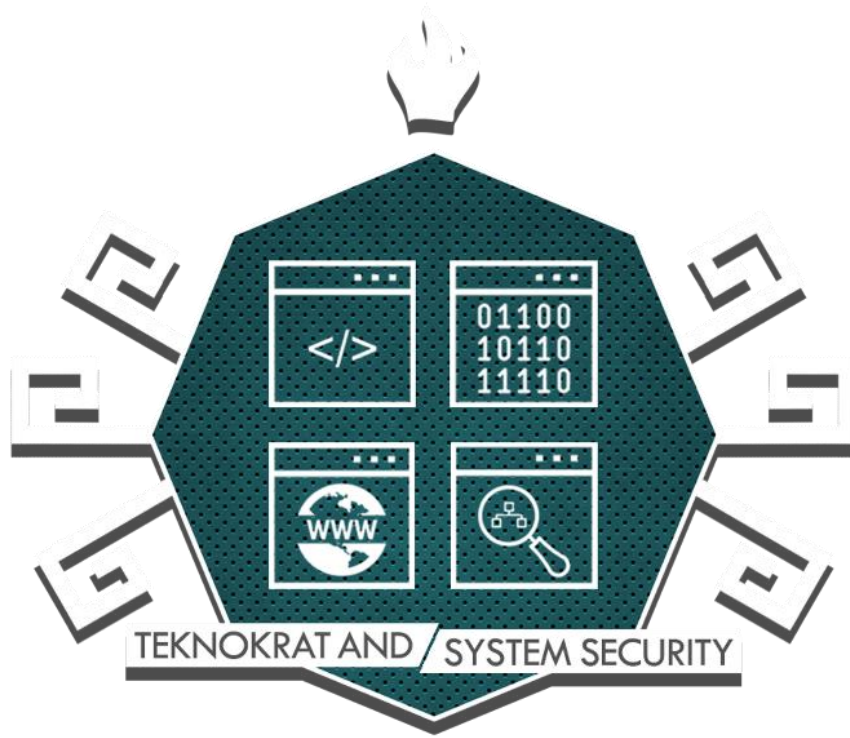


CTF Writeups By

TENESYS

"Ice CTF 2016"



> IceCTF is a computer security contest targeted at anyone with an interest in computer science. The game consists of a series of challenges where participants must reverse engineer, break, hack, decrypt, or do whatever it takes to solve the challenge. The challenges are all set up with the intent of being hacked, making it a great way to get some hands-on experience.

> Informasi Umum :

- Terdapat 4 Stage pada pembagian soal berdasarkan kesulitan.
- Login user SSH,
  - Host : `shell.icec.tf:22`
  - Username : `ctf-73374`
  - Password : `mGkzAWtv`

## STAGE 1

---

### ❖ Hello World!

*Point* : 1 pt

*Category* : Misc

*Flag* : IceCTF{h3l10\_wr0ld}

*Description* :

In this capture the flag competition you're hunting for these strings, we call them "flags". These flags always begin with "IceCTF{" followed by a message in 1337sp34k and end with "}". Here's an example flag "IceCTF{h3l10\_wr0ld}". Try submitting it through the text box down below!

*Solution* :

Paste flag yang sudah tertera pada deskripsi, yaitu IceCTF{h3l10\_wr0ld}.

### ❖ Spotlight

*Point* : 10 pt

*Category* : Web (spotlight.vuln.icec.tf)

*Flag* : IceCTF{5tup1d\_d3v5\_w1th\_th31r\_l095}

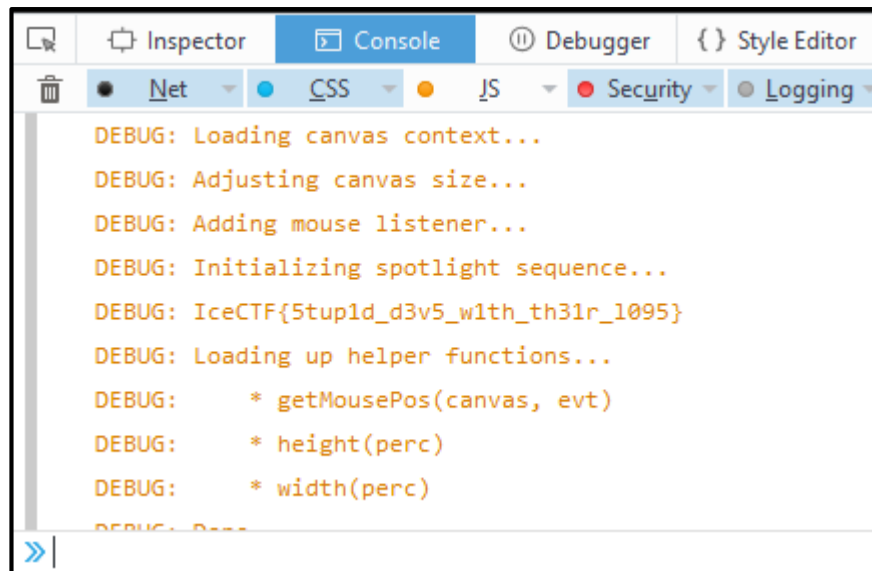
*Description* : Someone turned out the lights and now we can't find anything. Send help!.

*Solution* :

Misi ini menampilkan sebuah halaman web dengan tampilan gelap dimana saat *cursor* berpindah maka akan ada lingkaran kecil untuk melihat tampilan *frame* sebelumnya,



Flag dapat dilihat pada bagian *Console* > *JS* pada inspect element, atau pada source */spotlight.js*.



Tampilkan sebuah flag yaitu IceCTF{5tup1d\_d3v5\_w1th\_th31r\_l095}.

## ❖ All your Base are belong to us

*Point* : 15 pt

*Category* : Misc

*Flag* : IceCTF{a11\_y0ur\_bases\_are\_yours\_and\_all\_y0ur\_bases\_are\_mine}

*Description* : What a mess... we got a raw flag but now what do we do.

*Solution* :

```
01001001 01100011 01100101 01000011 01010100 01000110 01111011 01100001 01101100 00110001 01011111
01101101 01111001 01011111 01100010 01100001 01110011 01100101 01110011 01011111 01100001 01110010
01100101 01011111 01111001 01101111 01110101 01110010 01110011 01011111 01100001 01101110 01100100
01011111 01100001 01101100 01101100 01011111 01111001 00110000 01110101 01110010 01011111 01100010
01100001 01110011 01100101 01110011 01011111 01100001 01110010 01100101 01011111 01101101 01101001
01101110 01100101 01111101
```

Misi berupa bilangan biner, setelah didecode dalam bentuk *Binary > Text* maka akan mendapatkan string IceCTF{a11\_my\_bases\_are\_yours\_and\_all\_y0ur\_bases\_are\_mie}, namun flag belum bisa disubmit karena butuh sedikit perbaikan pada kata akhir “mie” menjadi “mine” barulah flag dapat disubmit.

## ❖ Rotated!

*Point* : 20 pt

*Category* : Cryptography

*Flag* : IceCTF{wait\_one\_plus\_1\_is\_3?}

*Description* :

They went and ROTated the flag by 5 and then ROTated it by 8! The scoundrels! Anyway once they were done this was all that was left VprPGS{jnvq\_bar\_cyhf\_1\_vf\_3?}.

*Solution* :

Decode flag menggunakan *ROT13 Chiper* maka akan mendapatkan flag yaitu IceCTF{wait\_one\_plus\_1\_is\_3?}.

## ❖ Move Along

Point : 30 pt

Category : Web (move-along.vuln.icec.tf)

Flag : IceCTF{tH3\_c4t\_15\_Ou7\_oF\_ThE\_b49}

Description : This site seems awfully suspicious, do you think you can figure out what they're hiding?.

