VishwaCTF

CHALLENGE NAME : [ROUTER |PORT|]

DEV : [SAKSHAM SAIPATWAR]

CATEGORY : [DIGITAL FORENSICS]

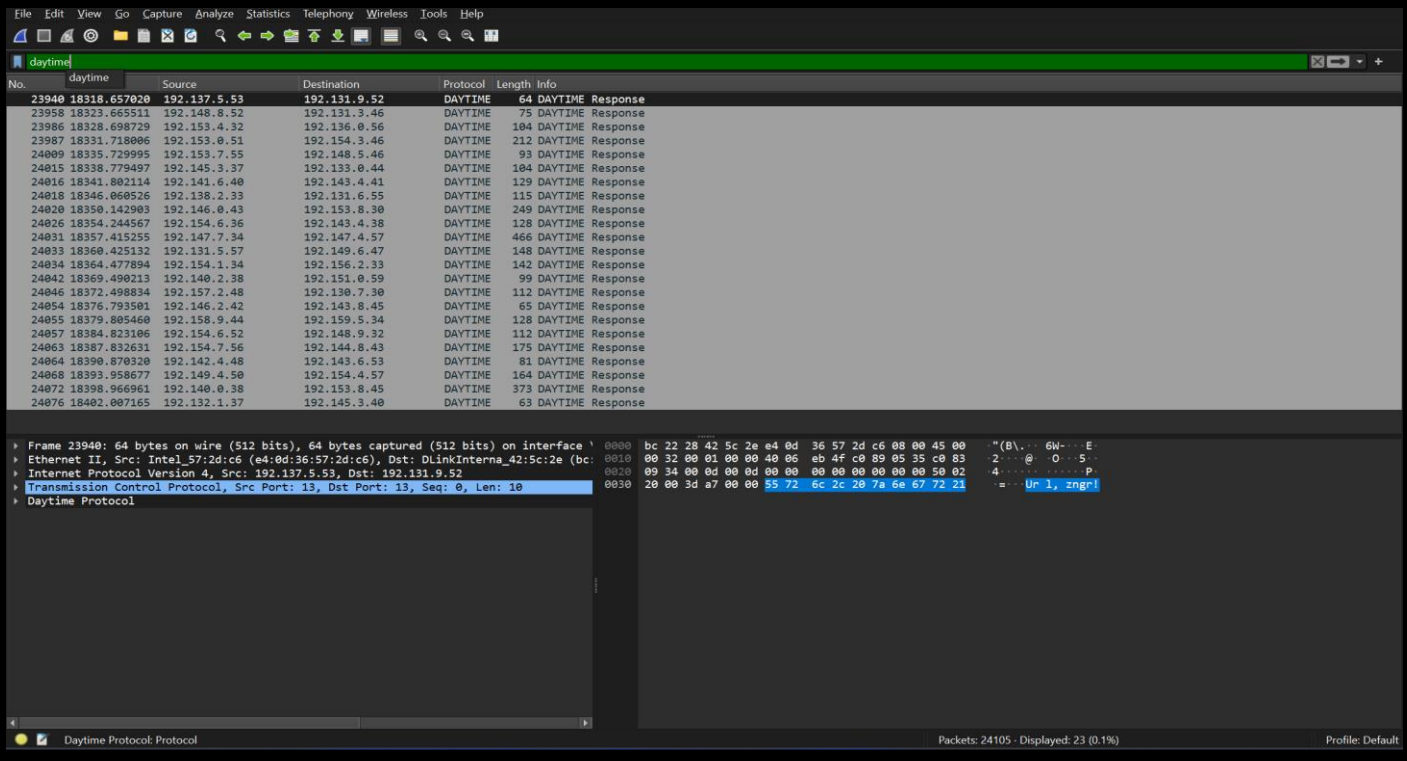
LEVEL : [MEDIUM]

2024

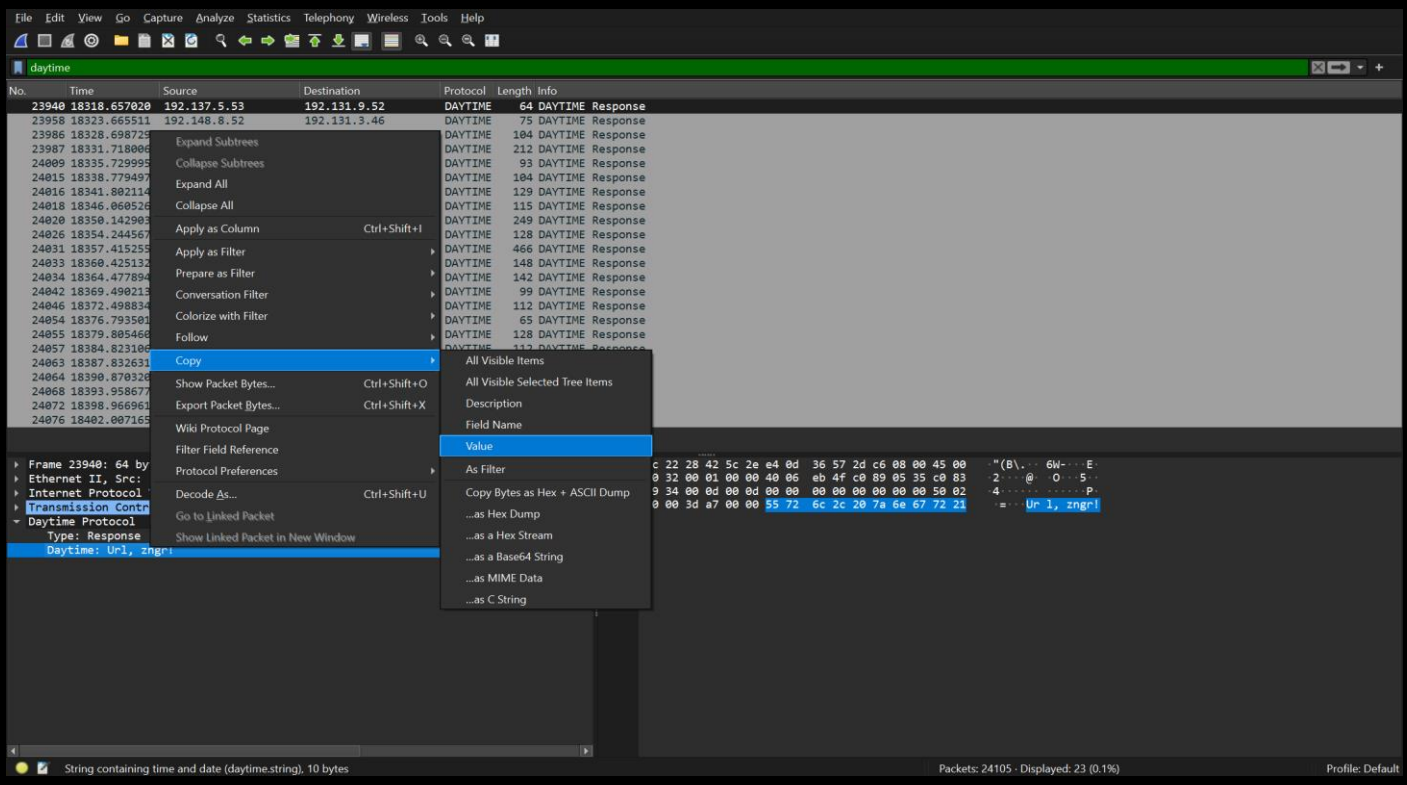
Description :- *There's some unusual traffic on the daytime port, but it isn't related to date or time requests. Analyze the packet capture to retrieve the flag.*

