

vishwaCTF

CHALLENGE NAME : [ROUTER |PORT|]

DEV : [SAKSHAM SAIPATWAR]

CATEGORY : [DIGITAL FORENSICS]

LEVEL : [MEDIUM]

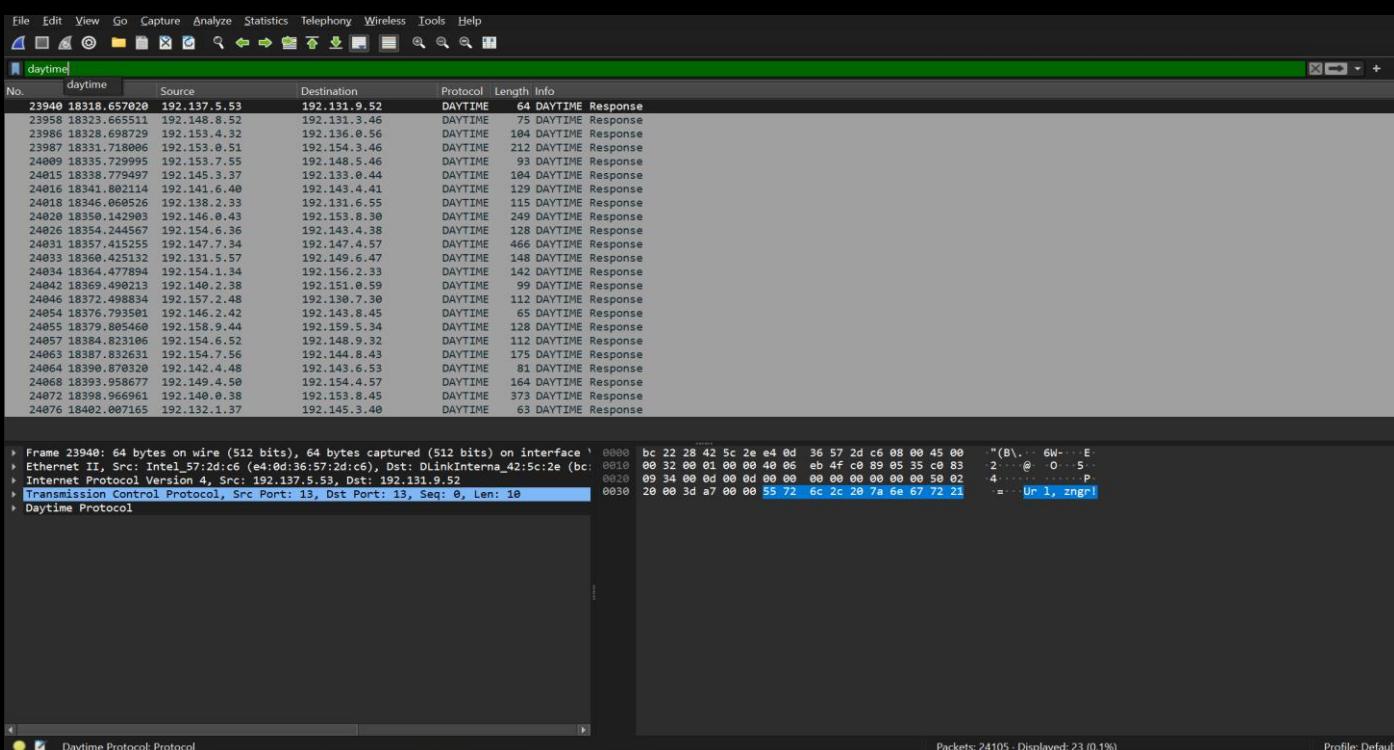


2024

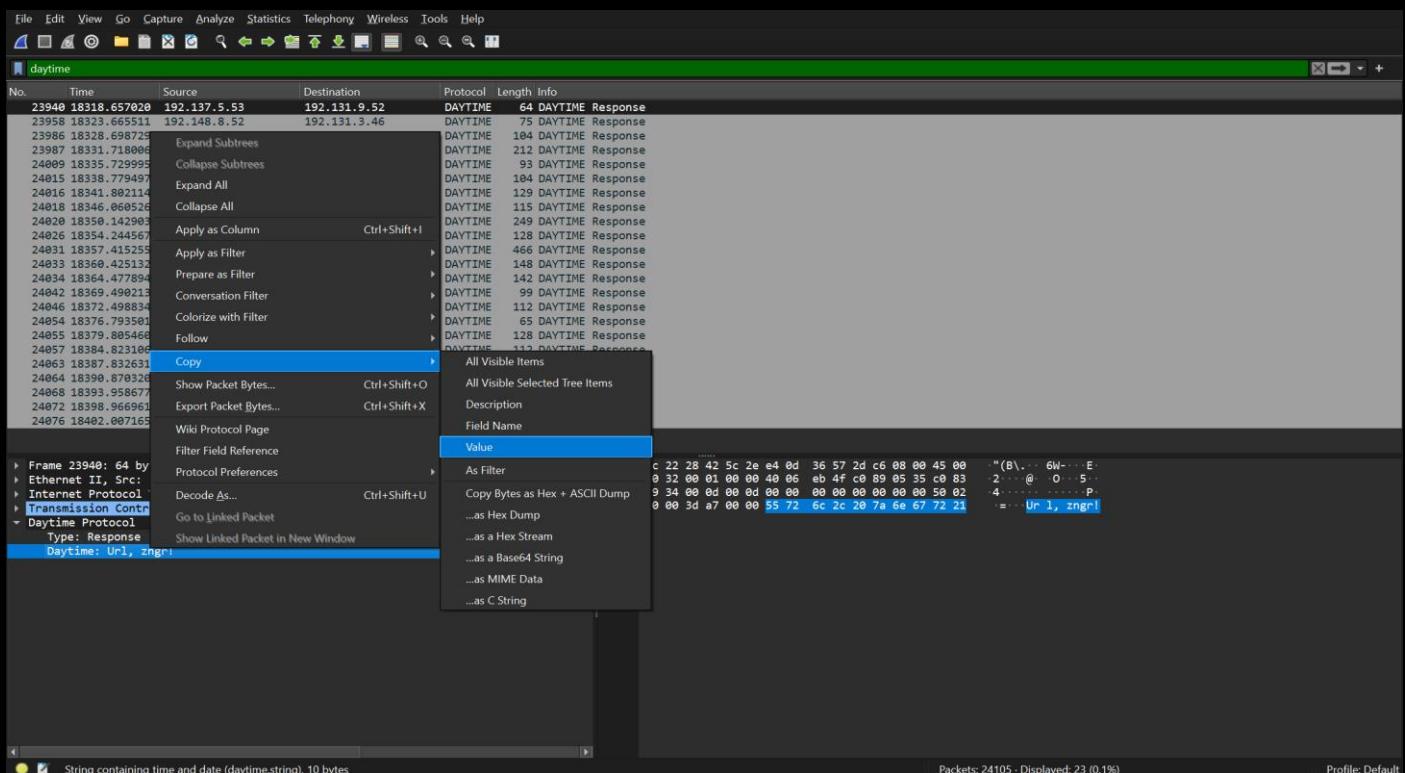
Description :- There's some unusual traffic on the daytime port, but it isn't related to date or time requests. Analyze the packet capture to retrieve the flag.