Solution :

```
<!DOCTYPE html>
<html>
  <head>
    <title>IceCTF 2016 - Move Along</title>
    <link rel="stylesheet" type="text/css" href="css/main.css">
  </head>
  <body>
    </img>
  </body>
</html>
```

Pada web tersebut hanya menampilkan sebuah gambar dimana gambar memiliki alamat yang menuju ke direktori `/move_along/` dimana didalamnya terdapat satu direktori lagi yaitu `/0f76da769d67e021518f05b552406ff6/`, dan didalamnya pula terdapat file yang bernama `secret.jpg`,



Didapatlah flag yaitu IceCTF{tH3\_c4t\_15\_Ou7\_oF\_ThE\_b49}.

## ❖ Substituted

*Point* : 30 pt

*Category* : Cryptography

*Flag* : IceCTF{always\_listen\_to\_your\_substitute\_flags}

*Description* : We got a substitute flag, I hear they are pretty lax on the rules...

*Solution* :

Didapat sebuah plaintext yang berupa substitution cipher sebagai berikut,

Lw!

Gyzvecy ke WvyVKT!

W'zz by reso dsbdkwksky tzjq teo kly ujr. Teo keujr, gy joy dksurwmq bjdvw vorakeqojalr jmu wkd jaazwvjkwemd. Vorakeqojalr ljd j zemq lwdkeor, jzklesql gwkl kly juxymk et vecaskyod wk ljd qekkm oyjzrz vecazwvjkyu. Decy dwcazy ezu vwalyod joy kly Vjydjo vwalyo, kly Xwqymyoy vwalyo, kly dsbdkwkskwem vwalyo, glwvl wd klwd emy, jmu de em. Jzcedk jzz et klydy vwalyod joy yjdwzr boeiym keujr gwkl kly lyza et vecaskyod. Decy myg ymvorakwem cykleud joy JYD, kly vsooymk dkjmujoy teo ymvorakwem, jzemq gwkl ODJ. Vorakeqojalr wd j xjdk twyzu jmu wd xyor wmkoyodkwem klesql. De iwvi bjvi, oyju sa em decy veez vwalyod jmu ljxy tsm!

El jmu teo reso oyveoud cr mjcy wd WvyVKT{jzgjrd\_zwdkym\_ke\_reso\_dsbdkwksky\_tzjqd}.

Setelah pesan di decode menggunakan cryptogram solver maka akan mendapatkan flag pada bagian akhir yaitu IceCTF{always\_listen\_to\_your\_substitute\_flags}.

## ❖ IRC I

*Point* : 35 pt

*Category* : Misc

*Flag* : IceCTF{pL3AsE\_D0n7\_5h4re\_fL495\_JUsT\_doNT}.

*Description* :

There is someone sharing flags on our IRC server, can you find him and stop him? glitch.is:6667.

*Solution* :

Buka program IRC dengan alamat server *Glitch.is port 6667* lalu arahkan ke channel *#IceCTF*, lihat informasi tentang admin yang mempunyai nickname *@Glitch* maka munculah informasi mencurigakan pada bagian channel *#6470e394cb\_flagshare*,

```
* Now talking in #78a99bb_flagshare
* Topic is 'Want flags? We got 'em! IceCTF{pL3AsE_D0n7_5h4re_fL495_JUsT_doNT}'
* Set by Glitch!~Glitch@localhost on Wed Aug 17 05:34:47 2016
```

Setelah mencoba masuk, maka akan tampil sebuah flag yaitu IceCTF{pL3AsE\_D0n7\_5h4re\_fL495\_JUsT\_doNT}.

## ❖ Alien Message

Point : 40 pt

Category : Cryptography

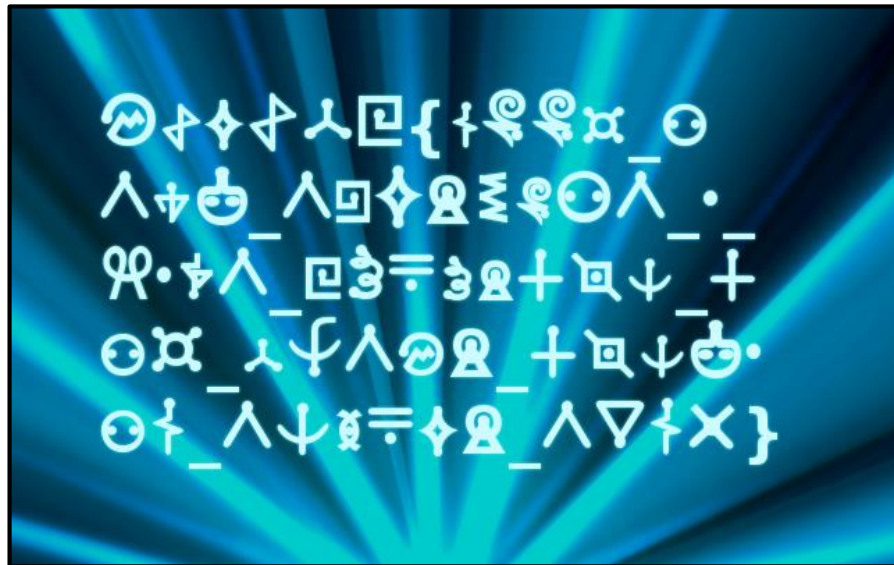
Flag : IceCTF{good\_n3wz\_3veryon3\_1\_l1k3\_fu7ur4ma\_4nd\_th3ir\_4maz1ng\_3as7er\_39g5}

Description :

We found this suspicious image online and it looked like it had been planted there by an alien life form. Can you see if you can figure out what they're trying to tell us?.

Solution :

Didapat sebuah gambar seperti berikut,



Apabila di-searching, gambar tersebut merupakan sebuah *Alien Languages*,



Langkah selanjutnya hanya tinggal mencocokkan satu-per-satu karakter sehingga mendapat flag yaitu IceCTF{good\_n3wz\_3veryon3\_1\_l1k3\_fu7ur4ma\_4nd\_th3ir\_4maz1ng\_3as7er\_39g5}.

## ❖ Time Traveler

*Point* : 45 pt

*Category* : Forensic (time-traveler.icec.tf)

*Flag* : IceCTF{Th3y'11\_n3v4r\_f1\\|d\_m4h\_fl3g\_1n\_th3\_p45t}

*Description* : I can assure you that the flag was on this website at some point in time.

*Solution* :

Setelah web dibuka, hanya menampilkan teks [ REDACTED ], Yang perlu dilakukan adalah Pergi ke halaman web <http://archive.org/> dan paste-kan alamat link pada soal <http://time-traveler.icec.tf/>, lihat pada tanggal yang diberi tanda berwarna biru yaitu pada tanggal 1 juni 2016 dimana akan mengarah pada alamat <https://web.archive.org/web/20160601212948/http://time-traveler.icec.tf/>, setelah dibuka maka akan mendapatkan flag yaitu IceCTF{Th3y'11\_n3v4r\_f1\\|d\_m4h\_fl3g\_1n\_th3\_p45t}.

## ❖ Scavenger Hunt

*Point* : 50 pt

*Category* : Misc

*Flag* : IceCTF{Y0u\_c4n7\_533\_ME\_iM\_h1Din9}.

*Description* : There is a flag hidden somewhere on our website, do you think you can find it? Good luck!.

*Solution* :

Misi ini hanya diminta mencari flag yang disembunyikan pada web <http://icec.tf/>, lakukan pencarian manual yang mengarah pada halaman <https://icec.tf/sponsors/> lalu lihat pada bagian source dengan mencari kata kunci "IceCTF{",

```
<div class="col m6 s12 sponsor-padding">
  <div class="card">
    <div class="card-image waves-effect waves-block waves-light black">
      
    </div>
```

Dan terlihatlah flag yang bersembunyi pada gambar *syndis.png* yaitu IceCTF{Y0u\_c4n7\_533\_ME\_iM\_h1Din9}.



