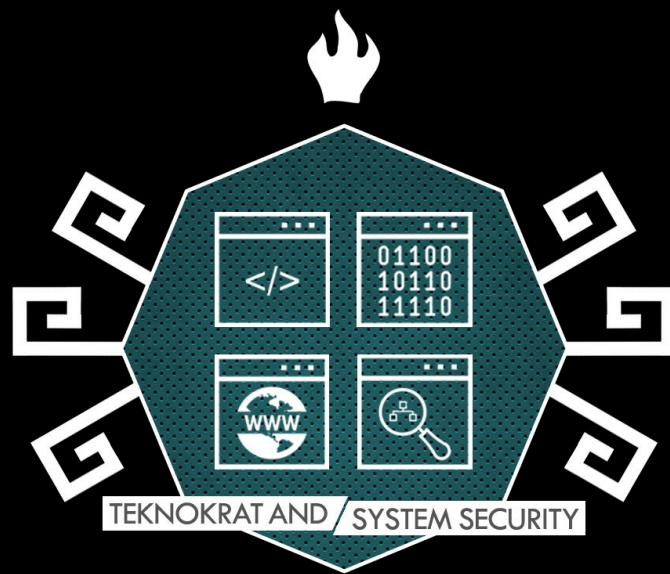


# Write Up HOLOGY 2.0

Ketua Penyelenggara



Andrian Setiawan

Zanshy Pebryansyah

M. Thomas Fadhila Yahya

Universitas Teknokrat Indonesia

## Misc

### Welcome to Hology CTF [1 Point]

Cara Pengerjaan :

Diberikan sebuah string flag copy dan paste

Flag :

**hctf{F1nd\_s0methin\_lik3\_thI5\_Ok}**

### Feedback [1 Point]

Cara Pengerjaan :

Diberikan sebuah google form <https://forms.gle/u4cuqiCa9QWKS2i59>

Lalu isi form nya dengan baik dan didapatkan flagnya ☺ atau bisa juga dengan ctrl+u dan hsctf

#### Feedback CTF Hology 2.0

Here is your flag: hctf{thank\_you\_very\_much\_hahahahahahaha}

[See previous responses](#)

```
["Here is your flag: hctf{thank_you_very_much_hahahahahahaha}",0,1,0,0]
null,[null,null,null,null,null,[null,null,[[39,120,24,null,2]
[209,234,194]
[209,234,194]
[103,184,52]
[39,120,24]
```

Flag :

**hctf{thank\_you\_very\_much\_hahahahahahaha}**

# Reverse

## Easy Dian [156 Point]

Cara Pengerjaan :

Diberikan sebuah file ELF lalu buka dengan IDA Pro

Lalu check dibagian dan tab sub\_401152

```
s = (char *)calloc(1uLL, 0x3EuLL);
puts("Masukkan kode: ");
fgets(s, 62, stdin);
if ( 1718903656 != *((_DWORD *)s
    || 1949518971 != *((_DWORD *)s + 1)
    || 1701601139 != *((_DWORD *)s + 2)
    || 1598968372 != *((_DWORD *)s + 3)
    || 1768189491 != *((_DWORD *)s + 4)
    || 1399156321 != *((_DWORD *)s + 5)
    || 829644597 != *((_DWORD *)s + 6)
    || 2037149805 != *((_DWORD *)s + 7)
    || 1650538079 != *((_DWORD *)s + 8)
    || 2100312422 != *((_DWORD *)s + 9)
    || 10 != *((_DWORD *)s + 10) )
    printf("Whoops, https://youtu.be/rgrdCIYXSjM", 62LL, a2);
else
    puts("Selamat!!!");
return 0LL;
```

Lalu ubah ke

```
s = (char *)calloc(1uLL, 0x3EuLL);
puts("Masukkan kode: ");
fgets(s, 62, stdin);
if ( 'ftch' != *((_DWORD *)s
    || 't3L{' != *((_DWORD *)s + 1)
    || 'e1_s' != *((_DWORD *)s + 2)
    || '_NR4' != *((_DWORD *)s + 3)
    || 'idn3' != *((_DWORD *)s + 4)
    || 'Sena' != *((_DWORD *)s + 5)
    || '1s_5' != *((_DWORD *)s + 6)
    || 'ylpm' != *((_DWORD *)s + 7)
    || 'ba6_' != *((_DWORD *)s + 8)
    || '}09F' != *((_DWORD *)s + 9)
    || 10 != *((_DWORD *)s + 10) )
    printf("Whoops, https://youtu.be/rgrdCIYXSjM", 62LL, a2);
else
    puts("Selamat!!!");
return 0LL;
```

