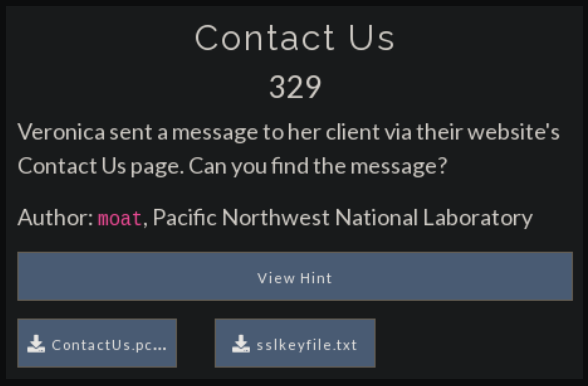
Contact Us

CSAW 2021 CTF

OreoByte



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

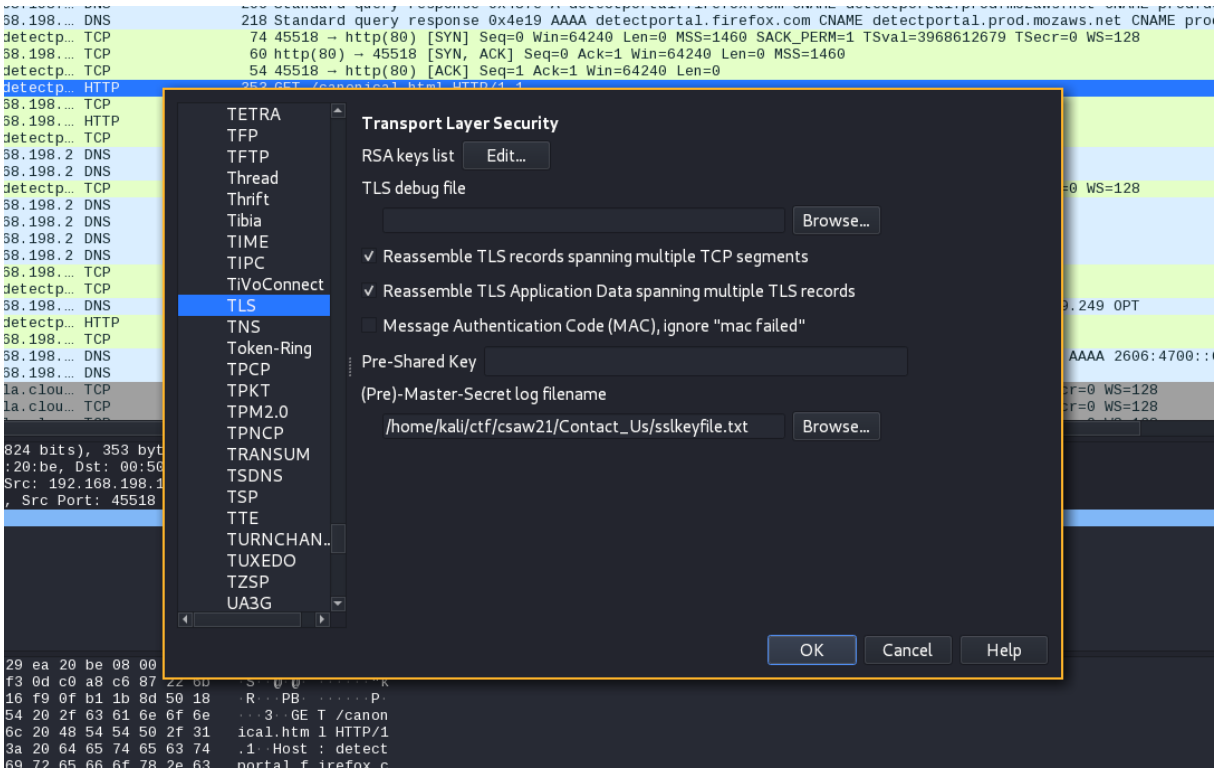
Writeup URL: GitHub

```
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
```