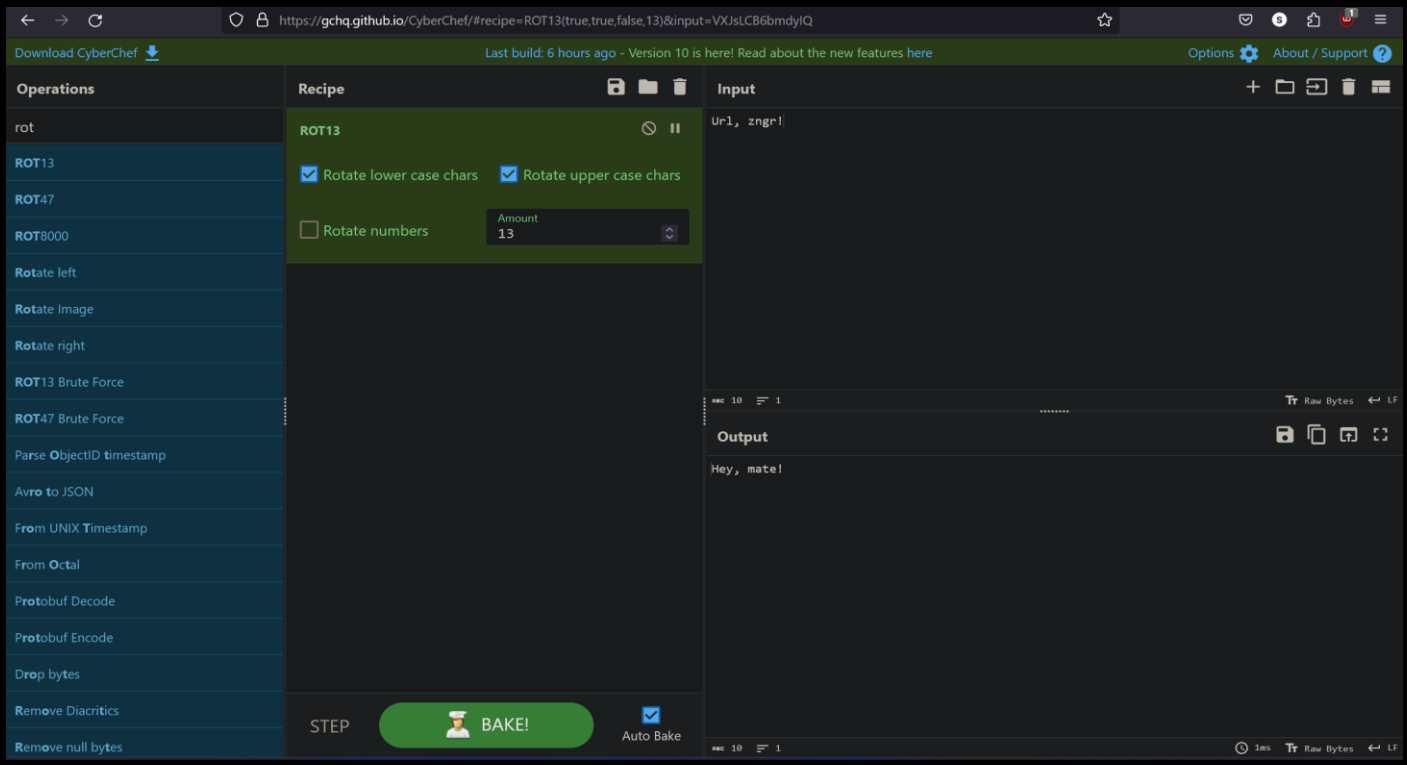
Interpretation :- *The daytime port mentioned in the description refers to TCP/UDP port 13. Additionally, the title provided hints about the encryption used 'ROT' and |port| refers to the number of rotations .*

Step 1 : *Open the capture file in wireshark and use 'daytime' as protocol filter .*



Step 2 : *In the filtered packets you can see that each packet contains some encrypted text … copy the entire conversation and decrypt it .*





Complete Conversation :-

User A: Hey, mate!

User B: Yo, long time no see!

User A: You sure this mode of communication is still safe?

User B: Yeah, unless someone else is capturing network packets on the same network we're using. Anyhow, our text is encrypted, and it would be difficult to interpret.

User A: So let's hope no one else is capturing.

User B: What's so confidential that you're about to share?

User A: It's about cracking the password of a person with the username 'Anonymous.'

User B: Oh wait! Don't you know I'm not so good at password cracking?

User A: Yeah, I know, but it's not about cracking. It's about the analysis of packets. I've completed most of the job, even figured out a way to get the session key to decrypt and decompress the packets.

User B: Holy cow! How in the world did you manage to get this key from his device?

User A: Firstly, I hacked the router of our institute and closely monitored the traffic, waiting for 'Anonymous' to download some software that requires admin privilege to install. Once he started the download, I, with complete control of the router, replaced the incoming packets with the ones I created containing malicious scripts, and thus gained a backdoor access to his device. The further job was a piece of cake.

User B: Whoa! It's so surprising to see how much you know about networking or hacking, to be specific.

User A: Yeah, I did a lot of research on that. Now, should we focus on the purpose of this meet?

User B: Yes, of course. So, what should I do for you?

User A: Have you started the packet capture as I told you earlier?

User B: Yes, I did.

User A: Great! I will be sending his SSL key, so find the password of 'Anonymous.'

User B: Yes, I would, but I need some details like where to start.

User A: The only details I have are he uses the same password for every website, and he just went on to register for a CTF event.

User B: Okay, I will search for it.

