

Hacklabs.id Mini Weekly CTF 2.0



Problems :

Keyless v1 (Crypto) – 50 pts

Designer (Misc.) – 50 pts

Broken Mirror (Crypto) – 50 pts

Ancient Scrolls (Misc.) – 50 pts

Keyless v2 (Crypto) – 75 pts

Catch The Ride (OSINT) – 75 pts

Pokemon Go! (Misc.) – 75 pts

How Hot It Is (OSINT) – 75 pts

Money Heist v2 (OSINT) – 75 pts

Keyless v1 (Crypto)



Seperti biasanya pada hacklabs, saya harus mendownload file dari link yang tertulis di caption post tersebut, lalu setelah mengecek file yang ada, saya melihat 2 file, 1 text file dan 1 python file, pertama saya melihat apa isi dari text file tersebut

```
Desc
```

```
-----  
Cryptography is very easy if there's online tools indeed :v.
```

```
But can you crack this one ? >:)
```

```
- Julius Caesar
```

```
Hint #1: No hint. Thx.
```

Dari deskripsi yang diberikan (karna tidak ada hint :p) kita dapat memastikan itu merupakan Caesar, dan dapat menggunakan online tools, tapi karna saya sudah diberikan file pythonnya, saya hanya perlu merubah sedikit saja

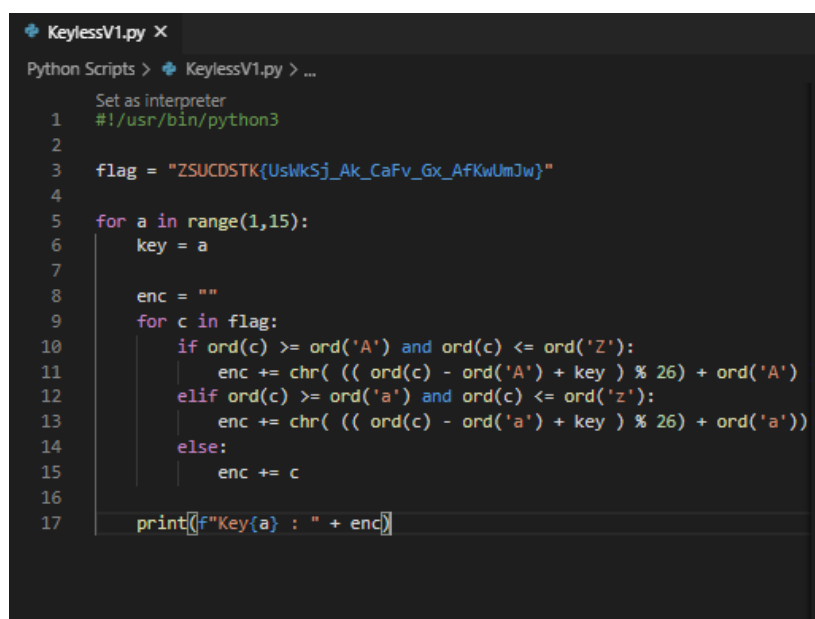
```
#!/usr/bin/python3

flag = "REDACTED"
key = "REDACTED"

enc = ""
for c in flag:
    if ord(c) >= ord('A') and ord(c) <= ord('Z'):
        enc += chr( (( ord(c) - ord('A') + key ) % 26) + ord('A') )
    elif ord(c) >= ord('a') and ord(c) <= ord('z'):
        enc += chr( (( ord(c) - ord('a') + key ) % 26) + ord('a'))
    else:
        enc += c

print(enc)
#ZSUCDSTK{UsWkSj_Ak_CaFv_Gx_AfKwUmJw}
```

Dari code di atas, dapat dilihat bahwa menggunakan fungsi “ord()” yang merubah parameter input menjadi unicode, kemudian dari code di atas saya merubah jadi seperti berikut



```
KeylessV1.py X
Python Scripts > KeylessV1.py > ...
Set as Interpreter
1  #!/usr/bin/python3
2
3  flag = "ZSUCDSTK{UsWkSj_Ak_CaFv_Gx_AfKwUmJw}"
4
5  for a in range(1,15):
6      key = a
7
8      enc = ""
9      for c in flag:
10         if ord(c) >= ord('A') and ord(c) <= ord('Z'):
11             enc += chr( (( ord(c) - ord('A') + key ) % 26) + ord('A') )
12         elif ord(c) >= ord('a') and ord(c) <= ord('z'):
13             enc += chr( (( ord(c) - ord('a') + key ) % 26) + ord('a'))
14         else:
15             enc += c
16
17     print(f"Key{a} : " + enc)
```

