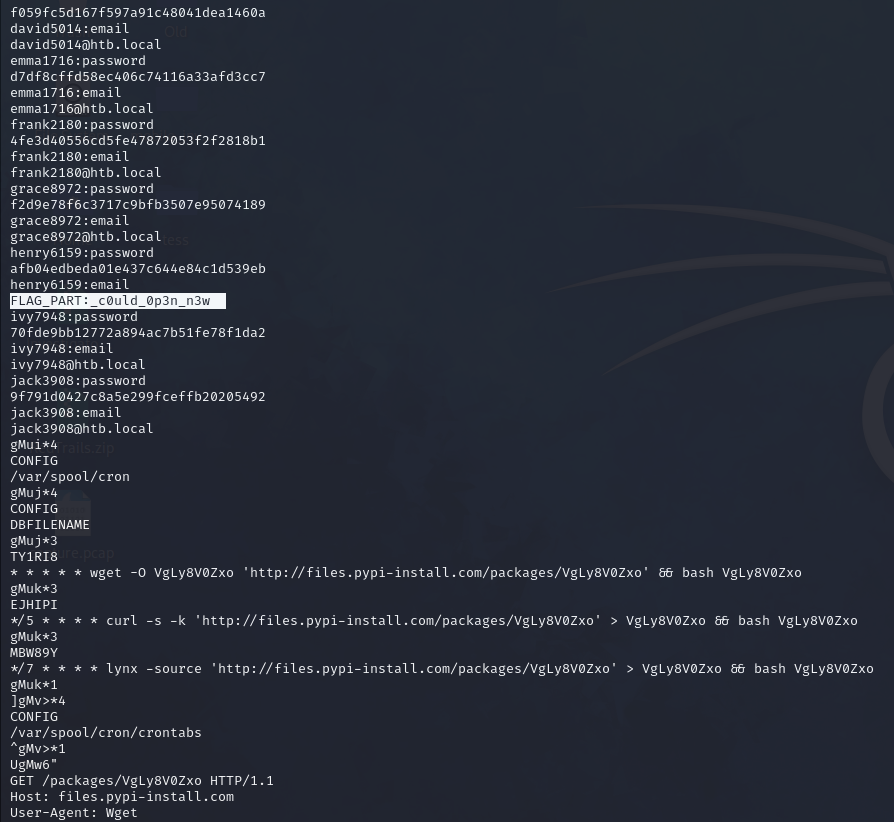
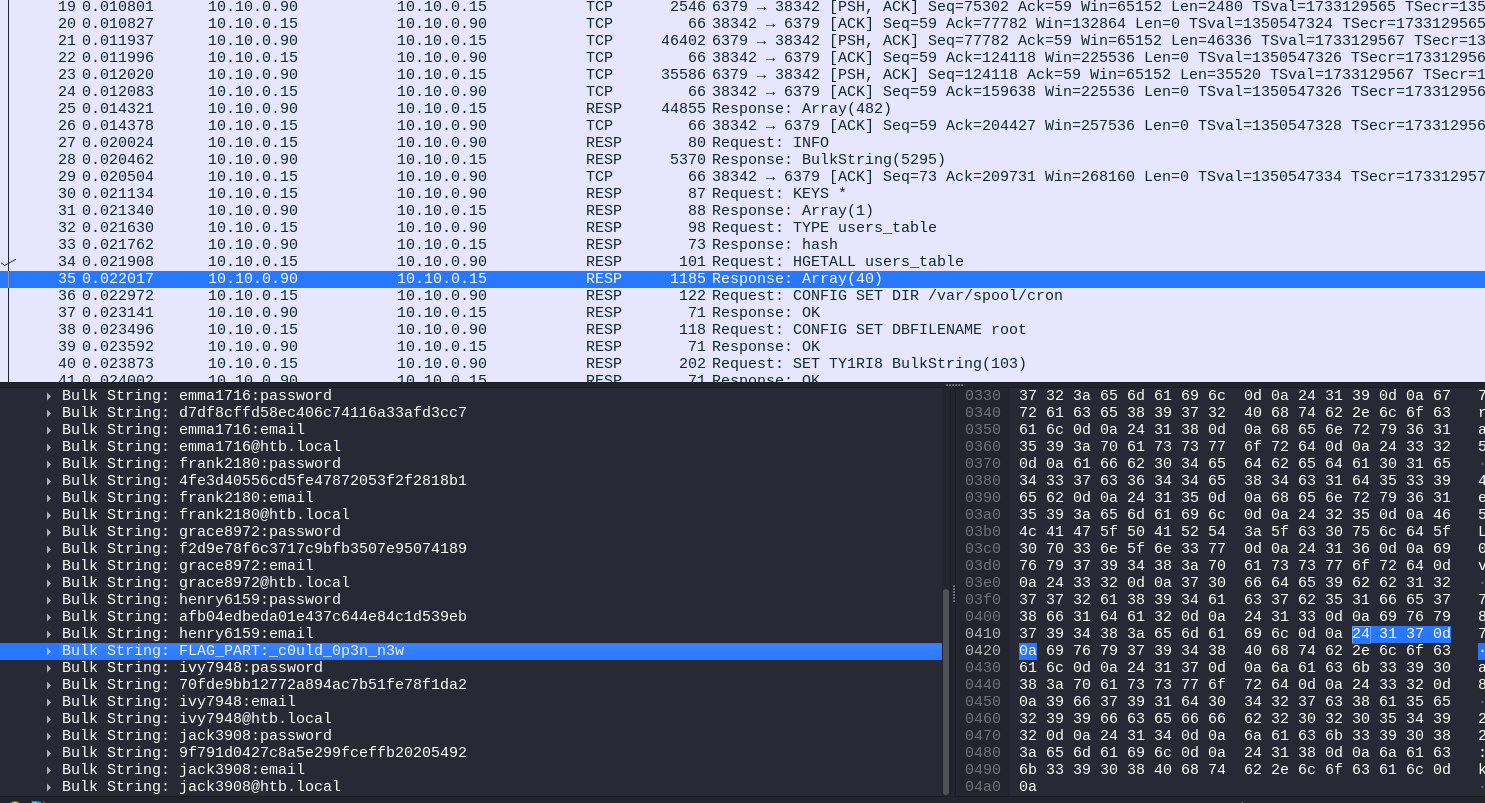
