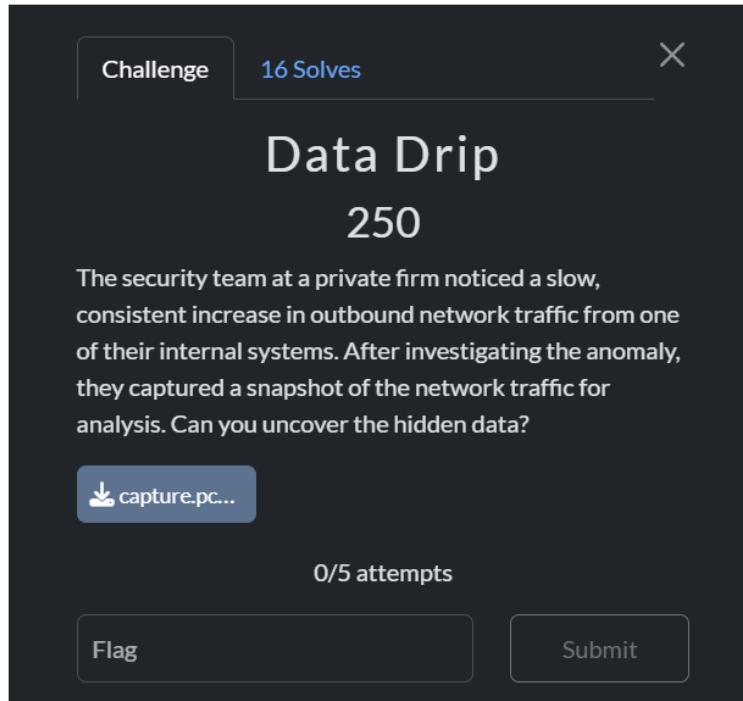
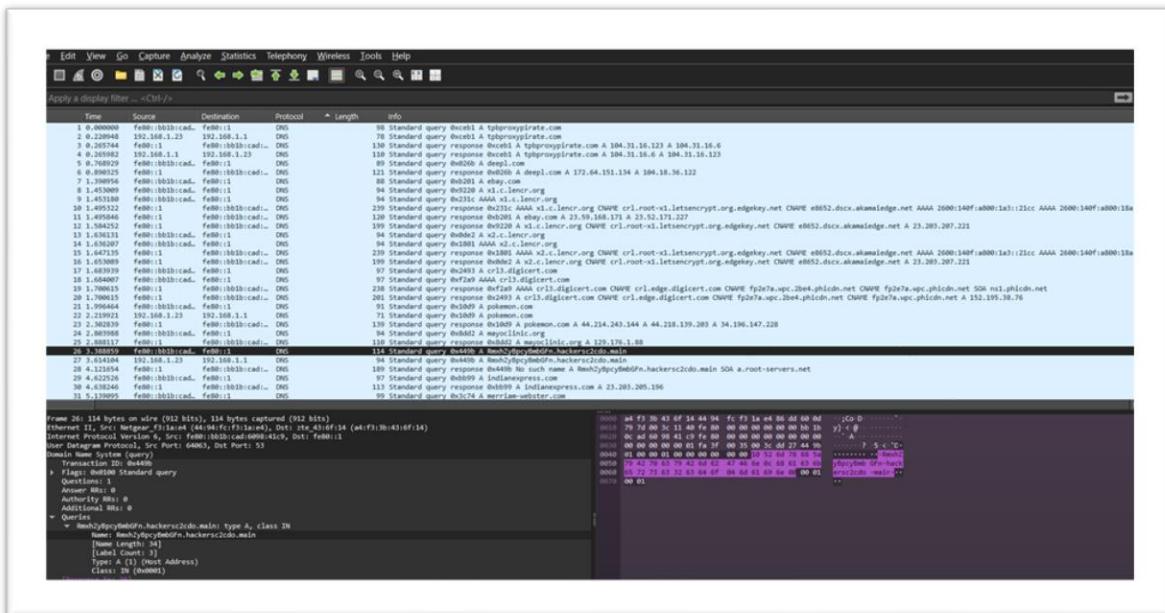


