Assignment- Wireshark SSL

Answer1-

1. I opened the picoctf_ssl_flag1 in Wireshark and checked the protocol hierarchy, where I found that HTTP is secure by TLS.
2. After that, I read one article about the HTTP secure connection where I found that HTTPS can be decrypted only using the key that is exchanged between receiver and sender during the connection established so the hint file premaster.txt may be the session key.
3. After that, I go to the Edit option in Wireshark and preferences, and under protocol, I go to TLS because TLS secures the HTTP request in that they ask to upload a premaster secret log file, and I upload that txt file there, and I see that there are some HTTP request are shown in Wireshark, and when I select those HTTP request and click on the decrypt I got the flag which is The HTTPS flag is f09ab0834bfa0238cd4b54aa

Flag–**f09ab0834bfa0238cd4b54aa**

Answer 2– To generate premaster.txt file before starting the session, we need to add the environment variable in the user variable name = **SSLKEYLOGFILE** and in value, put the path where you want to save that file suppose value=C:/premaster.txt it will save the file in C drive .So once we activate this after that if I open the browser and search it will store session keys.

Answer 3 – We can decrypt the HTTPS traffic only if we have the key file, which is securely exchanged between the sender and receiver we cannot easily get the key log file, and HTTPS relies on digital certificates issued by trusted Certificate Authorities (CAs). These certificates are used to verify the authenticity of the server, ensuring that the client is communicating with the intended website and not an impostor. This helps prevent man-in-the-middle attacks where an attacker intercepts communication between the client and server.