Description

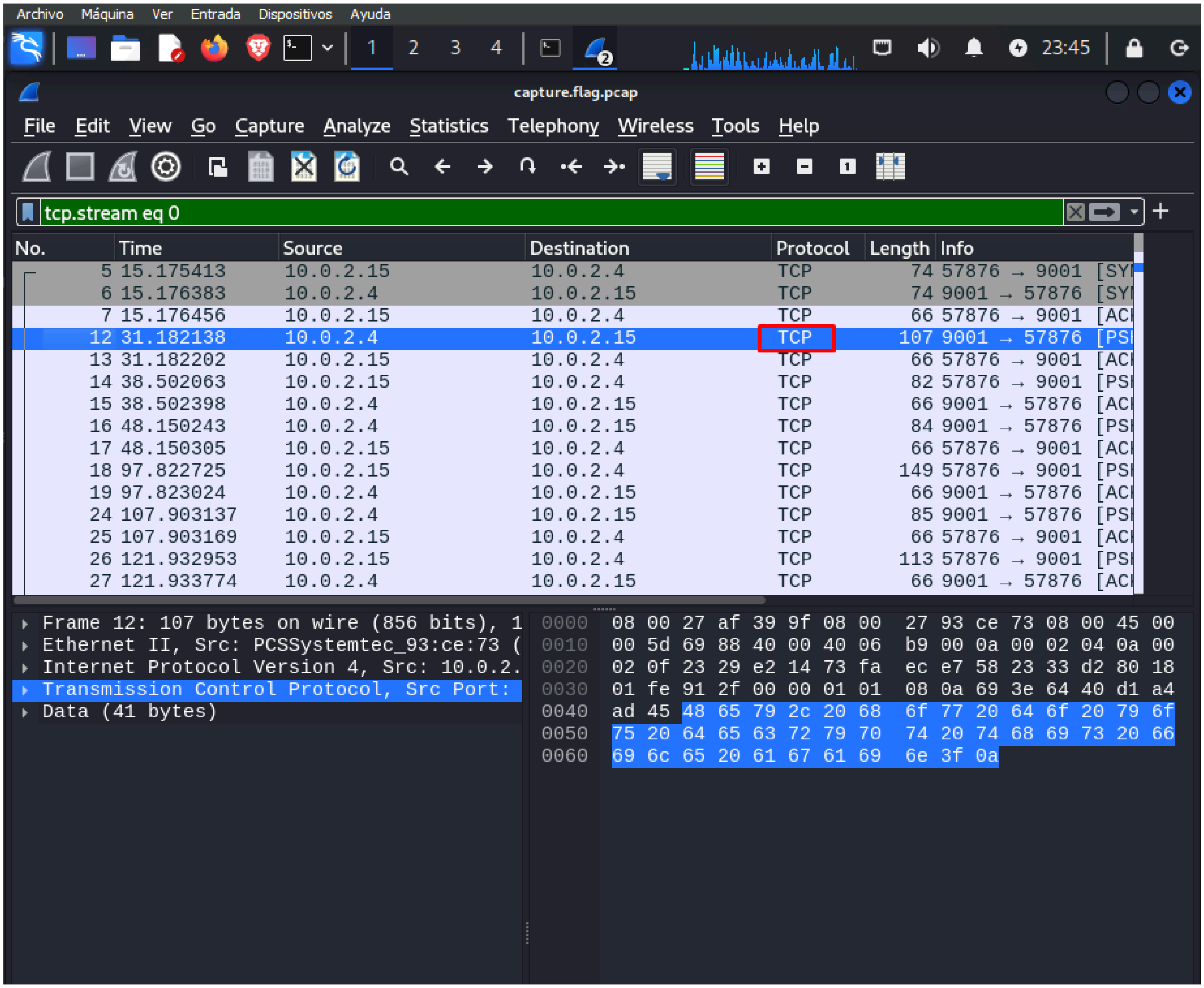
Download this packet capture and find the flag.

- [Download packet capture]

Hints

- All we know is that this packet capture includes a chat conversation and a file transfer.

