

Girls in CTF 2024



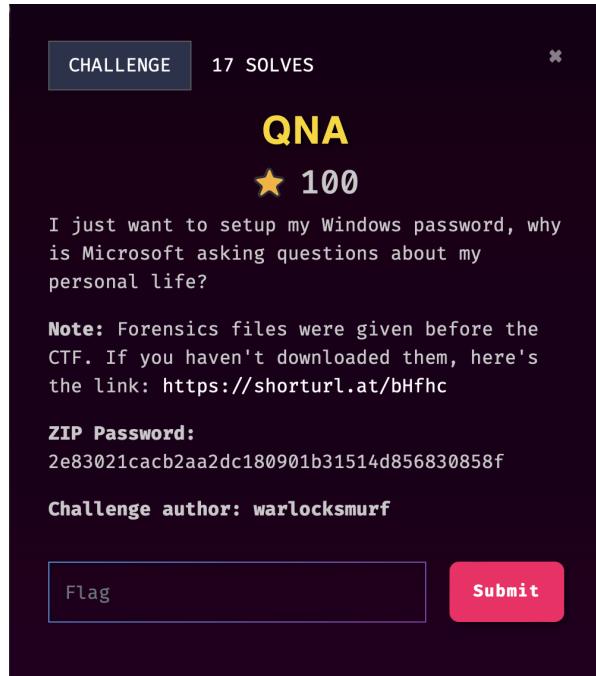
Empowering the Next Generation of Cybersecurity Enthusiasts