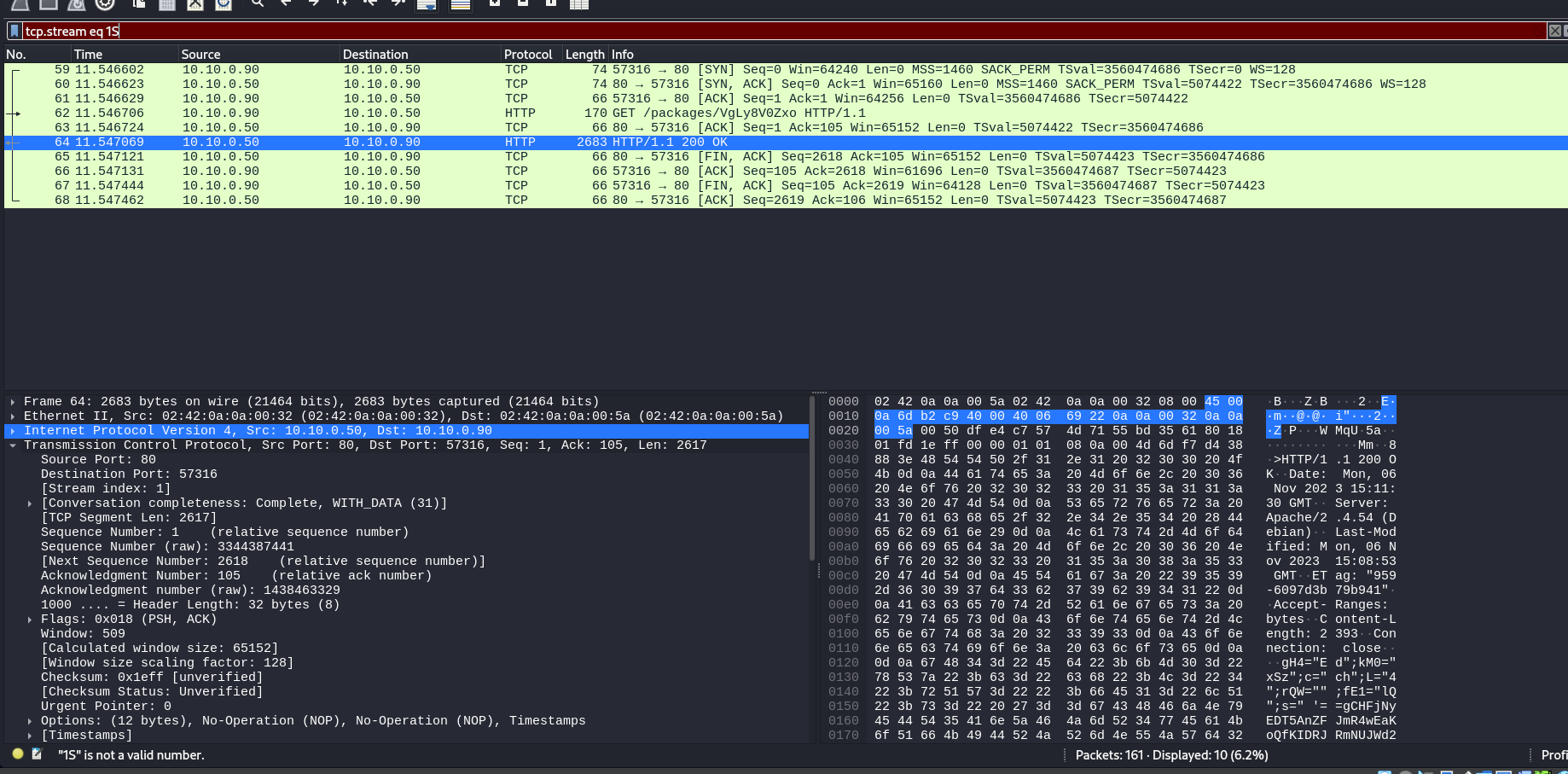
Red Trails