Kemudian dengan menjalankan python di atas, saya mendapatkan hasil flagnya.

```
Key1 : ATVDETUL{VtXlTk_Bl_DbGw_Hy_BgLxVnKx}
Key2 : BUWEFUVm{WuYmUl_Cm_EcHx_Iz_ChMyWoLy}
Key3 : CVXFGVwN{XvZnVm_Dn_FdIy_Ja_DiNzXpMz}
Key4 : DwYGHwXO{YwAoWn_Eo_GeJz_Kb_EjOaYqNa}
Key5 : EXZHIXYP{ZxBpXo_Fp_HfKa_Lc_FkPbZrOb}
Key6 : FYAIJYZQ{AyCqYp_Gq_IgLb_Md_GlQcAsPc}
Key7 : GZBJKZAR{BzDrZq_Hr_JhMc_Ne_HmRdBtQd}
Key8 : HACKLABS{CaEsAr_Is_KiNd_Of_InSeCuRe}
Key9 : IBDLMBCT{DbFtBs_Jt_LjOe_Pg_JoTfDvSf}
Key10 : JCEMNCDU{EcGuCt_Ku_MkPf_Qh_KpUgEwTg}
Key11 : KDFNODEV{FdHvDu_Lv_NlQg_Ri_LqVhFxUh}
Key12 : LEGOPEFW{GeIwEv_Mw_OmRh_Sj_MrWiGyVi}
Key13 : MFHPQFGX{HfJxFw_Nx_PnSi_Tk_NsXjHzWj}
Key14 : NGIQRGHY{IgKyGx_Oy_QoTj_Ul_OtYkIaXk}
```

HACKLABS{CaEsAr_Is_KiNd_Of_InSeCuRe}

Designer (Misc.) – 50 pts



Challenge di awali seperti biasa, harus membuka drive dari hacklabs dan di sana saya melihat 2 file saja , 1 file text dan 1 lagi file tanpa extension. Berdasarkan deskripsi dari challenge ini, hanya perlu merubah extension dari file tersebut, tertulis seperti di bawah :

Desc

Archie is an online 'architect'. He has mastered CorelDraw, Photoshop, and even he studied GNU Plot.

One day, he made a design in online sites but he forgot the extension of the file, so he doesn't know what type of the file is it with a lot of coordinates within. Can you help Archie to recover the image design?

All the coordinates are in (X , Y) with unknown G-likely-array (?) .

Notes: This challenge is not "cyber-based" at all, you just need to find the matched extensions and the coordinates PLOT only :).

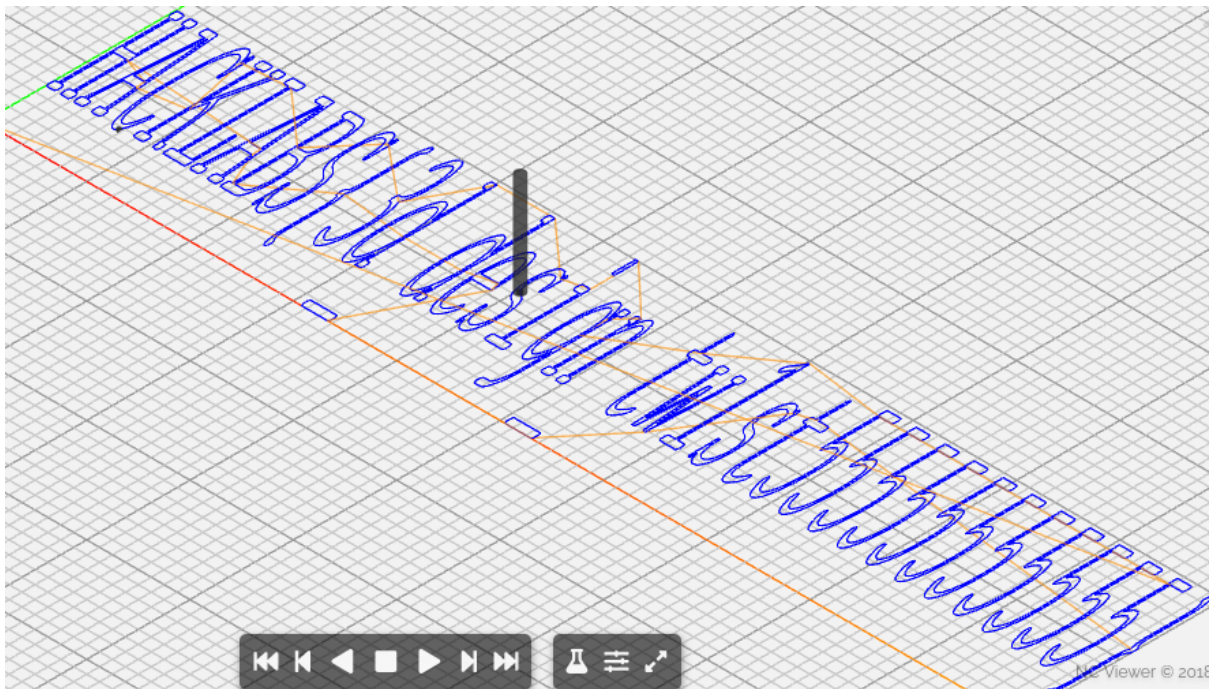
Setelah melakukan diskusi dengan salah seorang player, karna ini merupakan challenge mencari extension artinya berhubungan dengan file header signature, sehingga dengan menggunakan HxD kita dapat melihat file signature dari file tersebut.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	47	32	31	0D	0A	47	39	30	0D	0A	47	30	30	20	58	39	G21..G90..G00 X9
00000010	39	2E	36	34	31	33	37	20	59	31	31	2E	34	31	31	36	9.64137 Y11.4116
00000020	32	0D	0A	4D	31	30	30	32	0D	0A	47	30	31	20	58	39	2..M1002..G01 X9
00000030	39	2E	35	37	34	39	36	20	59	31	31	2E	36	37	38	36	9.57496 Y11.6786
00000040	38	0D	0A	47	30	31	20	58	39	39	2E	35	32	35	30	31	8..G01 X99.52501

