**Writeup Kessoku Band**

**Penyisihan Unity 2023**



**Anggota tim:**

**ryo**

**nijika**

**azunyan**

# **Daftar Isi**

[**Daftar Isi 2**](#_jtobumv3ewy0)

[**Crypto 4**](#_jymxxw9v0ao8)

[HEXagon 4](#_rp5oo69pgbzv)

[Flag: UNITY2023{Y4hh\_G4mp4n9\_Y444\_M4S1h\_34sy\_l00} 5](#_hezx61mum27e)

[Semangat64 5](#_tyyenwwhou5c)

[Flag: UNITY2023{Cum4\_84s364\_b4n9} 6](#_yph61lhmi9wx)

[DiffieDikky\_Broo 7](#_russqpd9clee)

[Flag: UNITY2023{64} 8](#_xzzg0bjtfh4l)

[TTSBukanTPS 9](#_h5nnrda0l2t)

[Flag: UNITY2023{bayijugatahu}: 10](#_nosp5vuq7elw)

[Coklat 11](#_dvjudobixmpl)

[Flag: 11](#_cjy8h6zg87ik)

[OnTheWayPak 11](#_omjppjqwxh6)

[Flag: ????? 12](#_vpekrr9easa)

[SnackCry 12](#_t89qg8mfnf16)

[Flag: ????? 13](#_mlc9x1cjc7n3)

[GAMAliel 13](#_j6n829rqjjj)

[Flag: ????? 14](#_dtvd6tbrh6wm)

[G0lden\_k3y 14](#_nxituiesae26)

[Flag: ????? 14](#_jstb7ka3vvpj)

[PADDDing 15](#_65p42u267bow)

[Flag: ????? 15](#_91n726wgehm2)

[**Rev 15**](#_qvpfgwk2a8qc)

[Cr4ck312 15](#_ropqufdfxzc1)

[Flag: UNITY2023{B3l4j4r\_J4d!\_Hacker\_B4n9} 16](#_fr2vz5x59zaf)

[STARlight 17](#_xji6vf5ynask)

[Flag UNITY2023{H3h3h3h3h3h3h3h3h\_Br0h\_ini\_masih\_belum\_apa\_apa} 17](#_8fmwsd6rpirh)

[Mr.Simple 17](#_xabsjjipn4ax)

[Flag: UNITY2023{H3h3\_S3d3rh4n4\_4J4} 18](#_kekhqmt6q38)

[Acak-Acakan\_D4hhhh 18](#_hzrchpkuc6l0)

[Flag: UNITY2023{H3h3\_D1K!t\_B12ut3\_B4n9} 18](#_j8mvam6xogyq)

[**OSINT 19**](#_855p3vmv29gn)

[Arts\_Of\_Angel 19](#_272aaiq5ksf1)

[Flag : UNITY2023{Michelangelo\_1501} 20](#_1yd27chfah80)

[FindIT!!!!!!! 20](#_vtqgbty7vx6)

[Flag: UNITY2023{Geopark\_Ciletuh} 21](#_ng0ynut6b4xg)

[YouSee1000 22](#_n4qc1fl7xpzy)

[Flag: UNITY2023{Y0U\_G07\_M3\_B1200} 24](#_1gez1jrcudaj)

[**Forensic 25**](#_m3snwxpu9te)

[Meowww 25](#_r98dsavdh831)

[Flag : UNITY2023{S4Nt4y\_DuLu\_G4\_SiEEE} 26](#_78n9sj3mvef7)

[CPNS 26](#_3s3s93tb0r7f)

[Flag : UNITY2023{5U8M1T\_Y0UR\_FL4G} 27](#_u6hll635jyjk)

[ES 27](#_fybii5sam9yc)

[Flag: UNITY2023{Th1s\_1s\_N07\_F149} 28](#_6qjrf4g2wm7)

[Ngump3t 28](#_4qqnz5pz0azt)

[Flag: UNITY2023{D4p3t\_Y44444\_B4n9999\_99\_93m!n9} 29](#_55ablcf7cnc5)

[**Misc 30**](#_ey8zwsr4q0gy)

[Squids 30](#_38urcrj5ehse)

[Flag: ????? 32](#_ie4rj5z1zqcw)

[**Free 33**](#_4yi2mm2q8j2q)

[Jogjess 33](#_cqearyqoqv16)

[Flag: UNITY2023{FR33\_FLAG\_S1r} 33](#_e722jqp1dk03)

# 

# Crypto

| HEXagon 100  Gatau Ah Brodi Gelap :v  554e495459323032337b593468685f4734  6d70346e395f593434345f4d345331685f333473795f6c30307d  FlagFormat : UNITY2023{}  Author : Chroniclesss |
| --- |

Diberikan sebuah strings random yang jika soalnya dibaca merupakan encoding HEX. Kami pun mencoba dengan cyberchef untuk mendecodenya lalu didapat flag

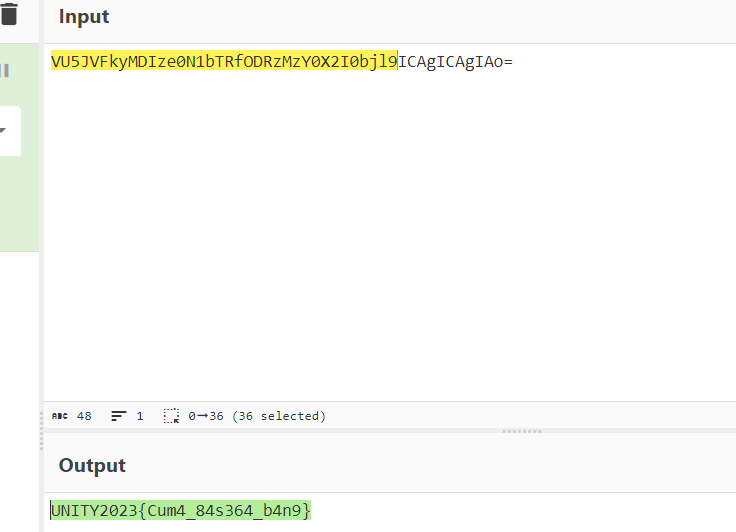
# 

Diberikan hex, decode dan flag diperoleh.