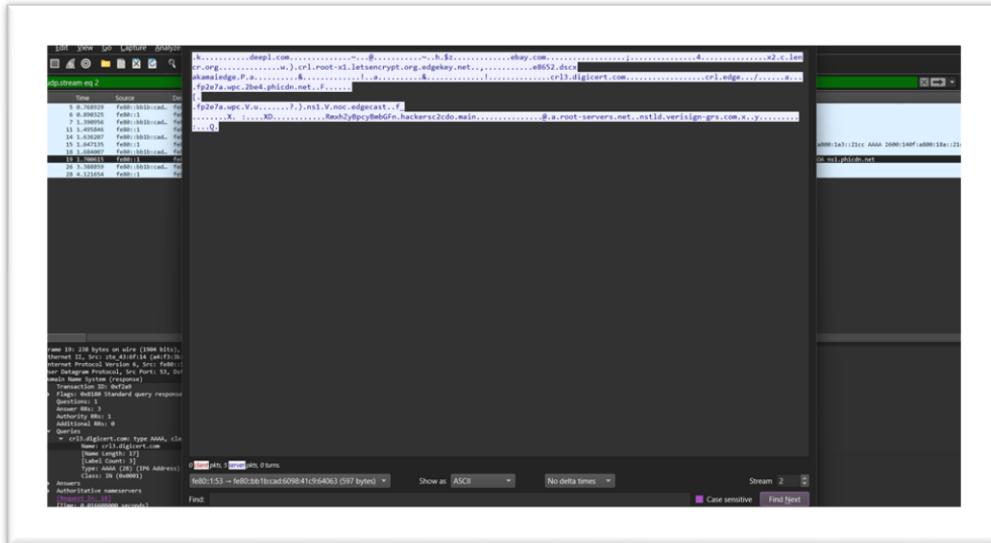
Challenge Name: Data Drip — 250pts (Forensics)



As the challenge shows the pcap file, so I directly download it to investigate further.

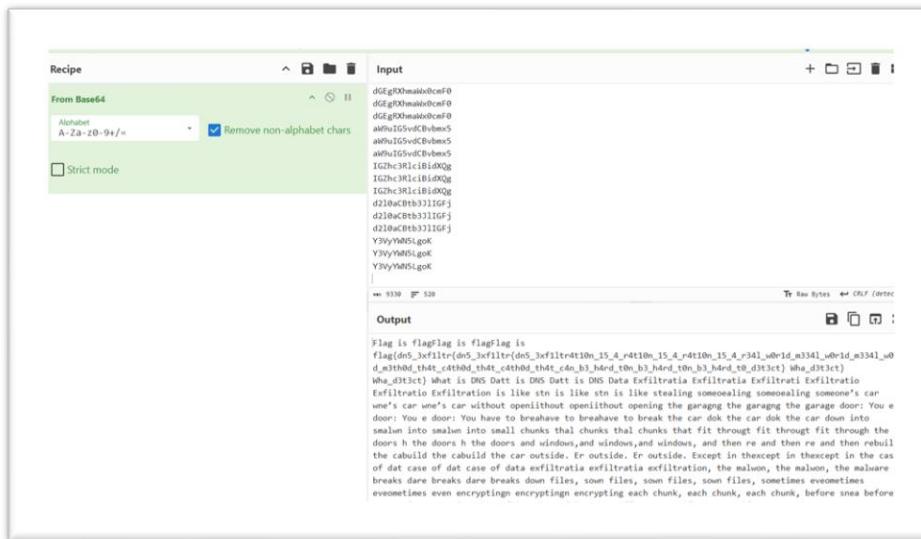


As I saw all the packet from the DNS and with further analysis, I got to know that some strings are transmitting with the domains as a subdomains.



As I got to know that many strings are there with subdomains with base64 strings as attached.

I just collect all with the strings function and got the proper flag by rearranging them.



This is how I got to complete this challenge 😊 .

FLAG: {dn5_3xf1ltr4t10n_15_4_r34l_w0r1d_m3th0d_th4t_c4n_b3_h4rd_t0_d3t3ct}

~By Team justahacker