Lalu, didapatkan flag yang terbalik

}09fba6\_ylpm1s\_5SenaIdn3\_NR4el\_st3L{ftch'

Lalu di balikan kembali

```
Python 2.7.6 (default, Nov 10 2013, 19:24:18) [MSC v.1500 32 bit (Intel)]
in32
Type "copyright", "credits" or "license()" for more information.
>>> "}09fba6_ylpm1s_5SenaIdn3_NR4el_st3L{ftch"[::-1]
'hctf{L3ts_le4RN_3ndianeS5_s1mply_6abf90}'
>>> |
```

Flag :

**hctf{L3ts\_le4RN\_3ndianeS5\_s1mply\_6abf90}**

# Forensic

## Green Milky Ways [180 Point]

Cara Pengerjaan :

Diberikan sebuah 400 gambar dan Enc.pyc

Decompiler file enc.pyc didapatkan file enc.py

```
from PIL import Image

def crop(image_path, coords, saved_location):
    image_obj = Image.open(image_path)
    cropped_image = image_obj.crop(coords)
    cropped_image.save(saved_location)
    cropped_image.show()

if __name__ == '__main__':
    l = 0
    for k in range(20):
        j = 0
        for i in range(20):
            image = 'Done.png'
            name = 'foto' + str(k) + '_' + str(i) + '.png'
            crop(image, (j, l, j + 80, l + 80), name)
            j += 80

        l += 80
```

Lalu, decrypt dengan script berikut :

```
import sys

from PIL import Image

images = map(Image.open,
['foto0_0.png', 'foto0_1.png', 'foto0_2.png', 'foto0_3.png',
'foto0_4.png', 'foto0_5.png', 'foto0_6.png', 'foto0_7.png',
'foto0_8.png', 'foto0_9.png', 'foto0_10.png', 'foto0_11.png',
'foto0_12.png', 'foto0_13.png', 'foto0_14.png', 'foto0_15.png',
'foto0_16.png', 'foto0_17.png', 'foto0_18.png', 'foto0_19.png',
'foto1_0.png', 'foto1_1.png', 'foto1_2.png', 'foto1_3.png',
'foto1_4.png', 'foto1_5.png', 'foto1_6.png', 'foto1_7.png',
'foto1_8.png', 'foto1_9.png', 'foto1_10.png', 'foto1_11.png',
'foto1_12.png', 'foto1_13.png', 'foto1_14.png', 'foto1_15.png',
'foto1_16.png', 'foto1_17.png', 'foto1_18.png', 'foto1_19.png',
'foto2_0.png', 'foto2_1.png', 'foto2_2.png', 'foto2_3.png',
'foto2_4.png', 'foto2_5.png', 'foto2_6.png', 'foto2_7.png',
'foto2_8.png', 'foto2_9.png', 'foto2_10.png', 'foto2_11.png',
'foto2_12.png', 'foto2_13.png', 'foto2_14.png', 'foto2_15.png',
'foto2_16.png', 'foto2_17.png', 'foto2_18.png', 'foto2_19.png',
'foto3_0.png', 'foto3_1.png', 'foto3_2.png', 'foto3_3.png',
'foto3_4.png', 'foto3_5.png', 'foto3_6.png', 'foto3_7.png',
'foto3_8.png', 'foto3_9.png', 'foto3_10.png', 'foto3_11.png',
'foto3_12.png', 'foto3_13.png', 'foto3_14.png', 'foto3_15.png',
'foto3_16.png', 'foto3_17.png', 'foto3_18.png', 'foto3_19.png',
'foto4_0.png', 'foto4_1.png', 'foto4_2.png', 'foto4_3.png',
'foto4_4.png', 'foto4_5.png', 'foto4_6.png', 'foto4_7.png',
'foto4_8.png', 'foto4_9.png', 'foto4_10.png', 'foto4_11.png',
'foto4_12.png', 'foto4_13.png', 'foto4_14.png', 'foto4_15.png',
'foto4_16.png', 'foto4_17.png', 'foto4_18.png', 'foto4_19.png',
'foto5_0.png', 'foto5_1.png', 'foto5_2.png', 'foto5_3.png',
'foto5_4.png', 'foto5_5.png', 'foto5_6.png', 'foto5_7.png',
'foto5_8.png', 'foto5_9.png', 'foto5_10.png', 'foto5_11.png',
'foto5_12.png', 'foto5_13.png', 'foto5_14.png', 'foto5_15.png',
'foto5_16.png', 'foto5_17.png', 'foto5_18.png', 'foto5_19.png',
'foto6_0.png', 'foto6_1.png', 'foto6_2.png', 'foto6_3.png',
'foto6_4.png', 'foto6_5.png', 'foto6_6.png', 'foto6_7.png',
'foto6_8.png', 'foto6_9.png', 'foto6_10.png', 'foto6_11.png',
'foto6_12.png', 'foto6_13.png', 'foto6_14.png', 'foto6_15.png',
'foto6_16.png', 'foto6_17.png', 'foto6_18.png', 'foto6_19.png',
'foto7_0.png', 'foto7_1.png', 'foto7_2.png', 'foto7_3.png',
'foto7_4.png', 'foto7_5.png', 'foto7_6.png', 'foto7_7.png',
'foto7_8.png', 'foto7_9.'])
```