### Flag: UNITY2023{Y4hh\_G4mp4n9\_Y444\_M4S1h\_34sy\_l00}

# 

| Semangat64 100  \*\*\*jalan jalan ke jakarta  pulangnya membeli tahu  ini cuma angka biasa  yakali ente ga tahu\*\*\*  VU5JVFkyMDIze0N1bTRfODRzMzY0X2I0bjl9ICAgICAgIAo=  FlagFormat : UNITY2023{}  Author : Chroniclesss |
| --- |



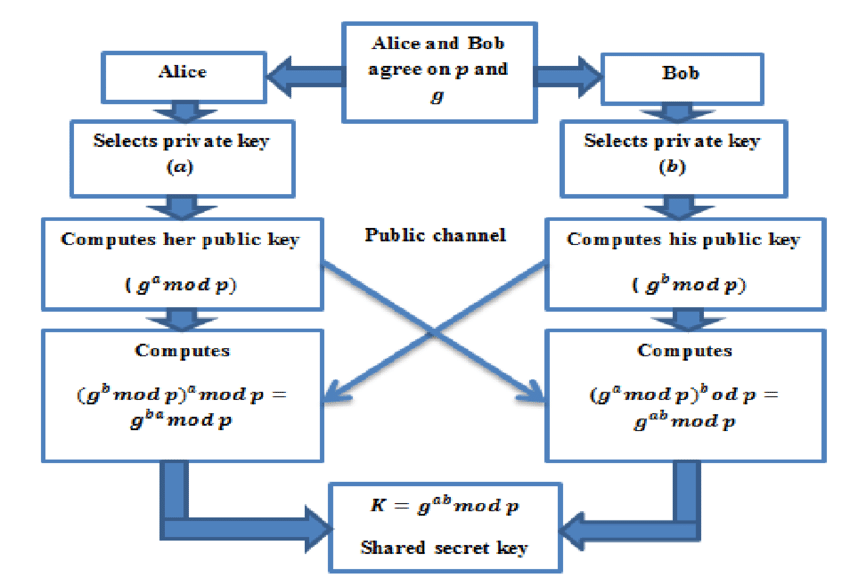
Diberikan base 64, decode dan flag diperoleh.

### Flag: UNITY2023{Cum4\_84s364\_b4n9}

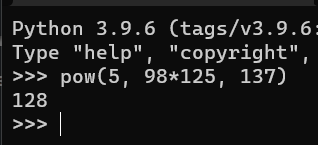
# 

| DiffieDikky\_Broo 500  carilah shared key nya brohhh  public key 1 P = 137 g = 5 a = 98  public key 2 p = 137 g = 5 b = 125  FormatFlag : UNITY2023{\*\*}  Author : Chronicless |
| --- |

Diberikan sebuah diffie hellman problem, kita diberikan public key, generator, serta secret key dari masing masing pihak. Hanya tinggal dihitung menggunakan rumus



Shared key = g\*\*(a\*b) mod p = 128



Ini merupakan jawaban yang seharusnya, namun kami jawaban terus incorrect.

Selain itu, kami juga menebak bahwa a dan b yang diberikan mungkin adalah bilangan yang sudah dipangkatkan pada generator (g\*\*a dan g\*\*b), maka kami coba melakukan brute force dengan script berikut:

p = 137

g = 5

a = 98

b = 125

for i in range(137):

if pow(g, i, p) == a:

x = i

for i in range(137):

if pow(g, i, p)==b:

y = i

print(pow(a, y, p))

print(pow(b, x, p))

print(pow(g, x\*y, p))

Diperoleh jawaban 2, tetapi itu juga salah.

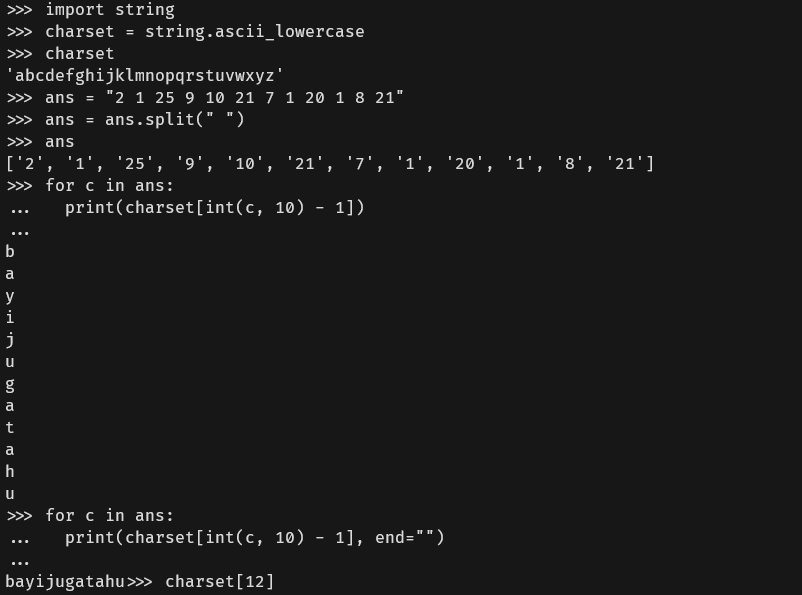
Kami menebak mungkin yang dimaksud soal, karena shared key jadi kita perlu membagi dari jawaban yang didapat (128/2 = 64). Sehingga didapat flag nya

### Flag: UNITY2023{64}

# 

| TTSBukanTPS 100  jadi sherlock holmes bentar dahh pecahin ya bwang (2 1 25 9 10 21 7 1 20 1 8 21)  FLagFormat : UNITY2023{}  Author : Chroniclesss |
| --- |

Diberikan sebuah sequence random yaitu 2 1 25 9 10 21 7 1 20 1 8 21. Kami pun bingung namun kami mengira itu merupakan sebuah representasi ascii dari character sehingga kami mencoba untuk men decode nya

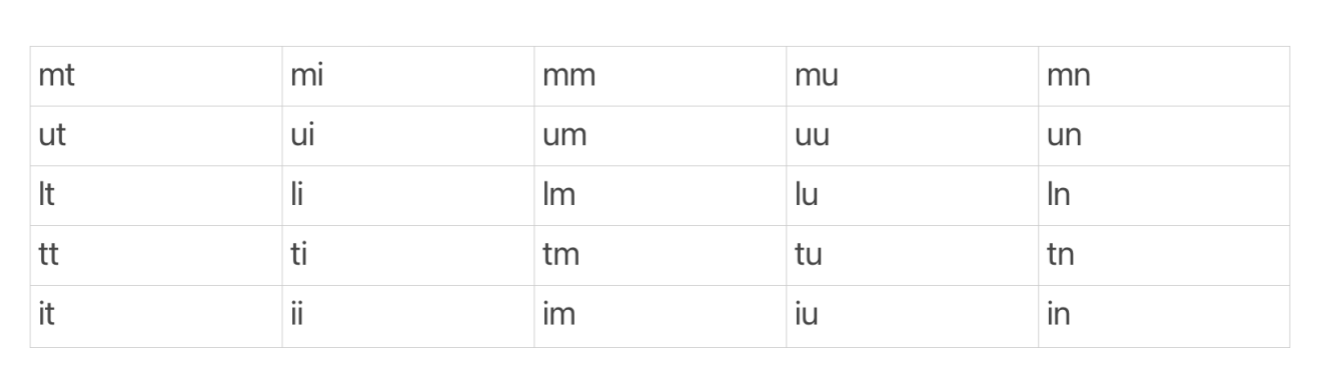


### Flag: UNITY2023{bayijugatahu}:

# 

| Coklat 559  TTS Itu Apa PAkk ?? Siapp!!! TEKA-TEKI-SULID  key 1 : MULTI key 2 : TIMUN  monggo : UNITY2023{LN TI UT MN\_TI IU MN\_UT MT MN\_UT MT LN MT TM UI}  FlagFormat : UNITY2023{}  Author : Chroniclesss |
| --- |

Pertama, kami mencurigai playfair cipher, tetapi setelah mencoba, tidak ada hasil yang ditemukan. Kemudian, setelah ngedukun berjam-jam, kami menyadari bahwa karakter di ciphertext semuanya ada dari kombinasi MULTI dan TIMUN. Kemudian, kami membuat tabel yang playfair-like.