Solución

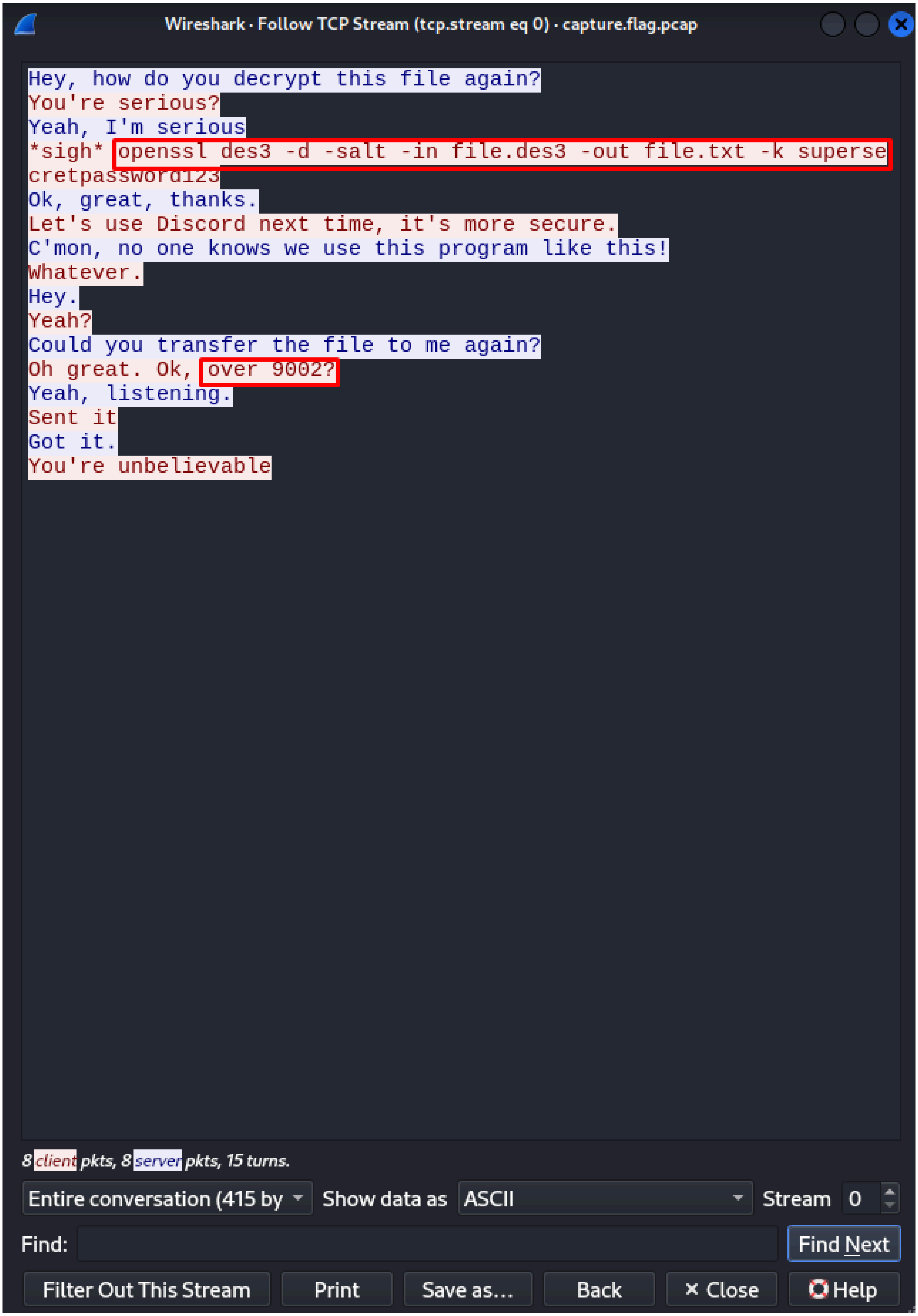

Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
23:45
capture.flag.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.stream eq 0

