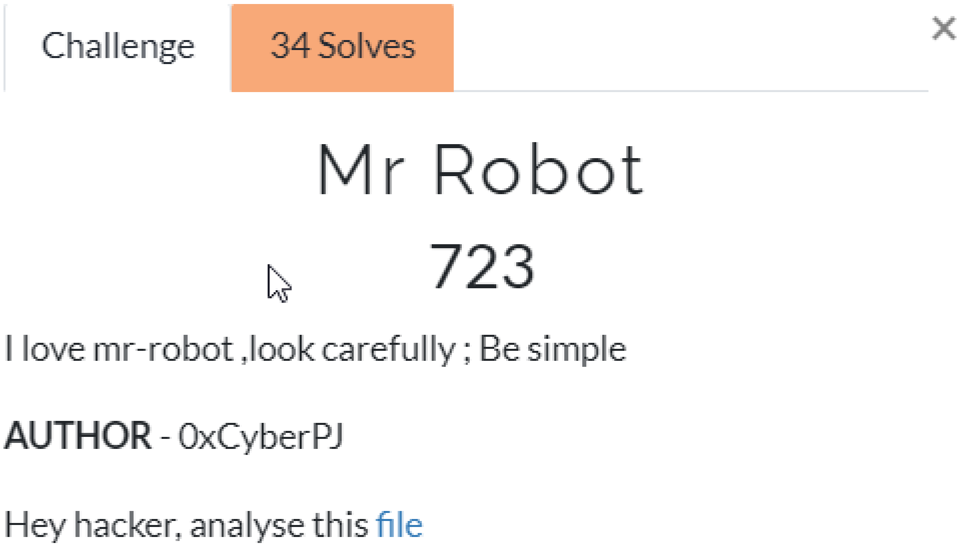
Challenge Name: Mr-robot

CATEGORY: FORENSICS

Level : medium

FLAG: TamilCTF{r7f_is_n0t_4_d0c}

AUTHOR: Paul Jeremiah



Mr Robot

723

I love mr-robot ,look carefully ; Be simple

AUTHOR - 0xCyberPJ

Hey hacker, analyse this file

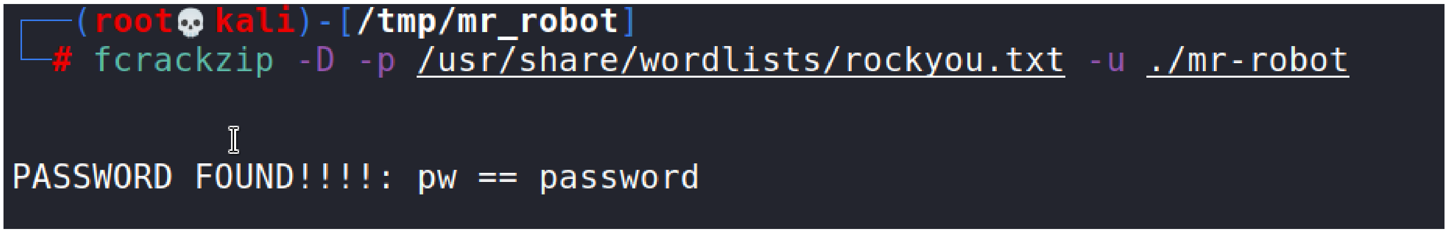
Given : a zip file named as mr-robot

```
┌──(root💀kali)-[/tmp/mr_robot]
└─# file mr-robot
mr-robot: Zip archive data, at least v2.0 to extract
```

```
┌──(root💀kali)-[/tmp/mr_robot]
└─# unzip mr-robot

Archive:  mr-robot
[mr-robot] mr_beta.rtf password:
```

who knows the password? : author, lol :)



```
┌──(root💀kali)-[/tmp/mr_robot]
└─# fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u ./mr-robot


PASSWORD FOUND!!!!: pw == password
```