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 .



String containing time and date (daytime.string), 10 bytes

Packets: 24105 · Displayed: 23 (0.1%)

Profile: Default

Last build: 6 hours ago - Version 10 is here! Read about the new features here

Download CyberChef [Download](#)

Operations

- rot
- ROT13
- ROT47
- ROT8000
- Rotate left
- Rotate Image
- Rotate right
- ROT13 Brute Force
- ROT47 Brute Force
- Parse ObjectId timestamp
- Avro to JSON
- From UNIX Timestamp
- From Octal
- Protobuf Decode
- Protobuf Encode
- Drop bytes
- Remove Diacritics
- Remove null bytes

Recipe

ROT13

ROT13

✓ Rotate lower case chars ✓ Rotate upper case chars

□ Rotate numbers Amount: 13

Input

Url, zngr!

Output

Hey, mate!

Raw Bytes

STEP BAKE! Auto Bake

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.

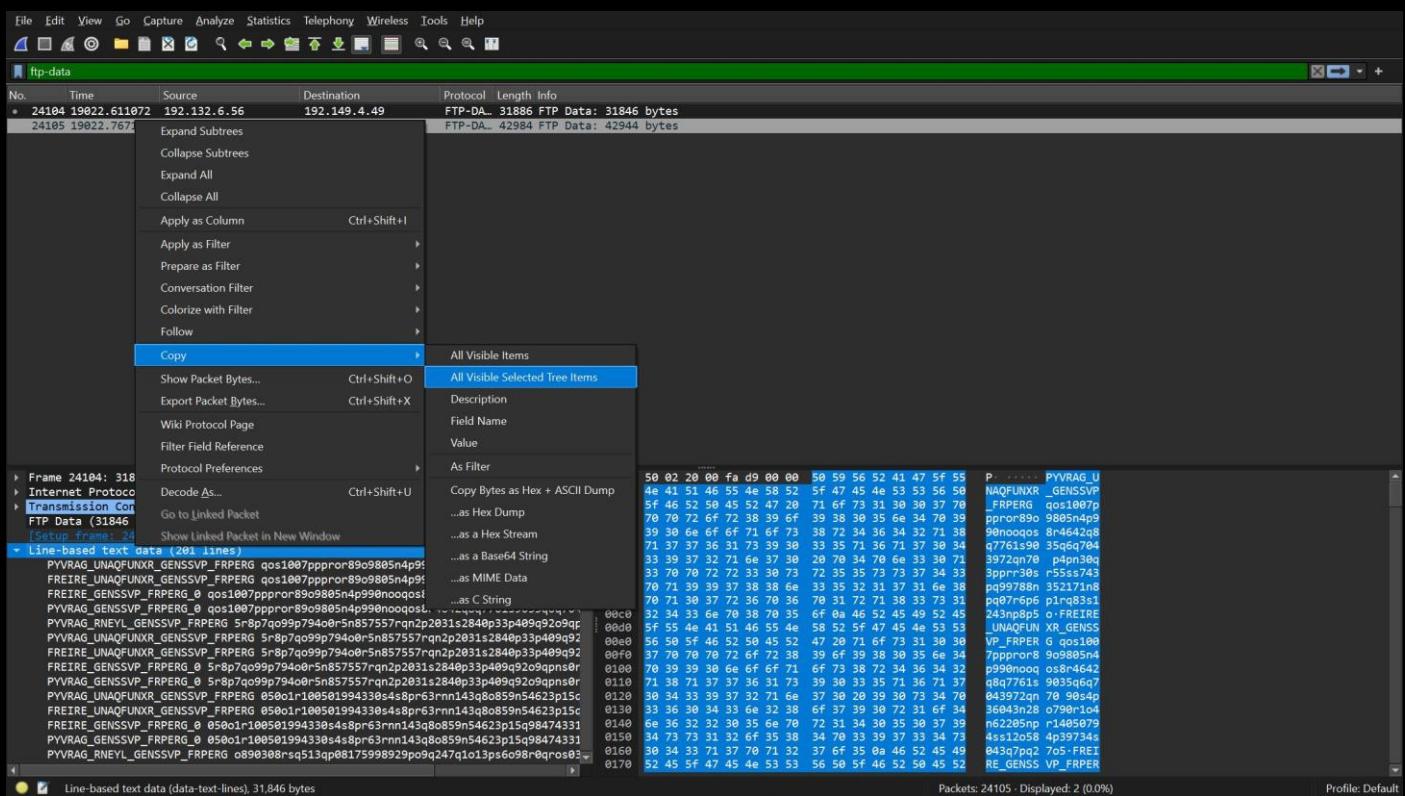
User A: Wait a second, I won't be sending the SSL key on this Daytime Protocol port; we need to keep this untraceable.