## STAGE 2

### ❖ Complacent

*Point* : 40 pt

*Category* : Reconnaissance (complacent.vuln.icec.tf)

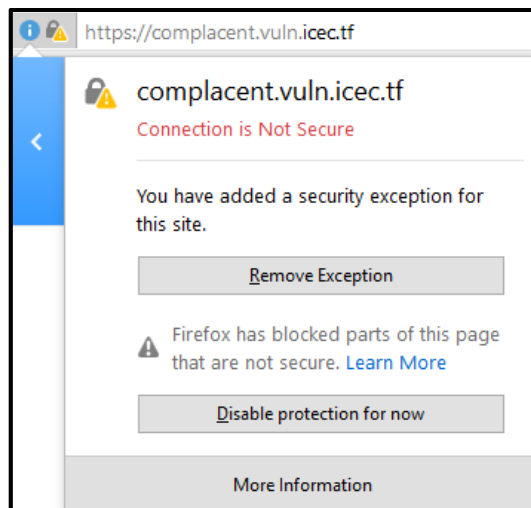
*Flag* : IceCTF{this\_1nformation\_wasnt\_h1dd3n\_at\_a11}

*Description* :

These silly bankers have gotten pretty complacent with their self signed SSL certificate. I wonder if there's anything in there.

*Solution* :

Misi ini hanya diminta untuk melihat informasi ssl pada web [http:// complacent.vuln.icec.tf/](http://complacent.vuln.icec.tf/), caranya adalah dengan menge-klik icon SSL pada samping kiri address bar,



Pilih *More Information*, dan pilih *View Certificate*,

<b>Issued To</b>	
Common Name (CN)	complacent.icec.tf
Organization (O)	Secret IceCTF Buisness Corp
Organizational Unit (OU)	Flag: IceCTF{this_1nformation_wasnt_h1dd3n_at_a11}
Serial Number	00:DF:8D:FC:51:A7:A2:00:7F
<b>Issued By</b>	
Common Name (CN)	complacent.icec.tf
Organization (O)	Secret IceCTF Buisness Corp
Organizational Unit (OU)	Flag: IceCTF{this_1nformation_wasnt_h1dd3n_at_a11}
<b>Period of Validity</b>	
Begins On	Rabu, 03 Agustus 2016
Expires On	Jumat, 10 Juli 2116

Maka flag akan terlihat yaitu IceCTF{this\_1nformation\_wasnt\_h1dd3n\_at\_a11}.

## ❖ Hidden in Plain Sight

*Point* : 45 pt

*Category* : ReverseEngineering

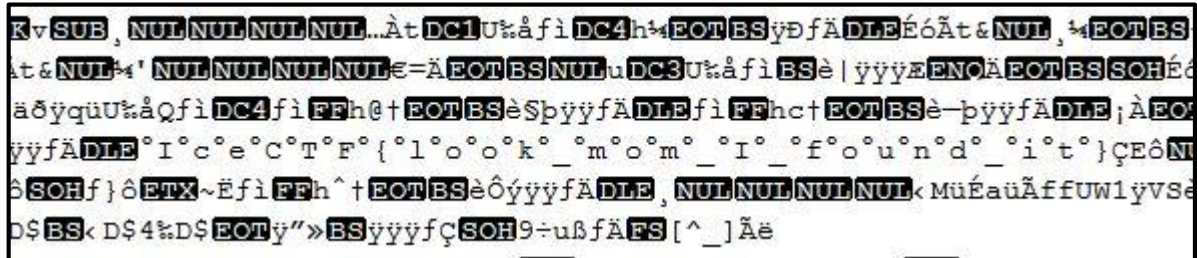
*Flag* : IceCTF{look\_mom\_I\_found\_it}

*Description* : Make sure you take a real close look at it, it should be right there! /home/plain\_sight/

- *Link File* : <http://bit.ly/2bZ9CL7>

*Solution* :

Buka file menggunakan *Notepad++* dan lihat pada bagian bawah,



Flag akan terlihat, dengan menghilangkan tanda ° maka akan mendapat flag IceCTF{look\_mom\_I\_found\_it}.

## ❖ Toke

*Point* : 45 pt

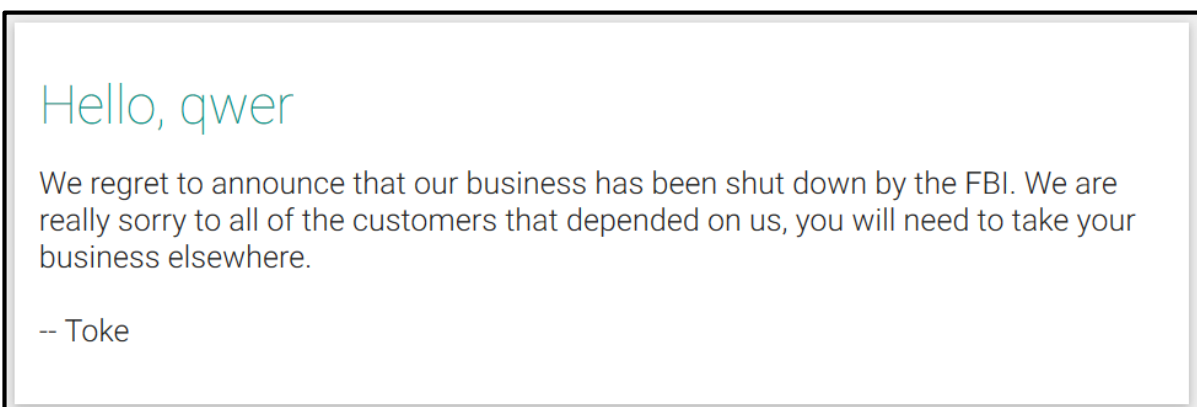
*Category* : Web (toke.vuln.icec.tf)

*Flag* : IceCTF{jW7\_t0K3ns\_4Re\_nO\_p14CE\_fOR\_53CrE7S}

*Description* : I have a feeling they were pretty high when they made this website...

*Solution* :

Terdapat halaman web yang dapat melakukan registrasi/login, cobalah untuk melakukan registrasi hanya dengan menginputkan *Username* dan *Password*, lalu login maka akan muncul halaman seperti berikut,



Lalu melihat cookies pada *Inspect Element > tab Network*, dan lihat bagian cookies maka akan tampil sebagai berikut,

Headers	Cookies	Params	Response	Timings	Preview
🔍 Filter cookies					
▼ Request cookies					
_cfduid: "d8921f9672e00df67628def72d3418beb1468596457"					
_ga: "GA1.2.1042356919.1468596472"					
_gat: "1"					
cf_clearance: "42071ea0995ace15dcbc17879ee91f4b0682d2e8-1471686085-1800"					
jwt_token: "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.e...J4PlE7kCg80cElQkl9VFL9STRUVdBADpnTerF0"					
session: "eyJ1c2Vyljo3NTI9.Cpm3zg.zX0mEzs9faZL_OM3sVSBlnhviU0"					

Ada bagian mencurigakan pada *jwt\_token* setelah didecode menggunakan *Base64* maka akan didapat flag yaitu `IceCTF{jW7_t0K3ns_4Re_nO_p14CE_fOR_53CrE7S}`.

## ❖ Flag Storage

*Point* : 50 pt

*Category* : Web (flagstorage.vuln.icec.tf)

*Flag* : IceCTF{why\_would\_you\_even\_do\_anything\_client\_side}

*Description* :

What a cheat, I was promised a flag and I can't even log in. Can you get in for me? They seem to hash their passwords, but I think the problem is somehow related to this ([en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)).

*Solution* :

Terdapat halaman login dengan memasukkan *Username* dan *Password*,

**Username:**

**Password:**

**LOG IN**

Karena telah diberi clue berupa *SQL-Injection* maka cobalah untuk memasukkan `' or 1=1 #` pada *Username* lalu submit, maka akan mendapat flag yaitu `IceCTF{why_would_you_even_do_anything_client_side}`.

## ❖ RSA?

*Point* : 50 pt

*Category* : Cryptography

*Flag* : IceCTF{falls\_apart\_so\_easily\_and\_reassembled\_so\_crudely}

*Description* :

John was messing with RSA again... he encrypted our flag! I have a strong feeling he had no idea what he was doing however, can you get the flag for us?.

