Chat with me[FOREN]

Description

Help JoPraveen to check his GF phone, in which she hides a message secretly

Writeup

```
❯ ls
Stickers.zip
```

- Let's unzip it

```
❯ ls
 Alarms    DCIM            Movies          Notifications   Podcasts
Stickers.zip
 Albums    download        Music           OTA-Updater     ppy_cross
whatsapp.zip.cpt
 Android   LOST.DIRmedia  'My Documents'   Pictures        Ringtones
```

- Here we got some folders.
- Looks like we got folders of **Internal storage**
- Let's run tree command to see what's there

```
❯ tree -a .
.
├── Alarms
├── Albums
├── Android
│   ├── data
│   │   └── com.tencent.ig
```

```
│   │       └── files
│   │           └── gunnnnnsss
│   └── obb
│       └── hidddddddeeennnnn_properlyyy.obb
├── DCIM
├── download
│   └── WhatsApp Chat with SECRET_DISCUSSIONS.txt
├── LOST.DIRmedia
├── Movies
├── Music
├── My Documents
├── Notifications
├── OTA-Updater
├── Pictures
├── Podcasts
├── ppy_cross
├── Ringtones
└── whatsapp.zip.cpt

19 directories, 4 files
```

Interesting files

```
hidddddddeeennnnn_properlyyy.obb
WhatsApp Chat with SECRET_DISCUSSIONS.txt
whatsapp.zip.cpt
```

- First let's see the .obb file

```
❯ file hidddddddeeennnnn_properlyyy.obb
hidddddddeeennnnn_properlyyy.obb: Zip archive data, at least v2.0 to
extract
```

- It's not an obb file, it's a zip file and its password protected
- Sad we don't have the password

- Now let's see the second interesting file **WhatsApp Chat with SECRET_DISCUSSIONS.txt**

```
❯ cat WhatsApp\ Chat\ with\ SECRET_DISCUSSIONS.txt
8/4/21, 3:36 PM - Messages and calls are end-to-end encrypted. No one
outside of this chat, not even WhatsApp, can read or listen to them.
Tap to learn more.
8/4/21, 3:36 PM - You created group "SECRET_DISCUSSIONS"
8/4/21, 3:36 PM - jopraveen: Hey are you there?
8/4/21, 3:36 PM - jopraveen: I want the password of that zip file
8/4/21, 3:37 PM - jopraveen: zipppppppppppp
8/4/21, 3:37 PM - jopraveen: hey
8/4/21, 3:38 PM - jopraveen: 😥😥😥
8/4/21, 3:38 PM - jopraveen: I want to get the flag
8/4/21, 3:38 PM - jopraveen: Help!
8/4/21, 3:38 PM - jopraveen: hellppppp
8/4/21, 3:40 PM - jopraveen: STK-20210804-WA0097.webp (file attached)
8/4/21, 4:00 PM - jopraveen: and there's no password
8/4/21, 4:17 PM - jopraveen: I'm gonna cramckkk ittttt🏃🏃🏃
```

- See the last few messages, Looks like there's no password here, and we need to crack it
- Let's use zip2john to crack it

Cracking zip file

```
❯ zip2john hidddddddeeennnnnn_properlyyy.obb > hash
ver 2.0 efh 5455 efh 7875
hidddddddeeennnnnn_properlyyy.obb/get_password.py PKZIP Encr: 2b chk,
TS_chk, cmplen=100, decmplen=94, crc=3654176C

❯ john -w=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
```

```
Press 'q' or Ctrl-C to abort, almost any other key for status
samantha.        (hidddddddeeennnnn_properlyyy.obb/get_password.py)
1g 0:00:00:00 DONE (2021-08-20 14:46) 33.33g/s 3959Kp/s 3959Kc/s
3959KC/s 022893..bratzy
Use the "--show" option to display all of the cracked passwords
reliably
Session completed
```

- Cool we cracked the password and its `samantha.`
- Let's unzip it
- We got a python file

