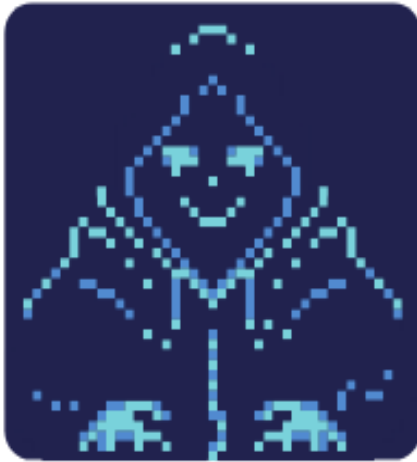


# CTF Hology 4.0 WRITEUP



**AVERAGE INTEL**  
ENJOYERS

sayang (Paska Parahita)  
Iya sayang (Muhammad Ichwan)  
Kamu kok cuek sayang (Ananda Fikri Ijlal Akbar)

**UNIVERSITAS AMIKOM YOGYAKARTA**

# [FORENSIC]

## it's Rokubi with g

Diberikan sebuah file zip, lakukan unzip terdapat file image “not here.png” dan juga sebuah file zip lagi yaitu “maybehere.zip”. Untuk membuka file “maybehere.zip” tersebut dibutuhkan sebuah password, namun password tidak diketahui. Kami mencoba melihat metadata dari file image dengan exiftool terdapat beberapa encoding. Kami mencoba melakukan decode semua encoding yang ada pada metadata menggunakan tools basecrack (<https://github.com/mufeedvh/basecrack>) dan mendapatkan password pada encoding base62, lakukan unzip terhadap file “maybehere.zip” dengan password yang didapatkan. Outputnya yaitu sebuah file image “saiken.png”, cek menggunakan zsteg didapatkan flag nya.

```
banua@basiber:~/Downloads/HOLOGY/forensic/rokubi
```

```
$ exiftool not\ here.png
```

```
ExifTool Version Number      : 10.80
File Name                    : not here.png
Directory                   : .
File Size                    : 44 kB
File Modification Date/Time  : 2021:08:29 13:01:33+07:00
File Access Date/Time       : 2021:10:24 09:07:48+07:00
File Inode Change Date/Time  : 2021:10:24 09:07:41+07:00
File Permissions             : rw-r--r--
File Type                    : PNG
File Type Extension          : png
MIME Type                    : image/png
```

```
Subject                      : nPkf9RxzfNI34yY2JQfE95GzNDccwNXygsTkwa86ji8Qbp
```

```
History Params               : gz48eJzjZBgFowABWAbaAaNgwAEAMNgADg==
```

```
History Blendop params       : gz14eJxjYIAACQYY00HEgAZY0QVwggZ7CB6pfNoAAE8gGQg=
```

```
[ - ] Encoded Base: nPkf9RxzfNI34yY2JQfE95GzNDccwNXygsTkwa86ji8Qbphcusf7MmODfoI6hvW
```

```
[ > ] Decoding as Base62: now you know the password heythisisthepassword
```

```
[ - ] The Encoding Scheme Is Base62
```

```
banua@basiber:~/Downloads/HOLOGY/forensic/rokubi
```

```
$ zsteg saiken.png
```

```
imagedata                  .. file: MIPSEL-BE MIPS-III ECOFF executable not stripped -
version 0.3
b1,r,lsb,xy                .. text: "hology4{H0W_D0_y0U_KN0W_?}"
b1,rgb,msb,xy              .. text: "j[Im[Im+IR"
```

FLAG : hology4{H0W\_D0\_y0U\_KN0W\_?}

# [FORENSIC]

Ms.Shyvana

Diberikan file zip dan pcap, pcap tersebut berisi traffic sniffing dari protocol telnet, dilakukan filter untuk mempermudah.