png','foto7\_10.png','foto7\_11.png','foto7\_12.png','foto7\_13.png','foto7\_14.png','foto7\_15.png','foto7\_16.png','foto7\_17.png','foto7\_18.png','foto7\_19.png','foto8\_0.png','foto8\_1.png','foto8\_2.png','foto8\_3.png','foto8\_4.png','foto8\_5.png','foto8\_6.png','foto8\_7.png','foto8\_8.png','foto8\_9.png','foto8\_10.png','foto8\_11.png','foto8\_12.png','foto8\_13.png','foto8\_14.png','foto8\_15.png','foto8\_16.png','foto8\_17.png','foto8\_18.png','foto8\_19.png','foto9\_0.png','foto9\_1.png','foto9\_2.png','foto9\_3.png','foto9\_4.png','foto9\_5.png','foto9\_6.png','foto9\_7.png','foto9\_8.png','foto9\_9.png','foto9\_10.png','foto9\_11.png','foto9\_12.png','foto9\_13.png','foto9\_14.png','foto9\_15.png','foto9\_16.png','foto9\_17.png','foto9\_18.png','foto9\_19.png','foto10\_0.png','foto10\_1.png','foto10\_2.png','foto10\_3.png','foto10\_4.png','foto10\_5.png','foto10\_6.png','foto10\_7.png','foto10\_8.png','foto10\_9.png','foto10\_10.png','foto10\_11.png','foto10\_12.png','foto10\_13.png','foto10\_14.png','foto10\_15.png','foto10\_16.png','foto10\_17.png','foto10\_18.png','foto10\_19.png','foto11\_0.png','foto11\_1.png','foto11\_2.png','foto11\_3.png','foto11\_4.png','foto11\_5.png','foto11\_6.png','foto11\_7.png','foto11\_8.png','foto11\_9.png','foto11\_10.png','foto11\_11.png','foto11\_12.png','foto11\_13.png','foto11\_14.png','foto11\_15.png','foto11\_16.png','foto11\_17.png','foto11\_18.png','foto11\_19.png','foto12\_0.png','foto12\_1.png','foto12\_2.png','foto12\_3.png','foto12\_4.png','foto12\_5.png','foto12\_6.png','foto12\_7.png','foto12\_8.png','foto12\_9.png','foto12\_10.png','foto12\_11.png','foto12\_12.png','foto12\_13.png','foto12\_14.png','foto12\_15.png','foto12\_16.png','foto12\_17.png','foto12\_18.png','foto12\_19.png','foto13\_0.png','foto13\_1.png','foto13\_2.png','foto13\_3.png','foto13\_4.png','foto13\_5.png','foto13\_6.png','foto13\_7.png','foto13\_8.png','foto13\_9.png','foto13\_10.png','foto13\_11.png','foto13\_12.png','foto13\_13.png','foto13\_14.png','foto13\_15.png','foto13\_16.png','foto13\_17.png','foto13\_18.png','foto13\_19.png','foto14\_0.png','foto14\_1.png','foto14\_2.png','foto14\_3.png','foto14\_4.png','foto14\_5.png','foto14\_6.png','foto14\_7.png','foto14\_8.png','foto14\_9.png