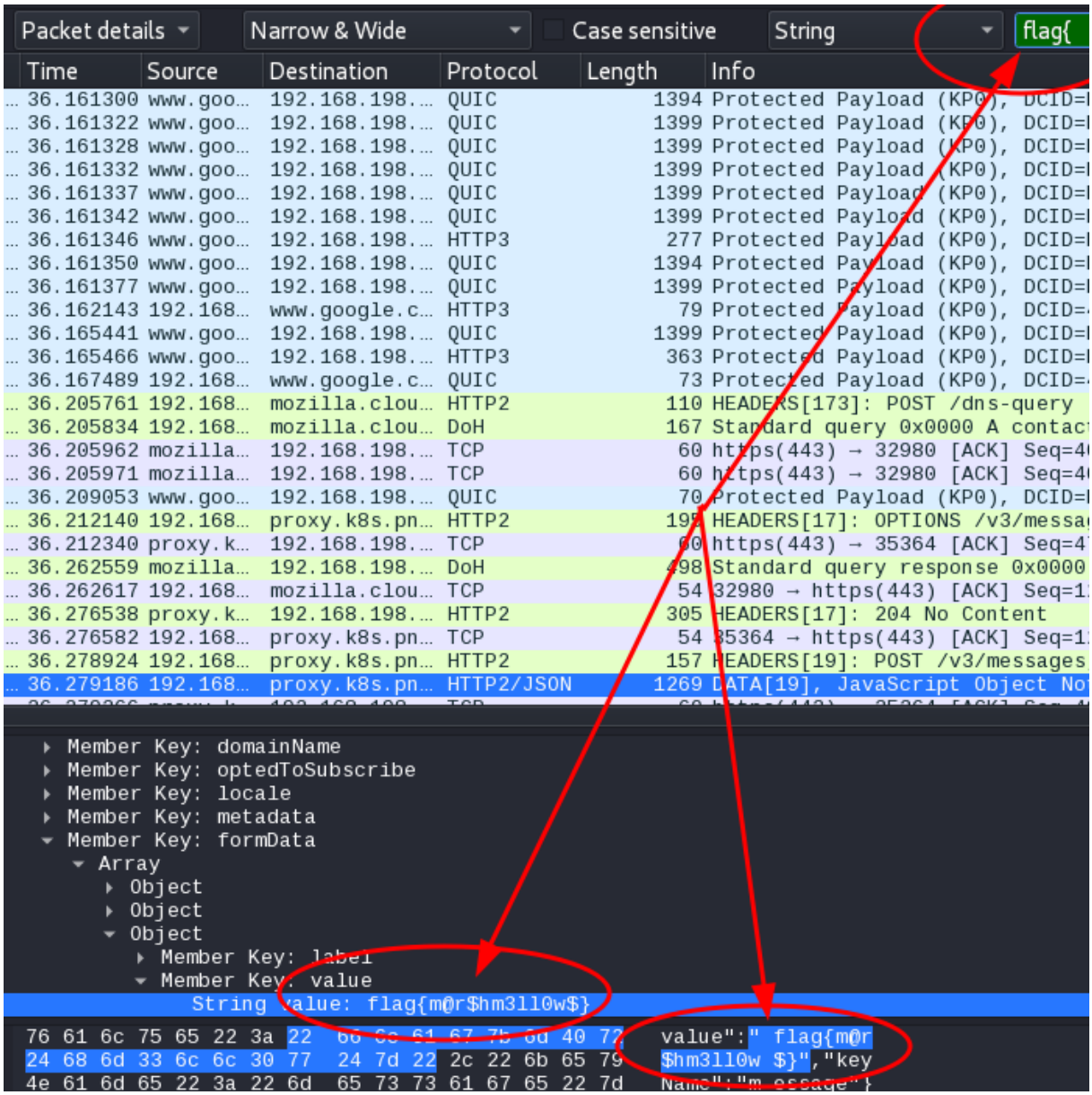
Using Wireshark Decrypt The SSL Traffic

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.



Using Tshark

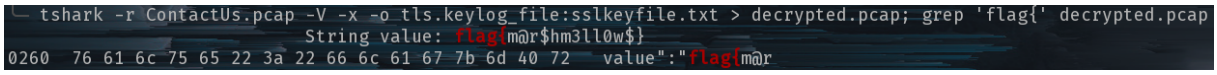
You can do the same thing but with `tshark`:

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`



Victory

Submit the flag and claim the points:

`flag{m@r$hm3ll0w$}`