No.  Time         Source       Destination  Protocol  Length Info
   5 15.175413    10.0.2.15    10.0.2.4     TCP           74 57876 → 9001 [SY
   6 15.176383    10.0.2.4     10.0.2.15    TCP           74 9001 → 57876 [SY
   7 15.176456    10.0.2.15    10.0.2.4     TCP           66 57876 → 9001 [AC
  12 31.182138    10.0.2.4     10.0.2.15    TCP          107 9001 → 57876 [PS
  13 31.182202    10.0.2.15    10.0.2.4     TCP           66 57876 → 9001 [AC
  14 38.502063    10.0.2.15    10.0.2.4     TCP           82 57876 → 9001 [PS
  15 38.502398    10.0.2.4     10.0.2.15    TCP           66 9001 → 57876 [AC
  16 48.150243    10.0.2.4     10.0.2.15    TCP           84 9001 → 57876 [PS
  17 48.150305    10.0.2.15    10.0.2.4     TCP           66 57876 → 9001 [AC
  18 97.822725    10.0.2.15    10.0.2.4     TCP          149 57876 → 9001 [PS
  19 97.823024    10.0.2.4     10.0.2.15    TCP           66 9001 → 57876 [AC
  24 107.903137   10.0.2.4     10.0.2.15    TCP           85 9001 → 57876 [PS
  25 107.903169   10.0.2.15    10.0.2.4     TCP           66 57876 → 9001 [AC
  26 121.932953   10.0.2.15    10.0.2.4     TCP          113 57876 → 9001 [PS
  27 121.933774   10.0.2.4     10.0.2.15    TCP           66 9001 → 57876 [AC
```

```
› Frame 12: 107 bytes on wire (856 bits), 1
› Ethernet II, Src: PCSSystemtec_93:ce:73 (
› Internet Protocol Version 4, Src: 10.0.2.
› Transmission Control Protocol, Src Port:
› Data (41 bytes)
```

```
0000  08 00 27 af 39 9f 08 00  27 93 ce 73 08 00 45 00
0010  00 5d 69 88 40 00 40 06  b9 00 0a 00 02 04 0a 00
0020  02 0f 23 29 e2 14 73 fa  ec e7 58 23 33 d2 80 18
0030  01 fe 91 2f 00 00 01 01  08 0a 69 3e 64 40 d1 a4
0040  ad 45 48 65 79 2c 20 68  6f 77 20 64 6f 20 79 6f
0050  75 20 64 65 63 72 79 70  74 20 74 68 69 73 20 66
0060  69 6c 65 20 61 67 61 69  6e 3f 0a
```

Abrimos `wireshark` y el `.pcap`, para comenzar a revisar los paquetes.

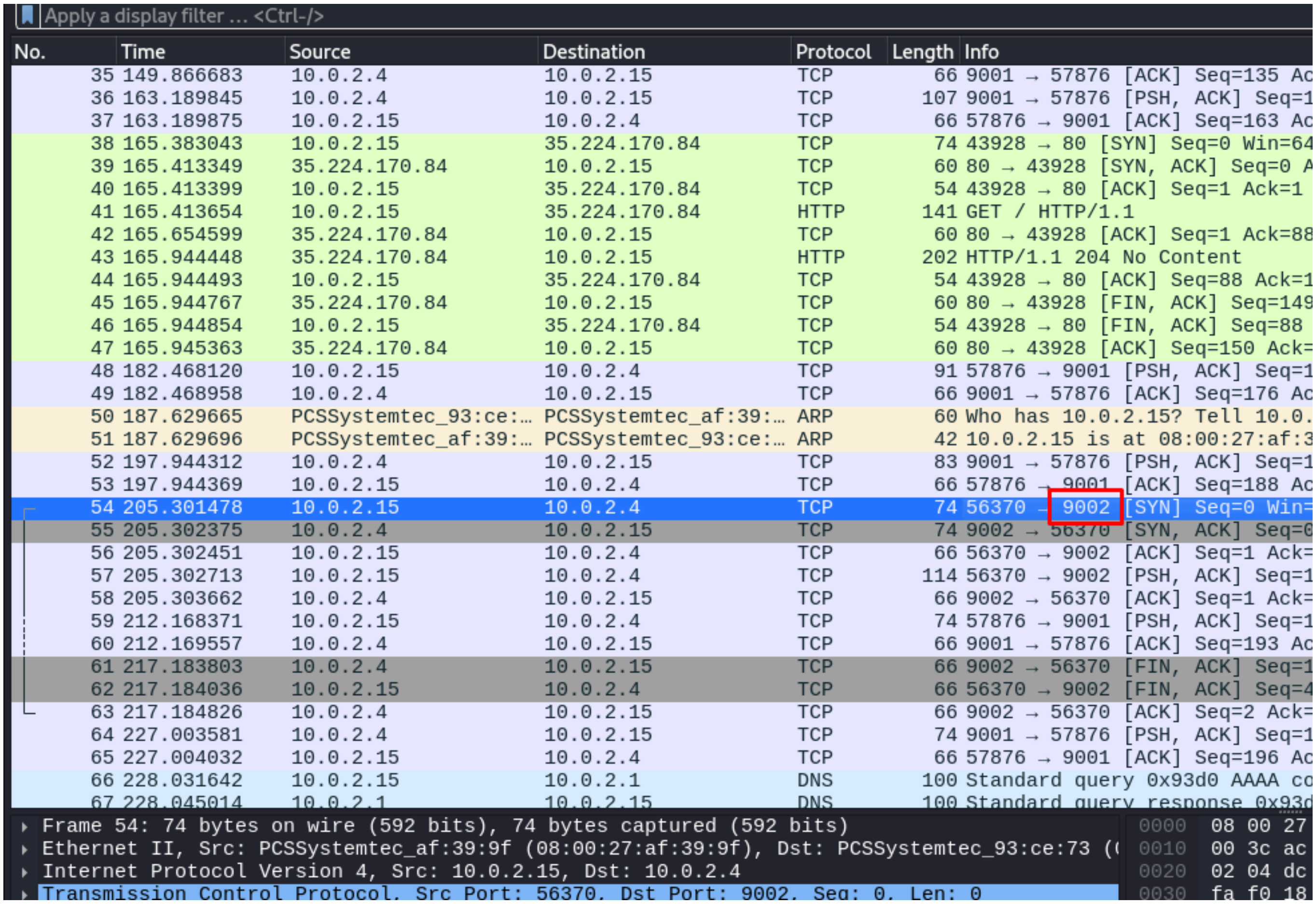

Wireshark · Follow TCP Stream (tcp.stream eq 0) · capture.flag.pcap
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
✕ Close
Help