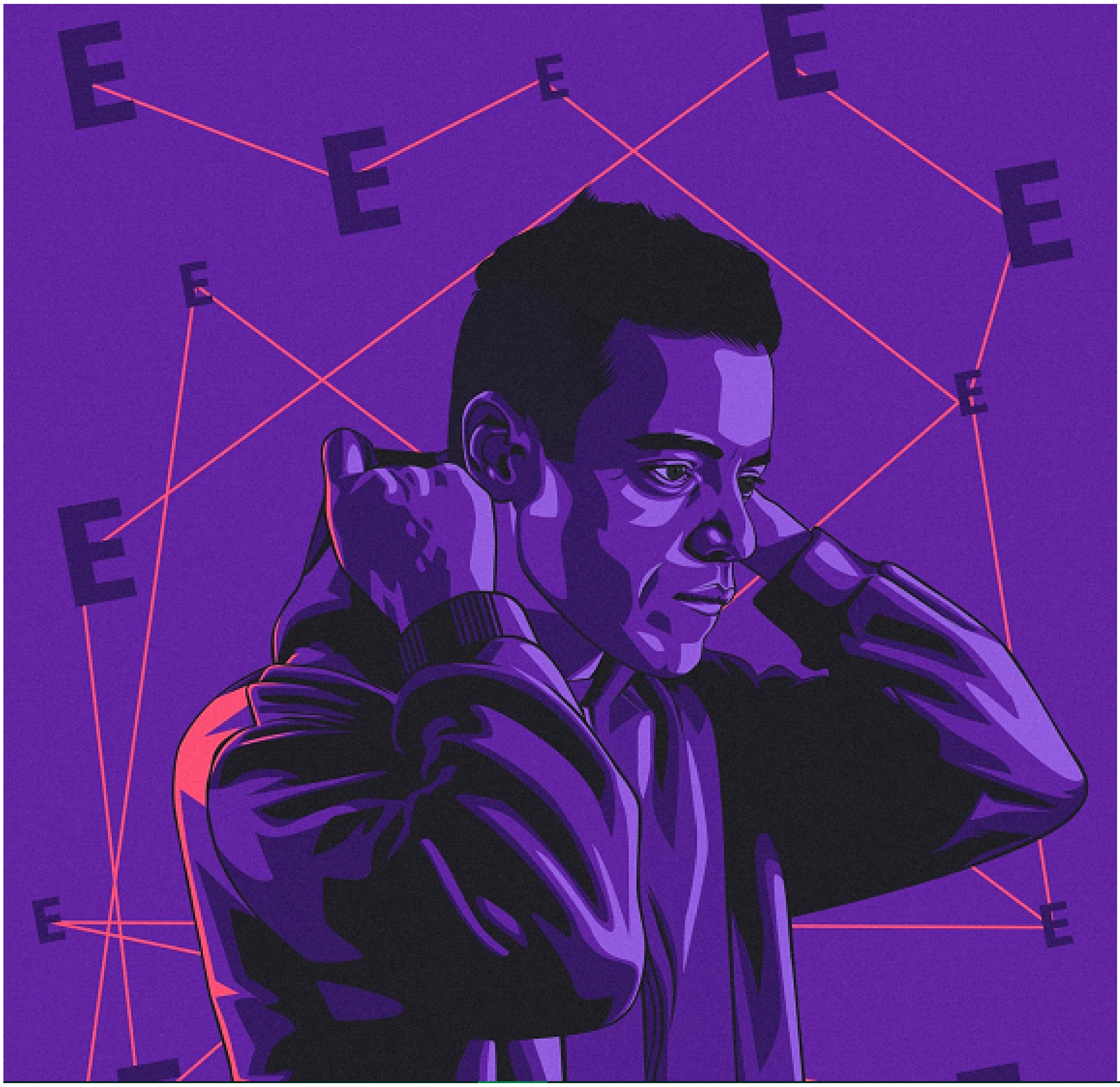
(strongest password! Ever)

