







main

Go to file

- Cryptography/John_the_Rocker
 - files
 - idrsa.id_rsa.docx
 - idrsa.id_rsa.txt
 - img
 - README.md
 - Forensic
 - So_Forgetful
 - files
 - Ghost.pcap
 - img
 - challenge.png
 - chef.png
 - export.png
 - tcpstream.png

[CTFwriteups](#) / [VishwaCTF_2022](#) / [Forensic](#) / [The_Last_Jedi](#) /

<div>  LambdaMamba </div> <div> Added writeup for VishwaCTF The Last Jedi </div> <div> 5641096 · 2 years ago </div> <div>  History </div>		
Name	Last commit message	Last commit date
 ..		
 files	Added writeup for VishwaCTF The Last Jedi	2 years ago
 img	Added writeup for VishwaCTF The Last Jedi	2 years ago
 README.md	Added writeup for VishwaCTF The Last Jedi	2 years ago

README.md

The Last Jedi (Category: Forensic)

The challenge is the following,

Challenge	315 Solves	X
Challenge	315 Solves	X

The Last Jedi
250

What it takes do you have?

 Y0D4.jpg

Flag

Submit

And we are given [Y0D4.jpg](#),



First of all, I decided to check the contents of this file by using,

```
% cat Y0D4.jpg
GR?F????-?-_-+??z-E?(%?????,(??(=?[?≥??-R??-???L?y0??J??_J&??-??3?]?6Y,*J?????????)?-?Y█[↑?EN[
?R?N??-???:"?0?]??2??2?先 10?%"??3??<?[2]??3?=
W?W?4Q?]&?J???I????M8*????s?
?jA?0<R??2??W?''???yY"P5??r??IT!?????6b0? 0? ? ????'q?????(0zQ$9??????T??
??K??;
????uz?.??X?:
? ! _MACOSX/$█f-fk █-fkY┘r-/D-|+ |f+
W?S??:~P≥??1
? _MACOSX/$█f-fk █-fkY┘r-
?->?:?4?3?
?S█f-fk █-fkY┘r-/D-|+ |f+
0值??:<?Y?!
? _MACOSX
?->?:?"I?$)
?Sacred archives
P$?:???w???QO_-B?X?YS?~V?N
??,"?8??
θ_MACOSX/$█f-fk █-fkY┘r-/D-|+ |f+/Y_-|Y_Y_|.┘±
?1?~:???w?RK??JM
???? ??>0?
/Sacred archives/Dont open/Is This Really It.jpg
DGt?:?wVQvagrant@ubuntu-bionic:/vagrant/vishwa$ 1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;2c1;
```

The last section showed `Sacred archives/Dont open/Is This Really It.jpg`, so I knew there was a file hidden inside `Y0D4.jpg`.

