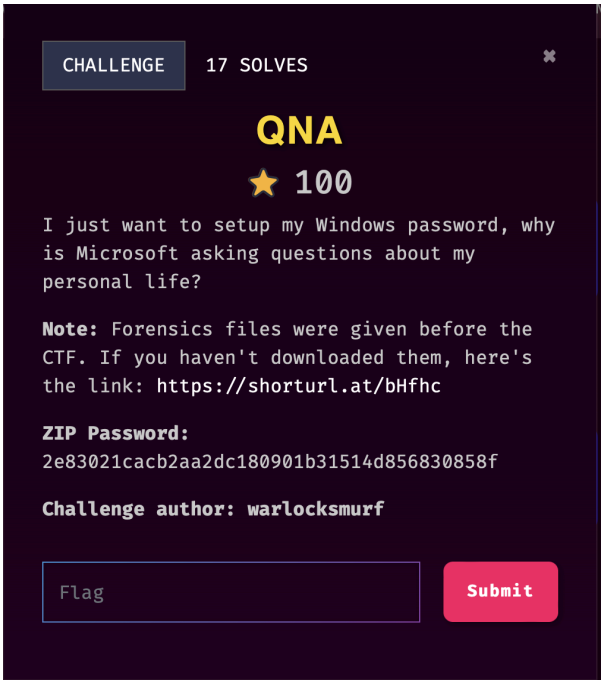
Wrote by

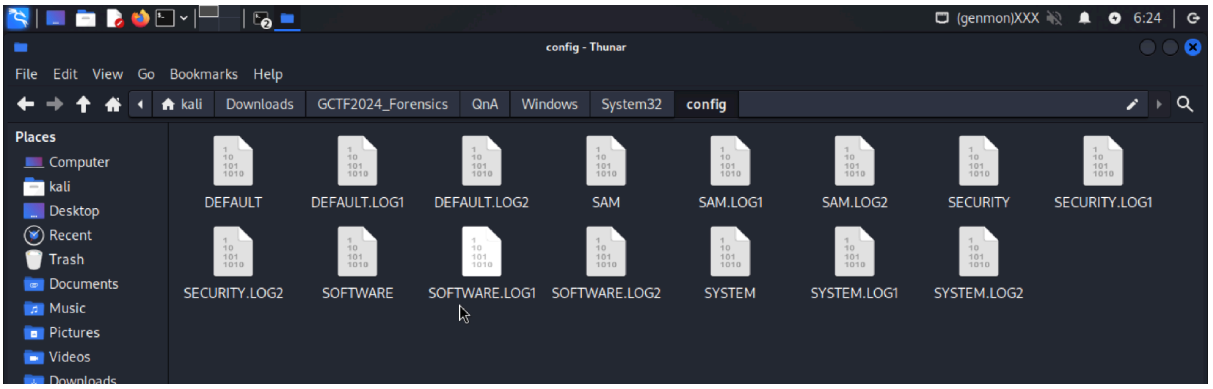
Dark Phoenix

FORENSIC

QnA



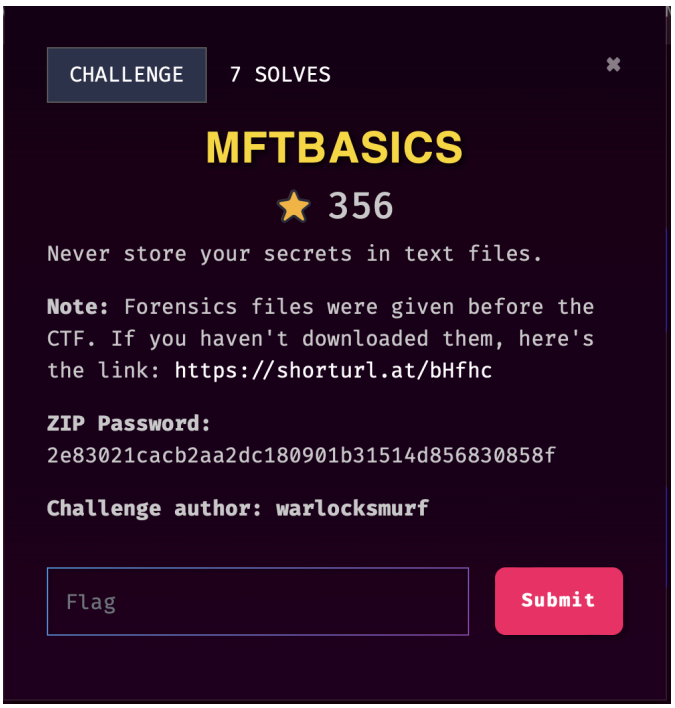
In this directory, I just look for the User's name which is SAM.



