Forensics – We are E.xtr – 350 Points :

We are E.xtr - Points: 350 - (Solves: 216)   Forensics - Solved

Solve   Hints

Flag is formatted as {plain_text}

Hint :

We are E.xtr - Points: 350 - (Solves: 216)   Forensics - Solved

Solve   Hints

E.xtr

First download the attachement file.

Running file against it only show us it's data file.


```
root@nexus:~/Téléchargements# file E.xtr
E.xtr: data
```

Using xxd for read the header, show us it's really seem a PNG header.


```
root@nexus:~/Téléchargements# xxd E.xtr | head
00000000: 8958 5452 0d0a 1a0a 0000 000d 4948 4452  .XTR........IHDR
00000010: 0000 0500 0000 02d0 0803 0000 018f a41d  ................
00000020: f200 0000 0173 5247 4200 aece 1ce9 0000  .....sRGB.......
00000030: 0004 6741 4d41 0000 b18f 0bfc 6105 0000  ..gAMA......a...
00000040: 0066 504c 5445 ffff ffdf dfdf 7f7f 7f40  .fPLTE.........@
00000050: 4040 2828 2800 0000 1818 1850 5050 f7f7  @@(((......PPP..
00000060: f7af afaf 9797 9710 1010 6868 68e7 e7e7  ..........hhh...
00000070: 2020 2078 7878 9f9f 9f08 0808 bfbf bf8f   xxx...........
00000080: 8f8f c7c7 c7a7 a7a7 7070 7030 3030 6060  ........ppp000``
00000090: 60cf cfcf b7b7 b758 5858 3838 38ef efef  `......XXX888...
```

Open E.xtr with vim, and press « i » for modify the file.

Replace « <89>XTR » with « <89>PNG », then press « esc » and type «:wq » for save the file and exit.

Then verify the picture was not « data » but « png » with file.

Open the picture and you got the flag !

Flag = peaCTF{read_banned_it}