```
Hey, how do you decrypt this file again?
You're serious?
Yeah, I'm serious
*sigh* openssl des3 -d -salt -in file.des3 -out file.txt -k superse
cretpassword123
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
```

8 client pkts, 8 server pkts, 15 turns.

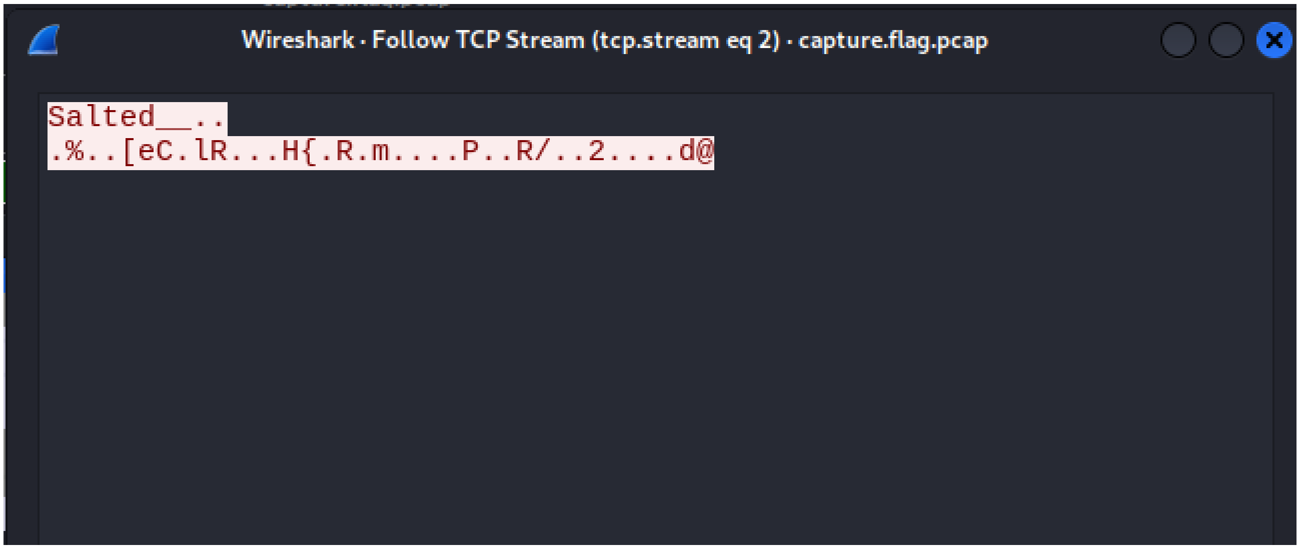
Entire conversation (415 by · Show data as: ASCII · Stream: 0

Se detecta esta conversación donde obtenemos un comando para desencriptar y un puerto donde se mandó un paquete que nos puede interesar.



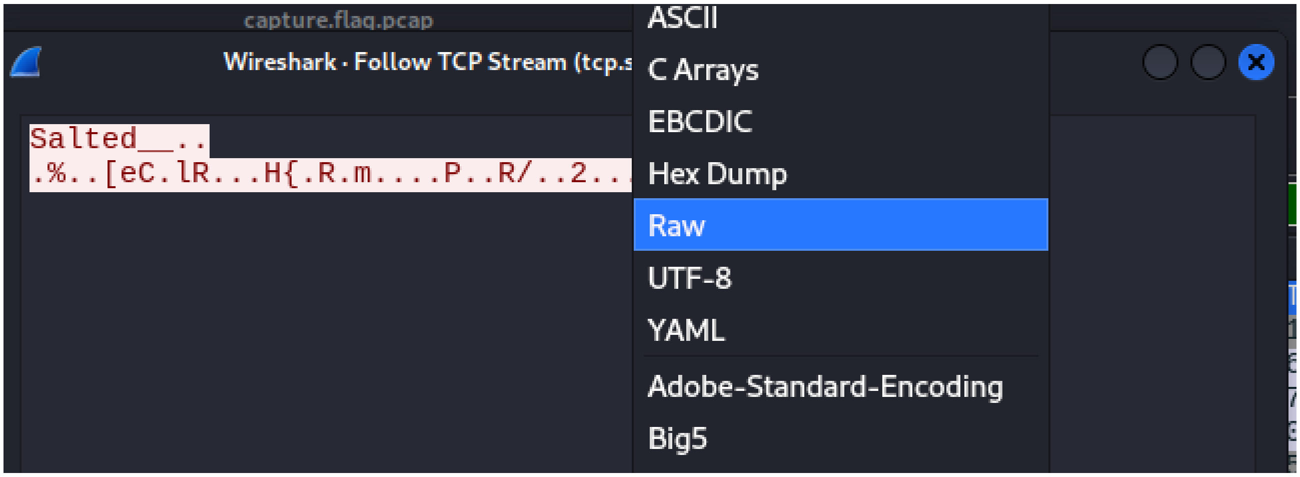
```
Apply a display filter … <Ctrl-/>
No.   Time          Source                 Destination            Protocol Length Info
   35 149.866683    10.0.2.4               10.0.2.15              TCP        66 9001 → 57876 [ACK] Seq=135 Ac
   36 163.189845    10.0.2.4               10.0.2.15              TCP       107 9001 → 57876 [PSH, ACK] Seq=1
   37 163.189875    10.0.2.15              10.0.2.4               TCP        66 57876 → 9001 [ACK] Seq=163 Ac
   38 165.383043    10.0.2.15              35.224.170.84          TCP        74 43928 → 80 [SYN] Seq=0 Win=64
   39 165.413349    35.224.170.84          10.0.2.15              TCP        60 80 → 43928 [SYN, ACK] Seq=0 A
   40 165.413399    10.0.2.15              35.224.170.84          TCP        54 43928 → 80 [ACK] Seq=1 Ack=1
   41 165.413654    10.0.2.15              35.224.170.84          HTTP      141 GET / HTTP/1.1
   42 165.654599    35.224.170.84          10.0.2.15              TCP        60 80 → 43928 [ACK] Seq=1 Ack=88
   43 165.944448    35.224.170.84          10.0.2.15              HTTP      202 HTTP/1.1 204 No Content
   44 165.944493    10.0.2.15              35.224.170.84          TCP        54 43928 → 80 [ACK] Seq=88 Ack=1
   45 165.944767    35.224.170.84          10.0.2.15              TCP        60 80 → 43928 [FIN, ACK] Seq=149
   46 165.944854    10.0.2.15              35.224.170.84          TCP        54 43928 → 80 [FIN, ACK] Seq=88
   47 165.945363    35.224.170.84          10.0.2.15              TCP        60 80 → 43928 [ACK] Seq=150 Ack=
   48 182.468120    10.0.2.15              10.0.2.4               TCP        91 57876 → 9001 [PSH, ACK] Seq=1