Setelah mendapatkan hex nya serta decoded text yang ada, saya melanjutkan pencarian dengan menggunakan keyword “G21 G90 G00 file header signature” selain menemukan daftar dari extension yang biasa digunakan (pada akhirnya tidak digunakan pada challenge ini) saya menemukan suatu extension bernama .gcode berdasarkan dari artikel di bawah ini :

inventables.zendesk.com › en-us › articles › 36001264...
Easel G-code Spec – Inventables
Aug 28, 2020 — 12/18/2015 : Add note to always include unit system (G20/G21), Published. This document describes the format of g-code files that can be sent by Easel. The range of ... G0, G1, G4, G17, G20, G21, G40, G54, G61, G90, G94. M0, M1 ... All settings commands with only one option (G54, G17, G90, etc.) are the ...
Missing: ~~signature~~ | Must include: **signature**

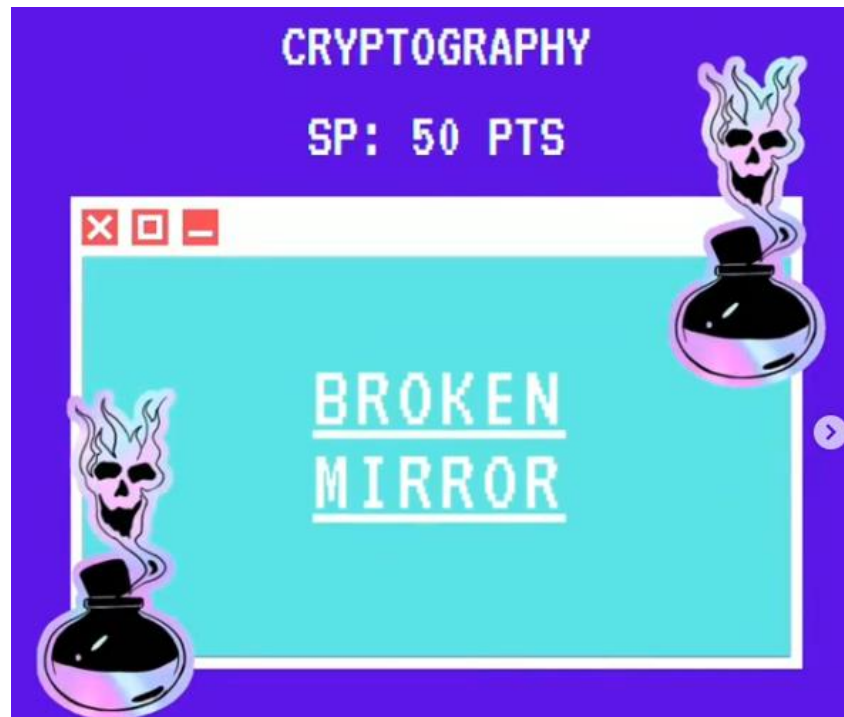
Kemudian saya merename file tersebut menjadi “designer.gcode” dan setelah mengecek gcode itu untuk apa, saya menggunakan [online tools](#) untuk mengecek isi dari file tersebut.



Gambar di atas saya berhasil dapatkan setelah menggunakan tools tersebut.

HACKLABS{3d_design_twist555555555555}

Broken Mirror (Crypto)



Pertama saya melihat terlebih dahulu apa yang diberikan di gdrive hacklabs dan menemukan file berisikan deskripsi sebagai berikut :

Desc

Snow White is actually alive until now. She is disguised as the Cyber Army PENTAGON in U.S. One day, her commander, Lucille Van Verne, gave her a very simple task. It's an encrypted text so that she has to decrypt it as fast as she could.

