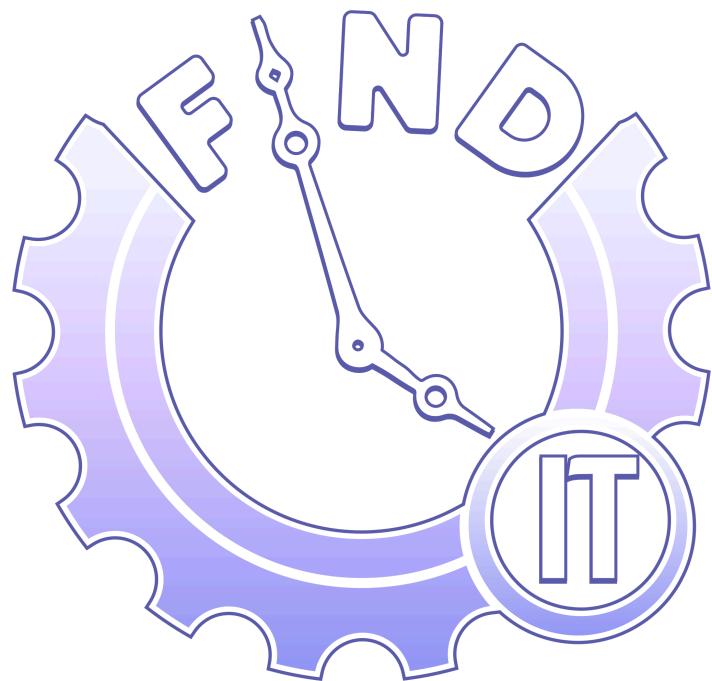


Writeup FindIT Capture the Flag 2025



by:
penghitamanMassal

Category: MISC

distorted

Deskripsi:

GAMBARNYA MLEYOTT. Setiap row bergeser 5 pixels lebih dari row sebelumnya. Gimana nih biar gambarnya kelihatan dan lokasinya bisa dicari?

- Format Flag: FindITCTF{Lintang_Bujur_Nama_Tempat}
- case insensitive

Hint:

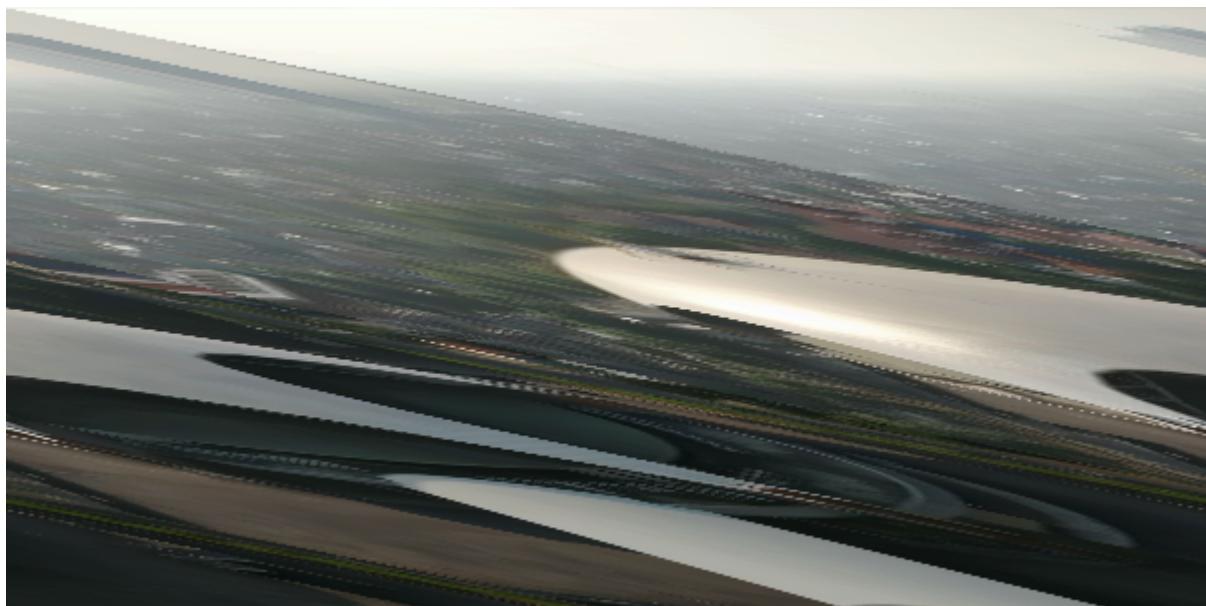
(4 angka di belakang desimal / .231245 = .2312) (Nama Lokasi Ikutin Format Google Maps)

File:

location.png

Penyelesaian:

Di challenge ini, kita diberikan sebuah file PNG yang terdistorsi sesuai dengan judul.