PYTHON

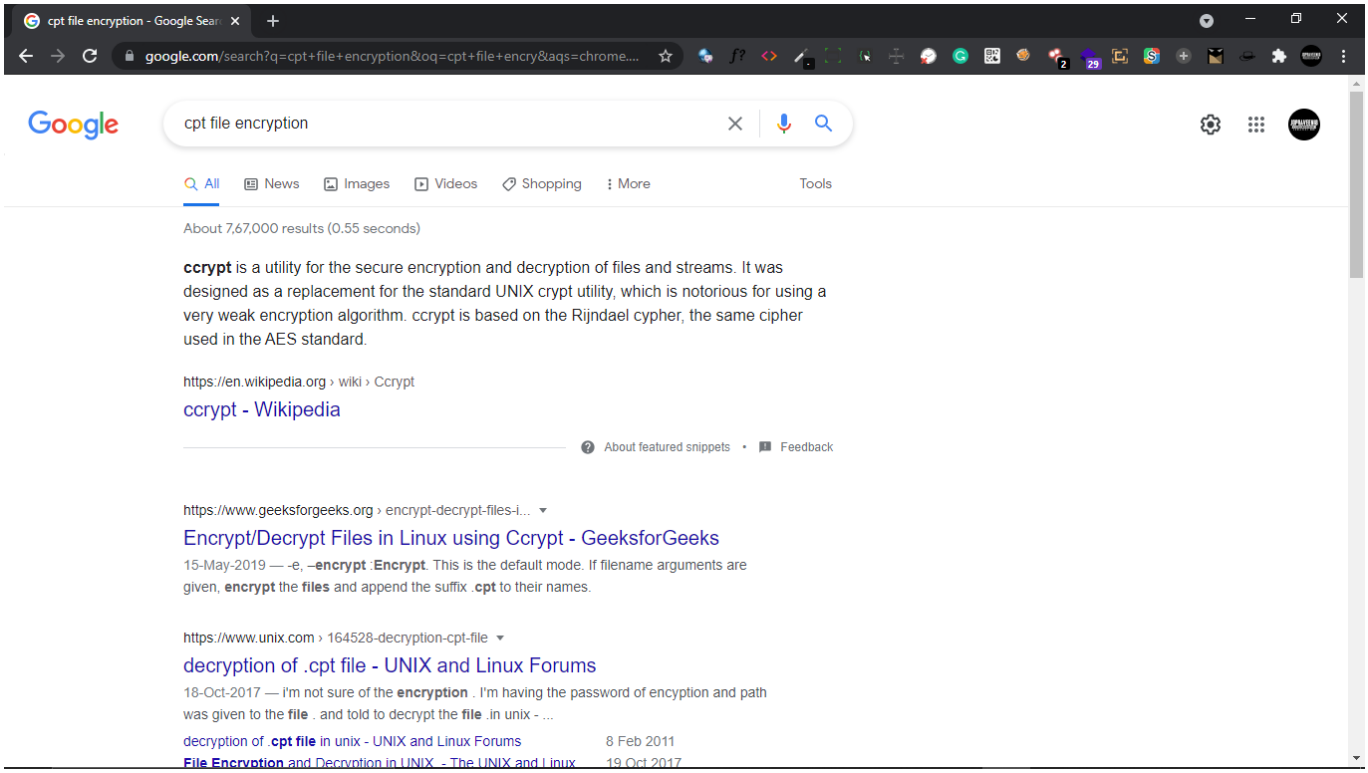
```python
❯ cat get_password.py
#!/usr/bin/python3
print("p4assW0rd_1s_n0t_s3cur333")
# this is the password for another file
```

- Ok I think this is the password for the third file `whatsapp.zip.cpt`

cracking whatsapp.zip.cpt

```
❯ file whatsapp.zip.cpt
whatsapp.zip.cpt: data
```