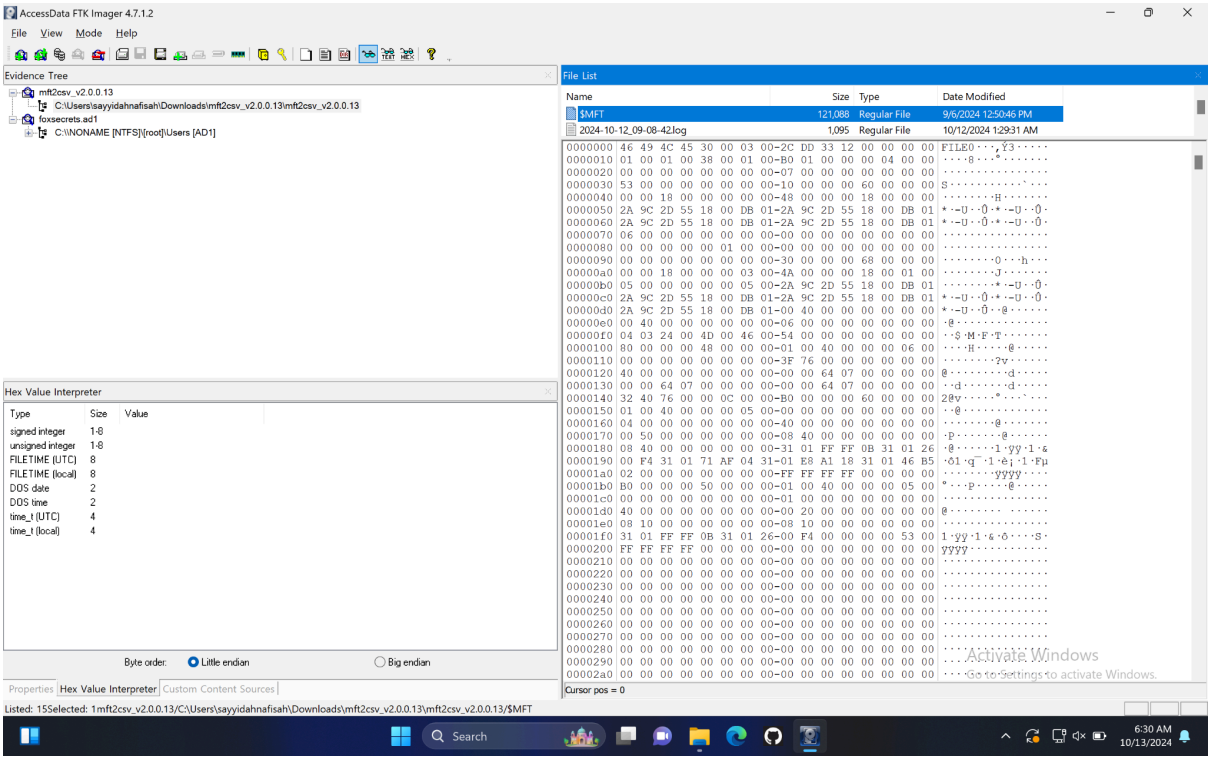
I used the command cat SAM to see the content and finally found the flag which was divided into 3 parts of the questions.

Flag: GCTF{p3rs0nal_s3cr3ts_r3g1stry}

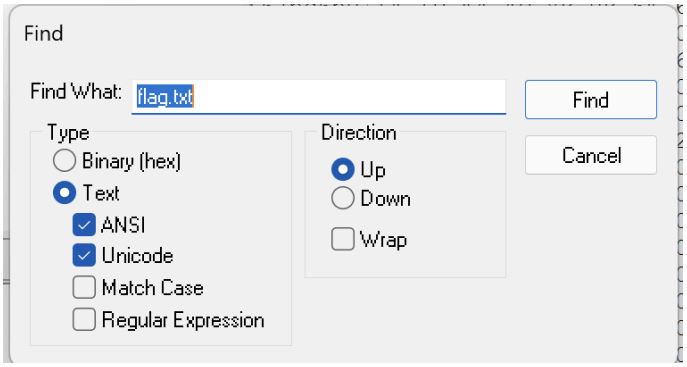
MFTBasics



To perform analysis on the $MFT file, I put it in a folder and opened it using FTK Imager.