Di deskripsi sudah diberi tahu bahwa gambar ini “Setiap row bergeser 5 pixels lebih dari row sebelumnya.”. Jadi, kita hanya perlu membalikkan operasinya untuk mengembalikan gambar ini seperti semula dan kita bisa menggunakan skrip Python dengan library [Pillow](#).

```
from PIL import Image
import numpy as np

img = Image.open("location.png")
img_array = np.array(img)
fixed_img_array = np.zeros_like(img_array)
height, width, channels = img_array.shape

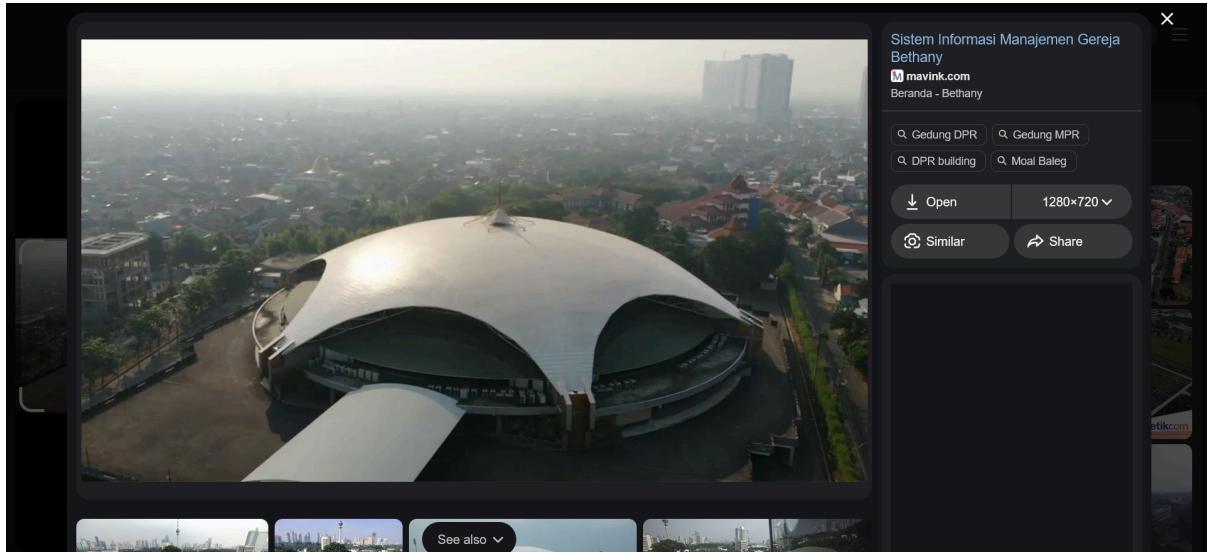
for row in range(height):
    shift = (row * 5) % width
    fixed_img_array[row] = np.roll(img_array[row], -shift,
axis=0)

fixed_img = Image.fromarray(fixed_img_array)
fixed_img.save("fixed_location.png")
```

