Shark 2 – Angstorm CTF 2022

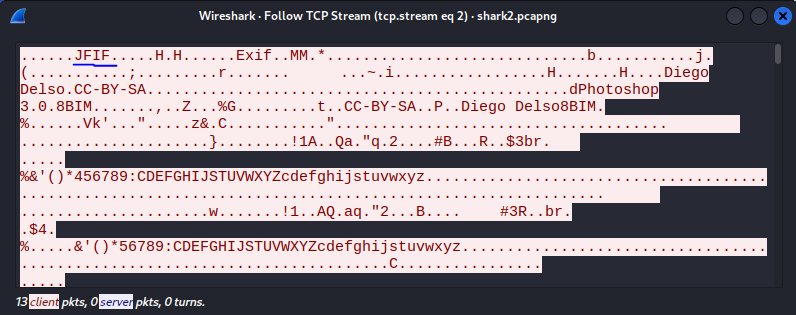
We we’re provided with a pcapng file (Wireshark format) so we opened it using Wireshark.  
It was a pretty small capture file with only 3 different TCP conversations.

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטי

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיThe first conversation had the following contents:

We then thought the flag might be in the photo so we tried to find the photo conversation  
it contained JFIF magic bytes which is JPEG format.

תמונה שמכילה טקסט, צג, מקורה, דג

התיאור נוצר באופן אוטומטיWe saved the raw data to a file and we got the flag! :)