Pertama, kami mensubtitusi tiap bigram dengan karakter a-y, dengan urutan a-e pada baris pertama, f-j pada baris kedua, dan seterusnya, tetapi tidak mendapatkan hasil. Kemudian, beberapa saat kemudian, kami mendapat pencerahan setelah mendengarkan lagu dukun berikut <https://www.youtube.com/watch?v=0T7eMctuJLQ>, dan mejejerkan karakter dengan urutan a-e, dst pada kolom, dan mendapatkan flag.

P.S. probset tidak wibu juga kah? :D

### 

### Flag: UNITY2023{WIBU\_ITU\_BAU\_BAWANG}

# 

| OnTheWayPak 1000  1x cukup gk kyk kb2 ini cuma 1  Teks Terenkripsi : UFJOXJGWSH key : EKMGAWZULN  FlagFormat : UNITY2023{} \*No spacing Trade With \_ |
| --- |

Berdasarkan <https://en.wikipedia.org/wiki/One-time_pad>, terdapat dua cara umum yang digunakan untuk enkripsi one time pad karakter ascii, yaitu cara biasa yaitu xor nilai ascii setiap karakter dengan key, dan menambahkan plaintext dengan key. Oleh karena itu, hanya ada dua cara dekripsi, yaitu mengurangkan ciphertext dengan key, atau melakukan xor.

Berikut solver yang digunakan:

key = "EKMGAWZULN"

text = "UFJOXJGWSH"

chars = [chr(ord("A") + i) for i in range(26)]

for a,b in zip(key, text):

posa = chars.index(a)

posb = chars.index(b)

l = (posb-posa) % 26

print(chars[l], end="")

Setelah mencoba keduanya, flag tidak didapatkan. Kekuatan dukun kami kurang kuat untuk menebak OTP yang digunakan probset seperti apa.

### 

### Flag: ?????

# 

| SnackCry 1000  Dekrypt brohhh  public key  n = 683 m = 497 a = [137, 247, 362, 400, 162, 84, 329, 138] ciphertext = 148  FormatFlag : UNITY2023{\*\*\*\*\*\*\*\_\*\*\*\*\*\*\*\*} \*Uppercase  Author : Chronicless |
| --- |

Enkripsi nampaknya dilakukan menggunakan knapsack cryptosystem. Karena nilai a yang digunakan sangat kecil, kita dapat langsung melakukan bruteforce untuk mencari plaintext awal. Berikut solver yang digunakan:

def powerset(s):

x = len(s)

for i in range(1 << x):

yield [s[j] for j in range(x) if (i & (1 << j))]

n = 683

m = 497

mi = pow(m, -1, n)

a = [137, 247, 362, 400, 162, 84, 329, 138]

cipher = 148

for c in powerset(a):

if (sum(c) % n) == cipher:

print(c)

*# [247, 362, 84, 138]*

*# 01100101*

Kami memperoleh hasil tepat satu subset yang memenuhi, yaitu [237, 362, 84, 138], atau 01100101 = ‘e’. Namun, setelah mensubmit jawaban tersebut, ternyata jawaban tidak benar.

Sekali lagi, teknologi perdukunan kami kurang kuat untuk menebak format plaintext yang diinginkan probset sebenarnya bagaimana.

### Flag: ?????

# 

| GAMAliel 1000  cari flag nya bang :)  public key p = 101 g = 7 y = 23  cipher  a = 11 b = 87  FormatFlag : UNITY2023{\_\*\*\*\*\*} \*uppercase  Author : Chroniclesss |
| --- |

Simple el gamal, private key tinggal di-brute force, dan dekripsi dapat dilakukan. Berikut solver yang digunakan:

p = 101

g = 7

y = 23

a = 11

b = 87

for i in range(p):

if pow(g, i, p) == y:

x = i

break

print(x)

s = pow(a, x, p)

m = pow(s, -1, p) \* b

m = m % p

print(m)

Didapatkan message 47, dan setelah kami coba mensubmitnya, ternyata jawaban salah. Dan lagi-lagi, teori dan keterampilan perdukunan kami kurang kuat untuk menerawang format message yang diinginkan seperti apa.

### Flag: ?????

### 

### 

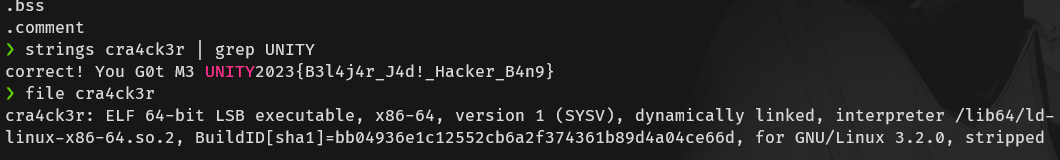
# **Rev**

NOTE: Sepertinya penyelesaian semua soal rev merupakan unintended, kayaknya probset lupa nge hide flag nya.

| Cr4ck312 **100**  Jadi Hengkel Bang :v  FormatFlag : UNITY2023{}  Author : Chronicless |
| --- |

### 

Diberikan sebuah file executables 64 bit. Hal yang pertama kami lakukan ialah mengecek executables dengan command strings yaitu strings <nama file> | grep UNITY2023 untuk mencarinya. Dan benar saja ternyata didapat flag pada executables.

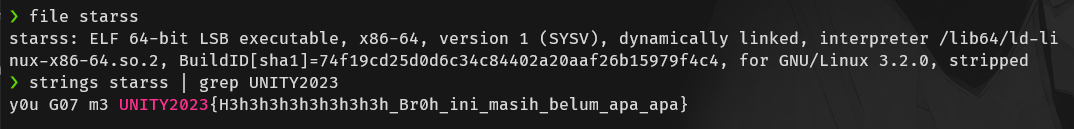


### Flag: UNITY2023{B3l4j4r\_J4d!\_Hacker\_B4n9}

| STARlight **100**  ATTACKKK BANGGGGGGG:v  FlagFormat : UNITY2023{}  Author : Chronicless |
| --- |

### 

Diberikan sebuah file executables 64 bit. Hal yang pertama kami lakukan ialah mengecek executables dengan command strings yaitu strings <nama file> | grep UNITY2023 untuk mencarinya. Dan benar saja ternyata didapat flag pada executables.

