

We have a PCAPNG file. When I saw there were 111 TCP Streams (Statistics -> Conversations) I ran the following shall code to reassemble all the TCP Streams and write them in a text file to read them better :

```
for stream in $(tshark -r TheOldDaysIntercepted.pcapng -Y "tcp.stream" -T fields -e  
tcp.stream | sort -n | uniq); do  
    echo "==== TCP Stream $stream ==="  
    tshark -r TheOldDaysIntercepted.pcapng -q -z follow,tcp,ascii,$stream  
    echo  
done
```



```
chmod +x run.sh  
./run.sh file.txt
```

Analyzing file.txt, at the end of streams, I noticed a big big file at stream 100 :

So I went to Wireshark, to tcp.stream eq 100, I copied the text and I uploaded it on CyberChef. I got a PNG image :

The screenshot shows the CyberChef interface with the following details:

- Recipe:** From Base64
- Alphabet:** A-Za-z0-9+=
- Input:** A large hex dump of a Wireshark capture, starting with 0x0E...
- Output:** The decoded ASCII text, which is extremely long and contains many non-printable characters.
- Buttons:** BAKE!, Auto Bake, Power & Battery, Energy saver is on.

Save the file. It should look like this :



Because we have an image, it's stegano. I ran zsteg and I found this archive :

```
z4que@z4que /m/c/U/z/Desktop> zsteg download.png
[?] 237 bytes of extra data after image end (IEND), offset = 0x9af2
extradata:0 .. file: Zip archive data, made by v3.0 UNIX, extract using at least v1.0, last modified May 10 2025
11:25:48, uncompressed size 43, method=store
00000000: 50 4b 03 04 0a 00 09 00 00 00 38 5b aa 5a fd b1 |PK,.....8[Z..|
00000010: ef be 37 00 00 00 2b 00 00 00 08 00 1c 00 66 6c |....+.....fl|
00000020: 61 67 2e 74 78 74 55 54 09 00 03 fc 6f 1f 68 d2 |ag.txtUT.....o.h.|
00000030: 6f 1f 68 75 78 0b 00 01 04 e8 03 00 00 04 e8 03 |o.hux.....|
00000040: 00 00 01 d8 9d e1 ef 4c 05 55 c9 14 f7 da 90 c2 |.....L.U.....|
00000050: ff cc 3c f4 e3 59 17 be 63 01 c8 dc 4c 3a 66 47 |.<..Y..c..L:fG|
00000060: 9e 81 a9 07 bb 7e 55 26 34 d6 12 e7 84 a0 72 fa |.....~U&.....r.|
00000070: 8e 19 6d 19 25 1e e2 b9 fb 50 4b 07 08 fd b1 ef |..m%.....PK.|
00000080: be 37 00 00 00 2b 00 00 00 50 4b 01 02 1e 03 0a |....+.....PK.|
00000090: 00 09 00 00 00 38 5b aa 5a fd b1 ef be 37 00 00 |.....Z.....7..|
000000a0: 00 2b 00 00 00 08 00 18 00 00 00 00 00 01 00 00 |+.|
000000b0: 00 b4 81 00 00 00 00 66 6c 61 67 2e 74 78 74 55 |.....flag.txtU|
000000c0: 54 05 00 03 fc 6f 1f 68 75 78 0b 00 01 04 e8 03 |T.....o.hux.....|
000000d0: 00 00 04 e8 03 00 00 50 4b 05 06 00 00 00 00 01 |.....PK.|
000000e0: 00 01 00 4e 00 00 00 89 00 00 00 00 00 00 00 00 |.....N.|
b1,g,lsb,xy .. file: OpenPGP Public Key
b1,g,msb,xy .. file: OpenPGP Public Key
b1,rgb,lsb,xy .. text: "Definetly do not check this -> aHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj14dkZaam81UGdHMA="
```

Command :

```
zsteg -E "extradata:0" download.png > flag.zip
```

The archive is password protected. I tried John, Hashcat...nothing. The text of the problem said about 2 ppl communicating, so I continued looking in **file.txt** (TCPs). At **tcp.stream eq 10**, we can see a basic communication + I noticed the 1337 dstport :