   49 182.468958    10.0.2.4               10.0.2.15              TCP        66 9001 → 57876 [ACK] Seq=176 Ac
   50 187.629665    PCSSystemtec_93:ce:…   PCSSystemtec_af:39:…   ARP        60 Who has 10.0.2.15? Tell 10.0.
   51 187.629696    PCSSystemtec_af:39:…   PCSSystemtec_93:ce:…   ARP        42 10.0.2.15 is at 08:00:27:af:3
   52 197.944312    10.0.2.4               10.0.2.15              TCP        83 9001 → 57876 [PSH, ACK] Seq=1
   53 197.944369    10.0.2.15              10.0.2.4               TCP        66 57876 → 9001 [ACK] Seq=188 Ac
   54 205.301478    10.0.2.15              10.0.2.4               TCP        74 56370 → 9002 [SYN] Seq=0 Win=
   55 205.302375    10.0.2.4               10.0.2.15              TCP        74 9002 → 56370 [SYN, ACK] Seq=0
   56 205.302451    10.0.2.15              10.0.2.4               TCP        66 56370 → 9002 [ACK] Seq=1 Ack=
   57 205.302713    10.0.2.15              10.0.2.4               TCP       114 56370 → 9002 [PSH, ACK] Seq=1
   58 205.303662    10.0.2.4               10.0.2.15              TCP        66 9002 → 56370 [ACK] Seq=1 Ack=
   59 212.168371    10.0.2.15              10.0.2.4               TCP        74 57876 → 9001 [PSH, ACK] Seq=1
   60 212.169557    10.0.2.4               10.0.2.15              TCP        66 9001 → 57876 [ACK] Seq=193 Ac
   61 217.183803    10.0.2.4               10.0.2.15              TCP        66 9002 → 56370 [FIN, ACK] Seq=1
   62 217.184036    10.0.2.15              10.0.2.4               TCP        66 56370 → 9002 [FIN, ACK] Seq=4
   63 217.184826    10.0.2.4               10.0.2.15              TCP        66 9002 → 56370 [ACK] Seq=2 Ack=
   64 227.003581    10.0.2.4               10.0.2.15              TCP        74 9001 → 57876 [PSH, ACK] Seq=1
   65 227.004032    10.0.2.15              10.0.2.4               TCP        66 57876 → 9001 [ACK] Seq=196 Ac
   66 228.031642    10.0.2.15              10.0.2.1               DNS       100 Standard query 0x93d0 AAAA co
   67 228.045014    10.0.2.1               10.0.2.15              DNS       100 Standard query response 0x93d