Login: ff11aagg

Password: FnQ4Cq00aT\_Obm22mD\_s66Z

Berdasar deskripsi soal, password tersebut dienkripsi ke dalam caesar shift 13 atau rot 13. Dilakukan decrypt mendapatkan SaD4Pd00nG\_Boz22zQ\_f66M.

Input :

FnQ4Cq00aT\_Obm22mD\_s66Z

Encrypt / Decrypt

Shift key : 13

Brute-Force Shift Key

Output :

SaD4Pd00nG\_Boz22zQ\_f66M

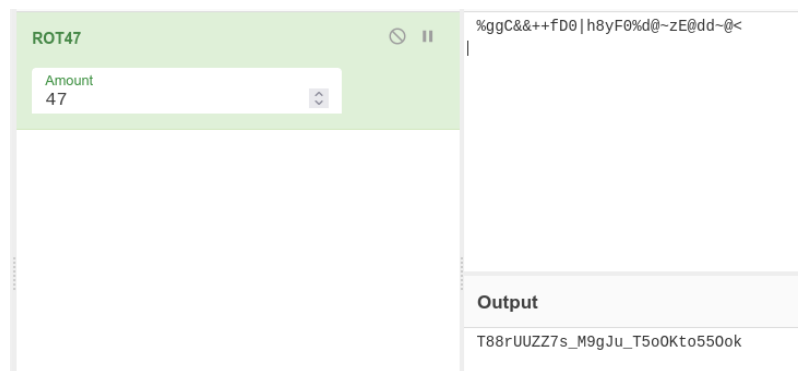
Password tersebut digunakan untuk extract file zip. Hasil extract yaitu file DOKUMENTOKTOK.txt yang berisi berbagai macam encoding dan enkripsi, beberapa diantaranya base32, base64, caesar, hex.

```
exzettabyte@avadra_kedavra:~/Documents/hology/foren/Ms.shyvana |  
→ cat DOKUMENTOKTOK.txt  
SUSJIEFEQUxBSCBET0tVTUV0 KJAUQOKTJFASAVKOKRKUWICNIVHEOQKNIFHEWQK0JZMUC  
CQ= 4B4954412047554E414B414E2042414E59414B2054454b4e494b QVBBS0FIIENBR  
VNBUIBJVFUGRUZFS1RJRIa/IAo= GRNXP HQ LQL GL VDMLNDQ VHFDUD HQFUBSW XQWX  
N PHQJDPDQNDQ LVL WHUVHEXW IFDUCURAKJAUQOKTJFASAUSPKQQFARKSKVJUCSCBIFH  
CAVCPJMQFIT2LEBKEKUSKIFGUSTQK 3437204b554e434920424552414e474b41532054  
455253454255542044492053494d50414e REV0R0F0IFBBU1NXT1JECg== %ggC&&+++fD  
0|h8yF0%d@~zE@dd~@<
```

Dilakukan decode maupun decrypt satu persatu lalu disusun menjadi seperti pada gambar, didapat clue bahwa *47 kunci berangkas* yang mengarah pada rot47.

```
exzettabyte@Avadra_Kedavra:~/Documents/hology/foren/Ms.shyvana|  
⇒ cat hasil  
INI ADALAH DOKUMEN RAHASIA UNTUK MENGAMANKANNYA KITA GUNAKAN BANYAK TE  
KNIK APAKAH CAESAR ITU EFEKTIF ? DOKUMEN INI DI SAJIKAN SECARA ENCRYPT  
UNTUK MENGAMANKAN ISI TERSEBUT ..... 47 KUNCI BERANGKAS TERSEBU  
T DI SIMPAN DENGAN PASSWORD %ggC&&++fD0|h8yF0%d@~zE@dd~@<
```