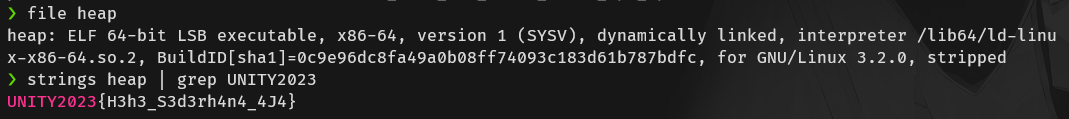


### Flag UNITY2023{H3h3h3h3h3h3h3h3h\_Br0h\_ini\_masih\_belum\_apa\_apa}

| Mr.Simple **100**  Simple is working broh if you can :v  FlagFormat : UNITY2023{}  Author : Chroniclesss |
| --- |

### 

Diberikan sebuah file executables 64 bit. Hal yang pertama kami lakukan ialah mengecek executables dengan command strings yaitu strings <nama file> | grep UNITY2023 untuk mencarinya. Dan benar saja ternyata didapat flag pada executables.



### Flag: UNITY2023{H3h3\_S3d3rh4n4\_4J4}

| Acak-Acakan\_D4hhhh **100**  Acak Aja Bang Kyk Main SUdoku  FlagFormat : UNITY2023{}  Author : Chroniclesss |
| --- |

Diberikan sebuah file executables 64 bit. Hal yang pertama kami lakukan ialah mengecek executables dengan command strings yaitu strings <nama file> | grep UNITY2023 untuk mencarinya. Dan benar saja ternyata didapat flag pada executables.



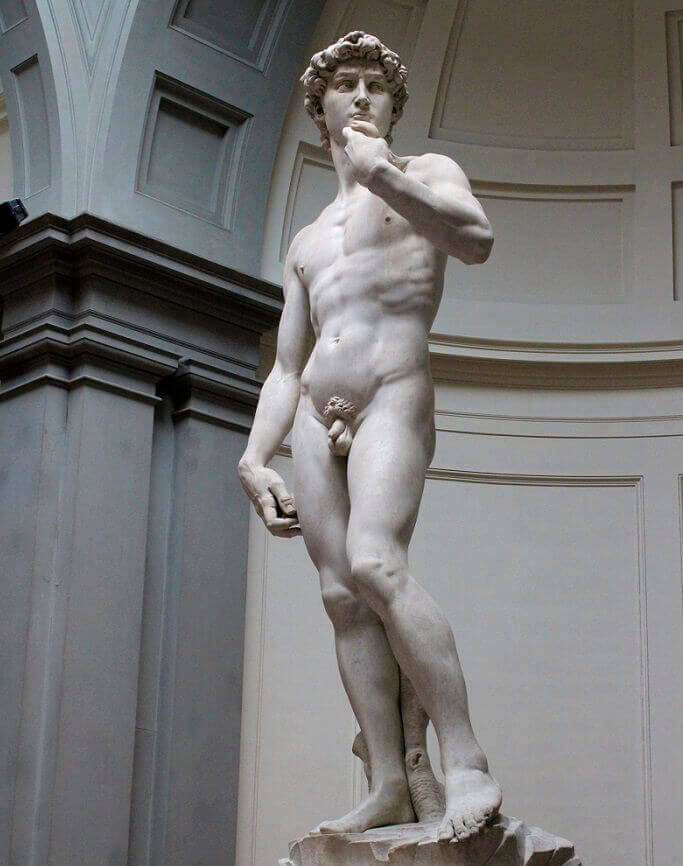
### Flag: UNITY2023{H3h3\_D1K!t\_B12ut3\_B4n9}

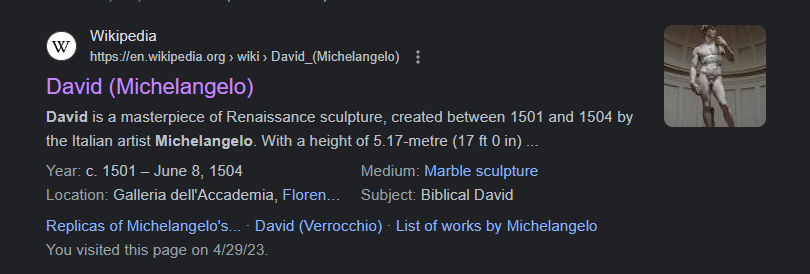
# 

# OSINT

| Arts\_Of\_Angel **100**  who's create that ? i think this statue full of art  FormatFlag : UNITY2023{Name\_Year}  Author : Chroniclesss |
| --- |

Diberikan sebuah foto patung. Kami mengetahui bahwa patung tersebut adalah patung David karya Michelangelo. A quick google search untuk mendapatkan tahun patung tersebut dibuat.





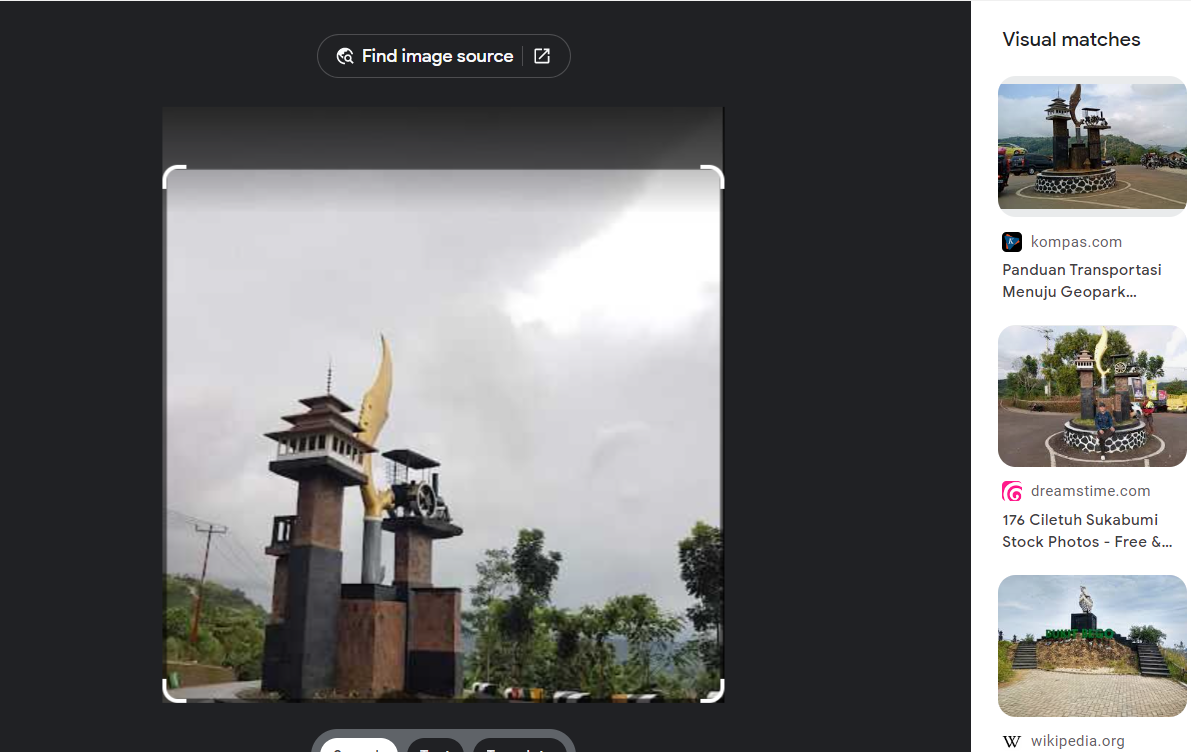
### Flag : UNITY2023{Michelangelo\_1501}