','foto14\_10.png','foto14\_11.png','foto14\_12.png','foto14\_13.png','foto14\_14.png','foto14\_15.png','foto14\_16.png','foto14\_17.png','foto14\_18.png','foto14\_19.png','foto15\_0.png','foto15\_1.png','foto15\_2.png','foto15\_3.png','foto15\_4.png','foto15\_5.png','foto15\_6.png','foto15\_7.png','foto15\_8.png','foto15\_9.png','foto15\_10.png','foto15\_11.png','foto15\_12.png','foto15\_13.png','foto15\_14.png','foto15\_15.png','foto15\_16.png','foto15\_17.png','foto15\_18.png','foto15\_19.png','foto16\_0.png','foto16\_1.png','foto16\_2.png','foto16\_3.png','foto16\_4.png','foto16\_5.png','foto16\_6.png','foto16\_7.png','foto16\_8.png','foto16\_9.png','foto16\_10.png','foto16\_11.png','foto16\_12.png','foto16\_13.png','foto16\_14.png','foto16\_15.png','foto16\_16.png','foto16\_17.png','foto16\_18.png','foto16\_19.png','f

```
oto17_0.png', 'foto17_1.png', 'foto17_2.png', 'foto17_3.png',  
, 'foto17_4.png', 'foto17_5.png', 'foto17_6.png', 'foto17_7.p  
ng', 'foto17_8.png', 'foto17_9.png', 'foto17_10.png', 'foto17  
_11.png', 'foto17_12.png', 'foto17_13.png', 'foto17_14.png',  
, 'foto17_15.png', 'foto17_16.png', 'foto17_17.png', 'foto17_1  
8.png', 'foto17_19.png', 'foto18_0.png', 'foto18_1.png', 'fot  
o18_2.png', 'foto18_3.png', 'foto18_4.png', 'foto18_5.png', '  
foto18_6.png', 'foto18_7.png', 'foto18_8.png', 'foto18_9.png  
, 'foto18_10.png', 'foto18_11.png', 'foto18_12.png', 'foto18  
_13.png', 'foto18_14.png', 'foto18_15.png', 'foto18_16.png',  
, 'foto18_17.png', 'foto18_18.png', 'foto18_19.png', 'foto19_0  
.png', 'foto19_1.png', 'foto19_2.png', 'foto19_3.png', 'foto1  
9_4.png', 'foto19_5.png', 'foto19_6.png', 'foto19_7.png', 'fo  
to19_8.png', 'foto19_9.png', 'foto19_10.png', 'foto19_11.png  
, 'foto19_12.png', 'foto19_13.png', 'foto19_14.png', 'foto19  
_15.png', 'foto19_16.png', 'foto19_17.png', 'foto19_18.png',  
, 'foto19_19.png']])
```

```
new_im = Image.new('RGB', (1600, 1600))
```

```
x_offset = 0
```

```
y_offset = 0
```

```
for im in images:
```

```
    new_im.paste(im, (x_offset,y_offset))
```

```
    x_offset+=80
```

```
    if (x_offset % 1600 ==0):
```

```
        y_offset+=80
```

```
        x_offset=0
```

```
out = new_im.transpose(Image.ROTATE_180)
```

```
out.save('flag.png')
```