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

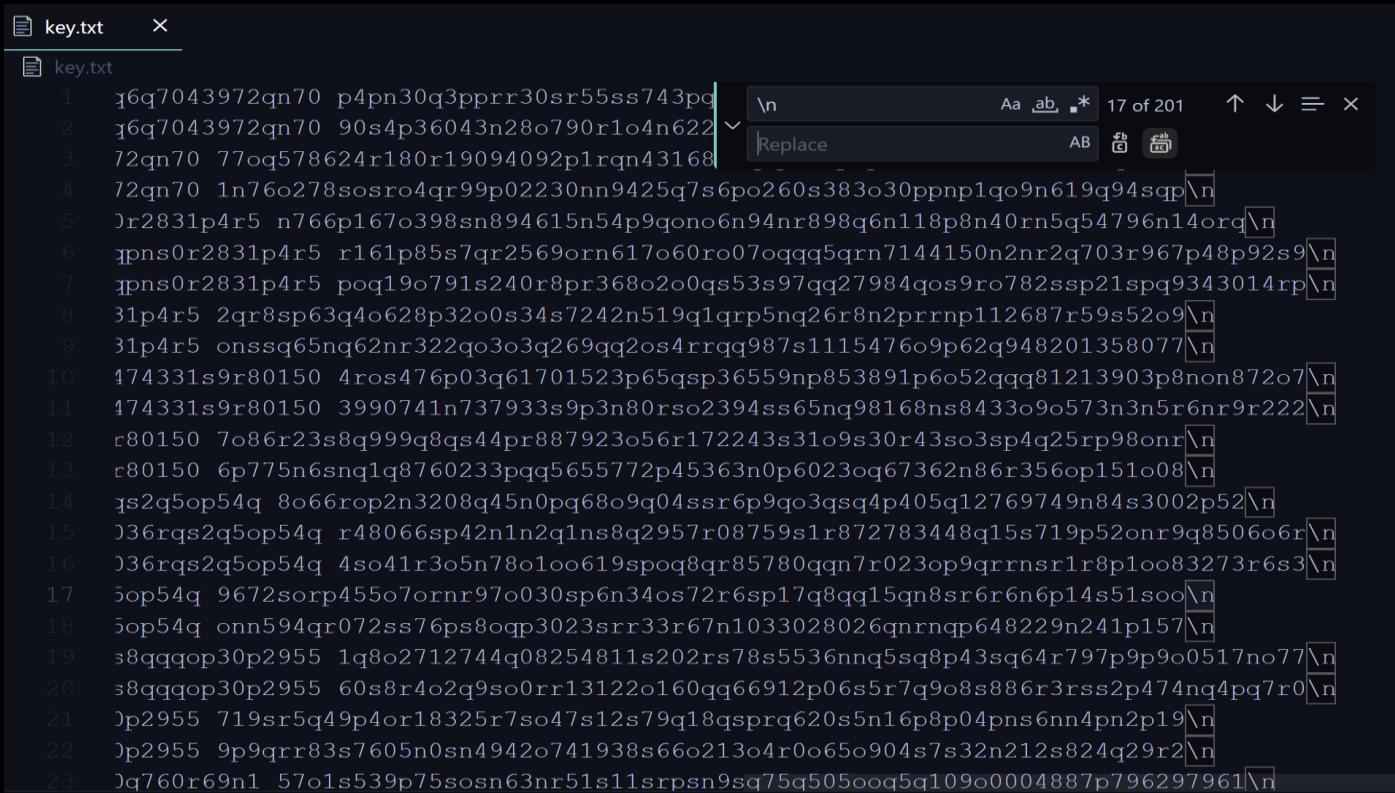
User A: I will be sending it through FTP. Since the file is too large, I will be sending it in two parts. Please remember to merge them before using it. Additionally, some changes may be made to it during transfer due to the method I'm using. Ensure that you handle these issues.

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.

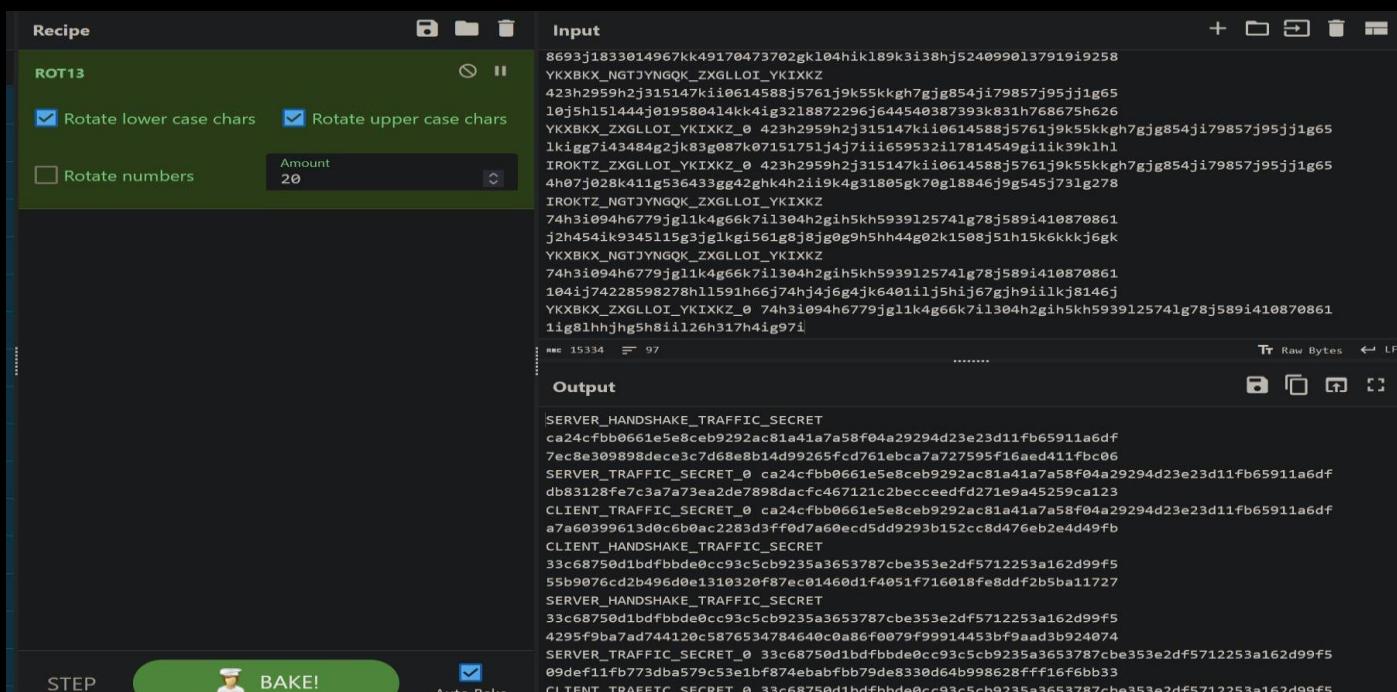


```

key.txt
1 j6q7043972qn70 p4pn30q3pprr30sr55ss743pq
2 j6q7043972qn70 90s4p36043n28o790r1o4n622
3 72qn70 77oq578624r180r19094092p1rqn43168
4 72qn70 1n76o278sosro4qr99p02230nn9425q7s6po260s383o30ppnp1qo9n619q94sqp\n
5 Jr2831p4r5 n766p167o398sn894615n54p9qono6n94nr898q6n118p8n40rn5q54796n14orq\n
6 qpns0r2831p4r5 r161p85s7qr2569orn617o60ro07oqqq5qrn7144150n2nr2q703r967p48p92s9\n
7 qpns0r2831p4r5 poq19o791s240r8pr368o2oqs53s97qq27984qos9ro782ssp21spq9343014rp\n
8 31p4r5 2qr8sp63q4o628p32o0s34s7242n519q1qrp5nq26r8n2prrnp112687r59s52o9\n
9 31p4r5 onssq65nq62nr322qo3o3q269qq2os4rrqq987s1115476o9p62q948201358077\n
10 474331s9r80150 4ros476p03q61701523p65qsp36559np853891p6o52qq81213903p8non872o7\n
11 474331s9r80150 3990741n737933s9p3n80rs02394ss65nq98168ns8433o9o573n3n5r6nr9r222\n
12 r80150 7o86r23s8q999q8qs44pr887923o56r172243s31o9s30r43so3sp4q25rp98onr\n
13 r80150 6p775n6snq1q8760233pqq5655772p45363n0p6023oq67362n86r356op151o08\n
14 qs2q5op54q 8o66rop2n3208q45n0pq68o9q04ssr6p9qo3qsq4p405q12769749n84s3002p52\n
15 036rqs2q5op54q r48066sp42n1n2q1ns8q2957r08759s1r872783448q15s719p52onr9q8506o6r\n
16 036rqs2q5op54q 4so41r3o5n78o1o0619spoq8qr85780qqn7r023op9qrrnsr1r8p1oo83273r6s3\n
17 5op54q 9672sorp455o7ornr97o030sp6n34os72r6sp17q8qq15qn8sr6r6n6p14s51soo\n
18 5op54q onn594qr072ss76ps8oqp3023srr33r67n1033028026qnrnqp648229n241p157\n
19 s8qqqop30p2955 1q8o2712744q08254811s202rs78s5536nnq5sq8p43sq64r797p9p9o0517no77\n
20 s8qqqop30p2955 60s8r4o2q9so0rr13122o160qq66912p06s5r7q9o8s886r3rss2p474nq4pq7r0\n
21 0p2955 719sr5q49p4or18325r7so47s12s79q18qsprq620s5n16p8p04pns6nn4pn2p19\n
22 0p2955 9p9qrr83s7605n0sn4942o741938s66o213o4r0o65o904s7s32n212s824q29r2\n
23 0q760r69n1 57o1s539p75sosn63nr51s11srpsn9sq75q505ooq5q109o0004887p796297961\n