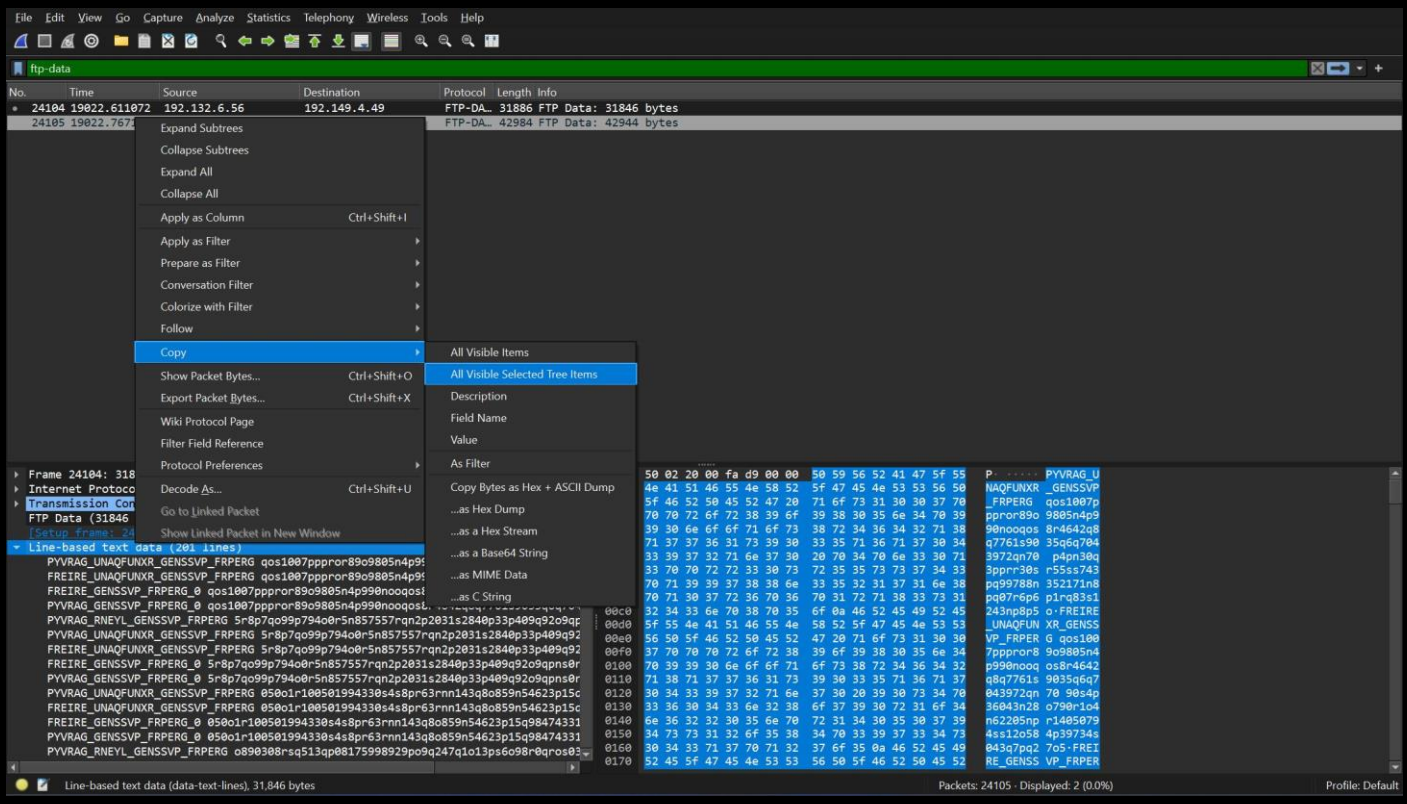
User A: Wait a second, I won't be sending the SSL key on this Daytime Protocol port; we need to keep this untraceable.

User B: Okay, so where should I look for the key?

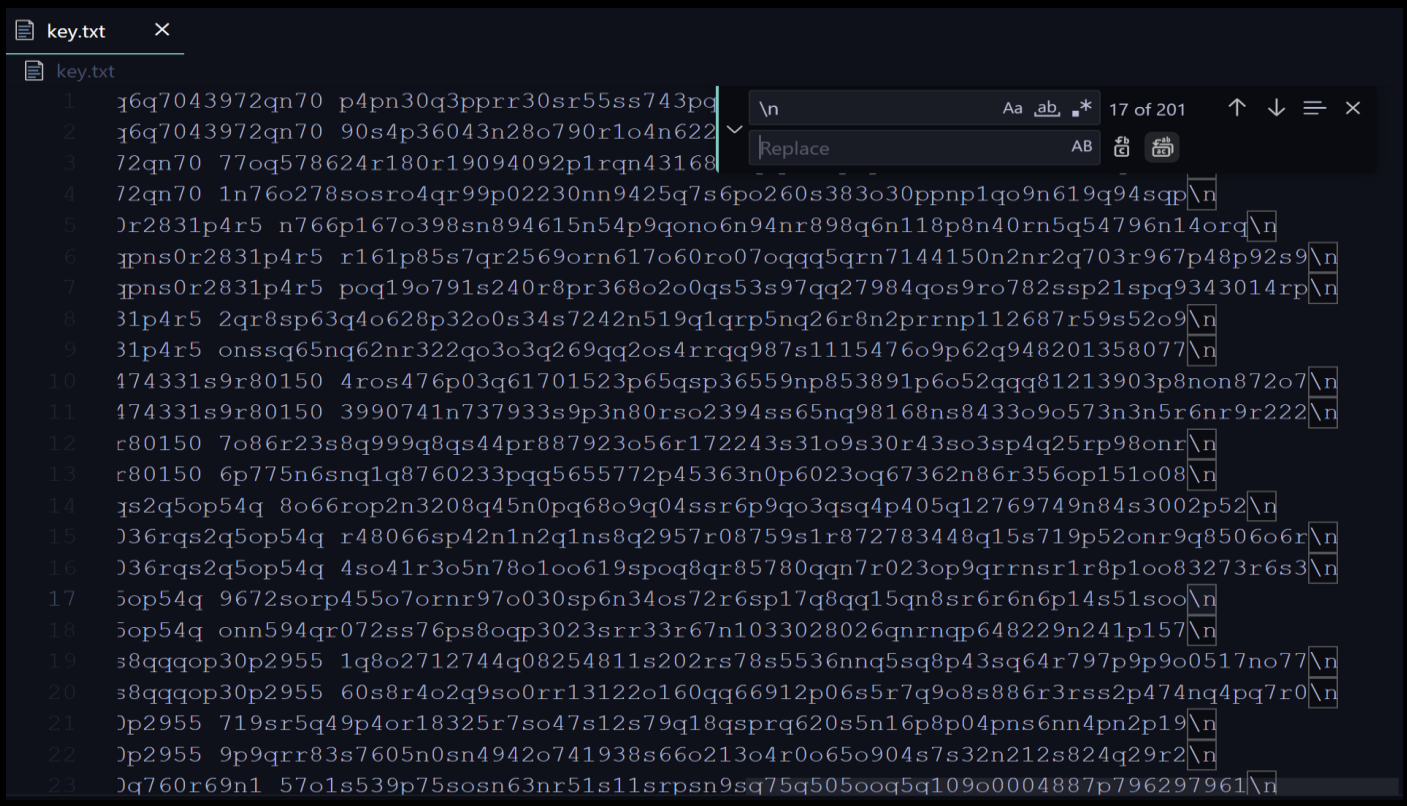
User A: I will be sending it through FTP. Since the file is too large, I will be sending it in two parts. Please remember to merge them before using it. Additionally, some changes may be made to it during transfer due to the method I'm using. Ensure that you handle these issues.