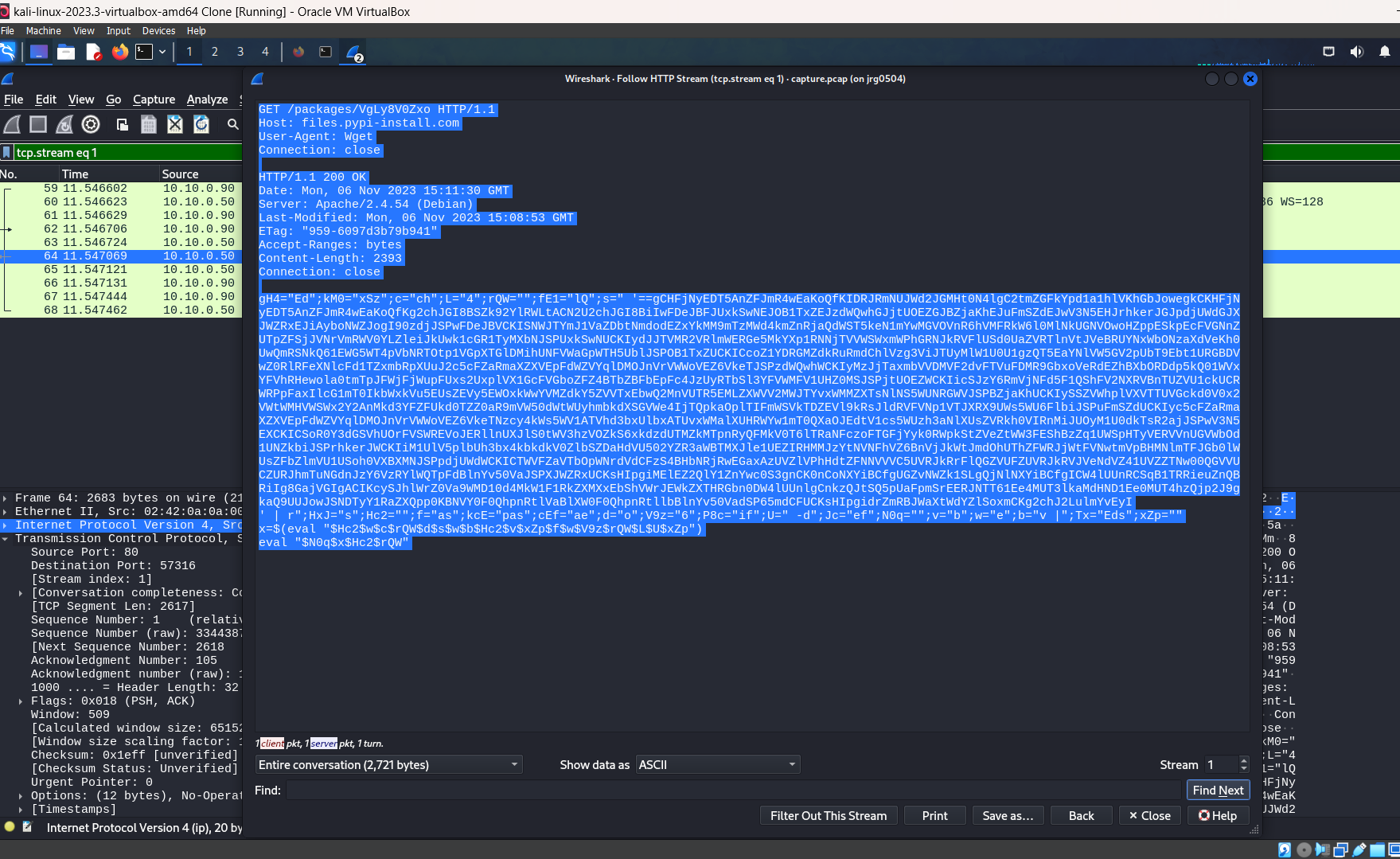
Using command : strings –n 6 capture.pcap



