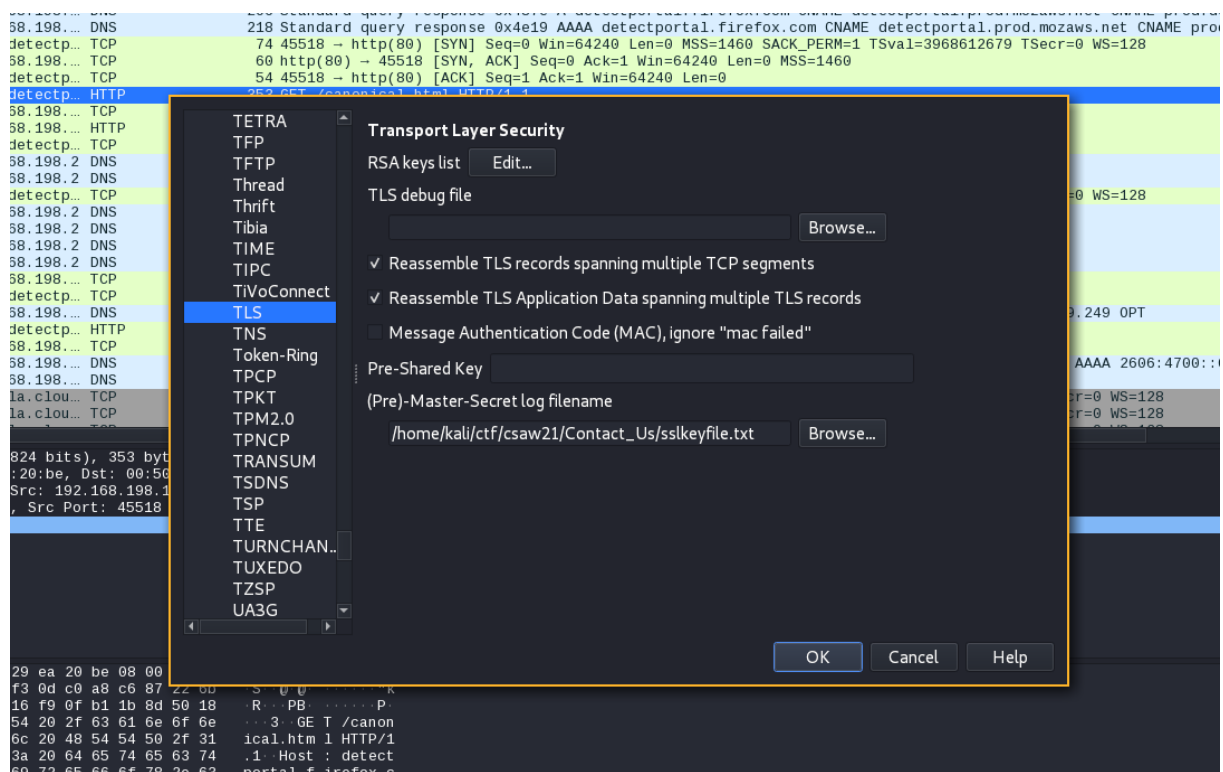
Writeup URL: GitHub

- 1 Veronica sent a message to her client via their website's Contact Us page. Can you find the message?
- 2
- 3 Author: moat, Pacific Northwest National Laboratory

Using Wireshark Decrypt The SSL Traffic

Using the given files `sslkeyfile.txt` and `ContactUs.pcap` we can start to decrypt the pcap.

Navigate through `Edit -> Preferences -> Protocols -> TLS -> (Pre)-Master-Secret log filename`, click browse and select the `sslkeyfile.txt` file.



Find the decrypted flag in the packet capture.

The image shows a Wireshark packet capture interface. At the top, the 'String' filter is applied, and the search term 'flag{' is entered. The packet list shows several QUIC and HTTP3 packets. The selected packet (36.279186) is an HTTP2/JSON packet. The packet details pane shows the following structure:

- Member Key: domainName
- Member Key: optedToSubscribe
- Member Key: locale
- Member Key: metadata
- Member Key: formData
 - Array
 - Object
 - Member Key: label
 - Member Key: value
 - String value: flag{m@r\$hm3110w\$}

The packet bytes pane shows the raw data, with the flag value highlighted in blue.

Using Tshark

You can do the same thing but with `tshark`:

1. Decrypt Pcap into a new file

- `tshark -r ContactUs.pcap -V -x -o tls.keylog_file:key.log > results`

2. `grep` to win for the flag

- `grep 'flag{' results`

```
tshark -r ContactUs.pcap -V -x -o tls.keylog_file:sslkeyfile.txt > decrypted.pcap; grep 'flag{' decrypted.pcap
String value: flag{m@r$hm3ll0w$}
0260 76 61 6c 75 65 22 3a 22 66 6c 61 67 7b 6d 40 72 value": "flag{m@r
```

Victory

Submit the flag and claim the points:

`flag{m@r$hm3ll0w$}`