Flag berada pada kata setelah *password*. Lakukan decrypt lalu didapat flagnya



Flag : hology4{T88rUZZ7s\_M9gJu\_T5oOKto55Ook}

# [FORENSIC]

## Hacked

Diberikan file launch-code.zip dan access.log, access.log tersebut berisi serangan sql injection dimana attacker sedang melakukan dump password.

```
192.168.100.1 - - [01/Oct/2021:15:00:00] "GET /users=ASC,(select (case when (substring(password,0,0) = a) then sleep(3) else sleep(1))) HTTP/1.0" 200 1200
192.168.100.1 - - [01/Oct/2021:15:00:01] "GET /users=ASC,(select (case when (substring(password,0,0) = b) then sleep(3) else sleep(1))) HTTP/1.0" 200 1200
192.168.100.1 - - [01/Oct/2021:15:00:02] "GET /users=ASC,(select (case when (substring(password,0,0) = c) then sleep(3) else sleep(1))) HTTP/1.0" 200 1200
192.168.100.1 - - [01/Oct/2021:15:00:03] "GET /users=ASC,(select (case when (substring(password,0,0) = d) then sleep(3) else sleep(1))) HTTP/1.0" 200 1200
```

Hasil analisa dari access.log, jika karakter valid maka akan mendapatkan response sleep selama 3 detik, sedangkan jika tidak valid maka sleep 1 detik. Dengan ini dapat diketahui passwordnya dengan cara melihat timestamp pada bagian detik ketika pada timestamp detik interval 3 detik maka karakter valid dan dicatat, begitu seterusnya sebanyak 3250 line :(.



Diidapat passwordnya SupEr\_s3CreT\_p4ssw0rd\_f0R\_sup3r\_seCr3t\_LaUnCh\_c0De. Password tersebut untuk extract file zip. Berhasil extract akan mendapatkan 8 qr yang dipotong menjadi 8 bagian dengan interval 10, jadi qr pertama 1,11,21,31,41,51,61,71,81.

```
ls launch-code
1  13 16 2  23 26 3  33 36 4  43 46 5  53 56 6  63 66 7  73 76 8  83 86 91 94 97
11 14 17 21 24 27 31 34 37 41 44 47 51 54 57 61 64 67 71 74 77 81 84 87 92 95 98
12 15 18 22 25 28 32 35 38 42 45 48 52 55 58 62 65 68 72 75 78 82 85 88 93 96
```

Buat script untuk menggabungkannya sekaligus decode qr dari qr 1 sampai qr ke 8.

```
import numpy as np
import PIL
from pyzbar.pyzbar import decode
from PIL import Image

def qr(x,output):
    list_im = []
    for i in range(x, 99,10):
        g = f'{i}'
        list_im.append(g)

    imgs = [PIL.Image.open(i) for i in list_im]
    min_shape = sorted( [(np.sum(i.size), i.size ) for i in imgs])[0][1]
    imgs_comb = np.hstack( (np.asarray( i.resize(min_shape) ) for i in imgs ) )
    imgs_comb = np.vstack( (np.asarray( i.resize(min_shape) ) for i in imgs ) )
    imgs_comb = PIL.Image.fromarray( imgs_comb)
    imgs_comb.save(output)

for i in range(1,9):
    qr(i,f"qr{i}.png")
    dec = decode(Image.open(f"qr{i}.png"))
    res = dec[0].data
    print(res.decode(),end="")
```

Jalankan dan pipe decode base64

```
⇒ python3 solv.py|base64 -d
hology4{c0ngr4tzzz_y0u_got_m3}
```