Wrote by

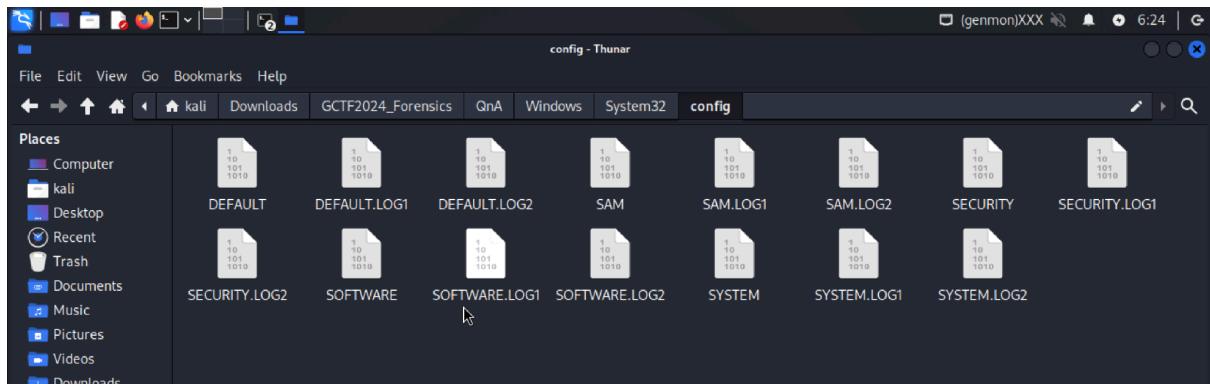
Dark Phoenix

FORENSIC

OnA



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

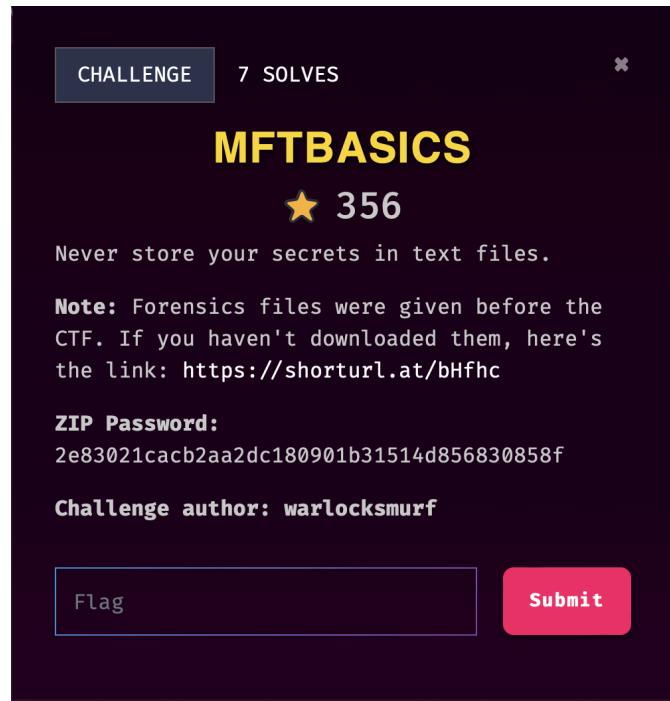


I used the command cat SAM to see the content and finally found the flag which was divided into 3 parts of the questions.

```
->(g!>y*)y*`'V* cF**h*** AdministratorsAdministrators have complete and unrestricted access to the computer/domain**O*M**K*****O*M**K*****nk #####`  
*****H *****Users 'x@***{"version":1,"questions":[{"question":"What was your first pet s name?", "answer":"GCTF{p3rs0nal"}, {"question":"What s the name of  
the city where you were born?", "answer":"_s3cr3ts_"}, {"question":"What was your childhood nickname?", "answer":"r3g1stry"}]]**1+!+g#7*!  
T=wYyyY***}+2***p_*+2*E*P***R***Yf*1S+pw*****'***nv-*C*(cpv*2+9***j1+*z***  
HUV,*****G*3*8{******-lyVf*H7***j***zQ***1***{+I***f*]***s***W***Deer:g*D*V*]***yC***a*G]*  
+*18*b*UJ***W***t***x***K*t*M***3=1L*2*E  
+*Dee... ehe...A?Y...e...e...Cp...e...e...Y...e...
```

Flag: GCTF{p3rs0nal_s3cr3ts_r3g1stry}

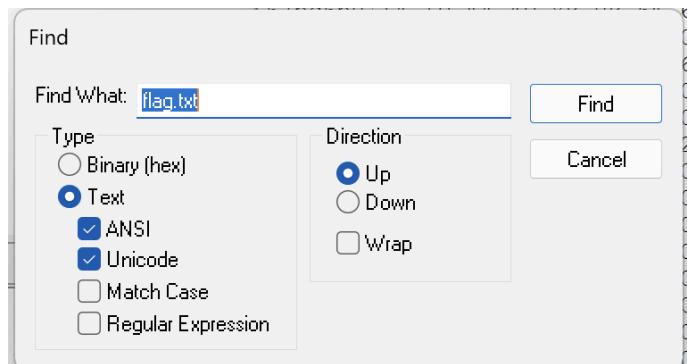
MFTBasics



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

The FTK Imager interface shows the Evidence Tree with a selected folder containing mft2csv_v2.0.0.13 and foresecrets.aid. The File List pane displays the contents of the \$MFT file, including its structure and data. The Hex Value Interpreter pane shows the raw byte values for various fields like FILETIME, FILETIME (local), and DOS date. The status bar at the bottom right indicates "Activate Windows".