Right click and click find to find a keyword for the secret text file which is flag.txt. Just find it until I find the secret code.

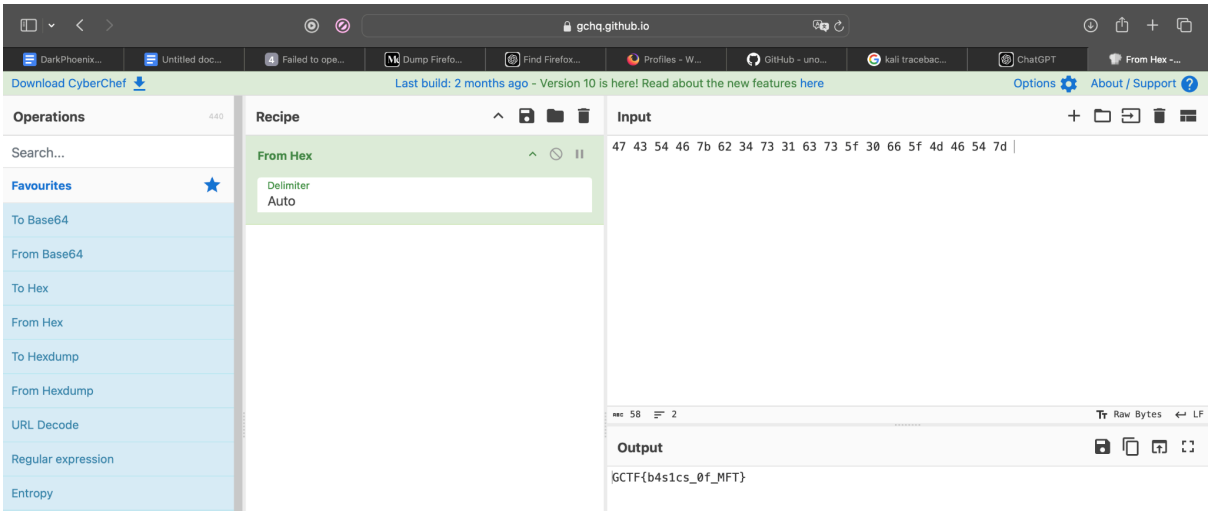


Finally found the secret code:

The secret code is: 47 43 54 46 7b 62 34 73 31 63 73 5f 30 66 5f 4d 46 54 7d 4d

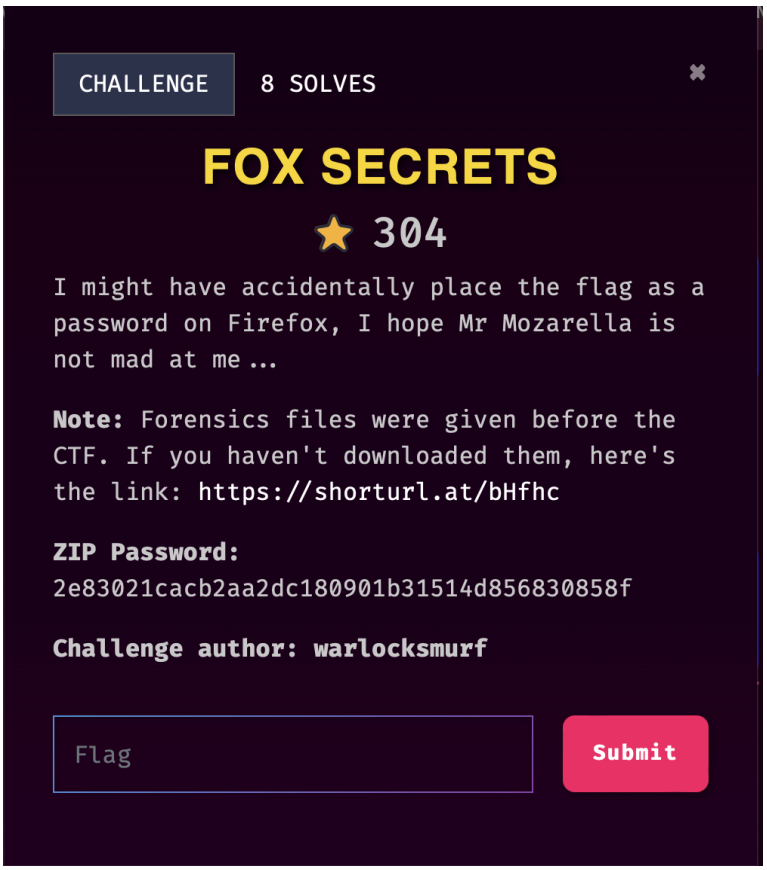
```
6fadcf0 08 03 66 00 6C 00 61 00-67 00 2E 00 74 00 78 00 ··f·l·a·g·.·t·x·
6fadd00 74 00 00 00 00 00 00 00-40 00 00 00 28 00 00 00 t······@···(···
6fadd10 00 00 00 00 00 00 05 00-10 00 00 00 18 00 00 00 ················
6fadd20 87 8D 61 04 88 6B EF 11-AB D7 00 0C 29 22 8E 27 ··a··kï·«×··)"·'
6fadd30 80 00 00 00 68 00 00 00-00 00 18 00 00 00 01 00 ····h···········
6fadd40 4C 00 00 00 18 00 00 00-54 68 65 20 73 65 63 72 L·······The secr