**Flag : hology4{c0ngr4tzzz\_y0u\_got\_m3}**

## [MISC]

### Sanity Check

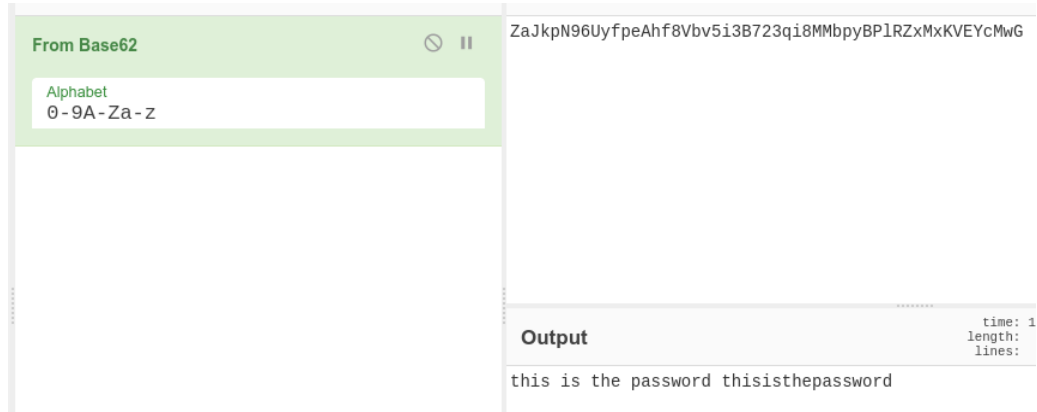
Flag berada di deskripsi soal

**Flag : hology4{w3lc0me\_to\_ctf\_h0logy\_4.0}**

## [MISC]

### Get link for the rubik's

Diberikan file zip yang didalamnya file jpg, ketika cek metadata pada file jpg didapat encoding base62 pada copyright, decode dengan cyberchef maka akan didapat password.



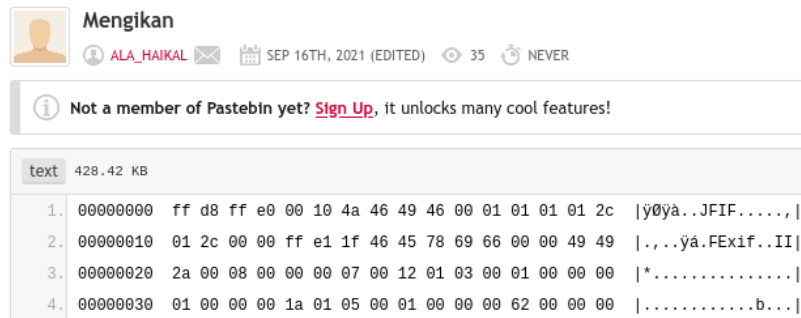
Extract data yang ada didalam file jpgnya dengan password yang sudah didapat maka akan mendapatkan ikan.zip. Ketika diextract maka mendapatkan 2 file fish.png dan uneedthis.txt.

```
exzettabyte@Avadra_Kedavra:~/Documents/hology/misc|  
⇒ steghide extract -sf fishtek.jpg  
Enter passphrase:  
wrote extracted data to "Ikan.zip".
```

Cek metadata pada file fish.png didapat link pastebin yang terlock, file uneedthis berisi link rumus rubik 3x3 yang merupakan hint untuk fish.png yang berupa gambar rubik 3x3, berdasarkan link yang diberikan kami mendapati rumus untuk solve pada situasi gambar fish.png.

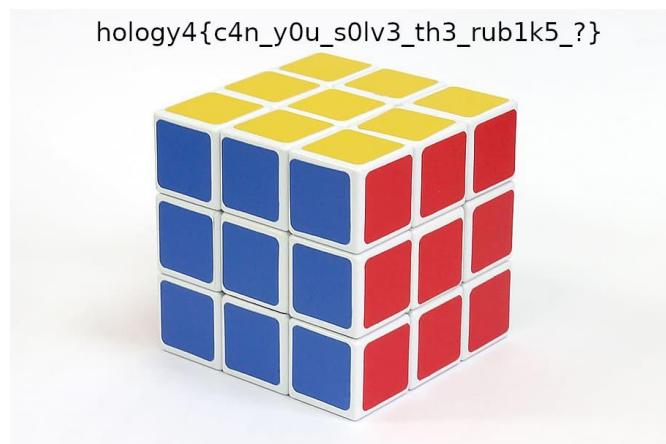


Menggunakan rumus tersebut (RUR'URU2R') untuk unlock pastebin dan berhasil. Pastebin tersebut berisi file jpg (berdasarkan file signaturenya) yang berupa text.