- let's search about .cpt file encryptions



- It's encrypted with **ccrypt**
- Let's decrypt it with the password `p4assW0rd_1s_n0t_s3cur333` that we got from the python file

```
❯ ccdecrypt whatsapp.zip.cpt
Enter decryption key:
```

- Cool, and now we got a zip file `whatsapp.zip`
- After unzipping we got some files

```
❯ tree -a .
.
├── backups
├── databases
├── media
│   ├── Whatsapp_cringesss
│   ├── Whatsapp_documents
│   ├── Whatsapp_images
│   ├── whatsapp_messagesssssssssss
│   │   └── WhatsApp Chat with GIMME FLAG VROO.txt
```

```
│   ├── Whatsapp_stickers
│   │   ├── STK-20210804-WA0136.webp
│   ├── Whatsapp_videos
│   └── Whatsapp_voice_notes
└── .shared
```

▶ A chat backup file and a sticker are there

Let's read that chat

```
❯ cat WhatsApp\ Chat\ with\ GIMME\ FLAG\ VROO.txt
8/4/21, 5:07 PM - Messages and calls are end-to-end encrypted. No one
outside of this chat, not even WhatsApp, can read or listen to them.
Tap to learn more.
8/4/21, 5:07 PM - You created group "GIMME FLAG VROO"
8/4/21, 5:07 PM - jopraveen: Hey broo
8/4/21, 5:08 PM - 👀PJ HK3R: Hell0
8/4/21, 5:08 PM - jopraveen: finnaly I cracked the zip
8/4/21, 5:08 PM - jopraveen: where is the flag
8/4/21, 5:08 PM - jopraveen: Gimme flag vro
8/4/21, 5:08 PM - 👀PJ HK3R: What flag
8/4/21, 5:08 PM - 👀PJ HK3R: I'm Hecker !
8/4/21, 5:08 PM - jopraveen: ‎oh no
8/4/21, 5:09 PM - jopraveen: I need challenge's flag
8/4/21, 5:09 PM - jopraveen: TamilCTF{flag}
8/4/21, 5:09 PM - 👀PJ HK3R: STK-20210804-WA0170.webp (file attached)
8/4/21, 5:09 PM - jopraveen: ‎‎ohh nooo
8/4/21, 5:09 PM - 👀PJ HK3R: No
8/4/21, 5:09 PM - jopraveen: gime broo plss🥺
8/4/21, 5:09 PM - 👀PJ HK3R: I'm beluga 😇
8/4/21, 5:09 PM - jopraveen: Hey
8/4/21, 5:09 PM - 👀PJ HK3R: STK-20210804-WA0171.webp (file attached)
8/4/21, 5:09 PM - jopraveen: h-
8/4/21, 5:10 PM - jopraveen: hii
8/4/21, 5:10 PM - jopraveen: ho
```