```

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.



Input

```

8693j1833014967k49170473702gk104hik189k3i8hj5240990137919i9258
YKXBKX_NGTJYNGQK_ZXGLLOI_YKIXKZ
423h2959h2j315147k1i614588j5761j9k55kkgh7gjg854j1j9857j95jj1g65
10j151444j019580414kk43g3218872296j644540387393k831h768675h626
YKXBKX_ZXGLLOI_YKIXKZ_0 423h2959h2j315147k1i0614588j5761j9k55kkgh7gjg854j1j9857j95jj1g65
1kggg7i43484g2j83g087k0715175lj4j7ii659532il7814549g11k39klh1
IROKTZ_ZXGLLOI_YKIXKZ_0 423h2959h2j315147k1i0614588j5761j9k55kkgh7gjg854j1j9857j95jj1g65
4h07j028k411g536433gg42ghk4h2i9k4g31805gk70g18846j9g545j73lge278
IROKTZ_NGTJYNGQK_ZXGLLOI_YKIXKZ
74h3i094h6779jg1lk4g6k7i1304h2gi5kh5939125741g78j589i410870861
j2h454i9345115g3jglkgi561g838jg09g5h5h44g02k1508j51h15k6kkkj6gk
YKXBKX_NGTJYNGQK_ZXGLLOI_YKIXKZ
74h3i094h6779jg1lk4g6k7i1304h2gi5kh5939125741g78j589i410870861
1041j74228598278h1l591h66j74hj4j6g4j640ilij5hij67gjh9iilkj8146j
YKXBKX_ZXGLLOI_YKIXKZ_0 74h3i094h6779jg1lk4g6k7i1304h2gi5kh5939125741g78j589i410870861
1ig81hhnjng5h8i1l26h317h4ig971