6fadd50 65 74 20 63 6F 64 65 20-69 73 3A 20 34 37 20 34 et code is: 47 4
6fadd60 33 20 35 34 20 34 36 20-37 62 20 36 32 20 33 34 3 54 46 7b 62 34
6fadd70 20 37 33 20 33 31 20 36-33 20 37 33 20 35 66 20  73 31 63 73 5f
6fadd80 33 30 20 36 36 20 35 66-20 34 64 20 34 36 20 35 30 66 5f 4d 46 5
6fadd90 34 20 37 64 34 64 20 34-FF FF FF FF 82 79 47 11 4 7d4d 4ÿÿÿÿ·yG·
6fadda0 FF FF FF FF 82 79 47 11-00 00 00 00 18 00 00 00 ÿÿÿÿ·yG·····
6faddb0 FF FF FF FF 82 79 47 11-00 00 00 00 00 00 00 00 ÿÿÿÿ·yG·····
6faddc0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

To decrypt that i just threw it on cyberchef and finally cracked it.



Flag: GCTF{b4s1cs_0f_MFT}

Fox Secrets

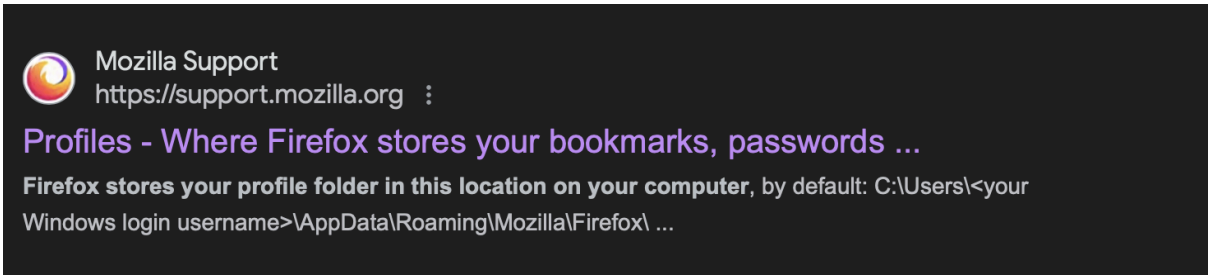


We were given an image file foxsecrets.ad1. To do an analysis on the image file, I opened it using FTK imager.

