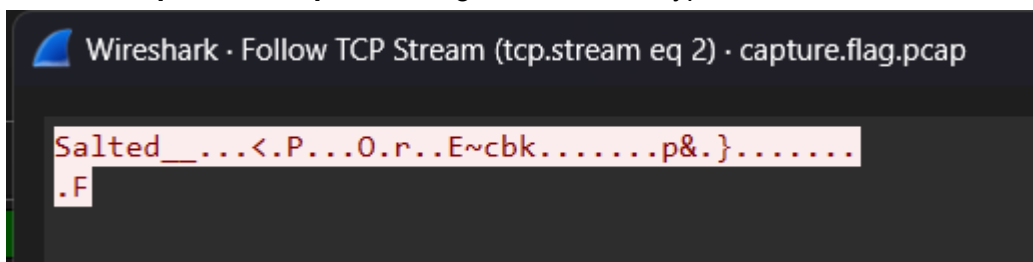


Looking through TCP Streams, I found these messages in **tcp.stream eq 0** (you can see how many TCP and UDP streams are to Statistics -> Conversations) :

```
Hey, how do you decrypt this file again?
You're serious?
Yeah, I'm serious
*sig* openssl des3 -d -salt -in file.des3 -out file.txt -k supersecretpassword123
Ok, great, thanks.
Let's use Discord next time, it's more secure.
C'mon, no one knows we use this program like this!
Whatever.
Hey.
Yeah?
Could you transfer the file to me again?
Oh great. Ok, over 9002?
Yeah, listening.
Sent it
Got it.
You're unbelievable
```

Now, in **tcp.stream eq 2** we can get a salted encrypted text :



We need to save the text as **Hex Stream** and put the hex in Cyberchef and save the file to get the original content of the file, like this :

```
53616c7465645f5fd30c863ca650da1fff4fbe72a086457e63626beda615c692cdd27026ae7deea6d1e918b3d40a7f46
```

REC 96 1

Tr Raw Bytes LI

Output

```
Salted__0FF•<|PÚusŷ0%r•E~cbkí|NAKÆ•f0p&@}i|ñéCAN³0  
•F
```

If we save the file as **file.des3** and run the command mentioned in the first TCP stream, we can get the flag in a file named **file.txt** :

```
openssl des3 -d -salt -in d.des3 -out file.txt -k supersecretpassword123
```

THE FLAG : picoCTF{nc_73115_411_5786acc3}

~Z4que