```

Output

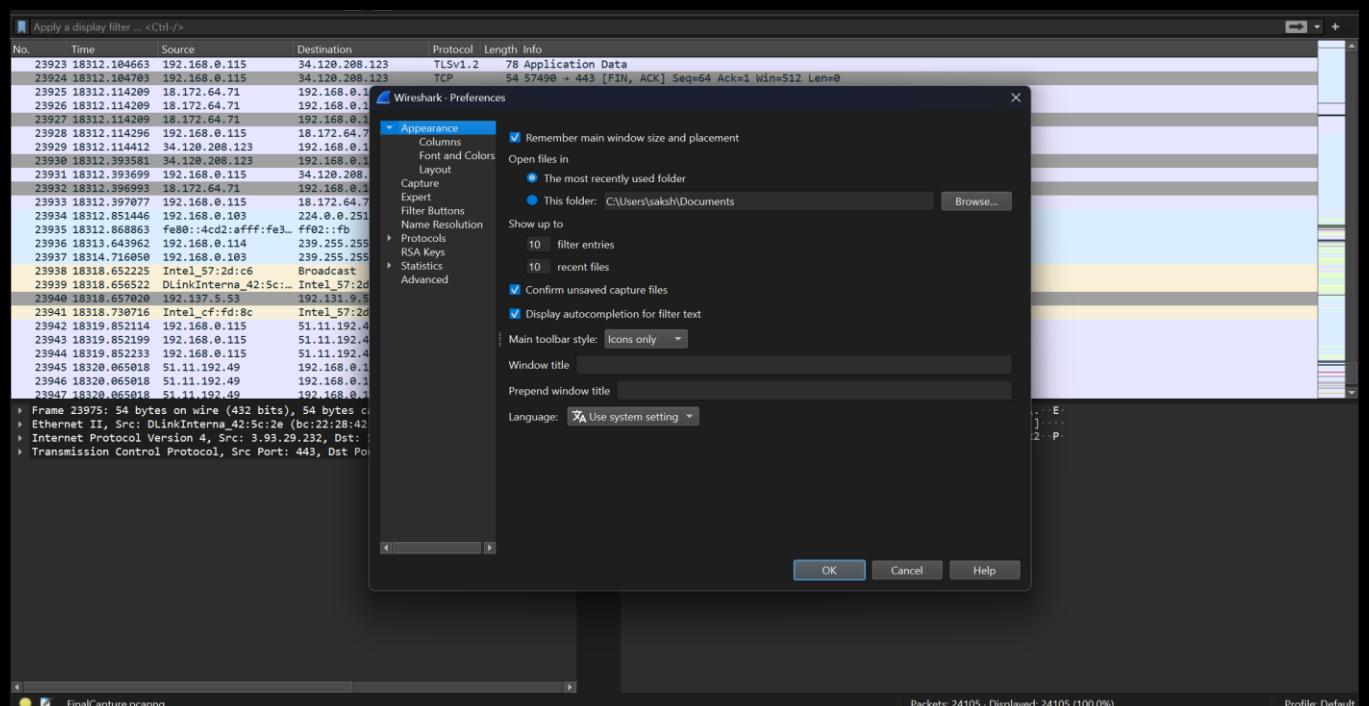
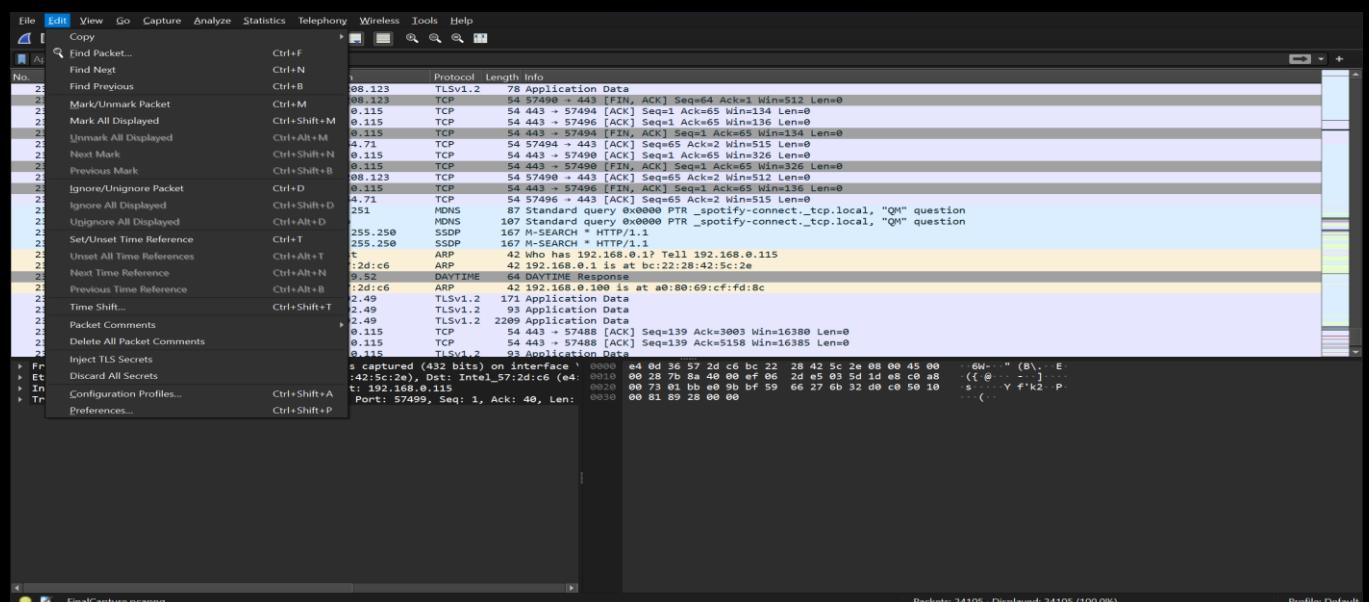
```

SERVER_HANDSHAKE_TRAFFIC_SECRET
ca24cfbb0661e5e8ceb9292ac81a41a7a58f04a29294d23e23d11fb65911a6df
7ec8e309898dece3c7d68e8b14d99265fc761ebca7a727595f16aed411fbc06
SERVER_TRAFFIC_SECRET_0 ca24cfbb0661e5e8ceb9292ac81a41a7a58f04a29294d23e23d11fb65911a6df
db83128fe7c5a7a73ea2de7898dacfc467121c2beccedfd271e9a45259ca123
CLIENT_TRAFFIC_SECRET_0 ca24cfbb0661e5e8ceb9292ac81a41a7a58f04a29294d23e23d11fb65911a6df
a7a60399613d0c6b0ac2283d3ff0d7a60ecd5dd9293b152cc8d476eb2e4d49fb
CLIENT_HANDSHAKE_TRAFFIC_SECRET
33c68750d1bdffbbde0cc93c5cb9235a3653787cbe353e2df5712253a162d99f5
55b9076cd2b496d0e1310320f7ec01460d1f4051f716618fe8ddfb2b5a1727
SERVER_HANDSHAKE_TRAFFIC_SECRET
33c68750d1bdffbbde0cc93c5cb9235a3653787cbe353e2df5712253a162d99f5
4295f9ba7ad744120c5876534784640c0a86f079f99914453bf9aad3b924074
SERVER_TRAFFIC_SECRET_0 33c68750d1bdffbbde0cc93c5cb9235a3653787cbe353e2df5712253a162d99f5
09def11fb773da579c53e1bf874ebabfb79de8330d64b998628ffff16f6bb33
CLIENT_TRAFFIC_SECRET_0 33c68750d1bdffbbde0cc93c5cb9235a3653787cbe353e2df5712253a162d99f5

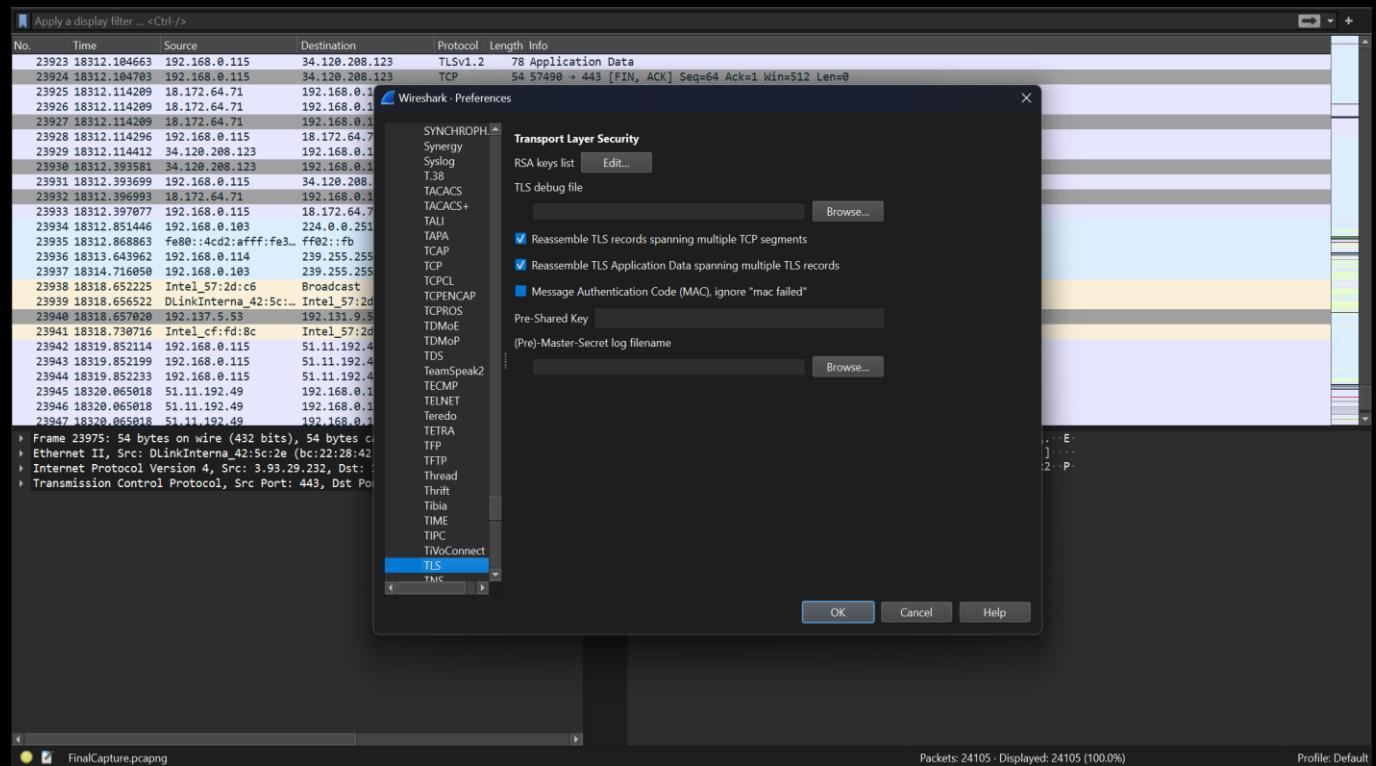
```