*Solution* :

Variabel yang didapat dari misi hanya  $N$ ,  $e$ , dan  $c$ ,

```
N=180be86dc898a3c3a710e52b31de460f8f350610bf63e6b2203c08fddad44601d96eb454
a34dab7684589bc32b19eb27cffff8c07179e349ddb62898ae896f8c681796052ae1598bd4
1f35491175c9b60ae2260d0d4ebac05b4b6f2677a7609c2fe6194fe7b63841cec632e3a2f5
5d0cb09df08eacea34394ad473577dea5131552b0b30efac31c59087bfe603d2b13bed7d14
967bfd489157aa01b14b4e1bd08d9b92ec0c319aeb8fedd535c56770aac95247d116d59cae
2f99c3b51f43093fd39c10f93830c1ece75ee37e5fcdc5b174052eccadcaded2f1b3a4a87
184041d5c1a6a0b2eeaa3c3a1227bc27e130e67ac397b375ffe7c873e9b1c649812edcd
```

$e=1$

```
c=4963654354467b66616c6c735f61706172745f736f5f656173696c795f616e645f726561
7373656d626c65645f736f5f63727564656c797d
```

Namun setelah mencoba hanya men-decode variabel  $c$ , ternyata sudah mendapatkan flag yaitu IceCTF{falls\_apart\_so\_easily\_and\_reassembled\_so\_crudely}

## ❖ Thor's a hacker now

*Point* : 55 pt

*Category* : Misc

*Flag* : IceCTF{h3l10\_wr0ld}

*Description* :

Thor has been staring at this for hours and he can't make any sense out of it, can you help him figure out what it is?.

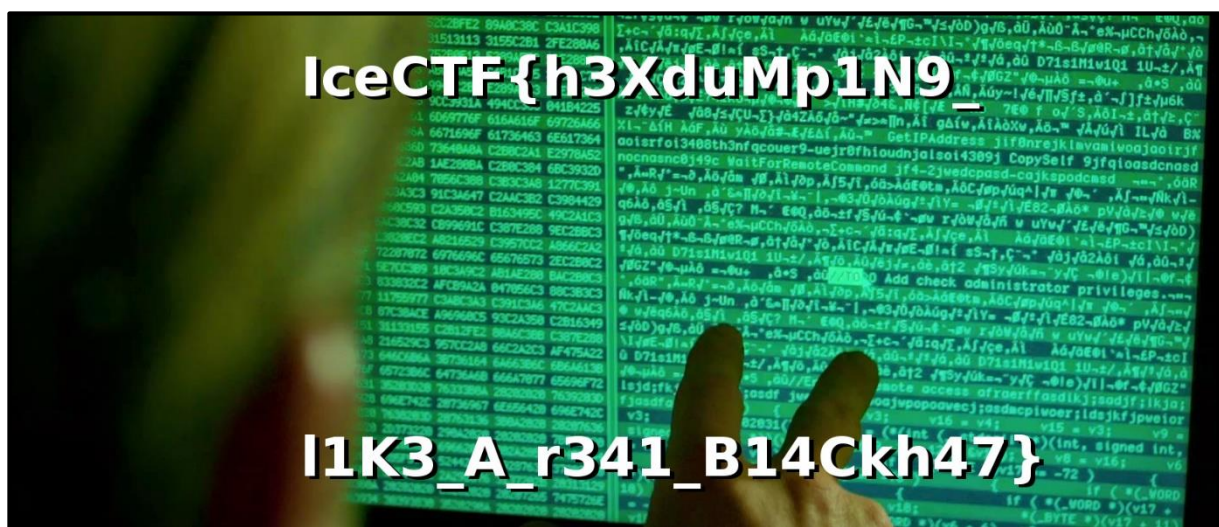
- *Link File* : <http://bit.ly/2bxepqv>

*Solution* :

File yang didapat berupa hex dari sebuah file mentah */zip*,

00000000:	4c5a	4950	01b3	007f	b61b	edf0	8440	58e3	LZIP.....@X.
00000010:	91de	1027	5861	8a67	4282	46a4	92f9	4cad	... 'Xa.gB.F...L.
00000020:	2d5d	14eb	3099	2c31	01c2	d13a	74d2	c620	-]..0.,1...:t..
00000030:	de27	3a8f	fa92	0644	5468	2d02	01fa	24bb	.':....DTh-...\$.
00000040:	719f	a0fd	a191	1678	8bff	a2c4	2627	9871	q.....x....&' .q
00000050:	83bf	cff2	f8af	99fa	c465	2b7c	6bdf	ee3c	.....e+ k..<
00000060:	b71b	f61b	0b5e	0ce7	d14f	f6a8	0466	6470	.....^....O...fdp
00000070:	de67	02da	7be1	1abd	e9f0	ac87	131a	bcc0	.g...{.....
00000080:	0b0b	9f31	9400	48e3	616a	8f3f	4804	79ad	...1..H.aj.?H.y.
00000090:	a6bb	863a	f641	01da	b1ee	c4fe	b338	9289	....:A.....8..
000000a0:	2a90	8302	4170	773c	88d3	2641	d274	f533	*...Apw<...&A.t.3
000000b0:	84cf	e7d9	f687	3b12	1516	970e	04c2	cfdd	.....?.....
000000c0:	c1ca	dc46	981d	2a7c	1b39	cb0b	4f8c	58cc	...F...* .9...O.X.
000000d0:	46b4	9744	4cb1	fbd3	c632	f36d	ecbf	4789	F..DL.....2.m..G.
000000e0:	00b8	d4fc	51a8	394e	de2a	1a2d	3c43	179c	....Q.9N.*.-<C..
000000f0:	9623	f971	2935	9564	9e15	c771	c3d5	d8b1	.#.q)5.d....q....
00000100:	a7fa	3c0c	f869	b829	f6d6	f145	6d57	b3a1	..<...i.)...EmW..

Pisahkan string hex dan paste kedalam *Hexeditor*, lalu simpan dalam output yang berekstensi *.lz* atau *.tar.lz*, dan langkah terakhir hanya tinggal meng-ekstrak file menggunakan *lunzip*,



Output file berupa gambar yang terdapat flag yaitu IceCTF{h3XduMp1N9\_I1K3\_A\_r341\_B14Ckh47}.

## ❖ Exposed!

**Point** : 60 pt

**Category** : Web (exposed.vuln.icec.tf)

**Flag** : IceCTF{secure\_y0ur\_g1t\_repos\_pe0ple}

**Description** :

John is pretty happy with himself, he just made his first website! He used all the hip and cool systems, like NginX, PHP and Git! Everyone is so happy for him, but can you get him to give you the flag?.

**Solution** :

Dapat dilihat informasi menarik pada file */robots.txt* seperti berikut,





Terdapat file *flag.php* dan ternyata tidak ada flag apa-apa didalam file tersebut, namun kami coba untuk mendumper pada direktori *.git* menggunakan *GitTools* (<https://github.com/internetwache/GitTools>), lalu setelah terdownload, masuk kedalam direktori Dumper dan jalankan file *gitdumper.sh* dengan perintah,

```
./gitdumper.sh https://exposed.vuln.icec.tf/.git/ dump/
```

Maka akan ter-download file-file *objects* yang ada pada direktori *.git* tersebut,

```
Creating exposed/.git/
Downloaded: HEAD
Downloaded: objects/info/packs
Downloaded: description
Downloaded: config
Downloaded: COMMIT_EDITMSG
Downloaded: index
Downloaded: packed-refs
Downloaded: refs/heads/master
Downloaded: refs/remotes/origin/HEAD
Downloaded: refs/stash
Downloaded: logs/HEAD
Downloaded: logs/refs/heads/master
Downloaded: logs/refs/remotes/origin/HEAD
Downloaded: info/refs
Downloaded: info/exclude
Downloaded: objects/17/46e11be489319bd8900318874b68304eb05288
Downloaded: objects/63/1503ff237e145c7bade484c44c05a223b51155
Downloaded: objects/00/0000000000000000000000000000000000000000
```