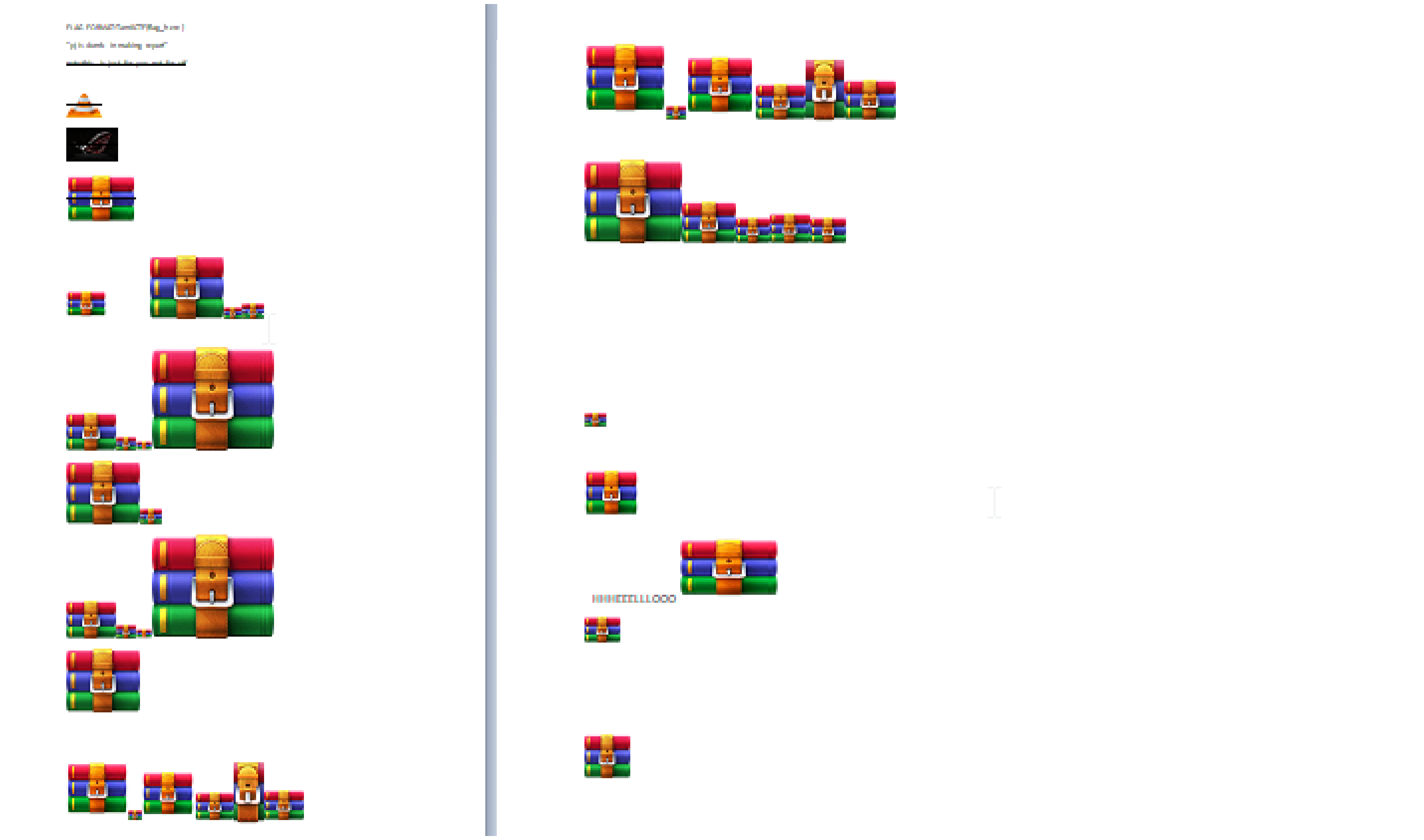
after unzip - `inflating: mr_beta.rtf`

```
┌──(root💀kali)-[/tmp/mr_robot]
└─# file mr_beta.rtf
mr_beta.rtf: Rich Text Format data, version 1, ANSI, code page 1252
```