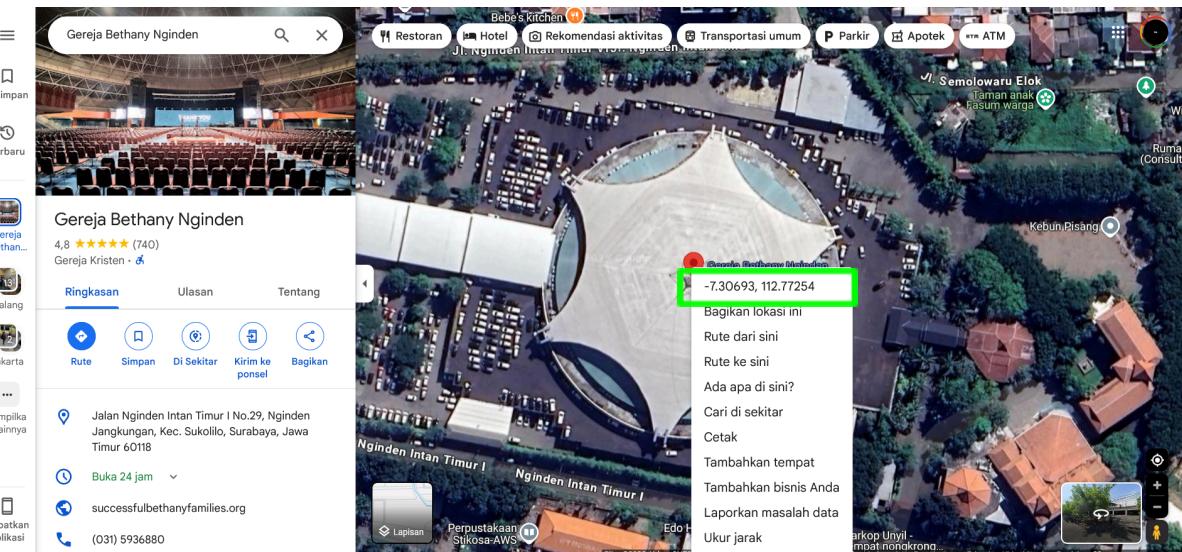
Setelah dijalankan, maka gambar yang sudah diperbaiki akan muncul.



Selanjutnya, untuk mencari koordinat dari tempat ini, kita bisa menggunakan *reverse image search* seperti milik Yandex.



Setelah dicari, ini adalah sebuah gereja yang terletak di kota Surabaya yang bernama Gereja Bethany. Dengan sedikit petunjuk yang kita dapat sekarang, kita bisa menggunakan Google Maps untuk mencari koordinat dan mencari format nama yang ada di Google Maps.



Dengan klik kanan pada lokasinya, kita bisa mendapatkan Lintang dan Bujur dari lokasi tersebut. Karena pada deskripsi yang diminta adalah empat angka di belakang koma, maka kita akan gunakan -7.3069 dan 112.7725 sebagai koordinatnya. Selanjutnya, Google Maps menunjukkan bahwa format namanya adalah Gereja Bethany Nginden. Oleh karena itu, kita bisa menyusun flag-nya.

FindITCTF{-7.3069_112.7725_Gereja_Bethany_Nginden}

Category: Cryptography

Spacemonkey

Deskripsi:

Our space monkey ceaser has gone missing in space, before he went missing he sent us two message.

Hint:

- He seems to encrypt the cipher with his favorite method (his name maybe?)
- YKSPWXSPFCBNNSSF
- Hint on working with cipher.txt: Shift 3
- 5x5, append, the rest is abcd

File:

cipher.txt
code.txt

Penyelesaian:

Di challenge ini kita diberikan dua file TXT yang disimpan di dalam arsip 7z. File code.txt berisi sebuah kode morse dan cipher.txt berisi sebuah string acak yang akan kita dekripsi nanti. Namun, seiring dengan berjalananya waktu, string tersebut tidak menghasilkan apa-apa dan ternyata memang diganti dengan yang ada pada deskripsi soal yaitu YKSPWXSPFCBNNSSF.

Sekarang, kita coba lihat apa isi dan arti dari kode morse yang diberikan di soal.

... - -- .- . . - . - / .--. - - / .. - / .. - / - / .--. - .. - - - - .. - .. - - .

Setelah diterjemahkan dengan tool online, ternyata arti dari kode morse tersebut adalah “FOREVER PUT IT IN THE PLAYFAIR”. Ini adalah sebuah clue bahwa cipher ini akan melibatkan [Playfair cipher](#) sebagai penyelesaiannya. Namun, untuk sekarang, kita perlu mendekripsi dengan menggunakan caesar cipher (shift) terlebih dahulu seperti pada hint.