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 :

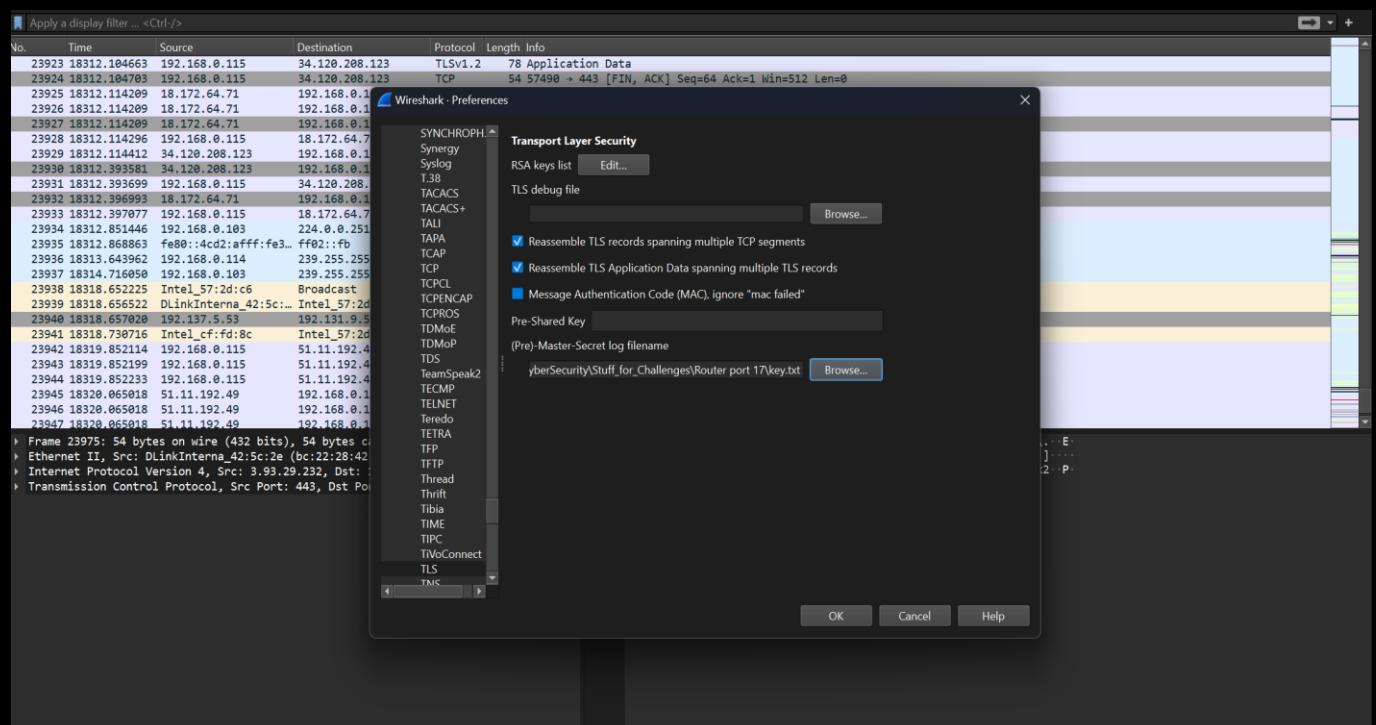
1) Click the edit tab and click preferences .