8/4/21, 5:10 PM - 👀PJ HK3R: T
8/4/21, 5:10 PM - jopraveen: Belegua is a good cat
8/4/21, 5:10 PM - 👀PJ HK3R: Y
8/4/21, 5:10 PM - 👀PJ HK3R: E
8/4/21, 5:10 PM - 👀PJ HK3R: P
8/4/21, 5:10 PM - jopraveen: S
8/4/21, 5:10 PM - jopraveen: st-
8/4/21, 5:10 PM - jopraveen: stop it
8/4/21, 5:10 PM - 👀PJ HK3R: STK-20210804-WA0172.webp (file attached)
8/4/21, 5:10 PM - 👀PJ HK3R: You want Flag?
8/4/21, 5:10 PM - jopraveen: yes catttt😻
8/4/21, 5:10 PM - jopraveen: meawwww
8/4/21, 5:10 PM - jopraveen: meaww
8/4/21, 5:10 PM - 👀PJ HK3R: 🏳
8/4/21, 5:10 PM - 👀PJ HK3R: 🏴
8/4/21, 5:10 PM - 👀PJ HK3R: 🏴‍☠️
8/4/21, 5:10 PM - 👀PJ HK3R: 🏁
8/4/21, 5:10 PM - 👀PJ HK3R: 🏳
8/4/21, 5:10 PM - 👀PJ HK3R: 🏳
8/4/21, 5:11 PM - jopraveen: gimee flag
8/4/21, 5:11 PM - 👀PJ HK3R: 🏳
8/4/21, 5:11 PM - 👀PJ HK3R: GT
8/4/21, 5:11 PM - 👀PJ HK3R: Ok?
8/4/21, 5:11 PM - jopraveen: nooo
8/4/21, 5:11 PM - jopraveen: the real flag
8/4/21, 5:11 PM - 👀PJ HK3R: IN
8/4/21, 5:11 PM - jopraveen: STK-20210804-WA0097.webp (file attached)
8/4/21, 5:11 PM - 👀PJ HK3R: STK-20210804-WA0136.webp (file attached)
8/4/21, 5:11 PM - jopraveen: oh noo
8/4/21, 5:11 PM - jopraveen: Bye vrooo
8/4/21, 5:11 PM - jopraveen: I'm upset
8/4/21, 5:11 PM - 👀PJ HK3R: 🏴‍☠️
8/4/21, 5:11 PM - jopraveen: you trolled me
8/4/21, 5:11 PM - 👀PJ HK3R: I'm depremssed
8/4/21, 5:12 PM - jopraveen: 😭mee too
8/4/21, 5:12 PM - 👀PJ HK3R: STK-20210804-WA0173.webp (file attached)

```
8/4/21, 5:12 PM - 👀PJ HK3R: B
8/4/21, 5:12 PM - 👀PJ HK3R: Y
8/4/21, 5:12 PM - 👀PJ HK3R: E
8/4/21, 5:12 PM - jopraveen: any hints? to find the flag?
8/4/21, 5:12 PM - 👀PJ HK3R: One sec
8/4/21, 5:12 PM - jopraveen: yehhhh
8/4/21, 5:12 PM - 👀PJ HK3R: TamilCTF{sorry}
8/4/21, 5:12 PM - 👀PJ HK3R: 😇
8/4/21, 5:13 PM - jopraveen: Okkk‍ let me try harder!!
8/4/21, 5:13 PM - 👀PJ HK3R: STK-20210804-WA0174.webp (file attached)
8/4/21, 5:13 PM - 👀PJ HK3R: EBY
8/4/21, 5:13 PM - jopraveen: bad cat
8/4/21, 5:13 PM - jopraveen: bye
8/4/21, 5:13 PM - You removed 👀PJ HK3R
8/4/21, 7:18 PM - jopraveen: Bad cat
8/4/21, 7:18 PM - jopraveen: 🐈
8/4/21, 7:20 PM - jopraveen: btw cool $tickers, let's add to favorites
👀💃
```

- Read the chat carefully
- Looks like something interesting in that sticker file
- Challenge name **Stickers**
- Challenge description `I hope you know how to send a WhatsApp sticker`
- Here in the above message `jopraveen: btw cool $tickers, let's add to favorites👀💃`
- Ok now let's analyze that file `STK-20210804-WA0136.webp`
- Nothing interesting in exiftool
- Let's use strings

```
{"sticker-pack-
id":"com.snowcorp.stickerly.android.stickercontentprovider 5661e2d0-
bfcd-40e6-8fed-7f91e43735c5","sticker-pack-
link":"https://sticker.ly/s/<sticker-pack-code>","sticker-pack-
code":"3HCM91","sticker-pack-publisher":"Sticker.ly *
jopraveen","android-app-store-
link":"https:\/\/play.google.com\/store\/apps\/details?
```