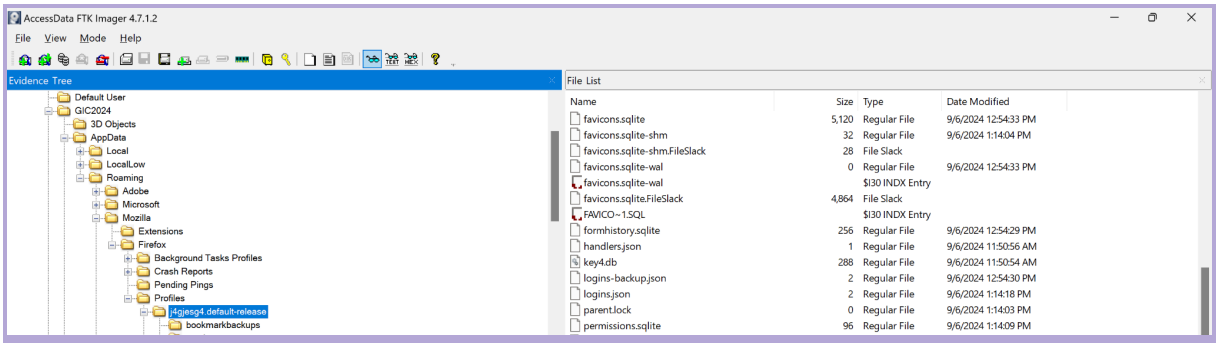
Since the clue said they stored the password on firefox, I must look for `key4.db` and `logins.json` according to https://support.mozilla.org/en-US/kb/profiles-where-firefox-stores-user-data,

So I looked for the path of the stored password on mozilla which is:

`username\AppData\Roaming\Mozilla\Firefox\Profiles`



So to look for the files, I just opened the directories on FTK imager GIC2024\AppData\Roaming\Mozilla\Firefox\Profiles\j4gjesg4.default-release and as shown below, there are key4.db and logins.json in that folder.

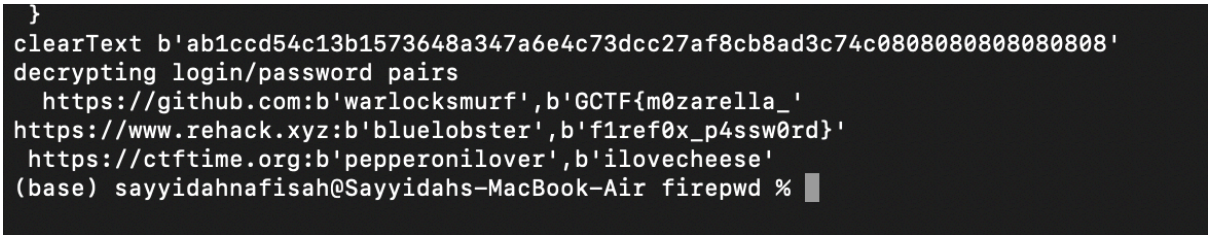


To retrieve the password, I used this website as my reference: https://medium.com/@s12deff/dump-firefox-passwords-with-firepwd-and-firefox-decrypt-65350fd74503

Since we already have key4.db and logins.json, the step to find the passwords are

1. git clone https://github.com/lclevy/firepwd
2. Put the key4.db and logins.json in the same folder as firepwd
3. python3 firepwd.py

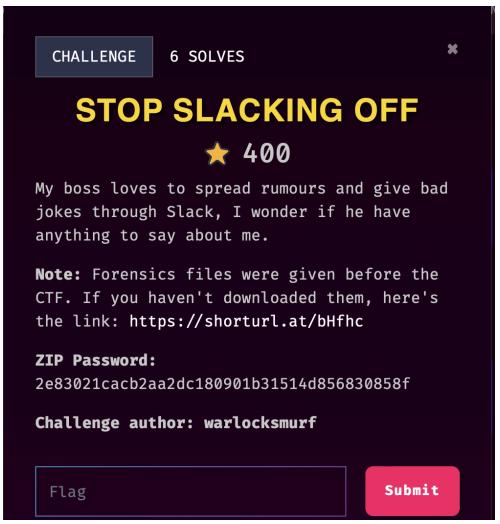
```
zsh: no such file or directory: https://github.com/lclevy/firepwd
(base) sayyidahnafisah@Sayyidahs-MacBook-Air fox secret % git clone https://github.com/lclevy/firepwd

Cloning into 'firepwd'...
remote: Enumerating objects: 88, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 88 (delta 2), reused 3 (delta 0), pack-reused 80 (from 1)
Receiving objects: 100% (88/88), 239.08 KiB | 2.28 MiB/s, done.
Resolving deltas: 100% (41/41), done.