› Frame 54: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)                    0000  08 00 27
› Ethernet II, Src: PCSSystemtec_af:39:9f (08:00:27:af:39:9f), Dst: PCSSystemtec_93:ce:73 (( 0010  00 3c ac
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4                             0020  02 04 dc
› Transmission Control Protocol, Src Port: 56370, Dst Port: 9002, Seq: 0, Len: 0          0030  fa f0 18
```

Seguimos el stream con el puerto `9002` para inspeccionarlo.



Wireshark · Follow TCP Stream (tcp.stream eq 2) · capture.flag.pcap

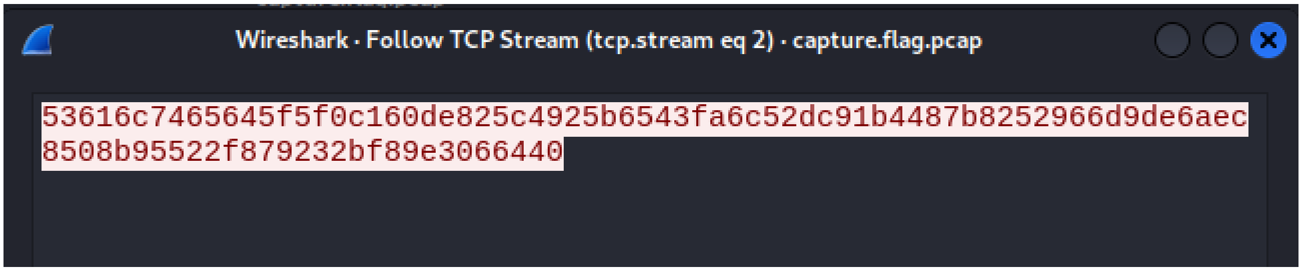
```
Salted__..
.%..[eC.lR...H{.R.m....P..R/..2....d@
```



capture.flag.pcap

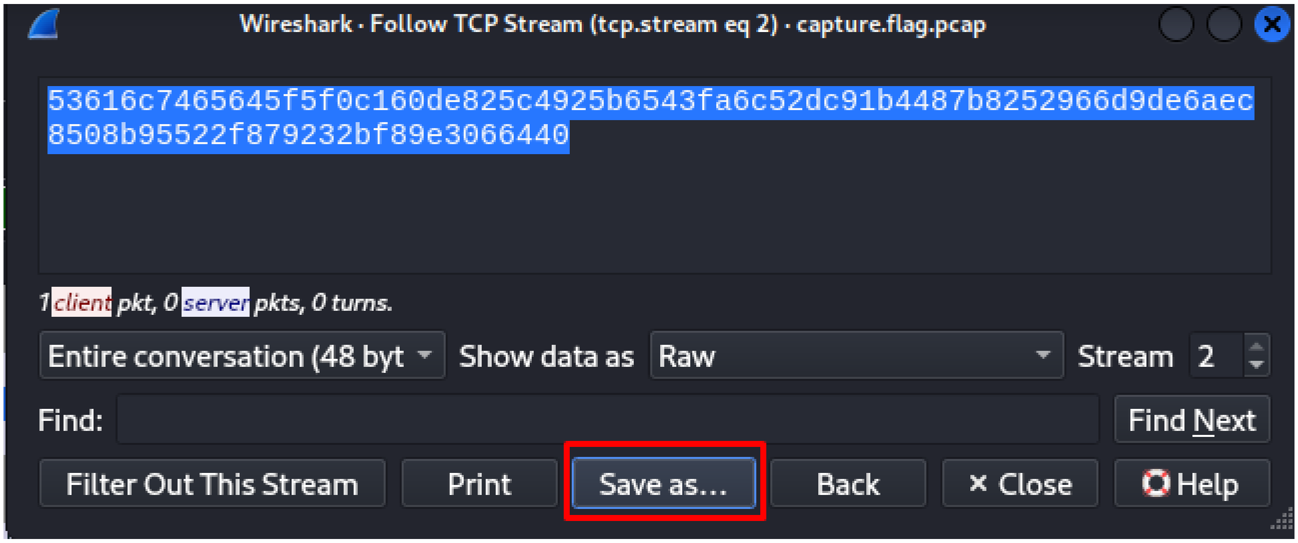
Wireshark · Follow TCP Stream (tcp.s