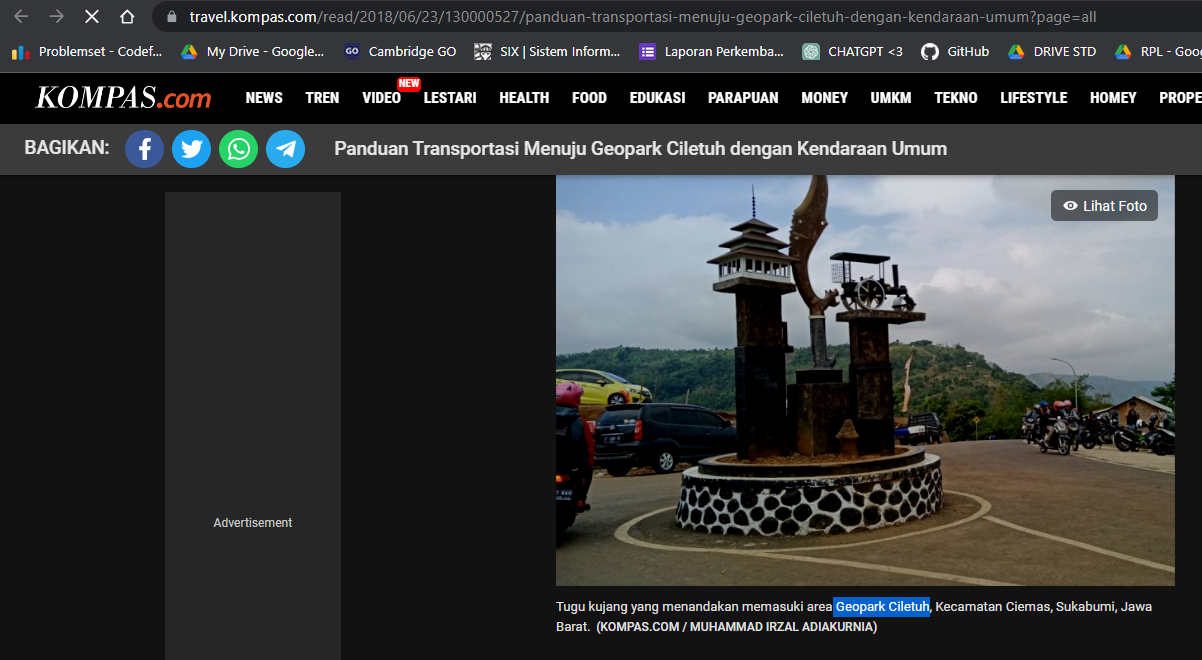
# 

| FindIT!!!!!!! **100**  eday i can go to newest beach with my motorcycleteam and the leader give we some photo. and he said "You Go to this place and find the beach in near here" i don't know where this is, can you help me find the place??  FlagFormat : UNITY2023{Firstname\_SecondName}  Author : Chroniclesss |
| --- |

Diberikan sebuah foto tugu. Kami melakukan google image reverse search dan mendapatkan lokasi foto tersebut.

\*Awalnya kami kebingungan karena kami mengira yang ditanyakan adalah pantai yang berada dekat tempat tersebut :”/