(base) sayyidahnafisah@Sayyidahs-MacBook-Air fox secret % ls
firepwd         key4.db         logins.json
(base) sayyidahnafisah@Sayyidahs-MacBook-Air fox secret % cd firepwd
(base) sayyidahnafisah@Sayyidahs-MacBook-Air firepwd % ls
LICENSE                 logins.json             mozilla_pbe.svg
firepwd.py              mozilla_db              readme.md
key4.db                 mozilla_pbe.pdf         requirements.txt
(base) sayyidahnafisah@Sayyidahs-MacBook-Air firepwd % python3 firepwd
python3: can't open file '/Users/sayyidahnafisah/Desktop/shared/fox secret/firepwd/firepwd': [Errno 2] No such file or directory
(base) sayyidahnafisah@Sayyidahs-MacBook-Air firepwd % python3 firepwd.py
globalSalt: b'b5dbfec66b891e193f516eccaf39209a93634332'
 SEQUENCE {
   SEQUENCE {
     OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
     SEQUENCE {
       SEQUENCE {
         OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
         SEQUENCE {
           OCTETSTRING b'eaa234484d176f2f091e1a9b2162b550a9874bf9ced92daa19c43e058b1328cf'
           INTEGER b'01'
           INTEGER b'20'
           SEQUENCE {
             OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
           }
         }
       }
       SEQUENCE {
         OBJECTIDENTIFIER 2.16.840.1.101.3.4.1.42 aes256-CBC
         OCTETSTRING b'c361eb13322fd6004ad463de0ef2'
       }
     }
   }
   OCTETSTRING b'c2cb6eb12879f4c649458e59d634f355'
 }
clearText b'70617373776f72642d636865636b0202'
password check? True
 SEQUENCE {
   SEQUENCE {
     OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
     SEQUENCE {
       SEQUENCE {
         OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
         SEQUENCE {
           OCTETSTRING b'ae2720e0964ce4beabedba40345712df4234f9ac9cd86e53a08982b65abbbd9c'
           INTEGER b'01'
           INTEGER b'20'
           SEQUENCE {
             OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
           }
         }
       }
       SEQUENCE {
         OBJECTIDENTIFIER 2.16.840.1.101.3.4.1.42 aes256-CBC
```



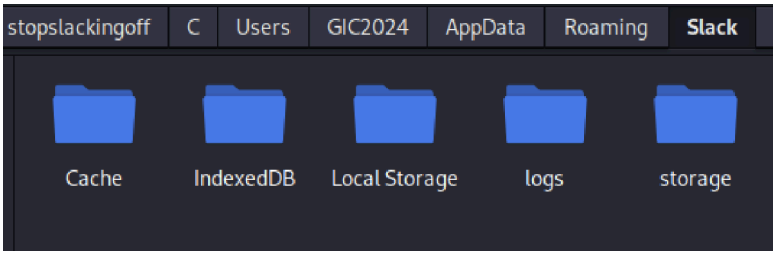
Finally we cracked the password and retrieved the flag after doing all the steps.

Flag:GCTF{m0zarella_f1ref0x_p4ssw0rd}

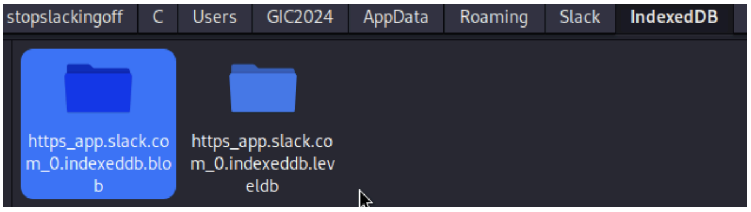
Stop Slacking Off



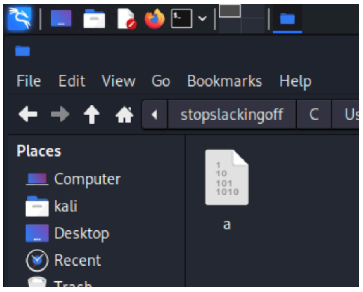
There are 5 folders in the Slack directory. I actually checked and `cat` all the files in those folders.