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

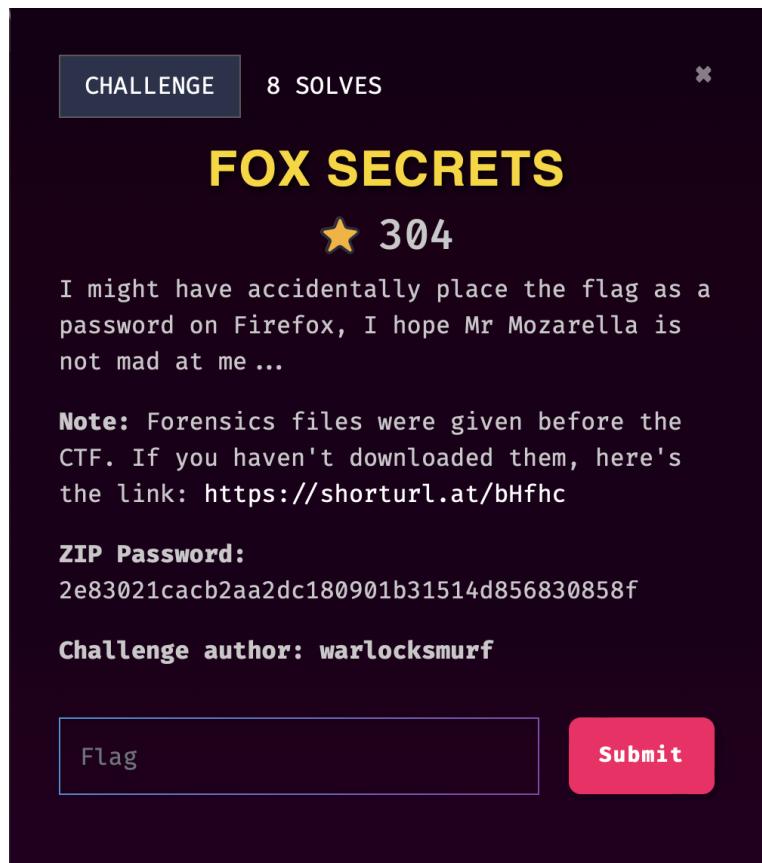
6fadfcf0	08 03 66 00 6C 00 61 00-67 00 2E 00 74 00 78 00	f · l · a · g · · t · x ·
6fadd00	74 00 00 00 00 00 00-40 00 00 00 28 00 00 00 00	t · · · · @ · (· · · ·
6fadd10	00 00 00 00 00 05 00-10 00 00 00 18 00 00 00 00	· · · · · · · · · ·
6fadd20	87 8D 61 04 88 6B EF 11-AB D7 00 0C 29 22 8E 27	· a · ki · <> ·) " ·
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 00	ÿÿÿÿ · yG · · · ·
6faddb0	FF FF FF FF 82 79 47 11-00 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.

The screenshot shows the CyberChef interface. The left sidebar has 'Operations' selected. Under 'From Hex', the 'Delimiter' is set to 'Auto'. The 'Input' field contains the hex dump: 47 43 54 46 7b 62 34 73 31 63 73 5f 30 66 5f 4d 46 54 7d. The 'Output' field shows the converted text: GCTF{b4s1cs_0f_MFT}.

Flag: GCTF{b4s1cs Of 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

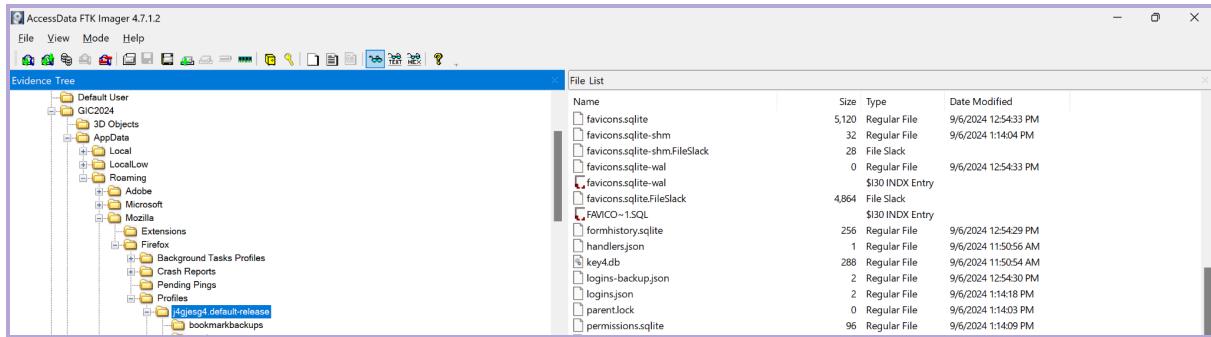


Mozilla Support
<https://support.mozilla.org> :

Profiles - Where Firefox stores your bookmarks, passwords ...

Firefox stores your profile folder in this location on your computer, by default: C:\Users\<your Windows login username>\AppData\Roaming\Mozilla\Firefox\ ...