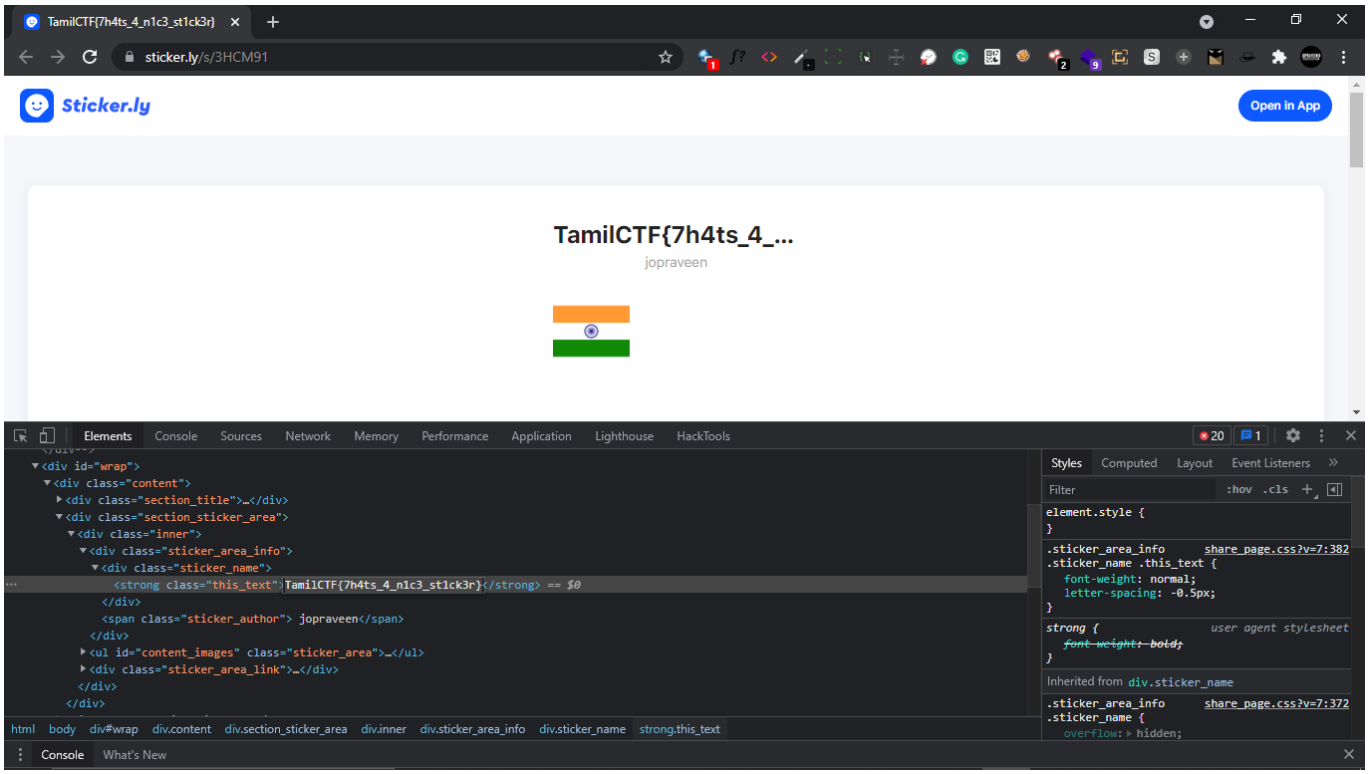
```
id=com.snowcorp.stickerly.android","ios-app-store-
link":"https:\/\/itunes.apple.com\/app\/id1458740001?mt=8"}
```

- We got this in the bottom of the strings output
- Look carefully here

```
"sticker-pack-link":"https://sticker.ly/s/<sticker-pack-code>"

"sticker-pack-code":"3HCM91"
```

- These are the interesting info from the above input
- Looks like we can access this sticker pack with the link
- To get a complete link we need to add the sticker pack's code in last part of the url (mentioned in the link)
- https://sticker.ly/s/3HCM91
- Ok now let's visit this link



Cool we got our flag `TamilCTF{7h4ts_4_n1c3_st1ck3r}`