User B: Okay! ...

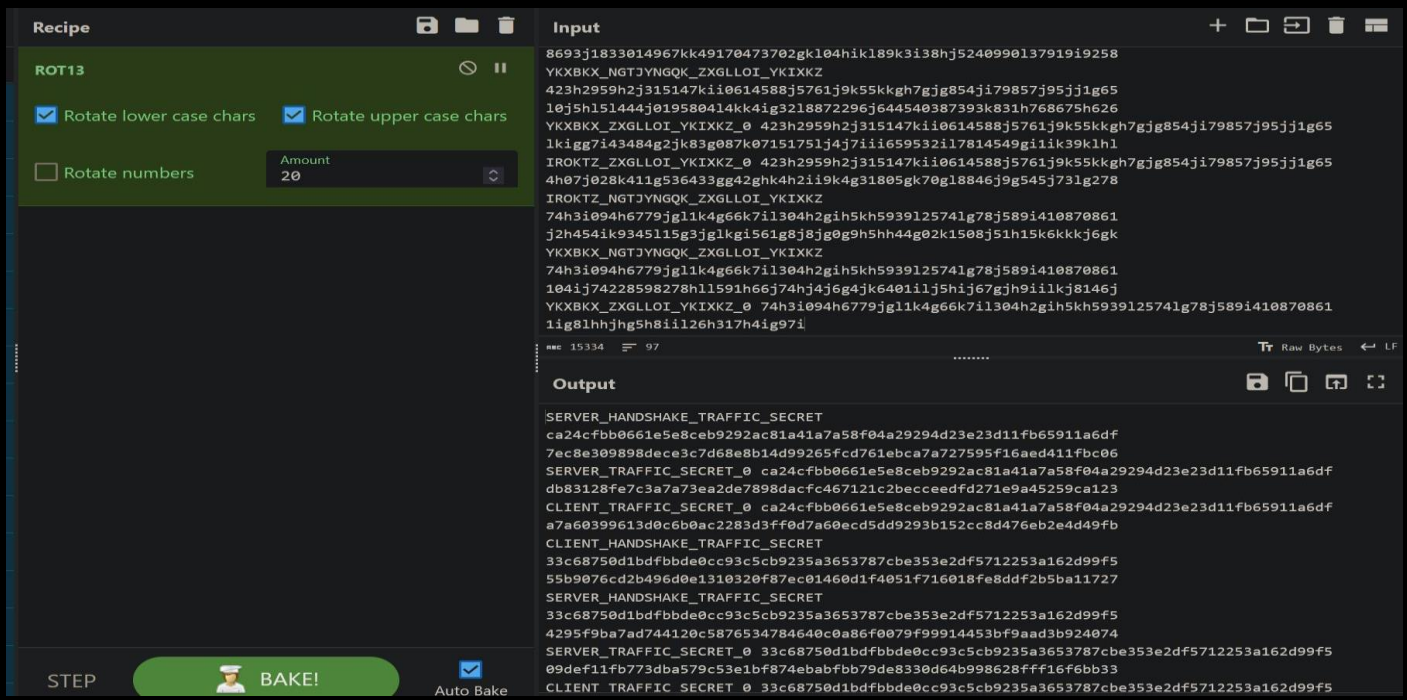
Step 3 : From the conversation its clear that we need to find password of a person with username ‘Anonymous’ , for that first we need to get SSL key on ftp port .



Note : *When you Google for FTP protocol port, you can see that it has two ports, one for command and the other for data. So, use "ftp-data" as a filter. Now, once we have copied the data, we must then remove the title that was copied, the '\n' characters appended at the end, and the extra spacing at the beginning.*