Caesar Cipher - Shift by 3

D, E, F, G, H, I, ... B, C
A, B, C, D, E, F, ... Y, Z

→3 (←23) VHPMTUPMCZYKKPPC
←3 (→23) BNVSZAVSIFEQQVVI

Di sini, kita dapatkan dua hasil, yaitu 3 ke kanan dan 3 ke kiri dan setelah dicoba, yang benar adalah 3 ke kiri yaitu BNVSZAVSIFEQQVVI. Maka, setelah ini kita bisa masuk ke Playfair cipher untuk mendapatkan pesan aslinya.

Di Playfair, kita butuh kunci dan kita bisa coba menggunakan kata FOREVER... sebagai kuncinya. Namun, karena tidak boleh ada huruf yang sama, maka sesuai hint, kita hanya bisa menggunakan 5 huruf pertama dan sisanya adalah huruf lain. Maka, dibantu dengan fitur autocomplete dari [dcode.fr](#), kunci yang kita miliki adalah FOREVABCDGHJKLMNPQSTUWXYZ.

Results



APETUGETHORSTROM

PlayFair Cipher - [dCode](#)

Tag(s) : Polygrammic Cipher, GRID_CIPHER

Ini adalah hasil dekripsinya. Karena di sini flag-nya belum sesuai format, kita perlu wrap terlebih dahulu dengan format flag-nya yaitu FindITCTF{ } .

FindITCTF{APETUGETHORSTROM}

Category: MISC

CEK-CEK

Deskripsi:

Hei, aku baru belajar python. Semoga aku tidak melupakan sesuatu.

Disini kita diberi file program python dan nc, saat run nc akan muncul interface:

```
Do you want check my file?  
1. yes  
2. no  
>>> |
```

jika memilih no akan muncul pesan ini:

ok, here the flag:

```
dd3d8c2ee95f1176de68c8a4869ecd5a75262a98d0cf8fd130a02830a043bd56  
b18a70700128c91441a6e5611963a81bf0e0acd211a84a8c91c1776bab80c19c
```

jika kita lihat di program python flag ini di hash dengan cara:

```
hash_obj = hashlib.blake2b()  
hash_obj.update(FLAG.encode())  
flag = hash_obj.hexdigest()
```

flag dish dengan black2b yang tidak bisa di reverse jadi ini bukan opsi.

jadi memilih yes akan muncul interface:

```
Do you want check my file?  
1. yes  
2. no  
>>> 1  
file name: |
```

kita lihat program pythonnya serta deskripsi challenge, apa yang mungkin dia lupakan, file name ini di check dengan:

```
def check(s):
    if "." in s or "flag" in s:
        return False
    return True

def open_file(file_name):
    if not check(file_name):
        return "eits tidak boleh begitu", 500

    try:
        file = os.open(file_name, os.O_RDONLY)
        data = os.read(file, 1024)
    except Exception:
        return "error bang"

    return data.decode("utf-8")

if __name__ == "__main__":
    with open("/flag.txt", "w") as f:
        f.write(FLAG)

    flag_file = os.open("/flag.txt", os.O_RDONLY)
    flag_data = os.read(flag_file, 1024)

    if FLAG.encode() != flag_data:
        print("flag file is corrupted")
        exit(1)
```

filename difilter agar tidak mengijinkan “.” dan “flag”. jdi memasukkan flag.txt tidak mungkin. Setelah memeriksa kode, terlihat bahwa /flag.txt dibuka dengan:
flag_file = os.open("/flag.txt", os.O_RDONLY)

tapi tidak pernah ditutup (os.close tidak dipanggil). Akibatnya file descriptor untuk flag.txt tetap terbuka selama program berjalan. mungkin ini yang dimaksud tentang “semoga aku tidak melupakan sesuatu”. karen flag.txt tidak memungkinkan diakses seperti itu, Kita dapat mengaksesnya secara indirect melalui /proc/self/fd/.. atau /dev/fd/.., di mana .. adalah nomor descriptor.

