Snake Oil

Goal

In the following exercise you will have to extract information from network data using Wireshark. You'll be asked generic questions, to which finding the answers could be approached in different ways. Don't be afraid to play with the program.

Description

Answer all questions, and remember to give in-depth answers

Steps

1. Take a look at the attached capture file.
    - Which protocol can you see there?
    - Can you identify the host name of the target server?
2. It seems like you need to add a secret ingredient.
    - Download the other attached file (secret.file), and open it with the document editor of your choice.
3. Can you guess what this file is?
4. Add the secret key file to your Wireshark's key file store.
    - If you don't know how to do it, look at Wireshark's Wiki page on SSL and RSA keys
    - Now, reload the capture file.
    - Can you see the real traffic now?
    - Where did the user try to go, and what did they try to do?

To submit

- A text file with your answers

Notes

- Try to focus on what's important and not be distracted by background noise.
- Please do not spend any time on IPv6 if stumbled upon.

References

- Wireshark Filter manpage: https://www.wireshark.org/docs/man-pages/wireshark-filter.html

- https://wiki.wireshark.org/TLS?action=show&redirect=SSL