So to look for the files, I just opened the directories on FTK imager
GIC2024\AppBarData\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

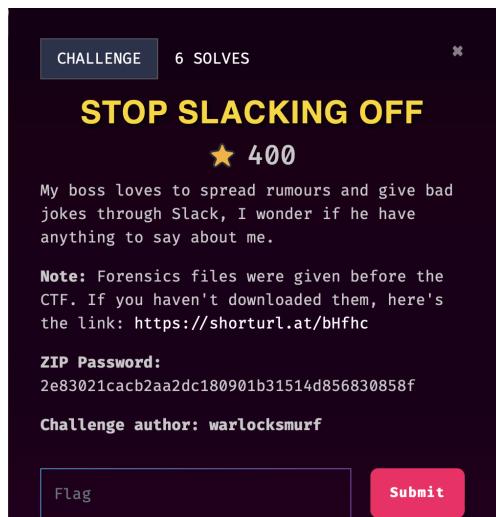
```
zsh: no such file or directory: https://github.com/lclevy/firepwd
(base) sayyidahnafish@Sayyidahs-MacBook-Air ~ % git clone https://github.com/lclevy/firepwd

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) sayyidahnafish@Sayyidahs-MacBook-Air ~ % ls
firepwd  key4.db  logins.json
(base) sayyidahnafish@Sayyidahs-MacBook-Air ~ % cd firepwd
(base) sayyidahnafish@Sayyidahs-MacBook-Air ~ % ls
LICENSE          logins.json        mozilla_pbe.svg
firepwd.py       mozilla_db        readme.md
key4.db          mozilla_pbe.pdf   requirements.txt
(base) sayyidahnafish@Sayyidahs-MacBook-Air ~ % python3 firepwd
python3: can't open file '/Users/sayyidahnafish/Desktop/shared/fox secret/firepwd/firepwd': [Errno 2] No such file or directory
(base) sayyidahnafish@Sayyidahs-MacBook-Air ~ % python3 firepwd.py
globalSalt: b'b5dbfe66b891e193f516eccaa39299a93634332'
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'ea23448d176f2f091e1a9b2162b550a9874bf9ced92daa19c43e058b1328cf'
                INTEGER b'81'
                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'c361eb13322fd600+ad463de0ef2'
    }
}
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'ae2720e0964ce4beabedba40345712df4234f9ac9cd86e53a08982b65abbdb9c'
                INTEGER b'81'
                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
    }
}
```

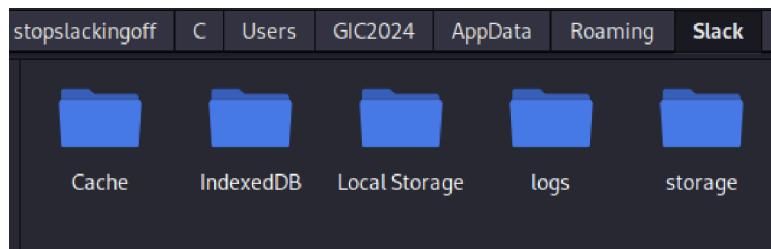
Finally we cracked the password and retrieved the flag after doing all the steps.

Flag:GCTF{m0zarella_f1ref0x_p4ssw0rd}

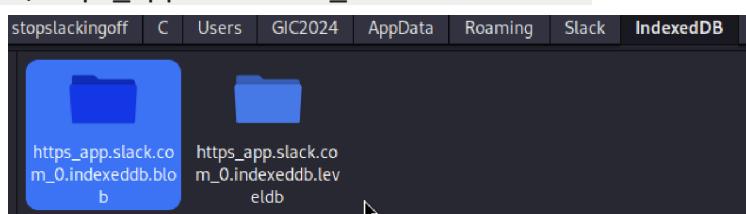
Stop Slacking Off



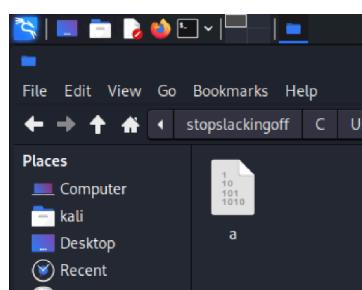
There are 5 folders in the Slack directory. I actually checked and cat all the files in those folders.