hctf{l3Ts\_M  
ak3\_a\_Scr1  
pt\_f0r\_Thi5\_  
ChalLange}

Flag :

hctf{l3Ts\_Mak3\_a\_Scr1pt\_f0r\_Thi5\_ChalLange}

## Putra Petir dalam Gelombang [500 Point] Bownous

Cara Pengerjaan :

Diberikan sebuah file exe lalu dicek dengan hex editor ternyata ini merupakan wav

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	B2	49	46	46	34	C0	A8	00	57	41	56	45	66	6D	74	20	RIFF4À".WAVEfmt
00000010	10	00	00	00	01	00	01	00	80	BB	00	00	00	77	01	00	.....€»...w..
00000020	02	00	10	00	64	61	74	61	10	C0	A8	00	00	00	81	1F	....data.À".....
00000030	13	3D	E2	56	59	6B	35	79	9A	7F	26	7E	EF	74	85	64	..=âVYk5yš.&~it...d
00000040	EB	4D	86	32	06	14	4A	F4	46	D5	E4	B8	E1	A0	B9	8E	ëM+2...JôFÖä,á ²Ž
00000050	8A	83	03	80	5D	84	53	90	27	A3	B3	BB	73	D8	A1	F7	Šf.€]„S.'£³»sØ;÷
00000060	53	17	96	35	8D	50	8F	66	41	76	AC	7E	4C	7F	16	78	S.-5.P.fAv¬~L...x
00000070	7C	69	65	54	1C	3A	3F	1C	A7	FC	42	DD	01	C0	AF	A6	ieT.:?.šüBÝ.À"!;

Lalu, awalnya buka file di audacity ternyata tidak ada apa apa lalu kembali mencoba mendengarkan ternyata ini merupakan sebuah gelombang tv yaitu sstv [https://en.wikipedia.org/wiki/Slow-scan\\_television](https://en.wikipedia.org/wiki/Slow-scan_television)

Lalu, mencoba decode dengan Robot36 di android dengan cara diplay gelombangnya dan hp didekatkan lalu gelombang otomatis

menjadi Martin 1 mode

<https://play.google.com/store/apps/details?id=xdsopl.robot36&hl=en>

Lalu didapatkan sebuah gambar gundala ternyata hanya sebagaian apakah ini ada kekurangan apa saya yang salah kami pun tidak tau ☹ sudah dicoba berkali kali tapi tetap kepotong juga ☹



Disitu terdapat sebuah barcode dan bisa diasumsikan flag ada dibarcode itu tetapi apakah daya gambar hanya sepotong ☹

# Crypto

ありあと [247 Point]

Diberikan sebuah file odt yang berisikan sebuah ciphertext

```
GZFYDAZQZF OIDAWFZSIZM JZEYF GZLZQ EZJI EYDZP AIFLZJZ. MCZF SIHFU IEYFLIP EYFUZF ZJNZ EZDZJ.
MYEFZUPZF NZFU-CI-MI-MZ AIMZ AYJZLI QNZFU CIMYMZ ZSIZM CIPJZDZCZJEQZFZ, ZLZW AIMZ GWSZ QNZFU
GWJCZCIMYMZ. PYEWZFNZ MZDZ-MZDZ GYJFZQ DYFOZEI JZOEI EI DZOZGZQIL.
DYFWJWL AZAZE LZFZQ OZCI EZF MYJZL PZFEZ, LHPHQ ZJNZ EZDZJ ZEVSZQ ZFZP AJZCIZNZ EZJI MYHJZFU
JZPMZMZ GYJYDZWZF AYJFZDZ YFEZFU MZMDIFLZGWJZ. OZEI, ZJNZ EZDZJ ZEVSZQ PZPZP LIJI MYPZSIUWM
ZNZQ ZFUPZL JZEYF GZLZQ.
DYFWJWL PJHFIP LIHFUPHP EI ZLZM, JZEYF GZLZQ ZEVSZQ GWLJZ AQJY PYJLZAQWDI, MYEFZUPZF MCZF
SIHFU ZEVSZQ GWLJZ QNZFU CIMYMZ EZJI MYHJZFU MYSIJ AYJEZJZQ LIHFUPHP. PIMZQ IFI LYJPMZF SYAIQ
DZMW P ZPZS EZJIGZEZ WJIZIF XYJMI AZAZE EZF MYJZL.

QRLT{MHDYLIIDYM_CY_HFSN_FYYE_LH_LQIFP_RJYZLIXY_TAZREYTVBNW}

MYSZFOWLFNZ EIPIMZQPZF GWSZ, MYLYSZQ PYPZSZQZF PWFU-LZ-AW-DI, DZOZGZQIL GWF DYFOZEI
AZCZQZF EYDZP. AYPZM PYJZQZF AYMZJ IFI PYDWEIZF EIGYJFLZQ HSYQ FNHH SZN CZ, MYHJZFU LIHFUQHZ
DWMSID MYAZUZI AWGZLI. GZEZ LZQWF 1486FNHH SZN CZ LYCZM PZJYFZ WFOWP JZMZ GYFEWEWP GLAWDI.
DZPZ, OIF AWF GWF DYFUZFUPZL IGZJFNZ, NZILW GZ-AW-LZ-SZ, DYFZFLW PWFU-LZ-AW-DI, MYAZUZI AWGZLI
AZJW.
```