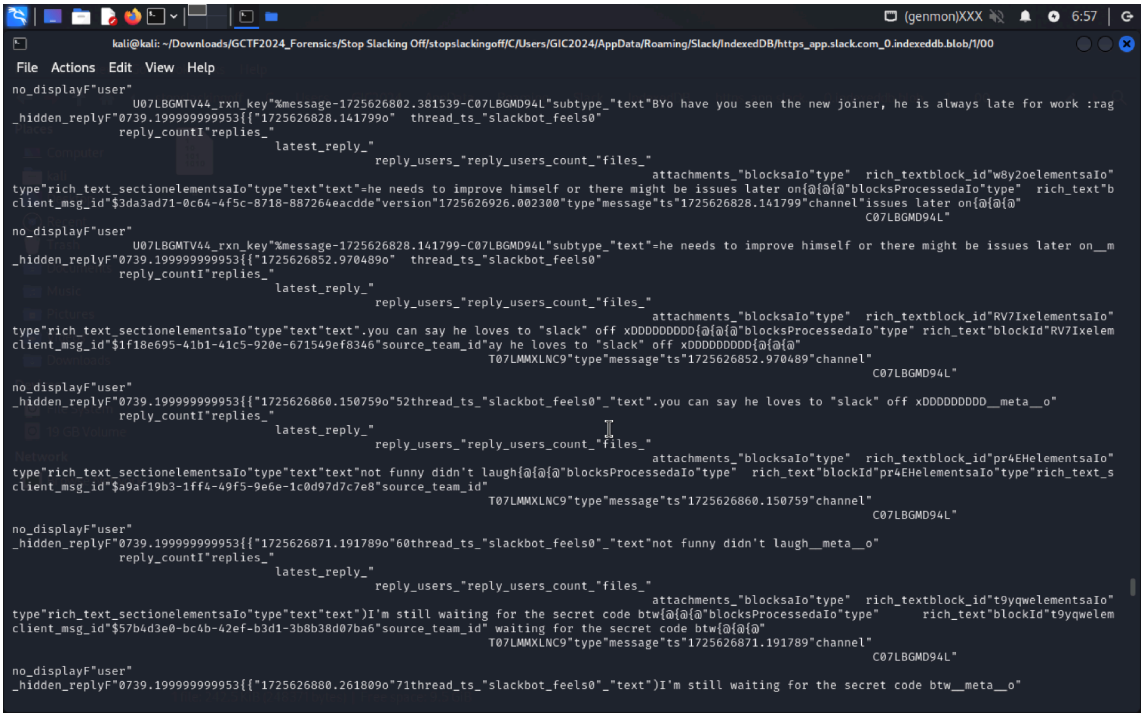
After carefully checked the content of the files, I finally found the conversations on `/Slack/IndexedDB/https_app.slack.com_0.indexeddb.blob`



Below was the only file in that folder and I checked the content using `cat a`.

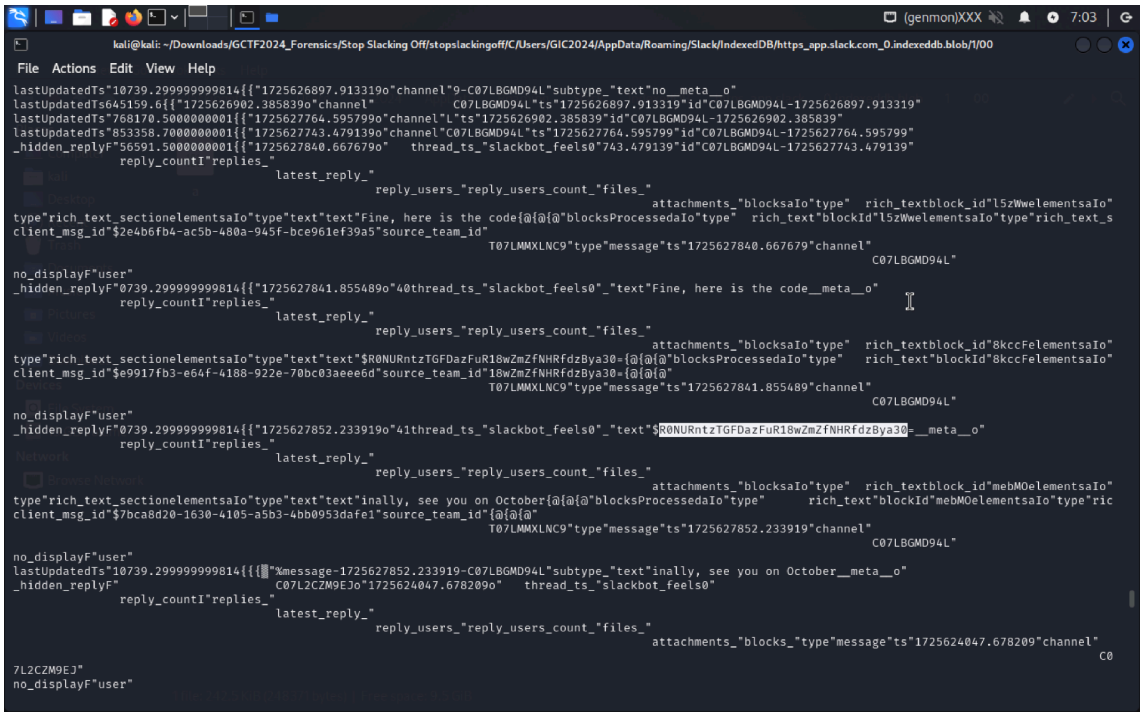


Found the conversation history on slack in that file.