Setelah semua file *objects* terdownload, masuk kedalam direktori Extractor dan ekstrak menggunakan perintah,

```
./extractor.sh /GitTools/Dumper/dump GitTools/Dumper/dump2
```

Maka akan didapat beberapa direktori dimana didalamnya terdapat pula file-file yang mengandung flag,

```
0-adf0ebdff8a972f3f6158304323feba4aa1fd482 18-971c67fd8ed67c3986844f627917c19c151d00bf
10-f5674cbaacd842cfacbf9f825c29f7f3e5150c7ef 19-bf55633224c5c76f49d42621ace07aa705ebae6e
11-584ae8349fe51e2cb25e11347003c11e92f88c74 20-631503ff237e145c7bade484c44c05a223b51155
12-590a15d32d9a494be5830f61c5c180ddef86e43e 21-d70b2e576c0f35e83d70027434050e06f729662b
13-5ea13398f975b53ff30b7ea162b2ec6897a48c68 22-fd2ac4d5260ee06f9a0e5f4808bf3862e2065fb8
1-4183a0cd7143899e4a5d34f01ce58317fd68921e 2-32b31838b757a00f2e296ac198ca7d9cb930e644
14-4de7e6fbbba6f94bc146b33bbfe6c0155f3c2fd4 23-90c2cd27cabb8ec7f55941ecce004558a070ccde
15-541e08f75514d1caec2a62fe3a1af308da6f35d8 24-ec95d11bb37f00fb8e17f6bdbc800124b79e3c32
16-672c8f636b6db9c79412db177dcca75cde27c82b 25-1f601ea8a09052234b53e2cc1bb12e4ceacbf8a6
17-97dcb30a5862aa43984b8beee84c9477a7315856 26-1746e11be489319bd8900318874b68304eb05288
```

Tak perlu mencari satu-per-satu, gunakan *grep* untuk mencari flag dengan perintah *grep -r "IceCTF{"* maka akan didapat beberapa string seperti berikut,

```
9-f521418118a088ef00fef0c3e199d30d6c7e96a5/index.php: font-size: 2em; /* IceCTF{secure_y0ur */
2-32b31838b757a00f2e296ac198ca7d9cb930e644/flag.txt:IceCTF{this_isnt_the_flag_either}
11-584ae8349fe51e2cb25e11347003c11e92f88c74/flag.txt:IceCTF{this_isnt_the_flag_either}
10-f5674cbaacd842cfacbf9f825c29f7f3e5150c7ef/index.php: echo 'Hello World! IceCTF{secure_y0ur_g1t_repos_pe0ple}';
6-6b3e1ffdc1d679c4815f08ef1d70d1b955451b36/index.php: echo 'Hello World! IceCTF{secure_y0ur_g1t_repos_pe0ple}';
4-60756b184c2d6b8f0247c152d8549562bc14d2d9/flag.php: echo 'IceCTF{not_this_flag}';
15-541e08f75514d1caec2a62fe3a1af308da6f35d8/flag.txt:IceCTF{this_isnt_the_flag_either}
17-97dcb30a5862aa43984b8beee84c9477a7315856/flag.php: echo 'IceCTF{not_this_flag}';
```

Akan tampak beberapa flag palsu seperti *IceCTF{this\_isnt\_flag\_either}* dan *IceCTF{not\_this\_flag}*, dimana hanya ada satu flag yang benar yaitu *IceCTF{secure\_y0ur\_g1t\_repos\_pe0ple}*.

## ❖ RSA

*Point* : 60 pt

*Category* : Cryptography

*Flag* : IceCTF{rsa\_is\_awesome\_when\_used\_correctly\_but\_horrible\_when\_not}

*Description* :

This time John managed to use RSA " correctly "&I think he still made some mistakes though.

*Solution* :

Terdapat variabel  $N$ ,  $e$ ,  $\phi$ ,  $d$ , dan  $c$ ,

```
N=1564aade6f1b9f169dcc94c9787411984cd3878bcd6236c5ce00b4aad6ca7cb0ca8a0334
d9fe0726f8b057c4412cfbfff75967a91a370a1c1bd185212d46b581676cf750c05bbd349d3
586e78b33477a9254f6155576573911d2356931b98fe4fec387da3e9680053e95a47099342
89dc0bc5cdc2aa97ce62a6ca6ba25fca6ae38c0b9b55c16be0982b596ef929b7c71da3783c
1f20557e4803de7d2a91b5a6e85df64249f48b4cf32aec01c12d3e88e014579982ecd04604
2af370045f09678c9029f8fc38ebaea564c29115e19c7030f245ebb2130cbf9dc1c340e2cf
17a625376ca52ad8163cfb2e33b6ecaf55353bc1ff19f8f4dc7551dc5ba36235af9758b
```

$e=10001$

```
phi=1564aade6f1b9f169dcc94c9787411984cd3878bcd6236c5ce00b4aad6ca7cb0ca8a03
34d9fe0726f8b057c4412cfbfff75967a91a370a1c1bd185212d46b581676cf750c05bbd349
d3586e78b33477a9254f6155576573911d2356931b98fe4fec387da3e9680053e95a470993
4289dc0bc5cdc2aa97ce62a6ca6ba25fca6ae366e86eed95d330ffad22705d24e20f9806ce
501dda9768d860c8da465370fc70757227e729b9171b9402ead8275bf55d42000d51e16133
fec3ba7393b1ced5024ab3e86b79b95ad061828861ebb71d35309559a179c6be8697f8a4f3
14c9e94c37cbbb46cef5879131958333897532fea4c4ecd24234d4260f54c4e37cb2db1a0
```

```
d=12314d6d6327261ee18a7c6ce8562c304c05069bc8c8e0b34e0023a3b48cf5849278d349
3aa86004b02fa6336b098a3330180b9b9655cdf927896b22402a18fae186828efac14368e0
a5af2c4d992cb956d52e7c9899d9b16a0a07318aa28c8202ebf74c50ccf49a6733327dde11
1393611f915f1e1b82933a2ba164aff93ef4ab2ab64aacc2b0447d437032858f089bcc0dde
ebc45c45f8dc357209a423cd49055752bfae278c93134777d6e181be22d4619ef226abb6bf
cc4adec696cac131f5bd10c574fa3f543dd7f78aeel0665992f28cdbcf55a48b32beb7a1c
0fa8a9fc38f0c5c271e21b83031653d96d25348f8237b28642ceb69f0b0374413308481
```

```
c=126c24e146ae36d203bef21fcd88fdeefff50375434f64052c5473ed2d5d2e7ac376707d
76601840c6aa9af27df6845733b9e53982a8f8119c455c9c3d5df1488721194a8392b8a97c
e6e783e4ca3b715918041465bb2132a1d22f5ae29dd2526093aa505fcb689d8df5780fa174
8ea4d632caed82ca923758eb60c3947d2261c17f3a19d276c2054b6bf87dcd0c46acf79bff
2947e1294a6131a7d8c786bed4a1c0b92a4dd457e54df577fb625ee394ea92b992a2c22e36
03bf4568b53cceb451e5daca52c4e7bea7f20dd9075ccfd0af97f931c0703ba8d1a7e00bb0
10437bb4397ae802750875ae19297a7d8e1a0a367a2d6d9dd03a47d404b36d7defe8469
```

Namun karena sudah mendapat variabel  $N$  dan  $d$  maka hal yang perlu dilakukan adalah langsung men-decrypt dengan ciphertext yang sudah ada yaitu variabel  $c$ , buat script seperti berikut,