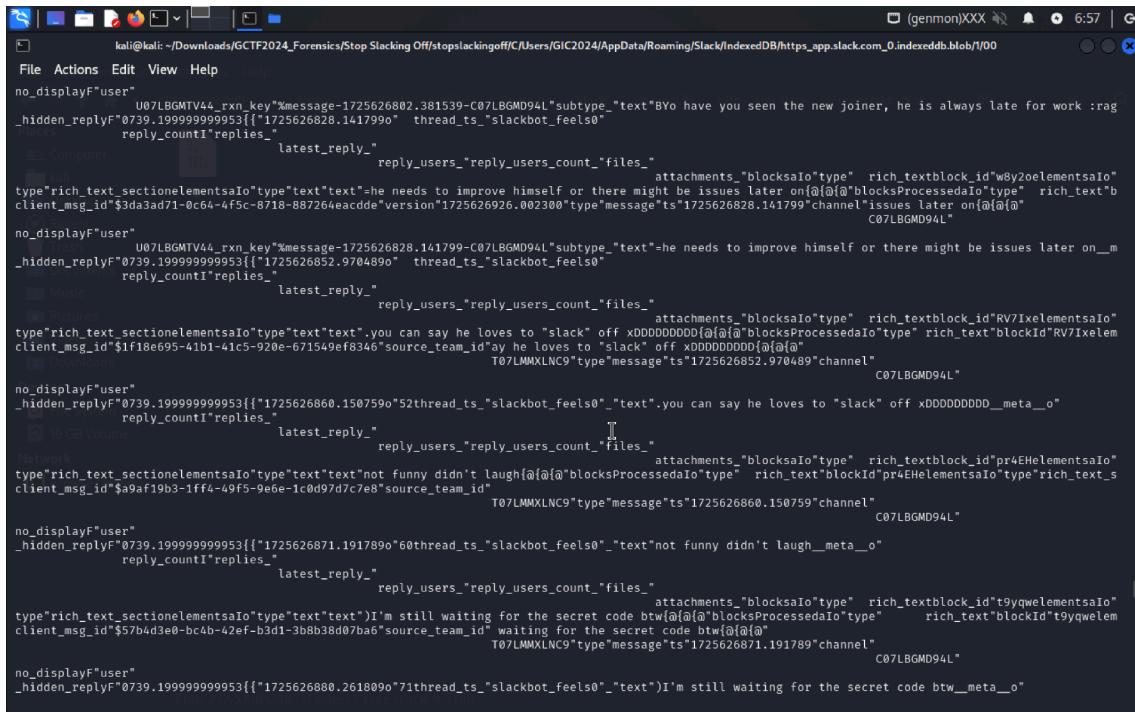
After carefully checked the content of the files, I finally found the conversations on /Slack/IndexedDB/https_app.slack.com_0.indexeddb.blob



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.