RTF!
let's view it I used Wordpad

(for the screenshot I zoomed out a lot)



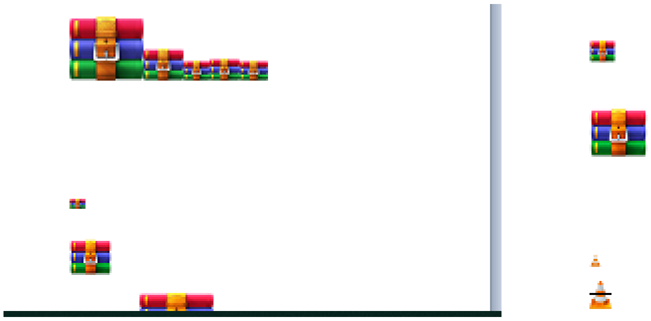


FLAG FORMAT:TamilCTF{flag_h ere }

"pj is dumb in making report"

[illegible]

HHHEEELLLOOO



> ahh something here
> lots of WinRAR icons and a vlc too
> might be object embedded into the rtf file
> (else drag and try to drop each one into thunar if yes :) move on)

So how to extract an object from the RTF ?

`pip3 install oletools`
oletools is a collection of tools related to object stuff under Docx,RTF,and etc.
awesome tools

rtfobj is a Python module to extract embedded objects from RTF files, such as. OLE ojects. It can be used as a Python library or a command-line tool

```
┌──(root💀kali)-[/tmp/mr_robot]
└─# rtfobj
rtfobj project website: http://www.decalage.info/python/rtfobj

  -s SAVE_OBJECT, --save=SAVE_OBJECT
                        Save the object corresponding to the provided number
                        to a file, for example "-s 2". Use "-s all" to save
                        all objects at once.
  -d OUTPUT_DIR         use specified directory to save output files.
```

lets extract object from rtf

```
rtfobj mr_beta.rtf -s all -d .
```

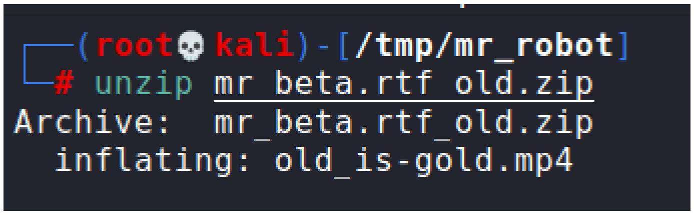
```
┌──(root💀kali)-[/tmp/mr_robot]
└─# rtfobj mr_beta.rtf -s all -d .
130 ×
rtfobj 0.60 on Python 3.9.2 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
```

```
Please report any issue at https://github.com/decalage2/oletools/issues

File: 'mr_beta.rtf' - size: 53019689 bytes
---+----------+---------------------------------------------------------------
id |index     |OLE Object
---+----------+-------------------------------------------------------------
0  |025A0624h |format_id: 2 (Embedded)
   |          |class name: b'Package'
   |          |data size: 3860079
   |          |OLE Package object:
   |          |Filename: 'old.zip'
   |          |Source path: 'C:\\Users\\pj\\3D
   |          |Objects\\doc\\test\\old\\old.zip'
   |          |Temp path = 'C:\\Users\\pj\\AppData\\Local\\Temp\\old.zip'
   |          |MD5 = 'e34b52c886624f92d468acb4848fb0db'
   |          |File Type: Zip Archive
---+----------+--------------------------------------------------------------
Saving file from OLE Package in object #0:
  Filename = 'old.zip'
  Source path = 'C:\\Users\\..\\3D Objects\\doc\\test\\old\\old.zip'
  Temp path = 'C:\\Users\\..\\AppData\\Local\\Temp\\old.zip'
  saving to file ./mr_beta.rtf_old.zip
  md5 e34b52c886624f92d468acb4848fb0db
```