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

d =
int("12314d6d6327261ee18a7c6ce8562c304c05069bc8c8e0b34e0023a3b48cf5849
278d3493aa86004b02fa6336b098a3330180b9b9655cdf927896b22402a18fae186828
efac14368e0a5af2c4d992cb956d52e7c9899d9b16a0a07318aa28c8202ebf74c50ccf
49a6733327dde111393611f915f1e1b82933a2ba164aff93ef4ab2ab64aacc2b0447d4
37032858f089bcc0ddeebc45c45f8dc357209a423cd49055752bfae278c93134777d6e
181be22d4619ef226abb6bfcc4adec696cac131f5bd10c574fa3f543dd7f78aee1d066
5992f28cdbcf55a48b32beb7a1c0fa8a9fc38f0c5c271e21b83031653d96d25348f823
7b28642ceb69f0b0374413308481",16)

c =
int("126c24e146ae36d203bef21fcd88fdeeffff50375434f64052c5473ed2d5d2e7ac
376707d76601840c6aa9af27df6845733b9e53982a8f8119c455c9c3d5df1488721194
a8392b8a97ce6e783e4ca3b715918041465bb2132a1d22f5ae29dd2526093aa505fcb6
89d8df5780fa1748ea4d632caed82ca923758eb60c3947d2261c17f3a19d276c2054b6
bf87dcd0c46acf79bff2947e1294a6131a7d8c786bed4a1c0b92a4dd457e54df577fb6
25ee394ea92b992a2c22e3603bf4568b53cceb451e5daca52c4e7bea7f20dd9075ccfd
0af97f931c0703ba8d1a7e00bb010437bb4397ae802750875ae19297a7d8e1a0a367a2
d6d9dd03a47d404b36d7defe8469",16)

n =
int("1564aade6f1b9f169dcc94c9787411984cd3878bcd6236c5ce00b4aad6ca7cb0c
a8a0334d9fe0726f8b057c4412cfbfff75967a91a370a1c1bd185212d46b581676cf750
c05bbd349d3586e78b33477a9254f6155576573911d2356931b98fe4fec387da3e9680
053e95a4709934289dc0bc5cdc2aa97ce62a6ca6ba25fca6ae38c0b9b55c16be0982b5
96ef929b7c71da3783c1f20557e4803de7d2a91b5a6e85df64249f48b4cf32aec01c12
d3e88e014579982ecd046042af370045f09678c9029f8fc38ebaea564c29115e19c703
0f245ebb2130cbf9dc1c340e2cf17a625376ca52ad8163cfb2e33b6ecaf55353bc1ff1
9f8f4dc7551dc5ba36235af9758b",16)

m = pow(c,d,n)

print num_to_str(m)
```

Python yang digunakan adalah versi 2.7, setelah dirunning maka akan didapat flag yaitu, lceCTF{rsa\_is\_awesome\_when\_used\_correctly\_but\_horrible\_when\_not}



## ❖ Miners!

*Point* : 65 pt

*Category* : Web (miners.vuln.icec.tf)

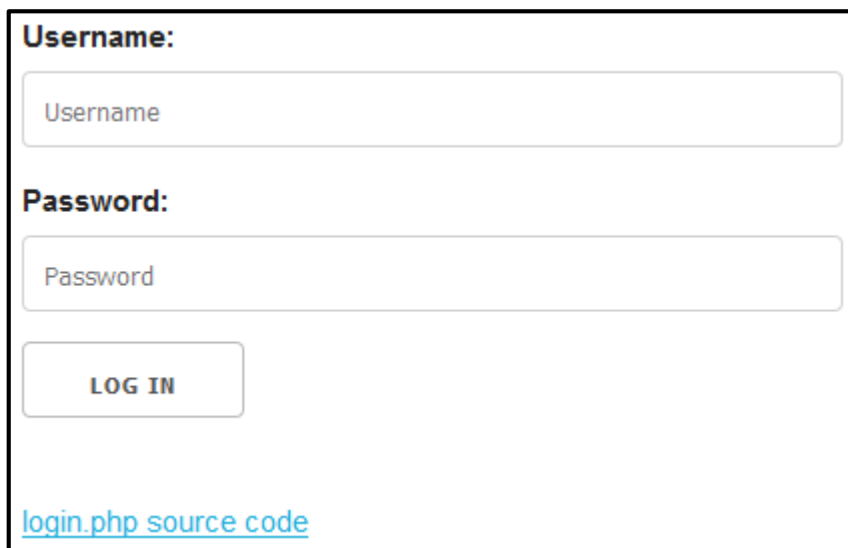
*Flag* : IceCTF{the\_miners\_union\_is\_a\_strong\_one}

*Description* :

The miners website has been working on adding a login portal so that all miners can get the flag, but they haven't made any accounts! However, your boss demands the flag now! Can you get in anyway?.

*Solution* :

Terdapat halaman login dengan memasukkan *Username* dan *Password*, dan terdapat pula source code untuk melihat isi dari *login.php* web tersebut,



Dalam *login.php* dapat dilihat source code berikut,

```
<?php
include "config.php";
$con = mysqli_connect($MYSQL_HOST, $MYSQL_USER, $MYSQL_PASS, $MYSQL_DB);
$username = $_POST["username"];
$password = $_POST["password"];
$query = "SELECT * FROM users WHERE username='$username' AND password='$password'";
$result = mysqli_query($con, $query);

if (mysqli_num_rows($result) != 1) {
    echo "<h1>Login failed.</h1>";
} else {
    echo "<h1>Logged in!</h1>";
    echo "<p>Your flag is: $FLAG</p>";
}

?>
```

Injeksi pada *Username* dengan memasukkan 'union select 1,2,info from information\_schema.processlist-- - lalu didapatkan flag yaitu IceCTF{the\_miners\_union\_is\_a\_strong\_one}.

## ❖ Over the Hill

*Point* : 65 pt

*Category* : Cryptography

*Flag* : IceCTF{linear\_algebra\_plus\_led\_zeppelin\_are\_a\_beautiful\_m1xture}

*Description* :

Over the hills and far away... many times I've gazed, many times been bitten. Many dreams come true and some have silver linings, I live for my dream of a decrypted flag.

*Solution* :

Misi berupa *Hill Chiper* dengan matrix ukuran 8x8,

Alphabet =

"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ123456789\_{}"

Matrix =

