The first part of the challenge involves extracting the http objects. There, we have a pcap capture, 4 pdfs, and a file containing 2 CLIENT_RANDOM values (let's name it secrets). Using secrets. We can decode the tls 1.2 present in the new pcap capture (Edit > Preferences> TLS), and reveal it contains a rdp session. A little bit of googling revealed https://haxor.no/en/article/analyzing-captured-rdp-sessions

A summary is as follows:

1. We export PDUs as OSI LAYER 7 and then save the file as a **pcap**, not pcapng. (second option of Save As)

2. We install pyrdp on a **linux** machine (I couldn't get it to work on windows) using **pipx**.

3. The command to use is **pyrdp-convert -o ./output rdpsession.pcap**

4. We can then play the recording using pyrdp-player.

After all that, we find a shorturl and after accessing it, the flag.

Made with love by: AndreiCat