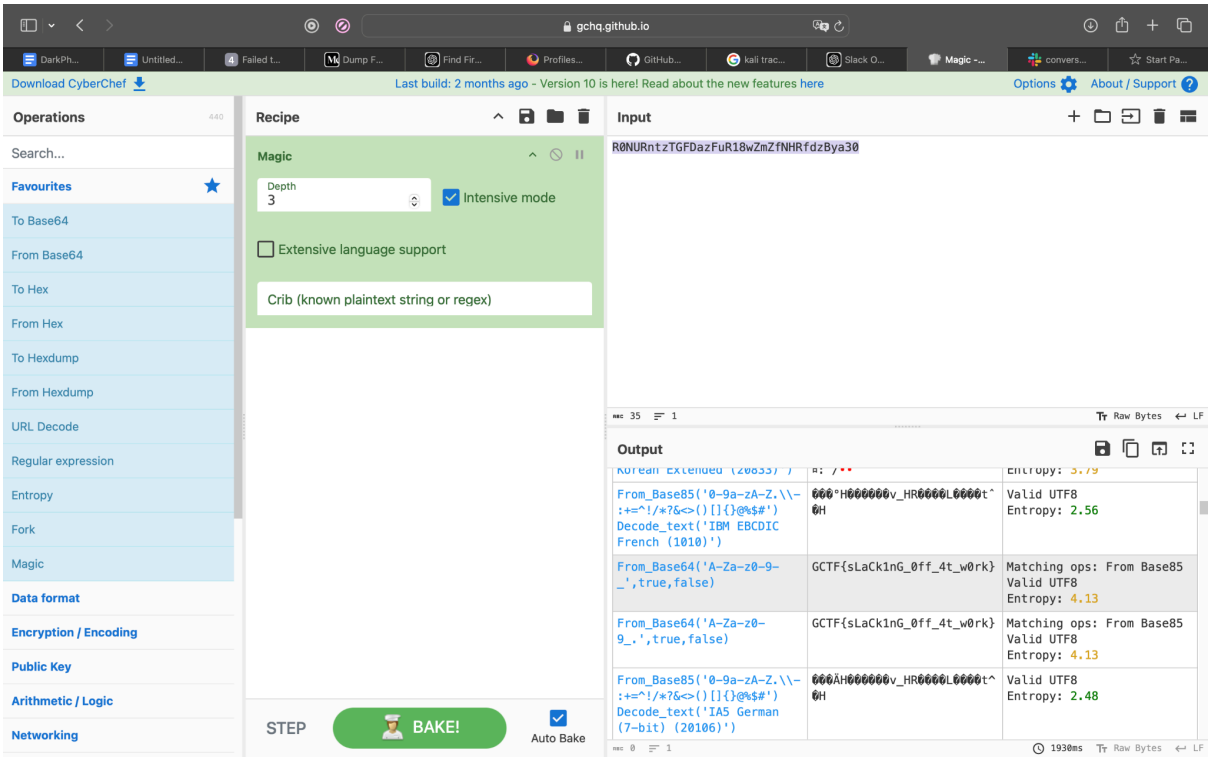


After carefully reading the conversations, I found the secret code which is:

R0NURntzTGFDazFuR18wZmZfNHRfdzBya30



As usual, to decrypt it, I just put in the cyberchef and let it do the work.



Flag: GCTF{sLaCk1nG_0ff_4t_w0rk}