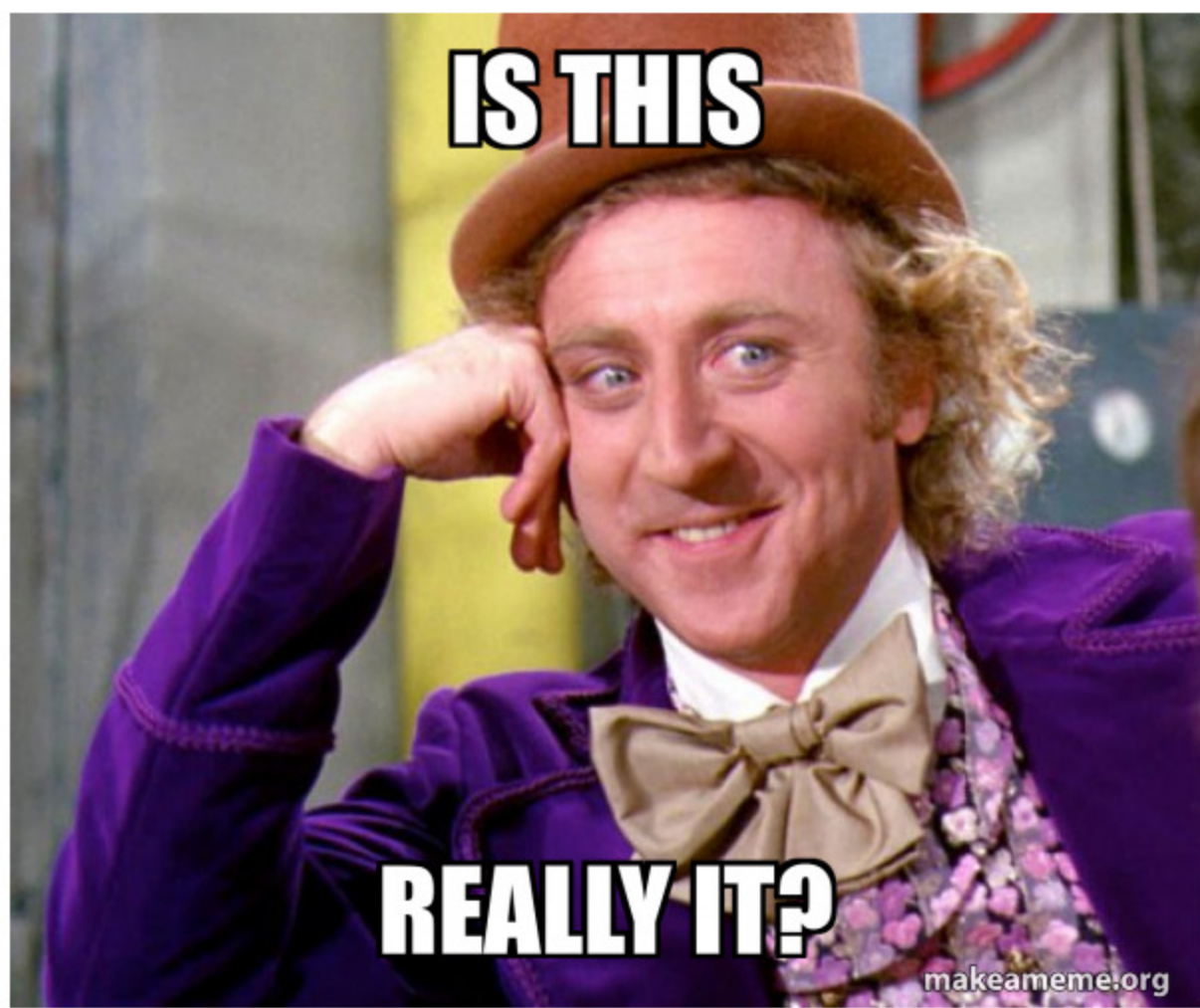
So I used [Stegextract](#) on [Y0D4.jpg](#), and it extracted a [Y0D4.rar](#) file.

```
vagrant@ubuntu-bionic: /vagrant/vishwa$ ./stegextract/stegextract Y0D4.jpg
Detected image format: JPG
Extracted trailing file data: binary data, might contain embedded files.
Performing deep analysis
Found embedded: RAR
Done
vagrant@ubuntu-bionic: /vagrant/vishwa$
```

Y0D4.rar was not password protected, and showed the following folders and files,

Y0D4.rar	337KB	3/21/2022
MACOSX	85KB	2022/03/18
Sacred archives	85KB	2022/03/18
Dont open	85KB	
is_this_it.jpg	85KB	2022/03/18
Sacred archives	255KB	2022/03/18
Dont open	255KB	
Is_This_Really_It.jpg	255KB	2022/03/18

Is_This_Really_It.jpg was a contained in Y0D4.rar



So I ran [Stegextract](#) on [Is_This_Really_It.jpg](#), and it extracted a ASCII text file that contained the string `flag:{H1DD3N_M34N1NG}`.

```

vagrant@ubuntu-bionic:~$ ./stegextract Is_This_Really_It.jpg
Detected image format: JPG
Extracted trailing file data:  ASCII text, with no line terminators
Performing deep analysis
Done
vagrant@ubuntu-bionic:~$ ./stegextract$ cat Is_This_Really_It_dumps
Flag: (HIDD3N_M34N1NG)vagrant@ubuntu-bionic:~$ ./stegextract$

```

Therefore, the flag is

```
vishwaCTF{H1DD3N M34N1NG}
```