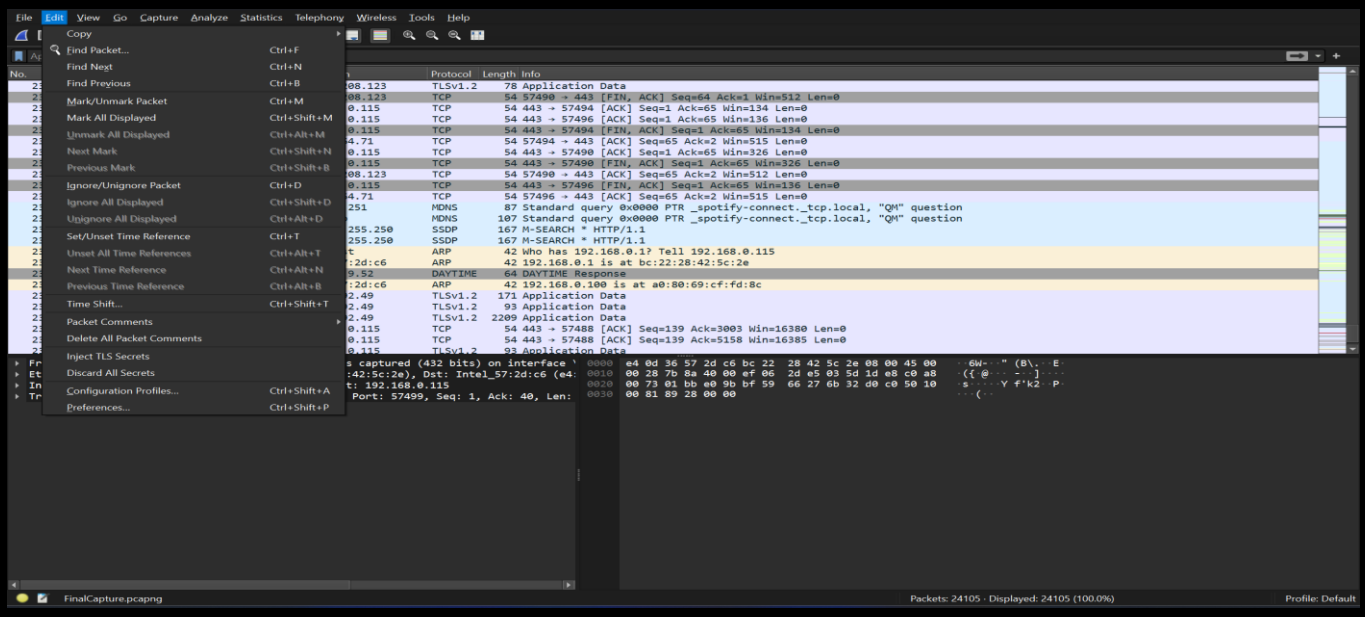


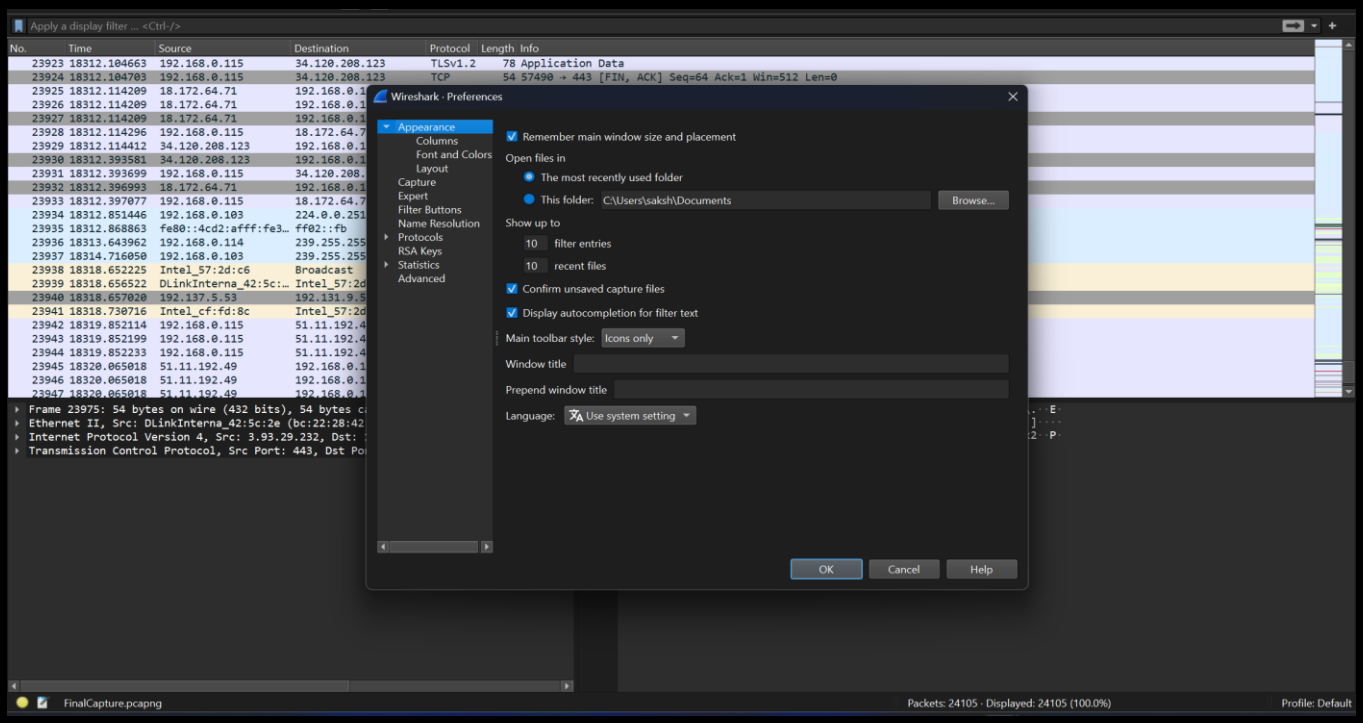
Step 4 :- *Do the same with the other part of the key and merge both of them. Finally, decrypt it using 'ROT13' with '20 or 6' rotations to obtain the final key.*



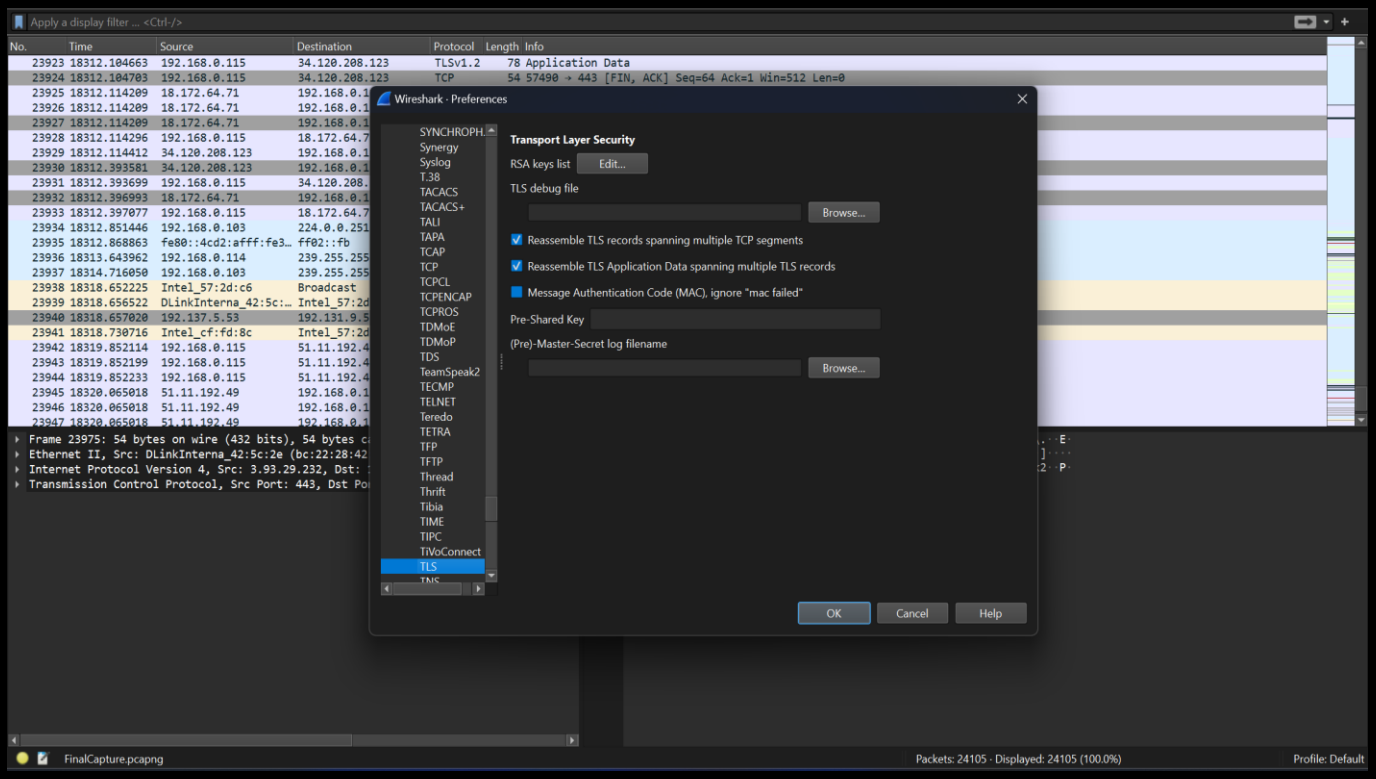
Step 5 :- *Now, once you have obtained the SSL key, you need to provide it to Wireshark so it can decrypt and decompress the network packets. To do this, follow the steps below :*

1) Click the edit tab and click preferences .