Nomor FD dimulai dari: 0 = stdin, 1 = stdout, 2 = stderr, 3, 4, 5, ... = file yang dibuka oleh program:

jadi kita brute force dan ternyata di fd ke 5 mendapat:

```
FindITCTF{cl0s3_y0ur_f1l3s_1mm3d14t3ly_0r_w0w0_w1ll_f1nd_y0u}
```

WEB

Simpe Heist

deskripsi: gampang sekali, tinggal cari kunci dari brankasnya cuma internal yang boleh tau banyak hal

berdasarkan deskripsi, kita coba /internal dan mendapat:

The Crypt Keepers Internal Bulletin:

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

Delete this endpoint before production!

yang berarti ada yg harus di hash dengan kunci tersebut. Untuk masuk ke /vault dan mendapat flag kita harus jadi admin seperti yang dikatakan:



Access denied. Only admins may enter.

di burp kita send to repeater saat GET /vault, pada cookie kita mencoba mengubah status user ke admin, tpi mendapat pesan

The Crypt Keepers Alert: Tampering detected!

artinya ada yg masih salah, selanjutnya berdasarkan /internal, kita coba encode dengan HMAC dan mencobanya lagi, tetapi masih sama. jdi kemungkinan selanjutnya adalah sig nya :

```
Cookie: auth="user:teller|bank:Fortis Bank"; sig=7a91f28871e4b9a78f12ff523f068806d6270aaa418fb2a842135faa68e43266
```

kita coba ubah signya dan mengubah teller ke admin:

sig=7f5976dc018b18b360aad2d4c5b3efe099db2bbba363bad5c1932b137f41ba

dan mendapat:

FindITCTF{BEtEc_10_&1J!})

Category:Reverse

xor_madness

Deskripsi : Bombombini Gusini adalah seorang mahasiswa tahun pertama jurusan Teknologi Informasi yang tengah mendalami cryptography dan malware analysis di mata kuliah Peretasan Beretika. Suatu hari, dosen memberikan tugas berupa sebuah binary file bernama xor_madness.bin. Katanya jika ia berhasil mendapatkan "sesuatu" dari binary file tersebut, maka ia akan langsung mendapatkan nilai A. Bantulah ia untuk bisa mendapatkan "sesuatu" tersebut.

File : xor_madness.bin

Penyelesaian : jadi pada challenge ini kita diberikan sebuah file xor_madness.bin , maka di challenge ini saya download dulu file lalu saya mencoba untuk membuka file tersebut.

```
root@LAPTOP-2UUUSR26:~/PICOtf# ./xor_madness.bin  
-bash: ./xor_madness.bin: Permission denied
```

Ternyata permission denied maka disini saya menggunakan command (chmod -R 777 .) Agar dapat mengakses file nya. Setelah saya gunakan command tersebut dan mencoba untuk mengakses ketika di akses menghasilkan tampilan berikut.

```
root@LAPTOP-2UUUSR26:~/PICOtf# ./xor_madness.bin  
./xor_madness.bin: line 1: $'Uz}wZGPGUhzjLq } aL"}"Lu\177tL{jLq}tn': command not found
```

Terdapat sebuah teks aneh berikut. karena tidak menemukan flag saya mencoba menggunakan ghidra untuk melihat isi kode program. dan ketika saya menggunakan ghidra untuk mengecek file nya didalam file nya terdapat sebuah kode berikut.

```
//  

00000000 55      ??      55h  U  

00000001 7a      ??      7Ah  z  

00000002 7d      ??      7Dh  }  

00000003 77      ??      77h  w  

00000004 5a      ??      5Ah  Z  

00000005 47      ??      47h  G  

00000006 50      ??      50h  P  

00000007 47      ??      47h  G  

00000008 55      ??      55h  U  

00000009 68      ??      68h  h  

0000000a 7a      ??      7Ah  z  

0000000b 6a      ??      6Ah  j  

0000000c 27      ??      27h  '  

0000000d 4c      ??      4Ch  L  

0000000e 71      ??      71h  q  

0000000f 20      ??      20h  ''  

00000010 7d      ??      7Dh  }  

00000011 20      ??      20h  ''  

00000012 61      ??      61h  a  

00000013 4c      ??      4Ch  L  

00000014 22      ??      22h  ''  

00000015 7d      ??      7Dh  }  

00000016 22      ??      22h  ''  

00000017 4c      ??      4Ch  H  

00000018 75      ??      75h  u  

00000019 7f      ??      7Fh  A  

0000001a 27      ??      27h  '  

0000001b 74      ??      74h  t  

0000001c 4c      ??      4Ch  L  

0000001d 7d      ??      7Dh  }  

0000001e 6a      ??      6Ah  j  

0000001f 27      ??      27h  '  

00000020 4c      ??      4Ch  L  

00000021 71      ??      71h  q  

00000022 27      ??      27h  '  

00000023 7d      ??      7Dh  }  

00000024 74      ??      74h  t  

00000025 6e      ??      6Eh  n
```