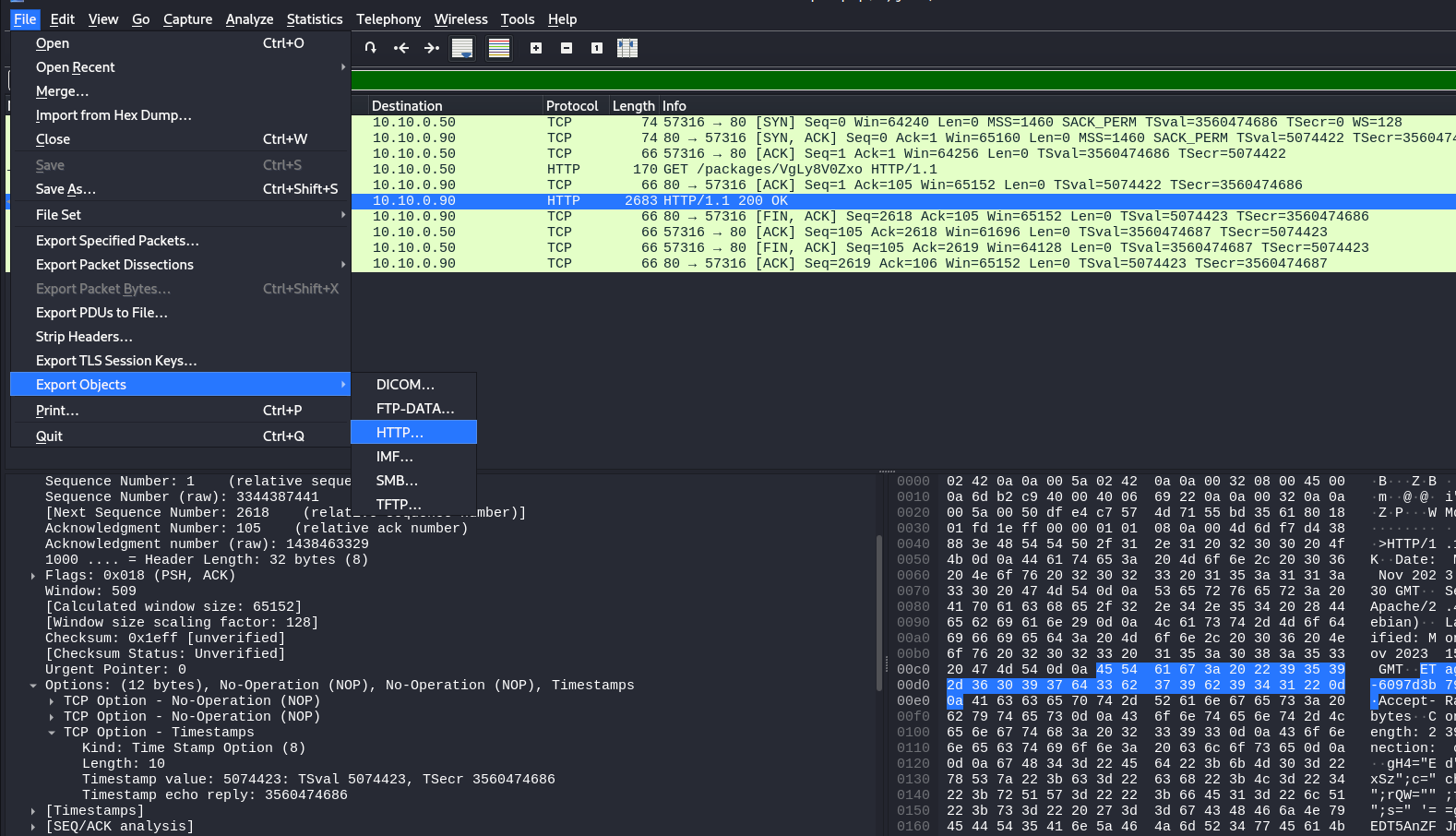
We found part 1 of 3 of the flag.