```
[
    [54, 53, 28, 20, 54, 15, 12, 7],
    [32, 14, 24, 5, 63, 12, 50, 52],
    [63, 59, 40, 18, 55, 33, 17, 3],
    [63, 34, 5, 4, 56, 10, 53, 16],
    [35, 43, 45, 53, 12, 42, 35, 37],
    [20, 59, 42, 10, 46, 56, 12, 61],
    [26, 39, 27, 59, 44, 54, 23, 56],
    [32, 31, 56, 47, 31, 2, 29, 41]
]
```

Ciphertext =

"7Nv7}dI9hD9qGmP}CR\_5wJDdkj4CKxd45rko1cj51DpHPnNDb\_\_EXDotSRCP8ZCQ"

Lakukan decoding dengan menggunakan script python (<http://bit.ly/2bKOgOf>), setelah di-running akan mendapat flag yaitu IceCTF{linear\_algebra\_plus\_led\_zeppelin\_are\_a\_beautiful\_m1xture}

## ❖ Kitty

*Point* : 70 pt

*Category* : Web (kitty.vuln.icec.tf)


*Flag* : IceCTF{i\_guess\_hashing\_isnt\_everything\_in\_this\_world}

*Description* :

They managed to secure their website this time and moved the hashing to the server :( We managed to leak the hash of the admin's password though! Can you get the flag?.

*Solution* :

Terdapat halaman login dengan memasukkan *Username* dan *Password*, dan berupa clue bahwa *Username* adalah "admin" sedangkan *Password* merupakan hasil enkripsi dari *SHA-256* yaitu (c7e83c01ed3ef54812673569b2d79c4e1f6554ffeb27706e98c067de9ab12d1a),



The image shows a login form with a black border. At the top, it says "Username:" in bold. Below it is a text input field containing the placeholder text "Username". Underneath that, it says "Password:" in bold. Below the password label is another text input field containing the placeholder text "Password". At the bottom of the form is a button labeled "LOG IN" in all caps.

Decode *Password* secara online pada web <http://md5decrypt.net/en/Sha256> sehingga didapat password Vo83\*, lalu login sehingga mendapatkan flag yaitu IceCTF{i\_guess\_hashing\_isnt\_everything\_in\_this\_world}.

## STAGE 3

### ❖ Audio Problems

*Point* : 50 pt

*Category* : Forensic

*Flag* : IceCTF{y0U\_b3t7Er\_l15teN\_cl053ly}

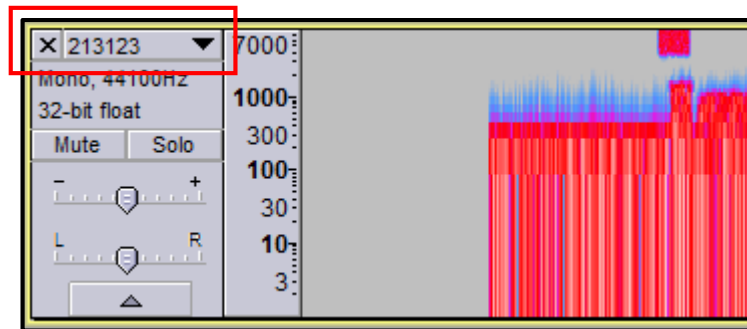
*Description* :

We intercepted this audio signal, it sounds like there could be something hidden in it. Can you take a look and see if you can find anything?.

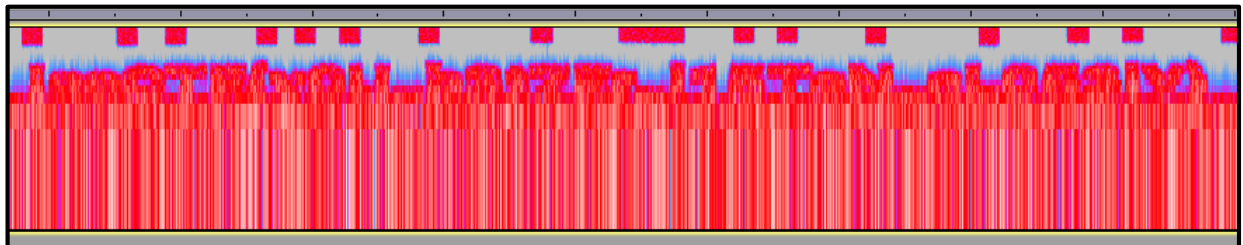
- *Link File* : <http://bit.ly/2bqaSEL>

*Solution* :

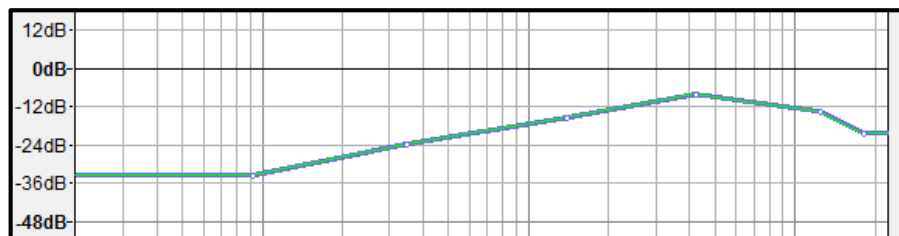
Buka file .wav menggunakan aplikasi Audacity, lalu pada bagian kiri panel audio yang telah ter-load, klik icon panah bawah lalu pilih *Spectral Selection Log (f)*,



Sehingga akan tampil baris *Spectral* seperti berikut,



Langkah selanjutnya adalah pilih pada bagian tab *Effect*, dan pilih *Equalization* lalu tinggal dimainkan titik pada garis agar flag semakin terlihat jelas,



Tidak terlihat jelas sempurna memang, maka hanya perlu menebak string yang terdapat pada *Spectral* sehingga didapat flag yaitu IceCTF{y0U\_b3t7Er\_l15teN\_cl053ly}.

## ❖ Corrupt Transmission

*Point* : 50 pt

*Category* : Forensic

*Flag* : IceCTF{t1s\_but\_4\_5cr4tch}

*Description* :

We intercepted this image, but it must have gotten corrupted during the transmission. Can you try and fix it?.

- *Link File* : <http://bit.ly/2bfZNEm>

*Solution* :

Buka gambar menggunakan aplikasi *Hexeditor*, maka akan terlihat bahwa *Majic Number* yang ada pada gambar tersebut (`90 50 4E 47 0E 1A 0A 1B`) tidak sesuai dengan *Majic Number* file *PNG* (`89 50 4E 47 0D 0A 1A 0A`) lalu pada akhir byte pula terdapat satu bilangan hex yang perlu dihapus yaitu `0A` lalu simpan,



Maka muculah gambar yang terdapat flag yaitu IceCTF{t1s\_but\_4\_5cr4tch}.

## ❖ Vape Nation

*Point* : 50 pt

*Category* : Stego

*Flag* : IceCTF{420\_CuR35\_c4NCeR}

*Description* : Go Green!

- *Link File* : <http://bit.ly/2bJKtk7>

*Solution* :

Buka gambar menggunakan aplikasi *Stegsolve* dan geser hingga bagian *Green Plane 0* maka akan mendapat flag IceCTF{420\_CuR35\_c4NCeR}

## ❖ Blue Monday

Point : 60 pt

Category : Misc

Flag : IceCTF{h3l10\_wr0ld}

Description :

Those who came before me lived through their vocations From the past until completion, they'll turn away no more And still I find it so hard to say what I need to say But I'm quite sure that you'll tell me just how I should feel today.

- Link File : <http://bit.ly/2bfZjOK>

Solution :

Buka file menggunakan *Notepad++* dan file yang didapat memiliki header *MThd*, *Mthd* merupakan file yang ber-ekstensi *.midi* adalah sebuah standar hardware dan software internasional untuk saling bertukar data (seperti kode musik dan MIDI Event) di antara perangkat musik elektronik dan komputer dari merek yang berbeda. ([id.wikipedia.org/wiki/MIDI](http://id.wikipedia.org/wiki/MIDI)),

```
MThdNULNULACKNULSOHNULSOHNULÜMTrkNULNULSOH*NULId\€I NULNULcd\€cNULNULed\€e
NULNULcd\€cNULNULtd\€tNULNULfd\€fNULNUL{d\€{ NULNULhd\€hNULNULad\€aNULNULcd\€c
NULNULkd\€kNULNULld\€lNULNULnd\€nNULNUL9d\€9NULNUL_d\€_NULNULmd\€mNULNULUd\€U
NULNUL5d\€5NULNULId\€I NULNULcd\€cNULNUL_d\€_NULNULwd\€wNULNULld\€lNULNUL7d\€7
NULNULhd\€hNULNUL_d\€_NULNULmd\€mNULNULId\€I NULNULDd\€DNULNULld\€lNULNUL5d\€5
NULNUL_d\€_NULNULld\€lNULNUL3d\€3NULNULtd\€tNULNUL5d\€5NULNUL_d\€_NULNULhd\€h
NULNUL4d\€4NULNULvd\€vNULNULEd\€ENULNUL_d\€_NULNULad\€aNULNUL_d\€_NULNULrd\€r
NULNUL4d\€4NULNULvd\€vNULNUL3d\€3NULNUL}d\€}NUL+hÿ/NUL
```

Namun yang mencurigakan disini adalah terdapat string kurung kurawal buka “{” dan kurung kurawal tutup “}”, sehingga clue ini mengarah pada adanya flag yang disisipi seperti berikut,