Kode nya seperti terlihat agak mencurigakan mungkin saja itu adalah sebuah plaintext maka langkah selanjutnya adalah saya mengambil semua teks tersebut dan mengubahnya ke decrypt xor sesuai dengan nama soal xor_madness

The screenshot shows the XOR section of the Cryptopals challenge interface. The 'Input' field contains the hex string: Uz]wZGPGUhjz'!q } aL}"Lu•'tL}j'Lq')tn. The 'XOR' section has 'Key' selected as the scheme. Under 'XOR Brute Force', 'Key length' is set to 1, 'Sample length' to 100, and 'Sample offset' to 0. 'Scheme' is set to 'Standard'. There are two checkboxes: 'Null preserving' (unchecked) and 'Print key' (checked). Below these are two more checkboxes: 'Output as hex' (unchecked) and 'Crib (known plaintext string)' (unchecked). The 'Output' section displays the decrypted key, which is a long string of characters including special symbols like '!', '•', and '•'. The interface also includes a 'STEP' button at the bottom left and a 'BAKE!' button with a chef icon at the bottom center.

Dan setelah saya decrypt gunakan xor bruteforce saya menemukan flag nya pada key=13

Flag : FindITCTF{iy4_b3n3r_1n1_fl4g_ny4_b4ng}

Category : Osint

destroyer

Deskripsi : Kau tahu? ada suatu kaum yang dikurung dari zaman dahulu hingga sekarang. Mereka bakal bisa naik pesawat gak ya wkwkwkkwkw.

Format FLAG: FindITCTF{coordinateX_coordinateY}

File : street_view.png

Penyelesaian : pada challenge kali ini kita diberikan sebuah file street_view.png , lalu saya mendownload file tersebut dan melihat apa isi dari foto tersebut ketika dibuka terdapat tampilan berikut.