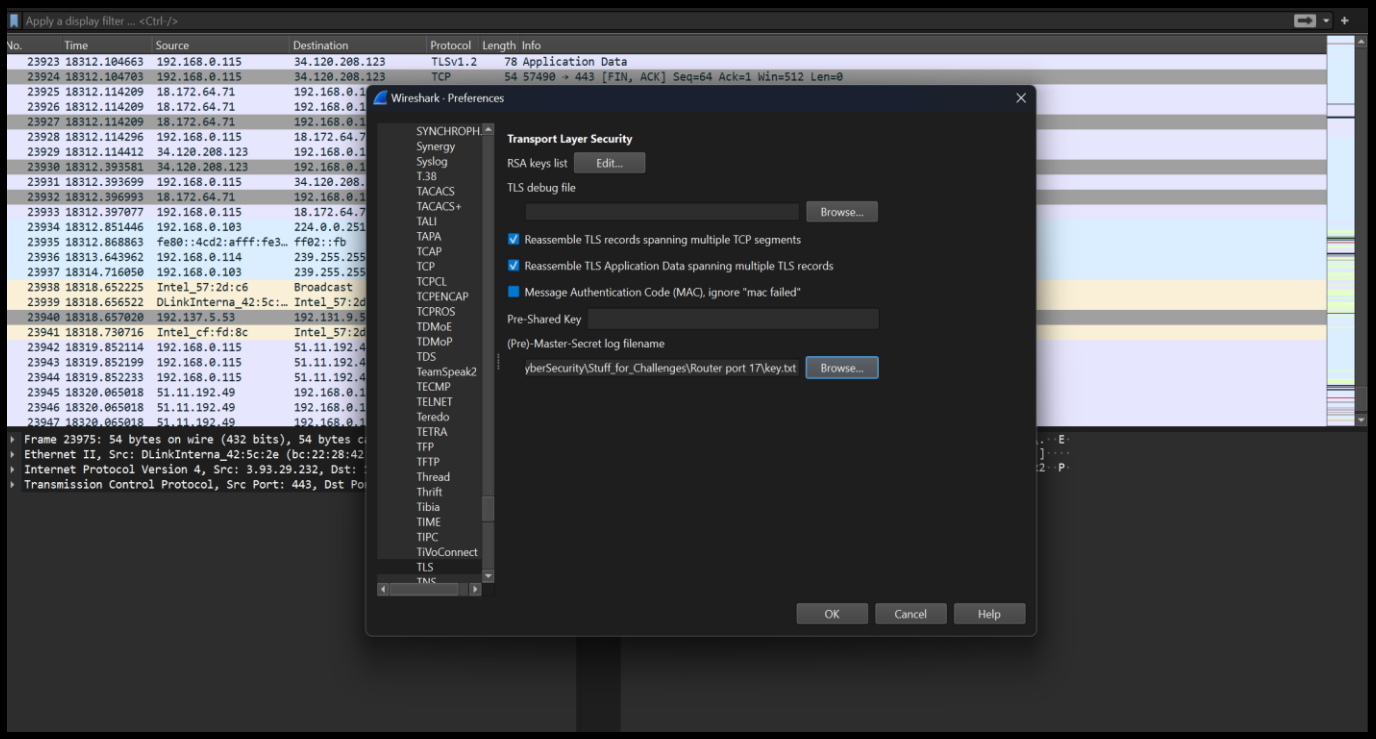




2) Now in protocols search for TLS and open it .