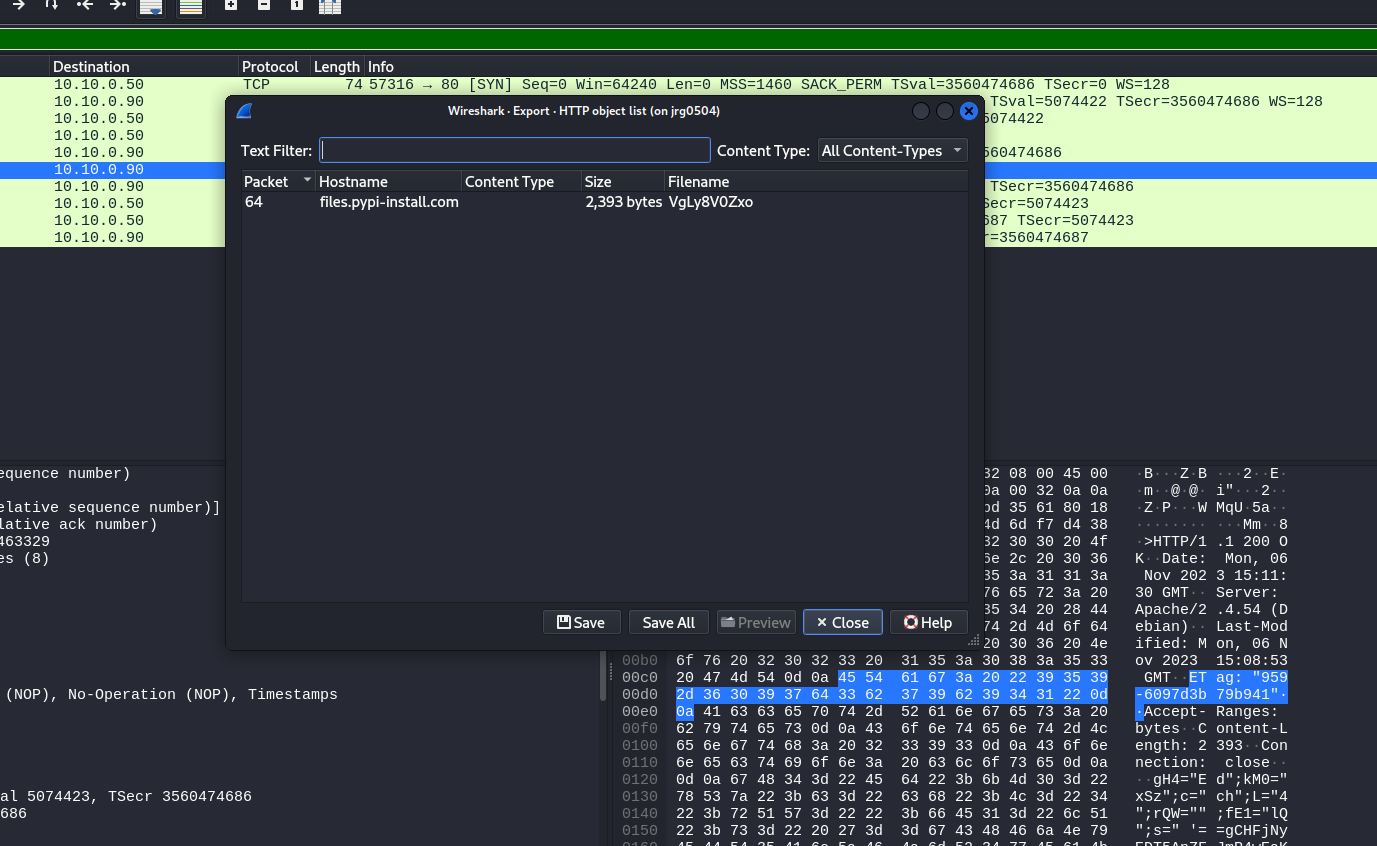
Using wireshark and looking for the packets which using Redis protocol:  


