Files

main

Go to file

- .github
- 2023
  - 0ByteCTF 2023
  - 0xL4ugh CTF 2023
  - 1337UP LIVE CTF
  - 24h@CTF 2023
  - ASC Cyber Wargames Qualificat...
  - AmateursCTF 2023
  - BDSec CTF 2023
  - BYUCTF 2023
  - BlueHens CTF 2023

daffainfo feat: grouped the challs   e6c48e5 · last month   History

Name	Last commit message	Last commit date
..		
images	feat: grouped the challs	last month
README.md	feat: grouped the challs	last month
initial-report.pcapng	feat: grouped the challs	last month

README.md

cheval de troie

cheval de troie
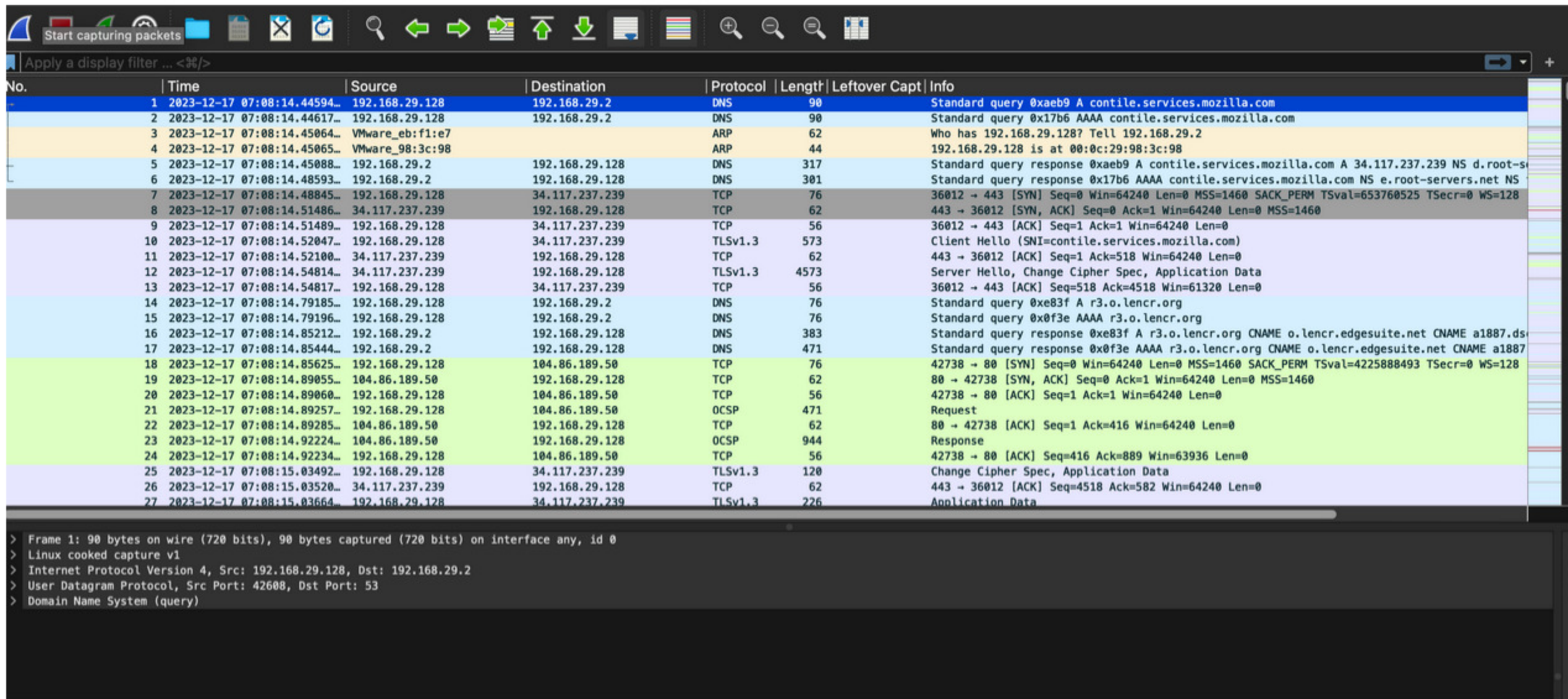