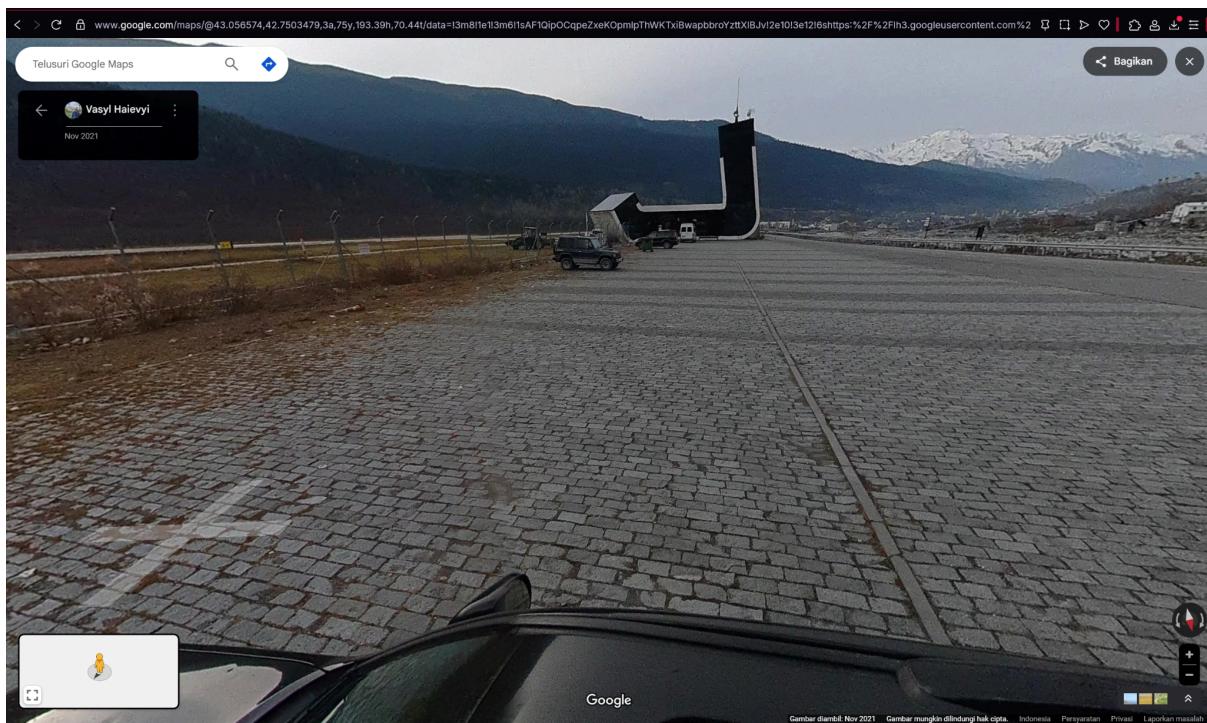


dari gambar mungkin gambar tersebut di suatu bandara, maka langkah selanjutnya adalah saya menggunakan yandex scanner img untuk mencari nama dari lokasi tersebut ketika saya gunakan yandex scanner img tersebut mendapatkan hasil berikut.



Ternyata dari foto tersebut. foto itu berada di Georgia mestia airport. maka disini saya menggunakan google maps untuk mencari lokasi tersebut berada dan mencari koordinat lokasi tersebut.

lalu saya akhir menemukan lokasi tersebut akan tetapi saya mencoba agar posisi sesuai dengan seperti yang foto berikan. maka saya mencoba membuka akses 3d



Karena ini sudah mirip dengan yang difoto maka saya cek koordinat nya dari link website nya terdapat koordinat nya adalah

'@43.056574,42.7503479,

Maka di dapatkan lah flag nya.

Flag : FindITCTF{43.056574_42.7503479}

Category : Cryptography

caesar cipher

Deskripsi: Pada suatu malam, Tung Tung Tung Sahur ingin mendatangi seorang pemuda yang tidak bangun sahur setelah dipanggil sahur sebanyak 3 kali, tetapi tidak nyaut. Masalahnya adalah pintu kamar pemuda tersebut terkunci dengan password tertentu, tetapi terdapat file cipher.txt yang tersimpan dalam flashdisk di dekatnya yang bisa digunakan untuk menemukan passwordnya. Bantulah Tung Tung Tung sahur untuk menemukan passwordnya!

File : cipher.txt

Penyelesaian : Jadi pada challenge ini kita diberikan sebuah file yaitu cipher.txt , maka disini saya mencoba untuk mendownload file berikut. ketika di akses file berikut terdapat sebuah teks.

```
Ymnx nx f xjhwjy ymj vzny htzw fyyjw. Qnkj ymj bnqq gj f xjhtsi bj bnqq gifyyj,  
jshwdyunts ymj knwxy ts ymj xtrj tk ymj ufxfrnsl gjktwj. Tzlm rjxxflj, ymj  
htsyfsy tk ymj xtrj qnkj f hfjxfw ns yjcy. Qjilmynnts ymj jshwduy rjxxflj kwtr  
f wifi ymj rjxxflj yt ymj fxyjw. Rjxxflj xynsl ymnx KnsiNYHYK{Mrrrr_1_W89qqd_i5sy_pstb_Ym8_U5xxbtwi}
```

Seperti nya sebuah teks terenkripsi, sesuai nama soal yaitu caesar cipher maka saya mencoba menggunakan caesar cipher untuk mengubah teks tersebut agar dapat dibaca. ketika saya gunakan caesar cipher saya menemukan teks berikut.

The image shows two side-by-side interfaces for cracking Caesar ciphers:

- dCode Caesar Decoder:** This tool uses a brute-force approach to test all 25 shifts. It displays two decrypted messages:
 - Shift 11: "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
 - Shift -5 (21): "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}
- Cryptopals Caesar Decoder:** This tool allows manual decryption with parameters like shift and key. It also has a brute-force option. The interface shows the same two decrypted messages as the dCode tool.

Disitu terdapat sebuah teks yang sudah bisa dibaca dan ada format flag yaitu FindITCTF{..} maka flag nya dari chall tersebut.

Flag : **FindITCTF{Hmmmm_1_R89lly_d5nt_know_Th8_P5ssword}**