```
MThdNULNULACKNULSOHNULSOHNULÜMTrkNULNULSOH*NULId\€I NULNULc\€cNULNULed\€e
NULNULc\€cNULNULt\€tNULNULf\€fNULNUL{d\€{ NULNULh\€hNULNULa\€aNULNULcd\€c
NULNULk\€kNULNULl\€lNULNULn\€nNULNUL9\€9NULNUL_d\€_NULNULm\€mNULNULU\€U
NULNUL5\€5NULNULI\€I NULNULc\€cNULNUL_d\€_NULNULw\€wNULNULl\€lNULNUL7\€7
NULNULh\€hNULNUL_d\€_NULNULm\€mNULNULI\€I NULNULD\€DNULNULld\€lNULNUL5\€5
NULNUL_d\€_NULNULl\€lNULNUL3\€3NULNULt\€tNULNUL5\€5NULNUL_d\€_NULNULh\€h
NULNUL4\€4NULNULv\€vNULNULE\€ENULNUL_d\€_NULNULa\€aNULNUL_d\€_NULNULr\€r
NULNUL4\€4NULNULv\€vNULNUL3\€3NULNUL}d\€}NUL+hÿ/NUL
```

Jika diurutkan akan didapat flag yaitu IceCTF{hAck1n9\_mU5lc\_W17h\_mID15\_L3t5\_H4vE\_a\_r4v3}.

## ❖ Pretty Pixels

Point : 80 pt

Category : Stego

Flag : IceCTF{puT\_Th4t\_1n\_yoUr\_cOlOrin9\_Book\_4nD\_5moKe\_1T}

Description :

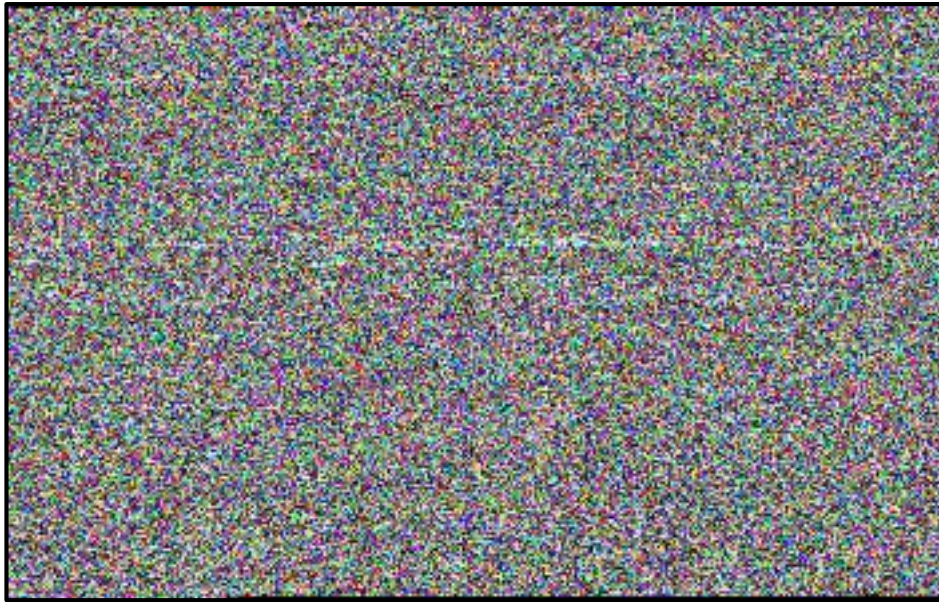
Don't get me wrong, I love pretty colors as much as the next guy... but what does it mean?

- Link File : <http://bit.ly/2bwZqZQ>

Solution :

Diberikan sebuah gambar berupa pixel warna yang tak beraturan dengan ukuran 350x222 seperti berikut,





Lalu ekstrak nilai *RGB* dengan script python berikut,

```
import os, sys
from PIL import Image

im = Image.open("pretty_pixels.png")
rgb_im = im.convert('RGB')
for y in range(0,222):
    for x in range (0,350):
        r, g, b = rgb_im.getpixel((x,y))
        sys.stdout.write(str(r)+" "+str(g)+" "+str(b)+" ")
```

Setelah script di running, maka akan didapat nilai decimal,

137 80 78 71 13 10 26 10 ..... 73 69 78 68 174 66 96 130

Lalu diubah dalam bentuk hex,

89 50 4E 47 0D 0A 1A 0A ..... 49 45 4E 44 AE 42 60 82

Dan simpan nilai hex tersebut menggunakan *Hexeditor* dengan ekstensi *.png*,



Tampilah gambar serta flag didalamnya yaitu IceCTF{puT\_Th4t\_1n\_yoUr\_cOlOrin9\_Book\_4nD\_5moKe\_1T}.

## ❖ RSA2

*Point* : 90 pt

*Category* : Cryptography

*Flag* : IceCTF{next\_time\_check\_your\_keys\_arent\_factorable}

*Description* : I guess the 3rd time is the charm? Or not...

*Solution* :

Terdapat variabel  $N$ ,  $e$ , dan  $c$ ,

```
N=ee290c7a603fc23300eb3f0e5868d056b7deb1af33b5112a6da1edc9612c5eeb4ab07d83
8a3b4397d8e6b6844065d98543a977ed40ccd8f57ac5bc2daee2dec301aac508f9befc27fa
e4a2665e82f13b1ddd17d3a0c85740bed8d53eeda665a5fc1bed35fbbcedd4279d04aa747a
c1f996f724b14f0228366aeae34305152e1f430221f9594497686c9f49021d833144962c2a
53dbb47bdbfd19785ad8da6e7b59be24d34ed201384d3b0f34267df4ba8b53f0f4481f9bd2
e26c4a3e95cd1a47f806a1f16b86a9fc5e8a0756898f63f5c9144f51b401ba0dd5ad58fb0e
97ebac9a41dc3fb4a378707f7210e64c131bca19bd54e39bbfa0d7a0e7c89d955b1c9f
```

$e=10001$

```
c=3dbf00a02f924a70f44bdd69e73c46241e9f036bfa49a0c92659d8eb0fe47e42068eaf15
6a9b3ee81651bc0576a91ffed48610c158dc8d2fb1719c7242704f0d965f8798304925a322
c121904b91e5fc5eb3dc960b03eb8635be53b995217d4c317126e0ec6e9a9acfd5d9152656
34a22a612de962cfaa2e0443b78bdf841ff901423ef765e3d98b38bcce114fede1f13e223b
9bd8155e913c8670d8b85b1f3bcb99353053cdb4aef1bf16fa74fd81e42325209c0953a694
636c0ce0a19949f343dc229b2b7d80c3c43ebe80e89cbe3a3f7c867fd7cee06943886b0718
a4a3584c9d9f9a66c9de29fda7cfee30ad3db061981855555eeac01940b1924eb4c301
```



Buat script python berikut lalu running,

```
import gmpy2

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

p = 57970027
q =
5186293680901708283310486635502296344443842997512729390771686489350756
0418067600639246452495312829384299644102277189071973181185294868495038
8211907532651941639114462313594608747413310447500790775078081191686616
8049877908183961043883327346779356847236471089608827714603412930237641
1718239373083841846848000698576838211544622542278111653190632304516180
3441960506496275763429558238732127362521949515590606221409745127192859
6304688546532903024910632927354962862337385040106133738380350739951407
4472494893383923885160063865231565550886172843918098825332494303936787
6070687033249730660337593825389358874152757864093

t = (p-1)*(q-1)
d = gmpy2.invert(65537,t)
c =
int("3dbf00a02f924a70f44bdd69e73c46241e9f036bfa49a0c92659d8eb0fe47e420
68eaf156a9b3ee81651bc0576a91ffed48610c158dc8d2fb1719c7242704f0d965f879
8304925a322c121904b91e5fc5eb3dc960b03eb8635be53b995217d4c317126e0ec6e9
a9acfd5d915265634a22a612de962cfaa2e0443b78bdf841ff901423ef765e3d98b38b
cce114fedelf13e223b9bd8155e913c8670d8b85b1f3bcb99353053cdb4aef1bf16fa7
4fd81e42325209c0953a694636c0ce0a19949f343dc229b2b7d80c3c43ebe80e89cbe3
a3f7c867fd7cee06943886b0718a4a3584c9d9f9a66c9de29fda7cfee30ad3db061981
855555eeac01940b1924eb4c301",16)

n = p*q
m = pow(c,d,n)
print num_to_str(m)
```

Maka akan didapat flag yaitu, lceCTF{next\_time\_check\_your\_keys\_arent\_factorable}.