> After accessing our private network, the hacker skillfully maneuvered through files, leaving behind a virtual trail of mystery. We managed to capture the packets, exposing the encrypted breadcrumbs scattered across the network. Before slipping away into the digital abyss, the intruder left a deliberate hint—a cryptic message that conceals the essence of their next move. Decrypt the message and unveil the obscured 'crypto' to thwart their cunning plan.
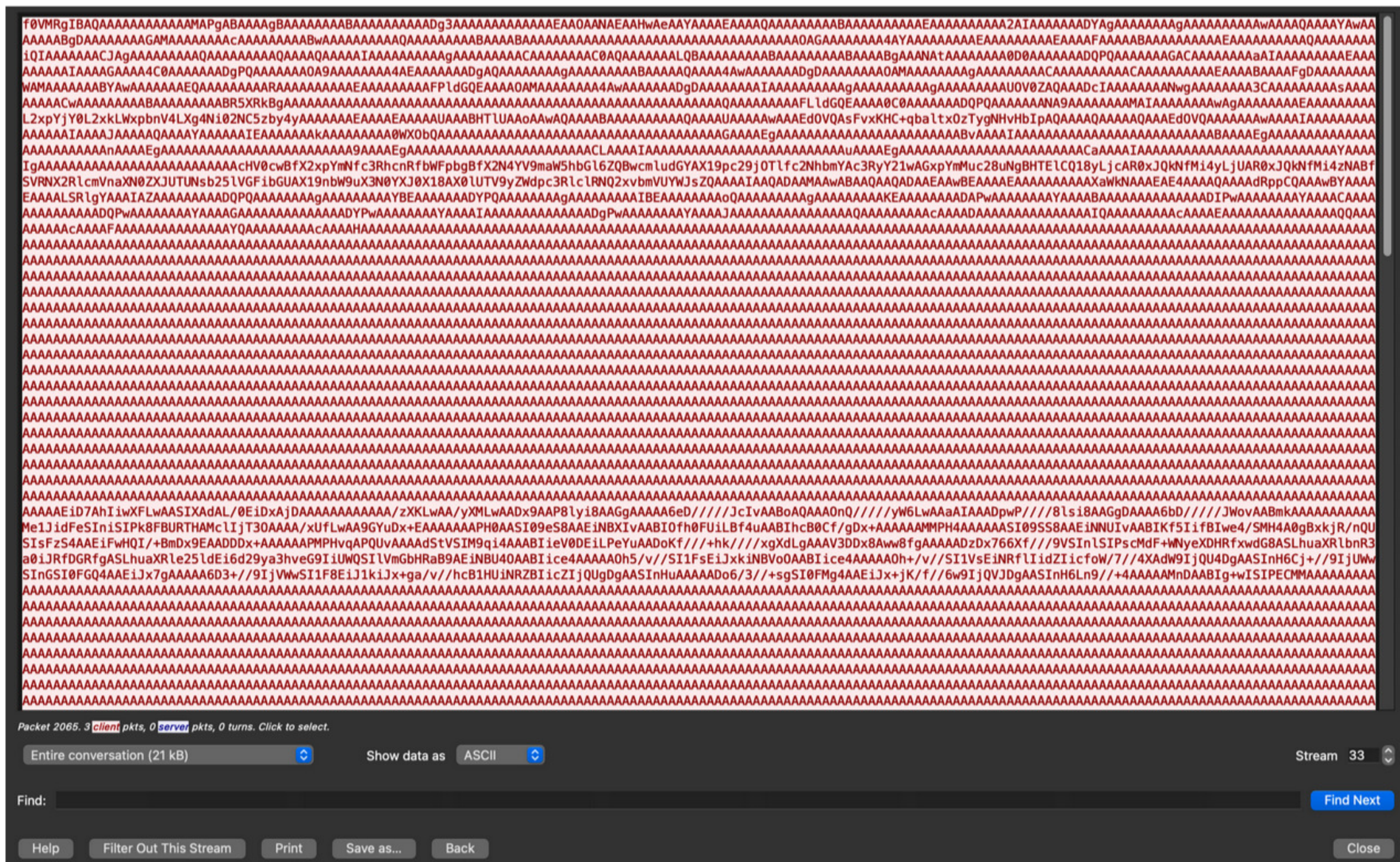
> Taupe will be visible after this challenge