File jpg tersebut dapat dikembalikan dengan menggunakan xxd, didapatkan flagnya.

```
exzettabyte@Avadra_Kedavra:~/Documents/hology/misc|  
⇒ file f.jpg  
f.jpg: UTF-8 Unicode text  
exzettabyte@Avadra_Kedavra:~/Documents/hology/misc|  
⇒ xxd -r f.jpg > hasil.jpg  
exzettabyte@Avadra_Kedavra:~/Documents/hology/misc|  
⇒ file hasil.jpg  
hasil.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI),  
ity 300x300, segment length 16, Exif Standard: [TIFF image data,  
e-endian, direntries=7, orientation=upper-left, xresolution=98, y  
ution=106, resolutionunit=2, software=GIMP 2.10.24, datetime=2021  
9 13:20:54], progressive, precision 8, 910x607, frames 3
```



Flag : hology4{c4n\_y0u\_s0lv3\_th3\_rub1k5\_?}



## [WEB]

HTTPS but without S

Ketika website dibuka menggunakan https menampilkan seperti pada gambar, berdasarkan response tersebut maka dilakukan pengecekan pada sertifikatnya.

Something wrong with certificate?

Ditemukan /theflaghere pada dns name yang menandakan lokasi flag

Subject Alt Names	
DNS Name	the flag is in here
DNS Name	/theflaghere

Lakukan request ke /theflaghere dan didapatkan flagnya

```
exzettabyte@Avadra_Kedavra:~|⇒ curl https://13.214.13.126:3446/theflaghere -k
The flag is HOLOGY4.0{SoMe_BaSiC_S5L_mIsTAkE} <br/> P.S. Sorry for the easy and meme web challenge, thinking of quitting from Cyber Security and CTFs. 🐼
```

Flag : HOLOGY4.0{SoMe\_BaSiC\_S5L\_mIsTAkE}

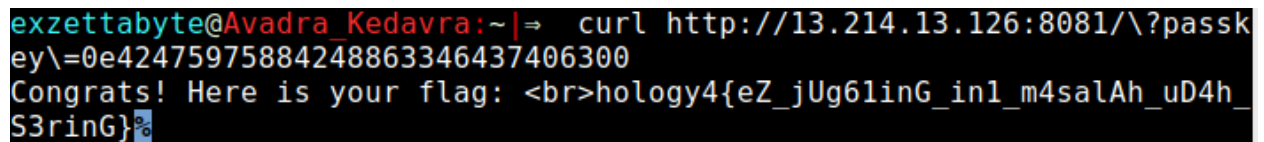
## [WEB]

### Juggle Juggle

Diberikan website ketika dibuka menampilkan source code, untuk mendapatkan flag nilai dari variable passkey harus sama dengan md5 dari DYAXWCA tetapi panjangnya tidak boleh sama.

```
if (isset($_GET['passkey']) &&
    hash("md5", "DYAXWCA") == $_GET['passkey'] &&
    strlen(hash("md5", "DYAXWCA")) != strlen($_GET['passkey'])) {
    echo "FLAG";
} else if (isset($_GET['passkey'])) {
    echo "False Password!";
} else {
    "File";
}
?>
```

Dilakukan pencarian terkait md5 dari DYAXWCA didapat 0e424759758842488633464374063001, karena panjangnya tidak boleh sama maka kita hapus 1 karakter menjadi 0e42475975884248863346437406300



```
exzettabyte@Avadra_Kedavra:~|⇒ curl http://13.214.13.126:8081/\?passk
ey\=0e42475975884248863346437406300
Congrats! Here is your flag: <br>hology4{eZ_jUg6linG_in1_m4salAh_uD4h_
S3rinG}
```

Flag : hology4{eZ\_jUg6linG\_in1\_m4salAh\_uD4h\_S3rinG}