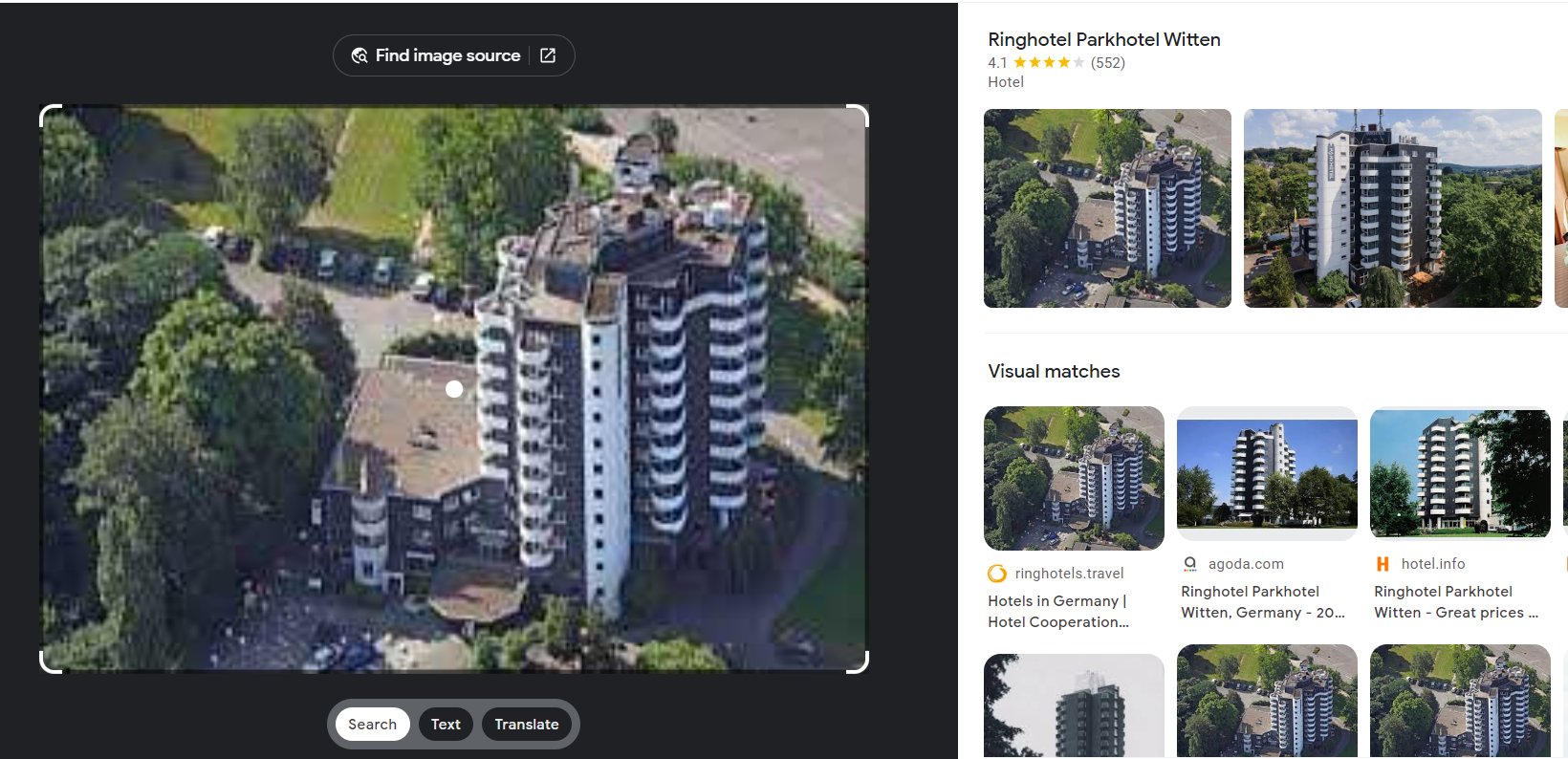


### Flag: UNITY2023{Geopark\_Ciletuh}

# 

| YouSee1000 **100**  somehow, somewhere, something in this picture has a flag, my GF not tell me where is this, help me to find it!!!  FlagFormat : UNITY2023{}  Author : Chronicless |
| --- |

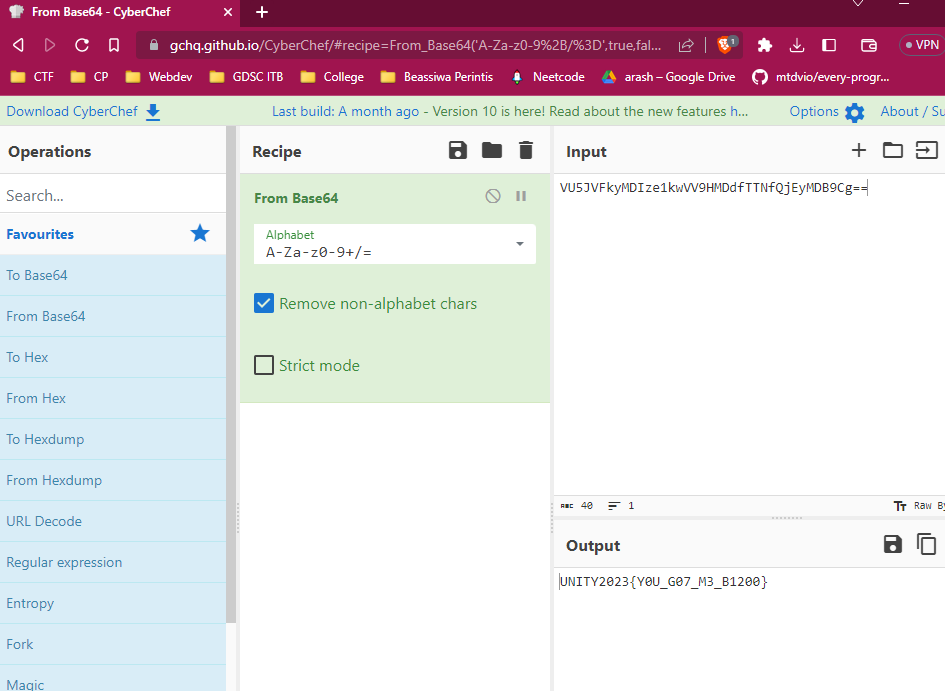
Diberikan sebuah foto bangunan tinggi. Kami melakukan google image reverse search dan mendapatkan bahwa bangunan tersebut adalah sebuah hotel.



Kami berusaha mencari di google map dan sekitarnya, kami pun menemukan sebuah galeri bernama Saalbau Witten yang jika dilihat pada reivews terdapat komentar authornya



Kami pun langsung mencoba untuk decode flag tersebut dengan base64 pada cyberchef sehingga didapat flag



### Flag: UNITY2023{Y0U\_G07\_M3\_B1200}

# 

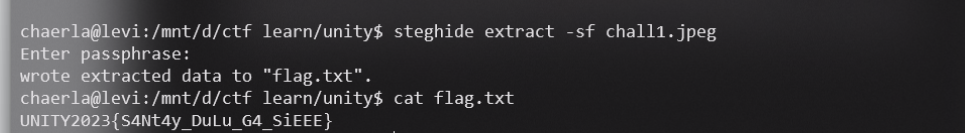
# Forensic

| Meowww 100  Didalam Khong Guan Ada Rengginangggggggggggg Selamat Lebaran  UNITY2023{}  Author : AC3 |
| --- |

Diberikan sebuah foto kucing:



Kami menggunakan stegsolve dengan passphrase kosong.