Found encoded text which is sent using http, which we found odd due it length for server status request:  




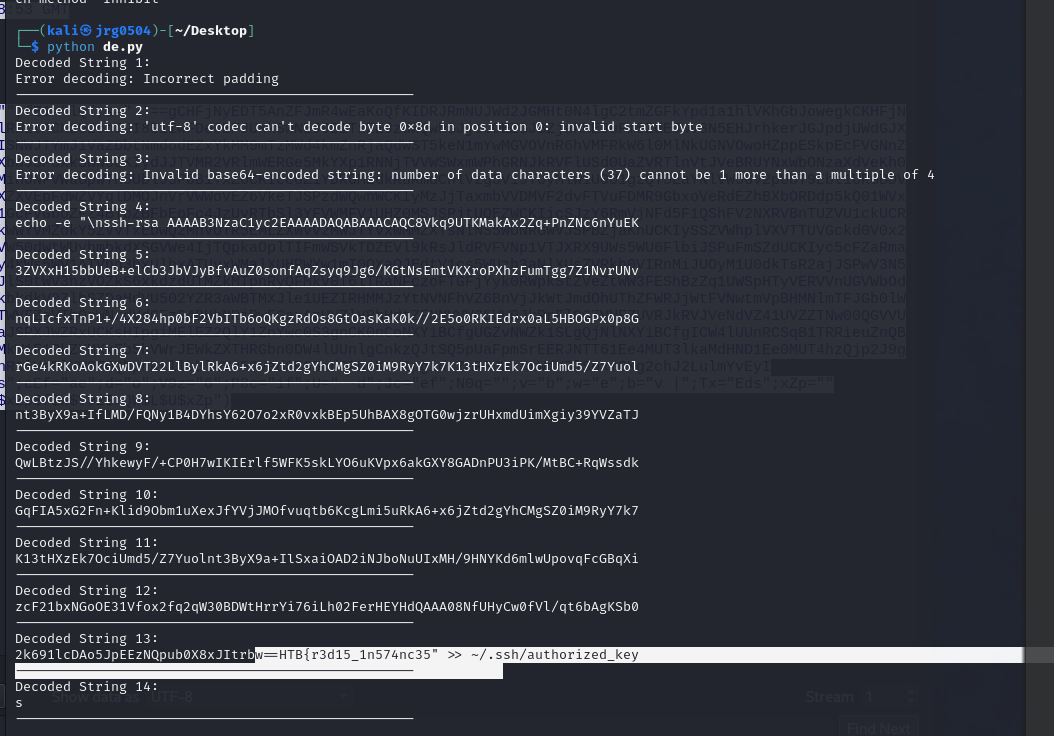
Now we exported the http packet which is transferred as a part of request.