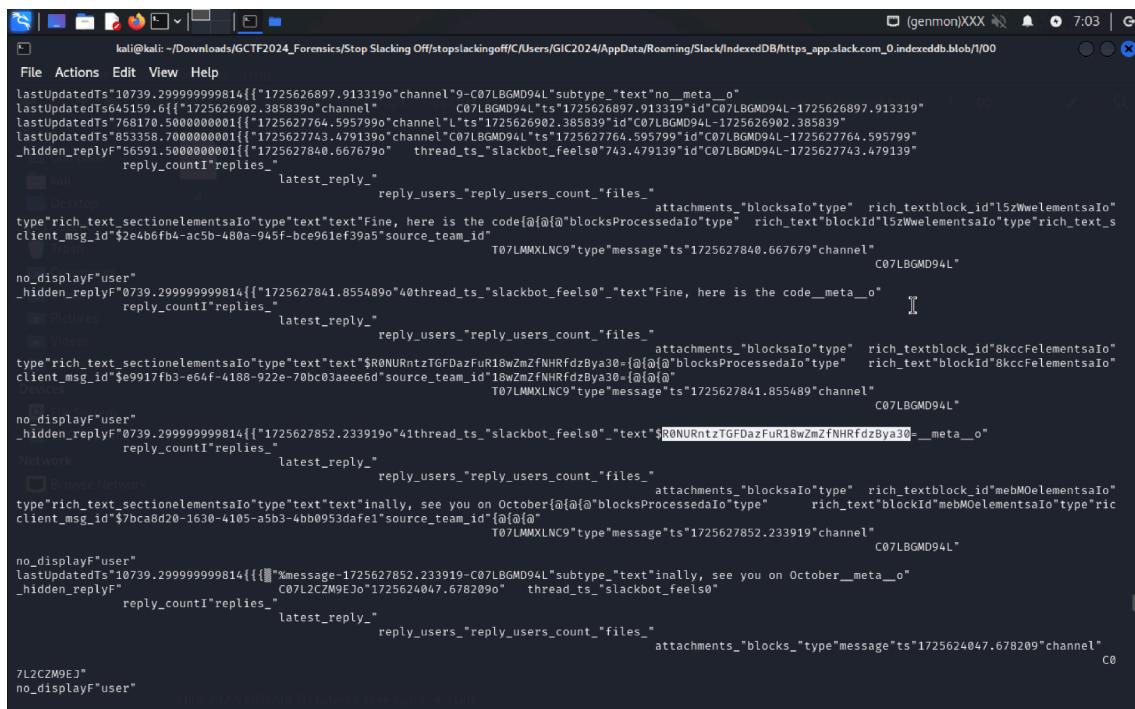


```
kali㉿kali: ~/Downloads/GCTF2024_Forensics/Stop Slacking Off/stopslackingoff/C/Users/GIC2024/AppData/Roaming/Slack/IndexedDB/https_app.slack.com_0_indexeddb.blob/f/00
File Actions Edit View Help
no_displayF"user"
    U07LBGMTV44_rxn_key"%message-1725626802.381539-C07LBGMD94L"subtype_"text"BYo have you seen the new joiner, he is always late for work :rag
_no_hidden_replyF"0739.199999999953[{"1725626828.1417990" "thread_ts_"slackbot_feels0"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"w8y2oelementsA0"
type"rich_text_sectionelementsA0"type"text"text"=he needs to improve himself or there might be issues later on@{@{@blocksProcessedA0"type" rich_text"b
client_msg_id"$3da3ad71-0c64-4fc-8718-887264eacdde"version"1725626926.00230"message"ts"1725626828.141799"channel"issues later on@{@{@
_c07LBGMD94L"
no_displayF"user"
    U07LBGMTV44_rxn_key"%message-1725626802.381539-C07LBGMD94L"subtype_"text"=he needs to improve himself or there might be issues later on_m
_no_hidden_replyF"0739.199999999953[{"1725626852.9704890" "thread_ts_"slackbot_feels0"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"RV7IxelementsA0"
type"rich_text_sectionelementsA0"type"text"text"=you can say he loves to "slack" off xDDDDDDDDD@{@{@blocksProcessedA0"type" rich_text"blockId"RV7Ixelem
client_msg_id$1f18e695-41b1-41c5-920e-671549ef8346"source_team_id"ay he loves to "slack" off xDDDDDDDDD@{@{@
T07LMMXLNC9"type"message"ts"1725626852.970489"channel"
C07LBGMD94L"
no_displayF"user"
_no_hidden_replyF"0739.199999999953[{"1725626860.1507590"52"thread_ts_"slackbot_feels0"_"text".you can say he loves to "slack" off xDDDDDDDDD__meta_o"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"pr4EHelementsA0"
type"rich_text_sectionelementsA0"type"text"text"not funny didn't laugh@{@{@blocksProcessedA0"type" rich_text"blockId"pr4EHelementsA0"type"rich_text_s
client_msg_id$a9af19b3-1ff4-49f5-9e6e-1c0d97d7c7e8"source_team_id"
T07LMMXLNC9"type"message"ts"1725626860.150759"channel"
C07LBGMD94L"
no_displayF"user"
_no_hidden_replyF"0739.199999999953[{"1725626871.1917890"60"thread_ts_"slackbot_feels0"_"text"not funny didn't laugh__meta_o"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"t9yqwelementsA0"
type"rich_text_sectionelementsA0"type"text"text"!m still waiting for the secret code btw@{@{@blocksProcessedA0"type" rich_text"blockId"t9yqwelem
client_msg_id$57b4d3e0-bc4b-42ef-b3d1-3bb38d07ba6"source_team_id" waiting for the secret code btw@{@{@
T07LMMXLNC9"type"message"ts"1725626871.191789"channel"
C07LBGMD94L"
no_displayF"user"
_no_hidden_replyF"0739.199999999953[{"1725626880.2618090"71"thread_ts_"slackbot_feels0"_"text")I'm still waiting for the secret code btw__meta_o"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"