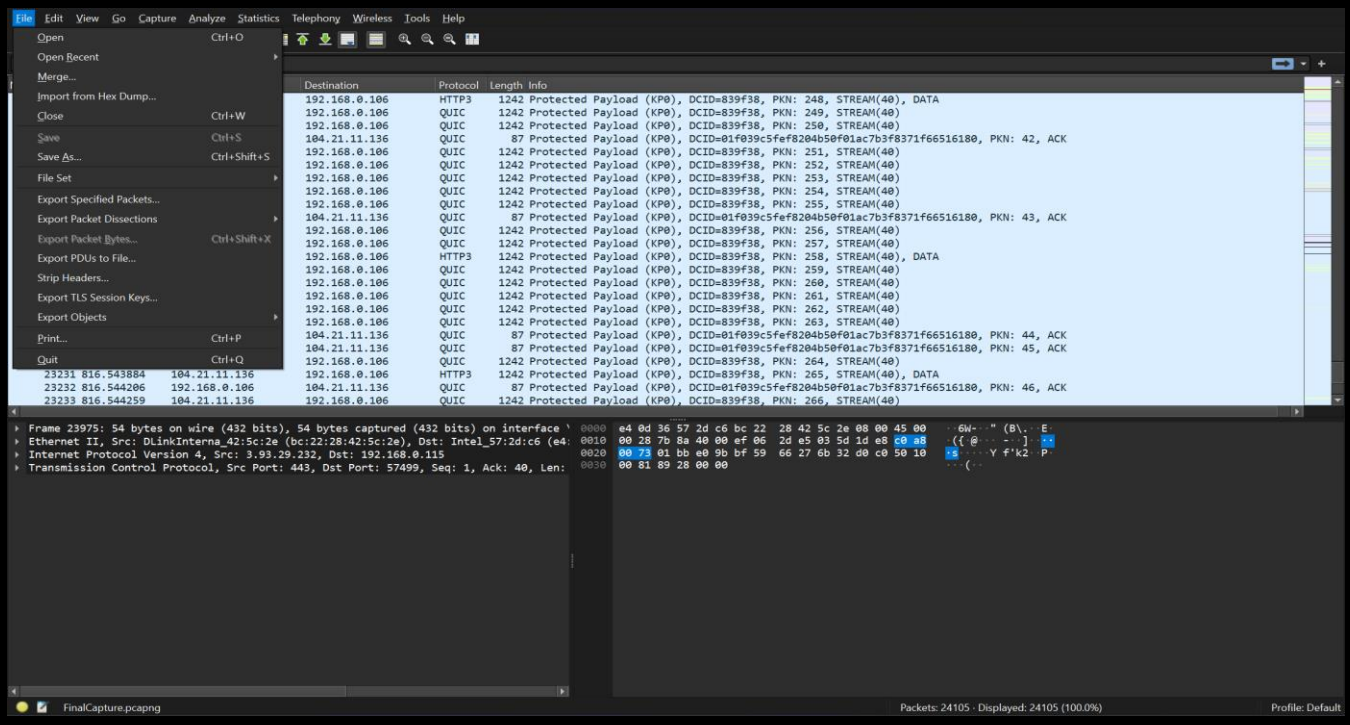


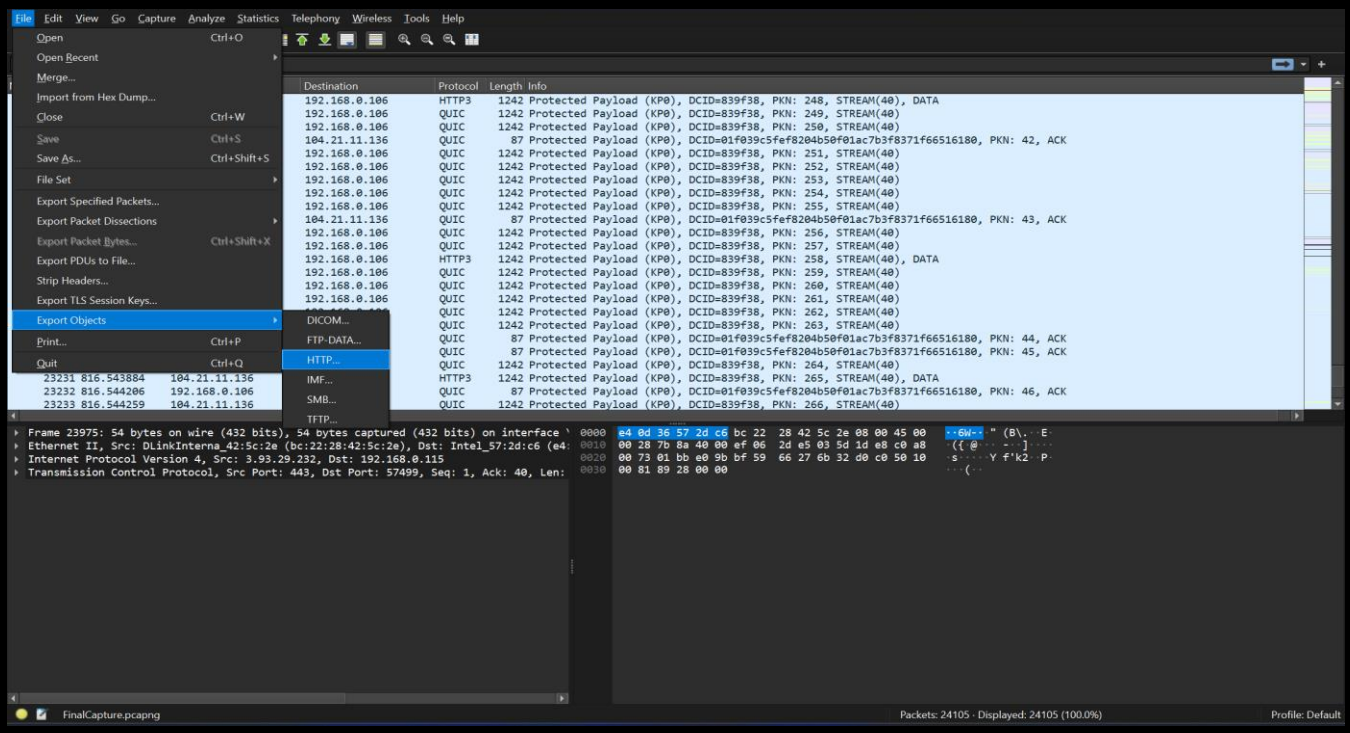
3) Finally add the decrypted SSL key to decrypt the captured packets .



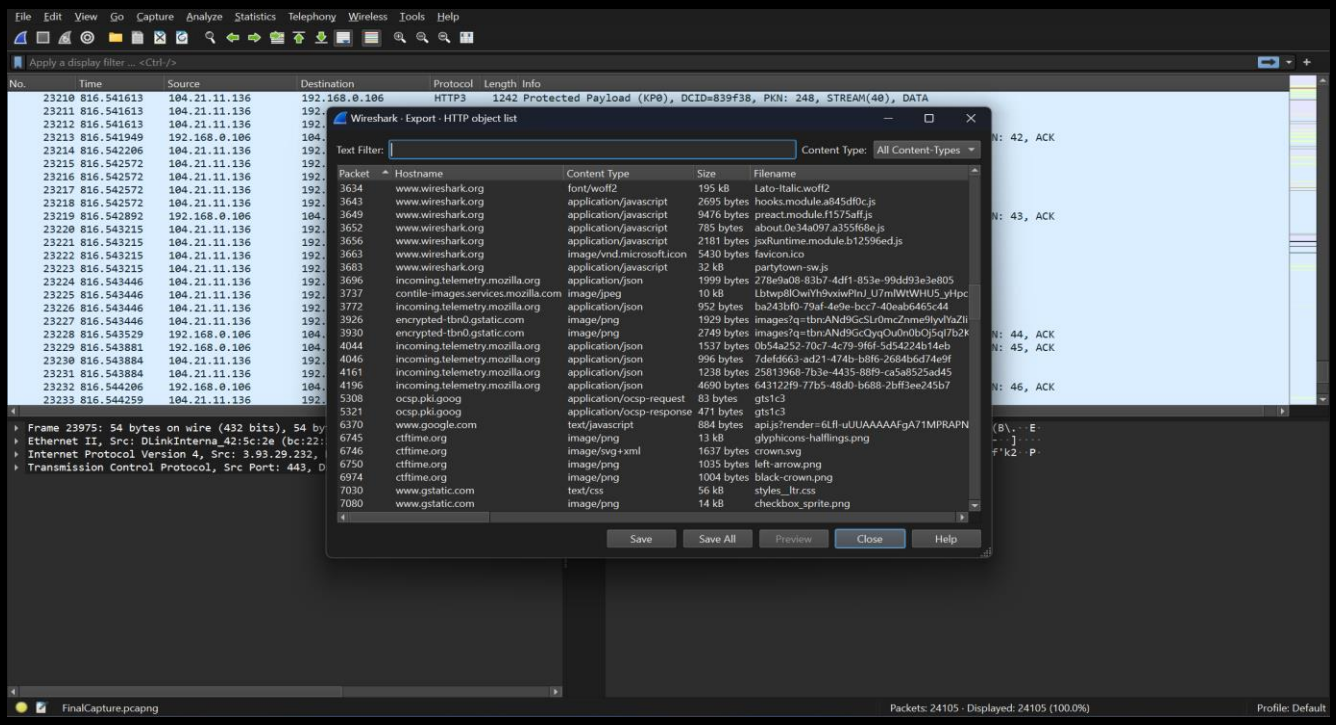
Step 6 :- Now, since the packets are decrypted, just look for the objects captured in this file. To do so, follow the steps below :

1) Click the "File" tab, and under "Export Objects," select 'HTTP'.