Lalu ambil bagian yang QRLT lalu coba dengan quipqiup

Puzzle:

QRLT{MHDYLIIDYM\_CY\_HFSN\_FYYE\_LH\_LQIFP\_RJYZLIXY\_TAZREYTVBNW}

Clues: For example G=R QVW=THE

QRLT=HCTF

dictionary

Solve

QR Code Generator

Add company logo

0 -1.171 HCTF{SOMETIMES\_BE\_ONLY\_NEED\_TO\_THINK\_CREATIVE\_F?ACDEF??Y?}

1 -1.525 HCTF{?O?ETI?E?\_BE\_ONLY\_NEED\_TO\_THINK\_CREATIVE\_F?ACDEF??Y?}

Terdapat ada tanda tanya, lalu dicoba terus dan menebak sisanya dan pilih huruf yang sering ada seperti setelah f pertama adalah b dan seterusnya dan didapatkanlah hasil tebakan

Flag :

hctf{sometimes\_we\_only\_need\_to\_think\_creative\_fb  
acdefxzyu}

## Eyes N Close [414 Point]

Cara Pengerjaan :

Diberikan sebuah  $n$  ,  $e$  dan  $c$

$n =$

22701048129543736333425996094749366889587533646608  
478003817325824700916267577973538979115157404916674  
7880487470296548479

$e = 31337$

$c =$

822771793134222725965388057340774806017683102992549  
844704514234955011499863965269592072564453205685101  
16948563902704353

Lalu,  $n$  dilakukan faktorisasi untuk mendapatkan  $p$  dan  $q$  dengan factordb.com

227010481295437363334259960947493668895875336466084780038173258247009162675779735389791151574049166747880487470296548479   Factorize! (?)		
Result:		
status (?)	digits	number
FF	120 (show)	<a href="#">2270104812...79&lt;120&gt;</a> = <a href="#">3274145556...83&lt;60&gt;</a> · <a href="#">6933426671...13&lt;60&gt;</a>

Didapatkan nilai  $p$  dan  $q$

$p =$

3274145556934980157511463037491414880636424032401714  
63406883

$q =$

6933426671108301811973254018997006413619658631273366  
80673013

lalu jalankan script berikut :

```
import gmpy2

def num_to_str(num):
    res = ""
    while num > 0:
        res = chr(num % 256) + res
        num = num / 256
    return res

p =
327414555693498015751146303749141488063642403240171
463406883

q =
693342667110830181197325401899700641361965863127336
680673013

t = (p-1)*(q-1)

e = 31337

d = gmpy2.invert(e,t)

c =
822771793134222725965388057340774806017683102992549
844704514234955011499863965269592072564453205685101
16948563902704353

n =
227010481295437363334259960947493668895875336466084
780038173258247009162675779735389791151574049166747
880487470296548479
```

```
m = pow(c,d,n)
```

```
print m
```

```
C:\Python27>python rsa.py
10409911610212303604905005509507305309508111704911605109510105311505111011607309
7108051115095098099057097098100101102125
```

Lalu decode decimal to text

ASCII text

```
hctf{$127_I5_Qu1t3_e5s3ntIal3s_bc9abdef}
```

Hex (bytes)

```
68 63 74 66 7B 24 31 32 37 5F 49 35 5F 51 75 31 74 33 5F 65 35 73
33 6E 74 49 61 6C 33 73 5F 62 63 39 61 62 64 65 66 7D
```

Binary (bytes)

```
01101000 01100011 01110100 01100110 01111011 00100100 00110001
00110010 00110111 01011111 01001001 00110101 01011111 01010001
01110101 00110001 01110100 00110011 01011111 01100101 00110101
```

Decimal (bytes)

```
10409911610212303604905005509507305309508111704911605109510105311
5051110116073097108051115095098099057097098100101102125|
```

Flag :

**hctf{\$127\_I5\_Qu1t3\_e5s3ntIal3s\_bc9abdef}**