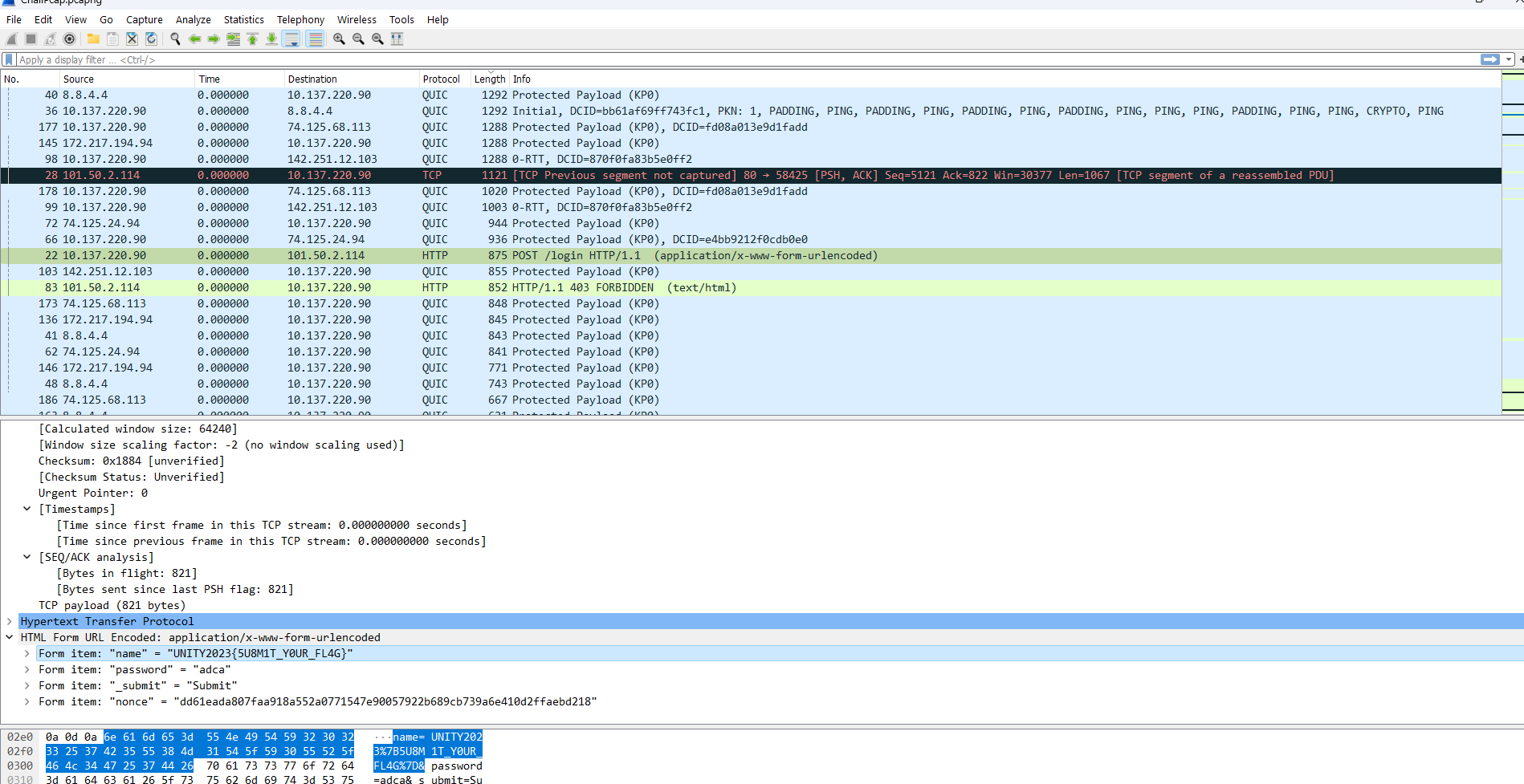


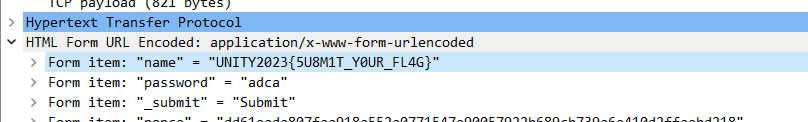
### Flag : UNITY2023{S4Nt4y\_DuLu\_G4\_SiEEE}

# 

| CPNS 100  Hiu + Buaya = Surabaya "Kepalanya aja Kok :)"  UNITY2023{}  Author : AC3 |
| --- |

Diberikan sebuah file ChallPcap.pcapng. Kami kemudian menganalisis file tersebut dengan wireshark. Kami melakukan sorting berdasarkan length dan menemukan sebuah POST request yang menarik pada endpoint /login. Kami mengecek request tersebut dan mendapatkan flag.



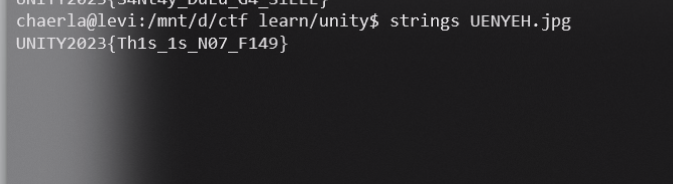


### Flag : UNITY2023{5U8M1T\_Y0UR\_FL4G}

# 

| ES 100  BRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR Dinginnnn  FormatFlag : UNITY2023{}  Author : Chronicless |
| --- |

Diberikan sebuah foto UENYEH.jpg. Kami melakukan commands `strings` pada file tersebut dan mendapatkan flag.



### Flag: UNITY2023{Th1s\_1s\_N07\_F149}

### 

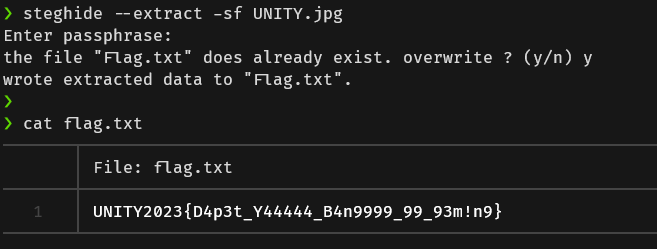
# 

| Ngump3t 100  Ada Udang Dibalik Batu Batu nya Hilang BNN Datang  FormatFlag : UNITY2023{}  Author : Chroniclesss |
| --- |

Diberikan sebuah file jpg UNITY.jpg



Awalnya kami bingung untuk menyelesaikan masalah ini karena kami tidak mengerti clue yang diberikan. Namun kami mencoba untuk mengextract dengan menggunakan steghide lalu didapatlah sebuah file flag.txt yang berisikan flag