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

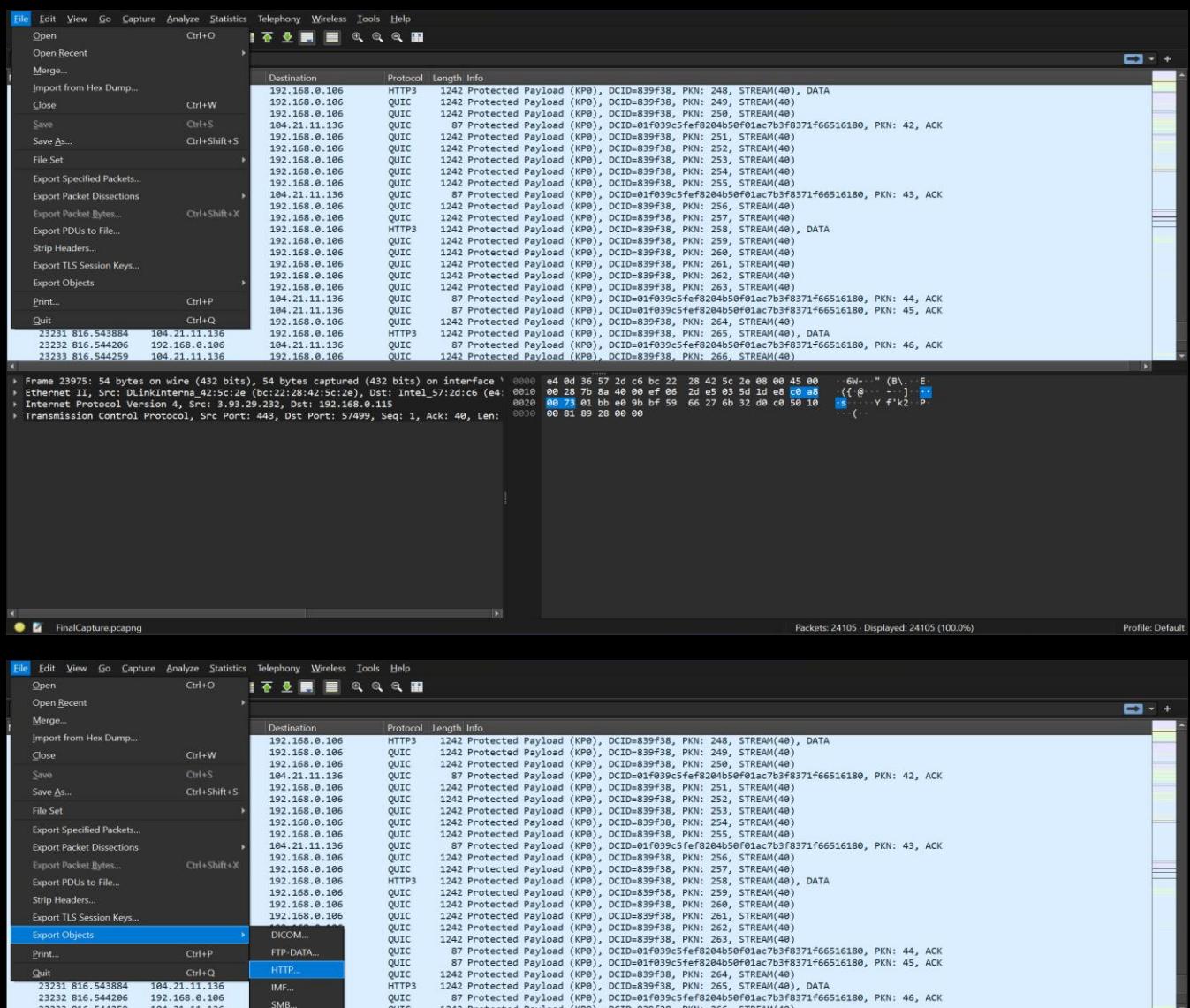


3) Finally add the decrypted SSL key to decrypt the captured packets .

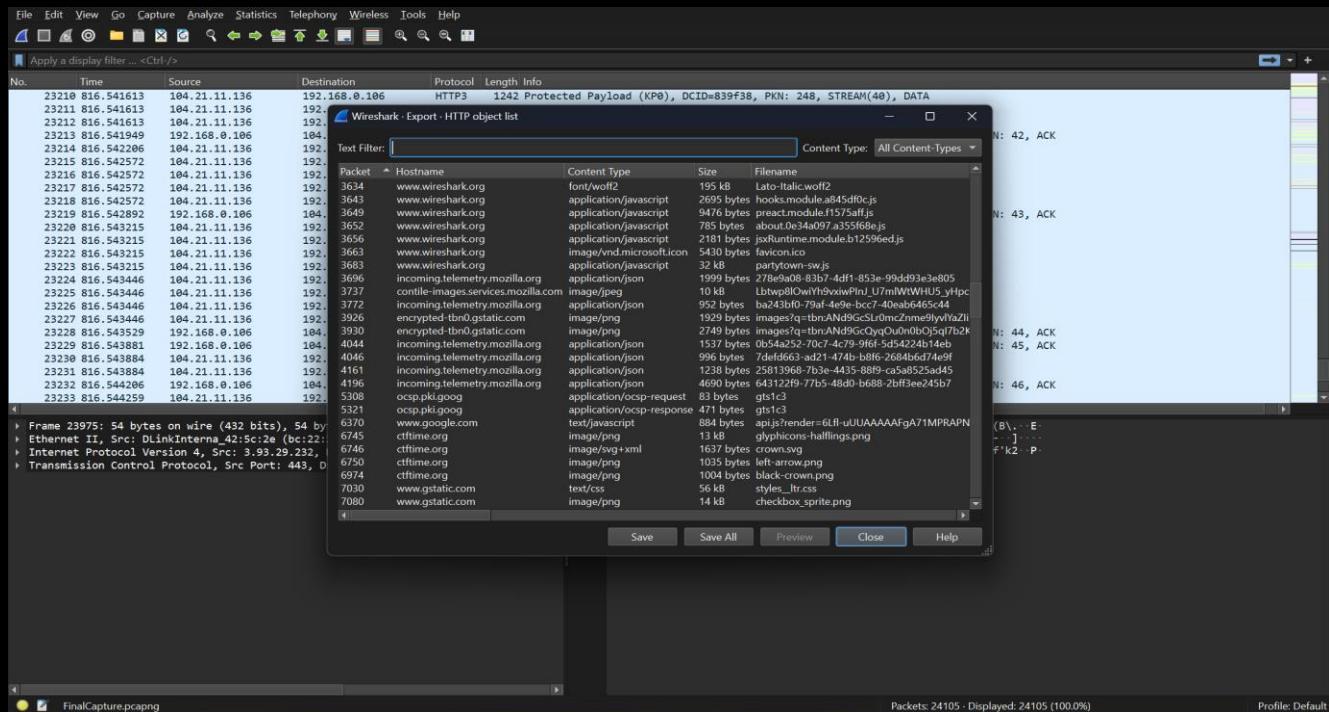


Step 6 :- Now, since the packets are decrypted, just look for the objects captured in this file. To do so, follow the steps below :