```

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

RONURntzTGF DazFuR18wZmZfNHRfdzBya30



```
kali㉿kali: ~/Downloads/GCTF2024_Forensics/Stop Slacking Off/stopslackingoff/C/Users/GIC2024/AppData/Roaming/Slack/IndexedDB/https_app.slack.com_0_indexeddb.blob/f/00
File Actions Edit View Help
lastUpdatedTs"10739.29999999814[{"1725626897.9133190"channel"9-C07LBGMD94L"subtype_"text"no__meta_o"
lastUpdatedTs"10739.29999999814[{"1725626902.3858390"channel"
C07LBGMD94L"ts"1725626897.913319"id"C07LBGMD94L-1725626897.913319"
lastUpdatedTs"768170.500000001[{"1725627764.5957990"channel"1"ts"1725626902.385839"id"C07LBGMD94L-1725626902.385839"
lastUpdatedTs"753358.700000001[{"1725627743.4791390"channel"1"ts"1725627764.595799"id"C07LBGMD94L-1725627764.595799"
_no_hidden_replyF"5691.500000001[{"1725627840.6676790" "thread_ts_"slackbot_feels0"743.479139"id"C07LBGMD94L-1725627743.479139"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"l5zWwelementsA0"
type"rich_text_sectionelementsA0"type"text"text"Fine, here is the code@{@{@blocksProcessedA0"type" rich_text"blockId"l5zWwelementsA0"type"rich_text_s
client_msg_id$2e4b6fb4-ac5b-480a-945f-bce691ef39a5"source_team_id"
T07LMMXLNC9"type"message"ts"1725627840.667679"channel"
C07LBGMD94L"
no_displayF"user"
_no_hidden_replyF"0739.29999999814[{"1725627841.8554890"40"thread_ts_"slackbot_feels0"_"text"fine, here is the code__meta_o"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"8kccFelementsA0"
type"rich_text_sectionelementsA0"type"text"text"$$RONURntzTGF DazFuR18wZmZfNHRfdzBya30=[@{@{@blocksProcessedA0"type" rich_text"blockId"8kccFelementsA0
client_msg_id$9917fb3-e64f-4188-922e-70bc03aeee6"source_team_id"18wZmZfNHRfdzBya30=[@{@{@
T07LMMXLNC9"type"message"ts"1725627841.855489"channel"
C07LBGMD94L"
no_displayF"user"
_no_hidden_replyF"0739.29999999814[{"1725627852.2339190"41"thread_ts_"slackbot_feels0"_"text"$$RONURntzTGF DazFuR18wZmZfNHRfdzBya30=__meta_o"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"mebMoelementsA0"
type"rich_text_sectionelementsA0"type"text"text"inally, see you on October@{@{@blocksProcessedA0"type" rich_text"blockId"mebMoelementsA0"type"ric
client_msg_id$7bca8d20-1630-4105-a5b3-4bb0953dafe1"source_team_id"[@{@{@
T07LMMXLNC9"type"message"ts"1725627852.233919"channel"
C07LBGMD94L"
no_displayF"user"
lastUpdatedTs"10739.29999999814[{"1725627852.233919-C07LBGMD94L"subtype_"text"inally, see you on October__meta_o"
_no_hidden_replyF" C07LB2CZM9EJ"0725624047.678209" "thread_ts_"slackbot_feels0"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocks_A0"type"message"ts"1725624047.678209"channel"
C07LB2CZM9EJ"
7L2CZM9EJ"
no_displayF"user"

```

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

The screenshot shows the CyberChef interface with the following details:

- Input:** R0NURntzTGFdazFuR18wZmZfNHRfdzBya30
- Recipe:** Magic (Depth 3, Intensive mode checked)
- Output:** Four rows of decrypted data:
 - From_Base85('0-9a-zA-Z.\\";:+=~!/*?&>()[]{}@%\$#') Decode_text('IBM EBCDIC French (1010)')
 - From_Base64('A-Za-z0-9_+',true,false)
 - From_Base64('A-Za-z0-9_+',true,false)
 - From_Base85('0-9a-zA-Z.\\";:+=~!/*?&>()[]{}@%\$#') Decode_text('IAS German (7-bit) (20106)')Each row includes raw bytes, hex dump, entropy, and validation information (Valid UTF8, Entropy: 2.56, Matching ops: From Base85, etc.).
- Buttons:** STEP, BAKE!, Auto Bake

Flag: GCTF{sLaCk1nG_0ff_4t_w0rk}