### Flag: UNITY2023{D4p3t\_Y44444\_B4n9999\_99\_93m!n9}

# 

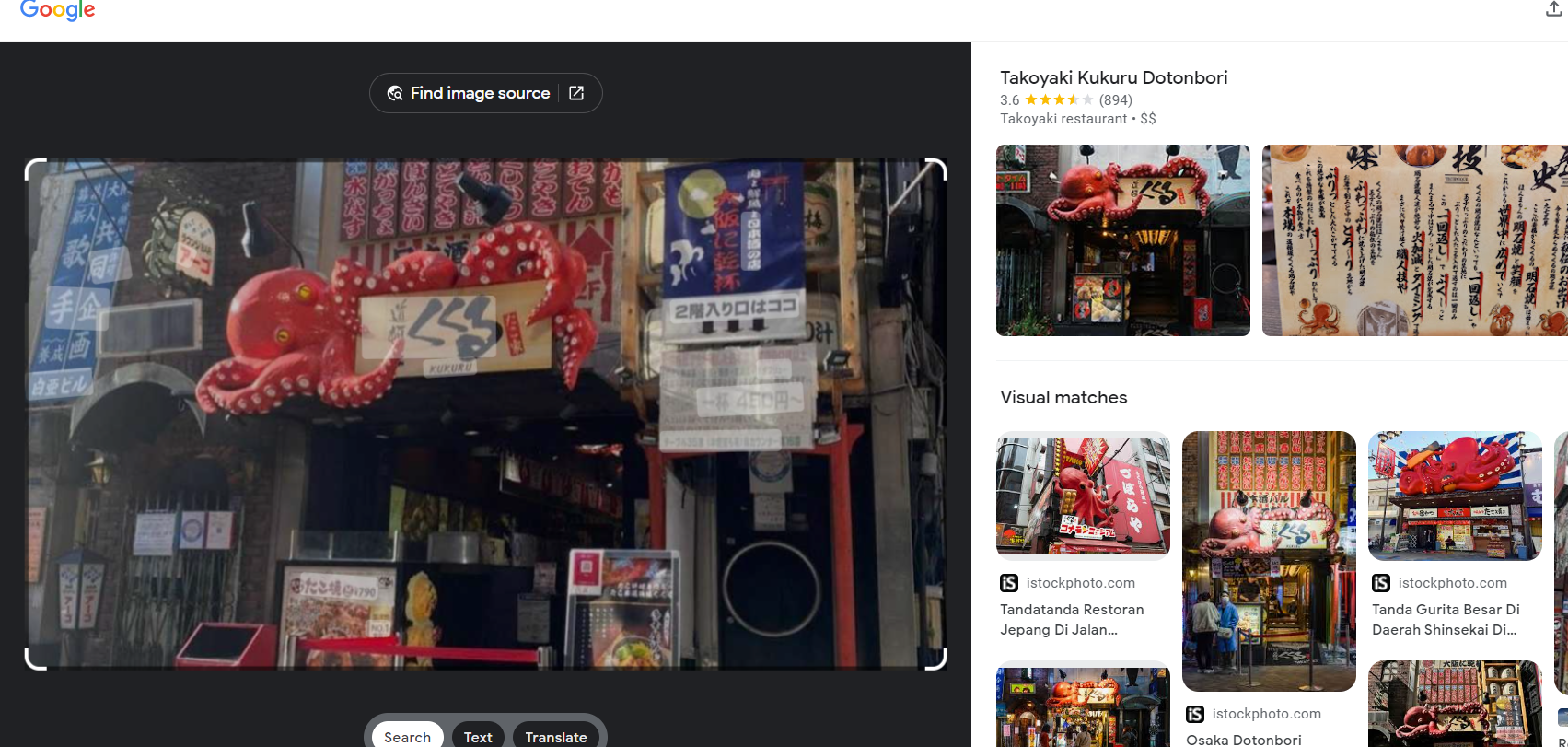
# Misc

| Squids **744**  suatu hari aku travelling bersama sodaraku ke sebuah negara yang bagus sekali saat aku jalan jalan aku tersesat dan tidak tau sedang berada dimana. kerika aku hubungi 911 aku dimintai postal code dan nama distrik. bisakah bantu mencari tempat aku berdiri sekarang??  FormatFlag : UNITY2023{Postal\_Distrik}  Author : Chroniclesss |
| --- |

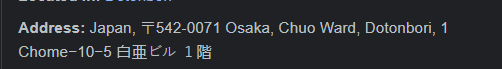
Diberikan sebuah file gurita.jpeg



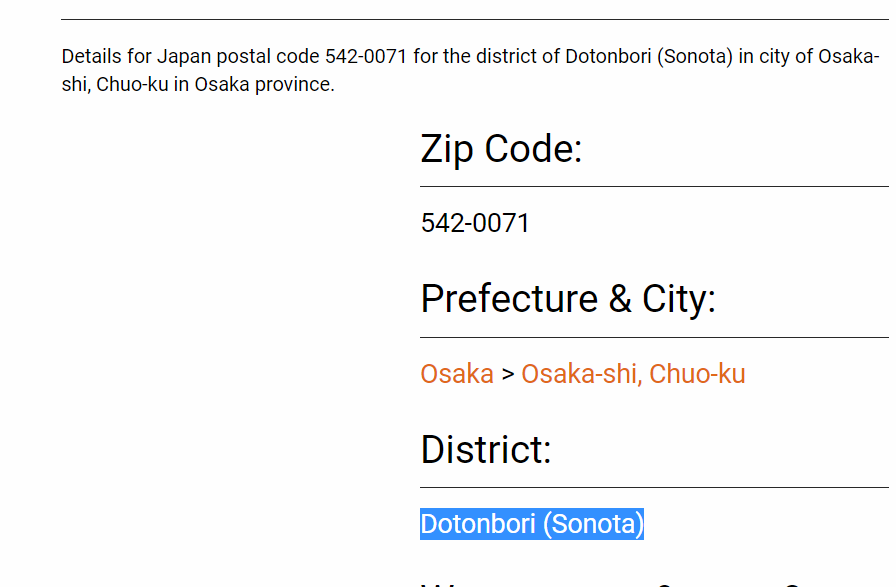
Kami melakukan google reverse image search dan mendapatkan alamat lokasi tersebut.

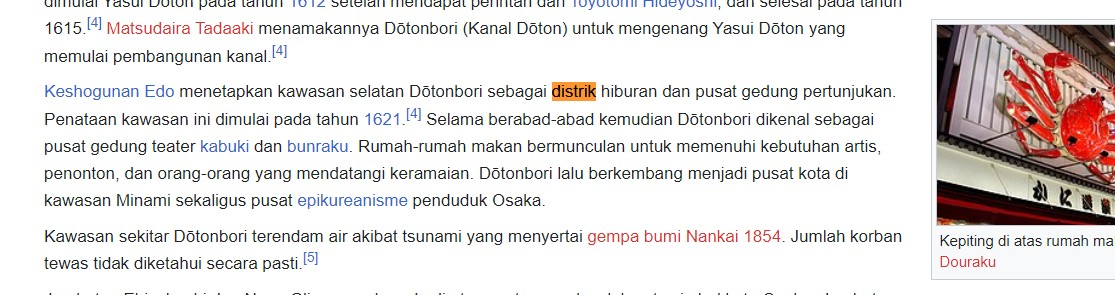


Alamat:



Awalnya kami mencoba beberapa kali dengan memasukkan postal code 542-0071, setelah bertanya ke admin, katanya postal codenya seharusnya tidak menggunakan dash.





Kami mencoba dengan UNITY2023{5420071\_Dotonburi} tetapi incorrect.

Lalu, kami bertanya pada admin dan diberitahu bahwa Dotonburi bukan district. Jadi kami mencari distrik tempat Chuo berada dan mendapatkan Minami, tetapi masih incorrect. Jadi, kami tidak tahu salahnya dimana :”DDD (agak disayangkan karena ini banyak solve tetapi poinnya sgt gede??1/1)

### Flag: ?????

# Free

| Jogjess **100** |
| --- |

Ini soal yang sangat dukun min. Tapi dengan kekuatan ilmu ghoib, kami berpikir untuk mengecek robots.txt pada web challenge.

NAMUN

KAMI

LUPA

SUBMIT

HEHE

:/

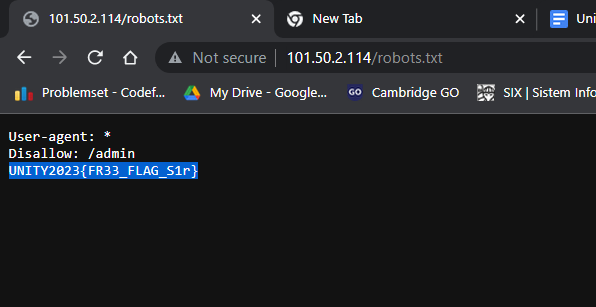
:/

:D

:D

KEBURU TUTUP

WKAOWKAOKWOAKWOKWOKWOKWWKAOWKAOKWOAKWOKWOKWOKWWKAOWKAOKWOAKWOKWOKWOKWWKAOWKAOKWOAKWOKWOKWOKWWKAOWKAOKWOAKWOKWOKWOKWWKAOWKAOKWOAKWOKWOKWOKWWKAOWKAOKWOAKWOKWOKWOKWWKAOWKAOKWOAKWOKWOKWOKWWKAOWKAOKWOAKWOKWOKWOKWWKAOWKAOKWOAKWOKWOKWOKWWKAOWKAOKWOAKWOKWOKWOKW GWS



### Flag: UNITY2023{FR33\_FLAG\_S1r}

### 