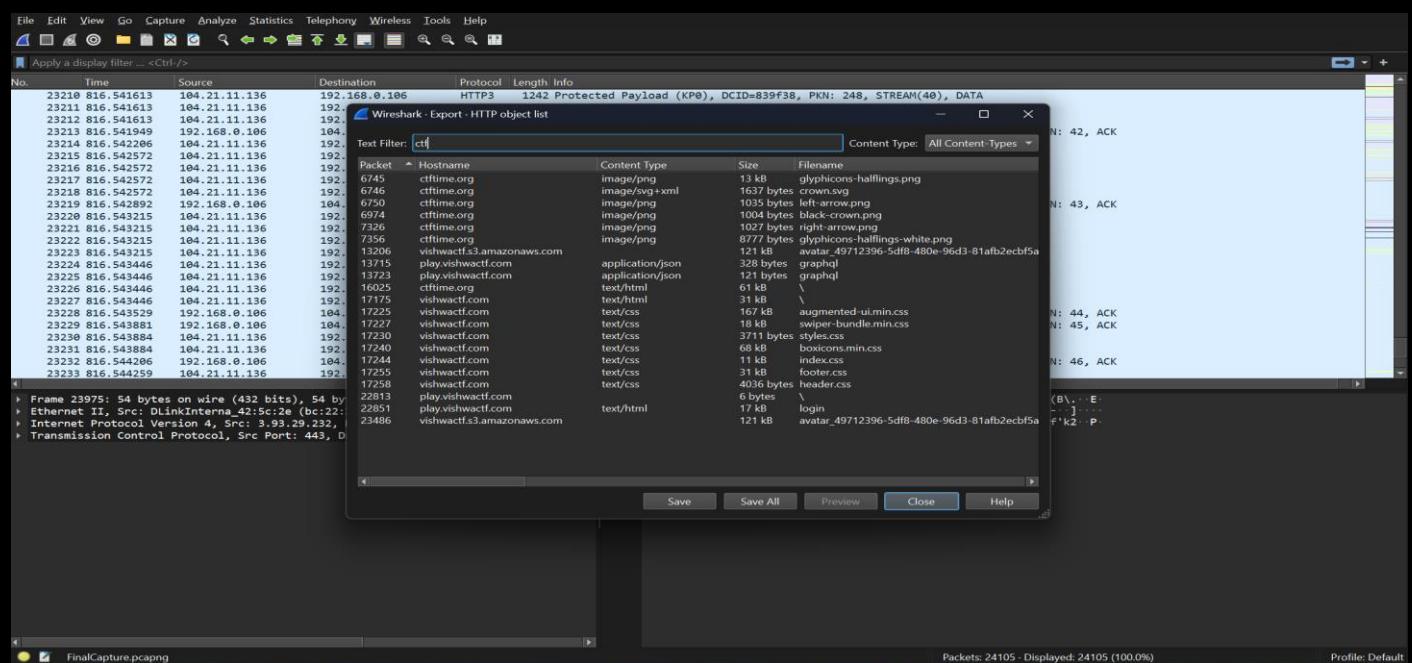
1) Click the "File" tab, and under "Export Objects," select 'HTTP'.



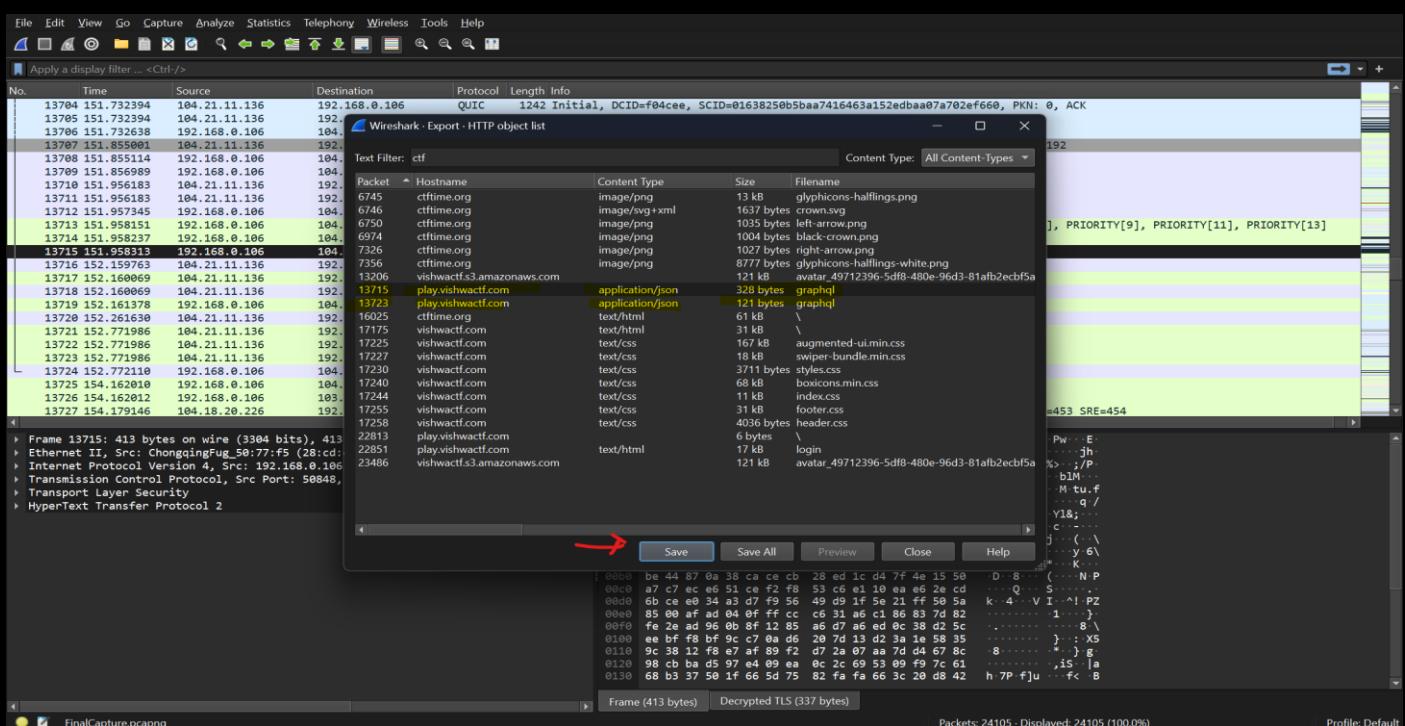
2) Now you can see various objects captured in this file .



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' .

```
graphql {graphql_2}
graphql
1 1 {"query": "mutation ($username: String!, $password: String!) {\n    (username: $username, password: $password) {\n        id\n        username\n        name\n        type\n    }\n},\n    \"variables\": {\n        \"username\": \"Anonymous\", \"password\": \"K3Y5_CAN_OP3N_10CK5\" }\n}"}
```

Flag :- VishwaCTF{K3Y5_CAN_OP3N_10CK5 }