```
Salted__..
.%..[eC.lR...H{.R.m....P..R/..2..
```



Wireshark · Follow TCP Stream (tcp.stream eq 2) · capture.flag.pcap

```
53616c7465645f5f0c160de825c4925b6543fa6c52dc91b4487b8252966d9de6aec
8508b95522f879232bf89e3066440
```



Wireshark · Follow TCP Stream (tcp.stream eq 2) · capture.flag.pcap

```
53616c7465645f5f0c160de825c4925b6543fa6c52dc91b4487b8252966d9de6aec
8508b95522f879232bf89e3066440
```

1 client pkt, 0 server pkts, 0 turns.

Entire conversation (48 byt

Show data as: Raw

Stream: 2

Find:

Guardamos el archivo como: `file.des3` y procedemos a utilizar el comando que encontramos en la conversación `openssl des3 -d -salt -in file.des3 -out file.txt -k supersecretpassword123`

```
┌──(kali㉿kali)-[~/…/parciales/parcial_02/parte_03_forensic_01/eavesdrop]
└─$ openssl des3 -d -salt -in file.des3 -out file.txt -k
supersecretpassword123
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(kali㉿kali)-[~/…/parciales/parcial_02/parte_03_forensic_01/eavesdrop]
└─$ cat file.txt
picoCTF{nc_73115_411_dd54ab67}
```

Bandera

```
flag: picoCTF{nc_73115_411_dd54ab67}
```

Notas Adicionales

Referencias

-