About the Challenge

We were given a `pcapng` file (You can download the file here). And here is the preview of the packet capture file
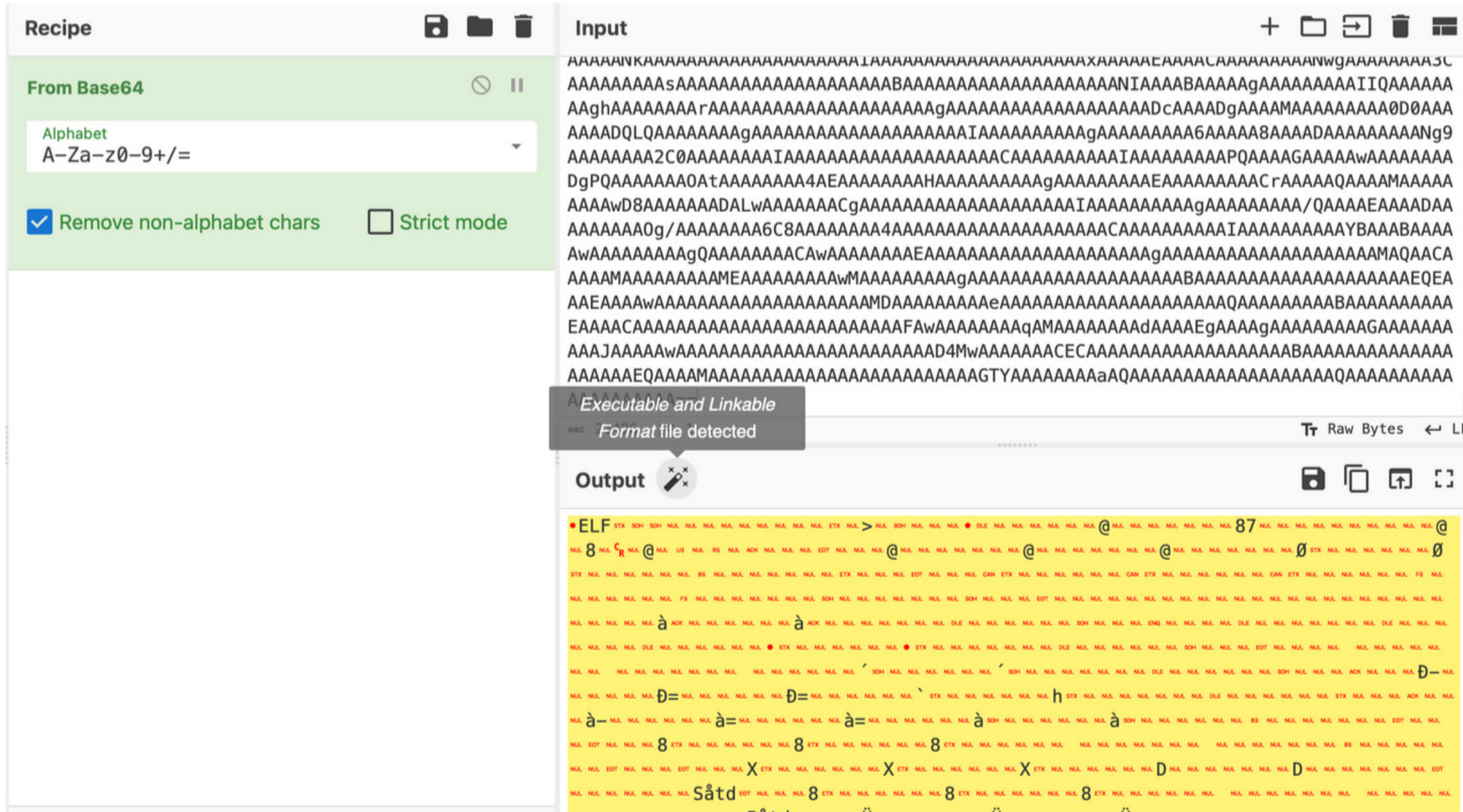

How to Solve?

There's an interesting encoded base64 message in stream 33

I copied the msg and then use cyberchef to decode it

Reverse engineer the program to obtain th eflag

```
//        (00000000000001103)
int __fastcall main(int argc, const
{
  char v4[32]; // [rsp+0h] [rbp-70h]
  char s2[64]; // [rsp+20h] [rbp-50h]
  char v6[16]; // [rsp+60h] [rbp-10h]

  strcpy(&v6[9], "crypto");
  strcpy(v6, "nitentwk");
  strcpy(v4, "nite{networkxoxo}");
  printf("Enter the first half of th
  __isoc99_scanf("%s", s2);
  if ( !strcmp(&v6[9], s2) )
  {
    puts("First half correct! Now en
    __isoc99_scanf("%s", s2);
    if ( !strcmp(v6, s2) )
```

nite{networkxoxo}