So We Got the interesting thing

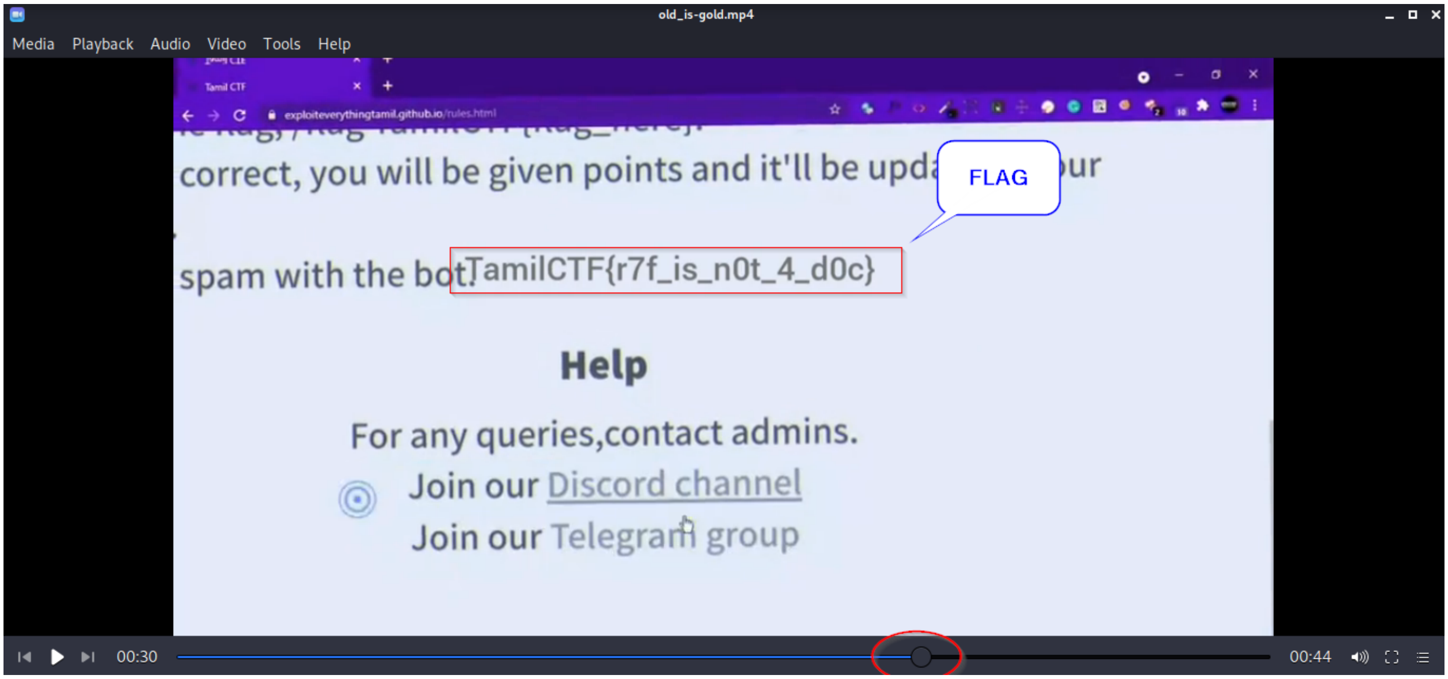
- unzip



```
┌──(root💀kali)-[/tmp/mr_robot]
└─# unzip mr_beta.rtf_old.zip
Archive:  mr_beta.rtf_old.zip
  inflating: old_is-gold.mp4
```

-
- play the old_is_gold.mp4
  -the video about the past event, which is conducted by tamilctf team

:30 seconds make sense



correct, you will be given points and it'll be upda ur

spam with the bot TamilCTF{r7f_is_n0t_4_d0c}

Help

For any queries,contact admins.

Join our Discord channel

Join our Telegram group

Flag : TamilCTF{r7f_is_n0t_4_d0c}

First Blood :

Les Pires Hat	2 days ago

THATS ALL

@cyberpj