

The first thing I did was to export the HTTP object, but after some research, I didn't find anything useful. There were a bunch of HTML pages. Then, I took a look at the packets and I spotted a PNG image in the first ICMP packet :

```

# 33 0.008200118 10.10.10.1      10.10.10.10    ICMP   98 Echo (ping) request id=0x2b9a, seq=0/0, ttl=64 (reply in 34)
← 34 0.008244205 10.10.10.10    10.10.10.1    ICMP   98 Echo (ping) reply id=0x2b9a, seq=0/0, ttl=64 (request in 33)
35 1.008437446 10.10.10.1      10.10.10.10    ICMP   98 Echo (ping) request id=0x2b9a, seq=1/256, ttl=64 (reply in 36)
36 1.008651334 10.10.10.10    10.10.10.1     ICMP   98 Echo (ping) reply id=0x2b9a, seq=1/256, ttl=64 (request in 35)
37 2.009787814 10.10.10.1      10.10.10.10    ICMP   98 Echo (ping) request id=0x2b9a, seq=2/512, ttl=64 (reply in 38)
38 2.010156995 10.10.10.10    10.10.10.1     ICMP   98 Echo (ping) reply id=0x2b9a, seq=2/512, ttl=64 (request in 37)
39 3.010669912 10.10.10.1      10.10.10.10    ICMP   98 Echo (ping) request id=0x2b9a, seq=3/768, ttl=64 (reply in 40)
40 3.010938520 10.10.10.10    10.10.10.1     ICMP   98 Echo (ping) reply id=0x2b9a, seq=3/768, ttl=64 (request in 39)
41 4.011626826 10.10.10.1      10.10.10.10    ICMP   98 Echo (ping) request id=0x2b9a, seq=4/1024, ttl=64 (reply in 42)

> Frame 33: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface virbr1, id 0
> Ethernet II, Src: 52:54:00:66:a2:40 (52:54:00:66:a2:40), Dst: 52:54:00:40:97:89 (52:54:00:40:97:89)
> Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.10
> Internet Control Message Protocol
0000  52 54 00 40 97 89 52 54  RT B RT f K E
0010  00 54 a0 1b 40 00 40 01  T P d I o
0020  0a 0a 00 00 35 94 2b 9a 00 00 89 50 4e 47 0d 0a  .5 + ...PNG
0030  1a 0a 00 00 00 0d 49 48 44 52 00 00 07 45 00 00  ..IH DR E
0040  00 45 00 00 00 00 00 35 b6 3e aa 00 00 00 04 73  E -5 > ...
0050  00 54 00 54 00 00 00 00 00 00 00 00 00 00 19 74  BIT ...I u t
0060  45 58  EX

# So I used the following command to extract ICMP Echo Request ( type 8 ) to export the image :
tshark -r captura.pcapng -Y "icmp and icmp.type==8" -T fields -e data | xxd -r -p
> img.png
```

And we found this image :

```
!
username admin password 7 03217838251474481E0D405144440A08532F7B732C666675465E425B0052080B040058051D44080000525302520F0C57550E53021702500C0A050A254A1650405542135B0D5037!
```

This is a Cisco type 7 password. We can use an online tool, like <https://ccnax.com/cisco-type-7-password-decryption/> to decrypt the flag.

THE FLAG :

```
ECSC{5d0d4436ad7e07d5375948ad13746fe2987aa7fd7126dfdd47acedf89905a0a4}
~Z4que
```