The capture is too big for wireshark to handle, so we rely on tshark. We first look to see if teamviewer is used, but it's not, so we take a look at the hierarchy. There we notice VNC being used, which is similar to teamviewer. We extract the packets with tshark -r t3am_vi3w3r.pcapng -Y "vnc" -w vnc_packets.pcapng and have a look in wireshark.

We follow the tcp stream and see some sort of text? That is separated by a lot of dots. We copy the text in a txt file and replace the dots with nothing, and now see the text:

RFB 003008

RFB 003008

qAi'Q%=f?8'c4 dani-pc!CCoonnttrraarryy ttoo ppooppuullaarr bbeelliieeff,, LLoorreemm IIppssuumm iiss nnoott ssiimmppllyy rraannddoomm tteexxtt IItt hhaass rroooottss iinn aa ppiieeccee ooff ccllaassssiiccaall LLaattiinn lliitteerraattuurree ffrroomm 4455 BBCC,, mmaakkiinngg iitt oovveerr 22000000 yyeeaarrss oolldd

….

DDCCTTFF{{*}}**

WWhhyy ddoo wwee uussee iitt??

IItt iiss aa lloonngg eessttaabblliisshheedd ffaacctt tthhaatt aa rreeaaddeerr wwiillll bbee

….

Basically, in the middle of it we have the flag, but each character repeats twice. we just need to skip every other character and recover the flag. For example, we can use:

```
input_string[::2]
```

After this we got the flag.

Made with love by: AndreiCat