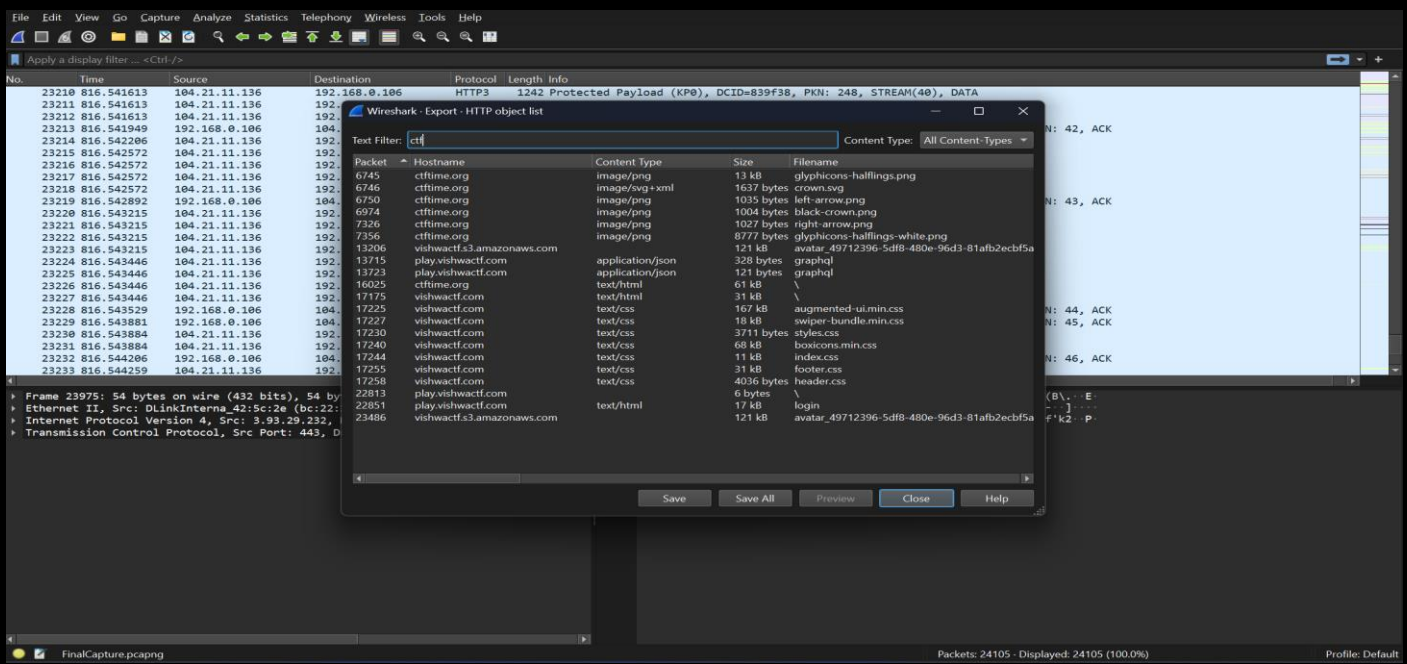




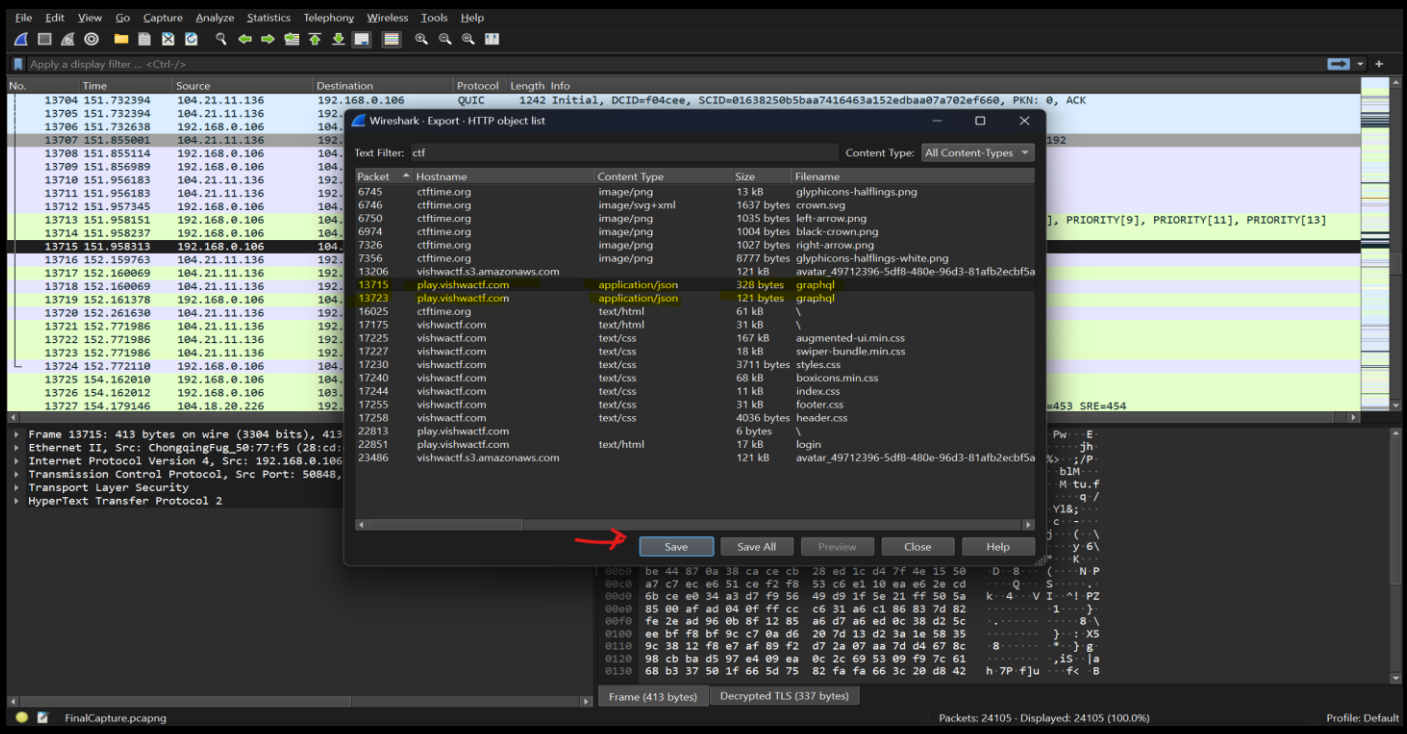
2) Now you can see various objects captured in this file .



Step 7 *:- As seen, there are many objects captured we need to filter some of them .The hint in the conversation suggests that 'Anonymous' was registering for a CTF, so you can use 'ctf' to filter the results.*



Step 8 :- *Even after applying the filter, there are still too many files to search. To narrow down the results, consider that you are looking for the password entered for validation. Focus on searching for query files. (In this case 'JSON' files) Save these files and search for the password inside them.*



Step 9 :- *Search for password of a person with username 'Anonymous' .*

Flag :- VishwaCTF{K3Y5_CAN_0P3N_10CK5 }