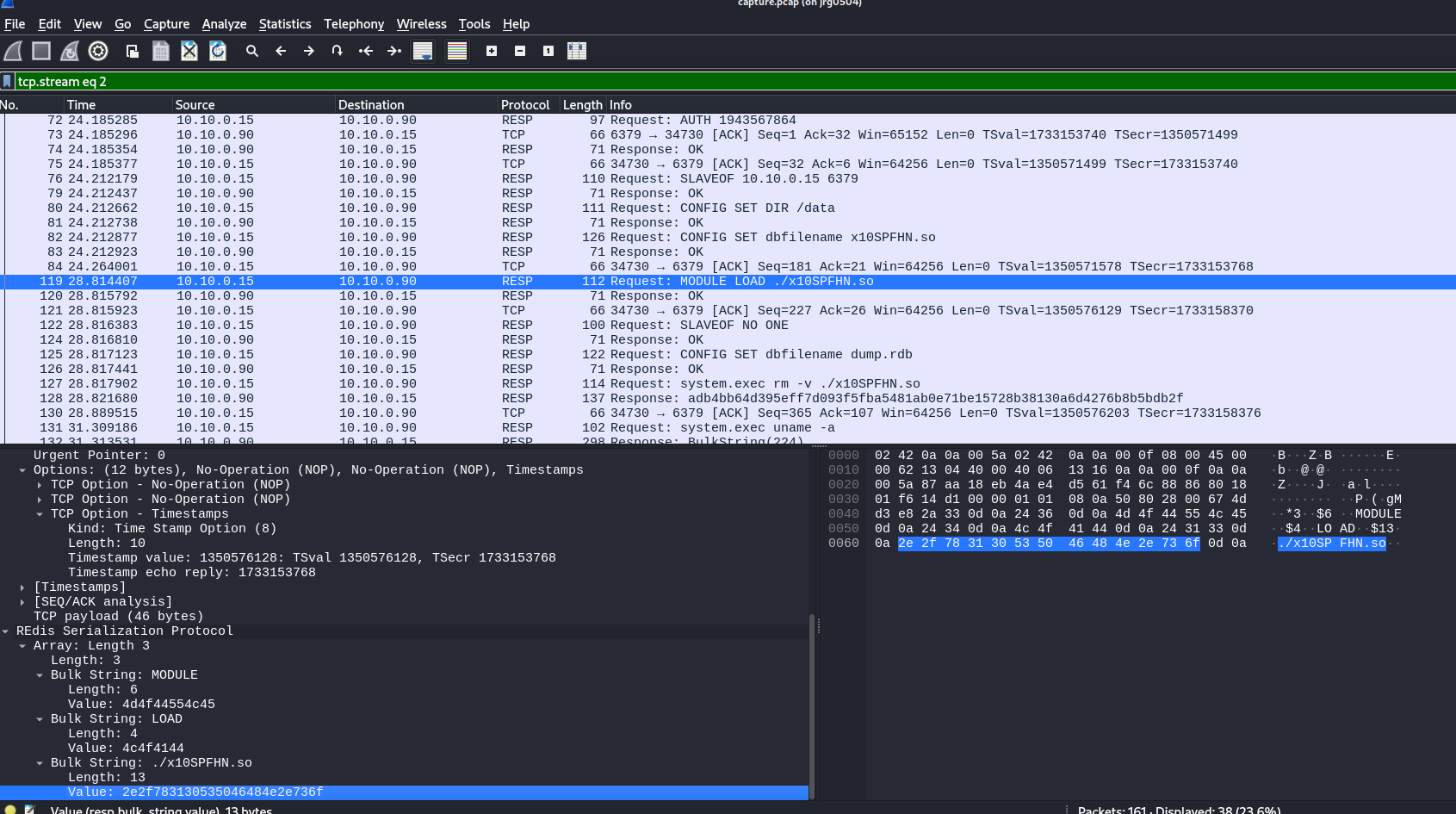


Used chatgpt to write a program to decode the above base64 text and we are able to get the other part of the flag.



So, we found part 2 of the 3 of the flag.

Something is loaded



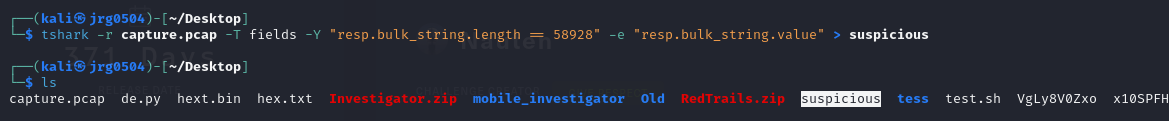
We found following string : “%2hhx

h02B6aVgu09Kzu9QTvTOtgx9oER9WIoz

YDP7ECjzuV7sagMN

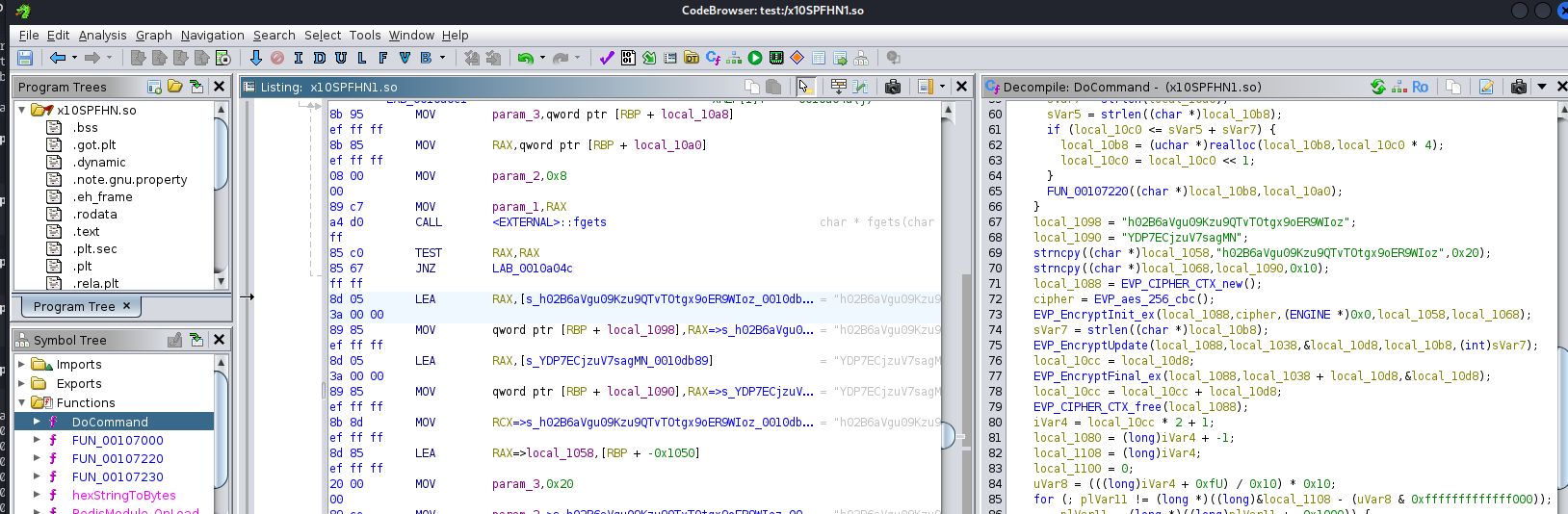
%02x” which looked odd.