| No. | Time | Source | Destination | Protocol | Length Info |
|-----|--------------|-----------|-------------|----------|-------------------------------------|
| 111 | 10.780545460 | 127.0.0.1 | 127.0.0.1 | TCP | 76 50290 → 1337 [SYN] Seq=0 W |
| 112 | 10.780554456 | 127.0.0.1 | 127.0.0.1 | TCP | 76 1337 → 50290 [SYN, ACK] Seq=1 A |
| 113 | 10.780560662 | 127.0.0.1 | 127.0.0.1 | TCP | 68 50290 → 1337 [ACK] Seq=1 A |
| 162 | 13.148541722 | 127.0.0.1 | 127.0.0.1 | TCP | 76 50290 → 1337 [PSH, ACK] Seq=1 A |
| 163 | 13.148568121 | 127.0.0.1 | 127.0.0.1 | TCP | 68 1337 → 50290 [ACK] Seq=1 A |
| 202 | 13.876556793 | 127.0.0.1 | 127.0.0.1 | TCP | 72 50290 → 1337 [PSH, ACK] Seq=1 A |
| 203 | 13.876581970 | 127.0.0.1 | 127.0.0.1 | TCP | 68 1337 → 50290 [ACK] Seq=1 A |
| 287 | 17.370784930 | 127.0.0.1 | 127.0.0.1 | TCP | 82 1337 → 50290 [PSH, ACK] Seq=13 A |
| 288 | 17.370812280 | 127.0.0.1 | 127.0.0.1 | TCP | 68 50290 → 1337 [ACK] Seq=13 A |
| 318 | 18.147539137 | 127.0.0.1 | 127.0.0.1 | TCP | 71 1337 → 50290 [PSH, ACK] Seq=13 A |
| 319 | 18.147569849 | 127.0.0.1 | 127.0.0.1 | TCP | 68 50290 → 1337 [ACK] Seq=13 A |
| 349 | 19.482121683 | 127.0.0.1 | 127.0.0.1 | TCP | 68 50290 → 1337 [FIN, ACK] Seq=14 A |
| 350 | 19.528900583 | 127.0.0.1 | 127.0.0.1 | TCP | 68 1337 → 50290 [ACK] Seq=18 A |
| 376 | 22.073603250 | 127.0.0.1 | 127.0.0.1 | TCP | 68 1337 → 50290 [FIN, ACK] Seq=14 A |
| 377 | 22.073613346 | 127.0.0.1 | 127.0.0.1 | TCP | 68 50290 → 1337 [ACK] Seq=14 A |

I filtered the TCP Streams by destination port (**tcp.dstport == 1337**), I followed some streams and I found this interesting message in the third followed TCP stream with destination port eq to 1337 (**tcp.stream eq 38** apparently):

| No. | Time | Source | Destination | Protocol | Length Info |
|------|--------------|-----------|-------------|----------|-------------------------------------|
| 818 | 51.853697130 | 127.0.0.1 | 127.0.0.1 | TCP | 76 54840 → 1337 [SYN] Seq=0 W |
| 819 | 51.853704730 | 127.0.0.1 | 127.0.0.1 | TCP | 76 1337 → 54840 [SYN, ACK] Seq=1 A |
| 820 | 51.853710371 | 127.0.0.1 | 127.0.0.1 | TCP | 68 54840 → 1337 [ACK] Seq=1 A |
| 845 | 55.073107543 | 127.0.0.1 | 127.0.0.1 | TCP | 80 1337 → 54840 [PSH, ACK] Seq=1 A |
| 846 | 55.073136564 | 127.0.0.1 | 127.0.0.1 | TCP | 68 54840 → 1337 [ACK] Seq=1 A |
| 858 | 56.860990618 | 127.0.0.1 | 127.0.0.1 | TCP | 74 54840 → 1337 [PSH, ACK] Seq=1 A |
| 859 | 56.861019474 | 127.0.0.1 | 127.0.0.1 | TCP | 68 1337 → 54840 [ACK] Seq=13 A |
| 1105 | 81.269602014 | 127.0.0.1 | 127.0.0.1 | TCP | 89 54840 → 1337 [PSH, ACK] Seq=13 A |
| 1106 | 81.269628276 | 127.0.0.1 | 127.0.0.1 | TCP | 68 1337 → 54840 [ACK] Seq=13 A |
| 1115 | 82.561156161 | 127.0.0.1 | 127.0.0.1 | TCP | 74 54840 → 1337 [PSH, ACK] Seq=13 A |
| 1116 | 82.561165738 | 127.0.0.1 | 127.0.0.1 | TCP | 68 1337 → 54840 [ACK] Seq=13 A |
| 1177 | 88.096381845 | 127.0.0.1 | 127.0.0.1 | TCP | 97 54840 → 1337 [PSH, ACK] Seq=63 A |
| 1178 | 88.096390596 | 127.0.0.1 | 127.0.0.1 | TCP | 68 1337 → 54840 [ACK] Seq=13 A |
| 1199 | 90.226065700 | 127.0.0.1 | 127.0.0.1 | TCP | 70 1337 → 54840 [PSH, ACK] Seq=63 A |
| 1200 | 90.226075117 | 127.0.0.1 | 127.0.0.1 | TCP | 68 54840 → 1337 [ACK] Seq=63 A |
| 1221 | 92.497895307 | 127.0.0.1 | 127.0.0.1 | TCP | 82 1337 → 54840 [PSH, ACK] Seq=63 A |
| 1222 | 92.497904344 | 127.0.0.1 | 127.0.0.1 | TCP | 68 54840 → 1337 [ACK] Seq=63 A |

This is a Base64. Decoded, is **S3crt\$oFt3hP45t** and also the archive password

THE FLAG : ctf{S3ems_Y0U_N3V3R_L3aRn_YeLeuRe_La3ka3r}
~Z4que