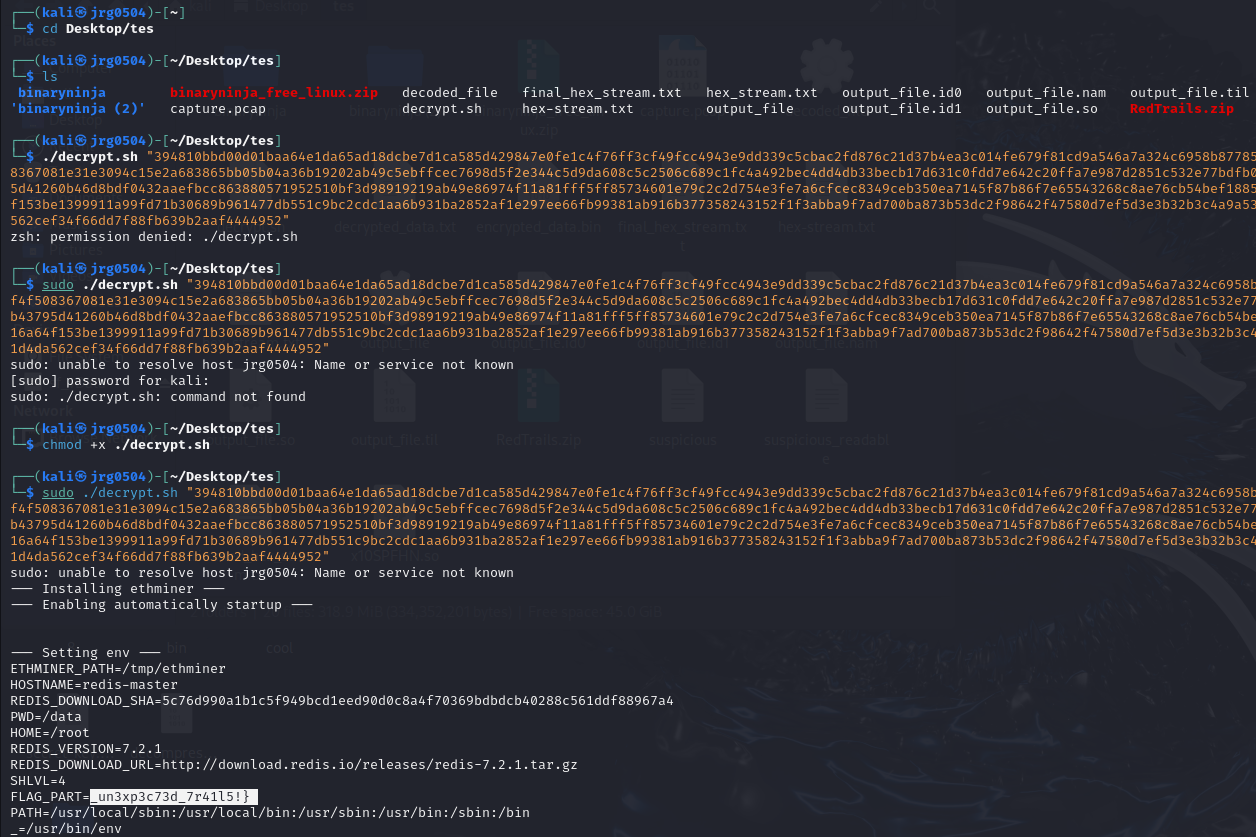
So, we the below command and saved the packet in a separate file.



After going to through the suspicious file and though of decompiling the file. So we went back to wireshark and saved the payload as hexadecimal stream and created the sharable object file and opened it using ghindra decompiler for decompiling the code.

Below is the code and in one of the function called do command we can see key and iv used by the aes crypto algorithm which are used to encrypt something when transferring the data.



Now created bash file to decrypyt the payload using the key and iv we found and we finally found the last part of the key:  


Decrypt.sh code:

#!/bin/bash

# Convert key and iv to hex

key="$(echo 'h02B6aVgu09Kzu9QTvTOtgx9oER9WIoz' | tr -d '\n'| xxd -p | xargs | tr -d '\ ')"

IV="$(echo 'YDP7ECjzuV7sagMN' | tr -d '\n'| xxd -p | xargs)"

echo "$1" | xxd -r -p > encrypted\_data.bin

# Decrypt using OpenSSL

openssl enc -aes-256-cbc -d -in encrypted\_data.bin -out decrypted\_data.txt -K "$key" -iv "$IV" -nopad

cat ./decrypted\_data.txt