Can you help her?

Hint #1: Snow White has a loyal assistant and he's a chef :).
Don't believe me?

Hint #2: The commander loves to use reversible encryption. Be careful!
You need to look from different angles.

Dari clue yang diberikan saya mengetahui bahwa challenge ini bisa disolve menggunakan cyberchef, namun arti dari hint ke 2 saya masih tidak mengetahuinya. Selain itu dari nama challengenya, saya dapat mengetahui bahwa ini merupakan reverse string karna sifat mirror adalah membalikkan yang ada di depannya.

```
PU1ETnpnek0wTVRNe1F6TXpNRE4ySXpNMFl6TXpRek14TUROek16TTFNek16Y2pOeU1qTjJRek0yTVRPemN6TXlNek56SXpNMllqTnpjek15TVROMl16TTJZRE56WXpN
NU16TnpJek0zTWpNellqTjJNek56SXpNMVlqTnp2ak4yTWpOMlV6TTFZak56Y3pNME1qTnpnek0yTVROelVqTjJNek56Y3pNMklUTXp2ak56TWpOMkl6TTFZak56Y3pN
M01qTnpnek0yWpOelVqTjJNak56a3pNM016TXpVak4yTXpOelF6TTJUNRE96WXpNMU1UTjJZek16TVRNeK16TXpNek16TXpNek16TnpJek4wTWpOelV6TTNNek16Y3pN
ME1UTjJZek0yTURPek16TTBNek56Z3pNMllqTnpjek15TVROMl16TTJZak56WXpNMklUTjJZek0zTUROel16TTRNak56VXpNMllETnpVak4yTWpOekV6TTJZek16WwPo
ek16TTJZek0zWURO
```

Foto di atas adalah isi dari challenge tersebut, kemudian saya membuka cyber chef dan memasukkannya kesana.

```
Input
length: 528
lines: 1
PU1ETnpnek0wTVRNe1F6TXpNRE4ySXpNMF16TXpRek14TUROek16TTFNek16Y2pOeU1qTjJRek0yTVRPemN6
TX1Nek56SXpNM1lqTnpjek15TVROM1l6TTJZRE56WXPnMU16TnpJek0zTWpNe1lqTjJNek56SXpNMV1qTnpZ
ak4yTwpOM1V6TTTFZak56Y3pNME1qTnpnek0yTVROe1VqTjJNek56Y3pNMk1UTXpZak56TWpOMk16TTTFZak56
Y3pNM01qTnpnek0yWwPoe1VqTjJNak56a3pNM016TXpVak4yTXpOe1F6TTJNRE96WXPnMU1UTjJZek16TVRN
ek16TXpNek16TXpNek16TnpJak4wTwPoe1V6TTNnek16Y3pNME1UTjJZek0yTURPek16TTBNek56Z3pNM1lq
Tnpjek15TVROM1l6TTJZak56WXPnMk1UTjJZek0zTUROe1l6TTRNak56VXPnM1lETnpVak4yTwPoeKv6TTJZ
ek16WwPoeK16TTJZek0zWURO

Output
=MDNzgzM0MTMzQzMzMDN2IzM0YzZmZmMDNzIzM1MzMzcjNyMjN2QzM2MT0zczMzMzNzIzM2YjNzczMzMzMTN
2YzM2YDNzYzM5MzNzIzM3MjMzYjN2MzNzIzM1YjNzYjN2MjN2UzM1YjNzczM0MjNzgzM2MTNzUjN2MzNzczM
2MTMzYjNzMjN2MzMTYjNzczM3MjNzgzM2YjNzUjN2MjNzZkzM3MzMzUjN2MzNzQzM2MD0zYzM1MTN2YzMzMTM
zMzMzMzMzMzMzMzIjN0MjNzUzM3MzMzczM0MTN2YzM2MD0zMzM0MzNzgzM2YjNzczMzMzMTN2YzM2YjNzYzM
2MTN2YzM3MDNzYzM4MjNzUzM2YDNzUjN2MjNzEzM2YzMzYjNzMzM2YzM3YDN
```

Setelah mencoba beberapa decode akhirnya saya menemukan decode yang cukup menarik yaitu base64, tapi letak '='nya berada di tempat yang salah oleh karna itu saya butuh melakukan reverse dan base64 decode lagi

```
Output
time: 2ms
length: 396
lines: 1
467366333663366313636653466353638363437366536363666366532373666383734333836366534373
33735363462373333333333333333366535363836343736653337393636653666383637373665336633663
136373736653536383634373665356636663665323736663237323739363466366532373666323732373
93634663267333532343134336432643334313438343
```

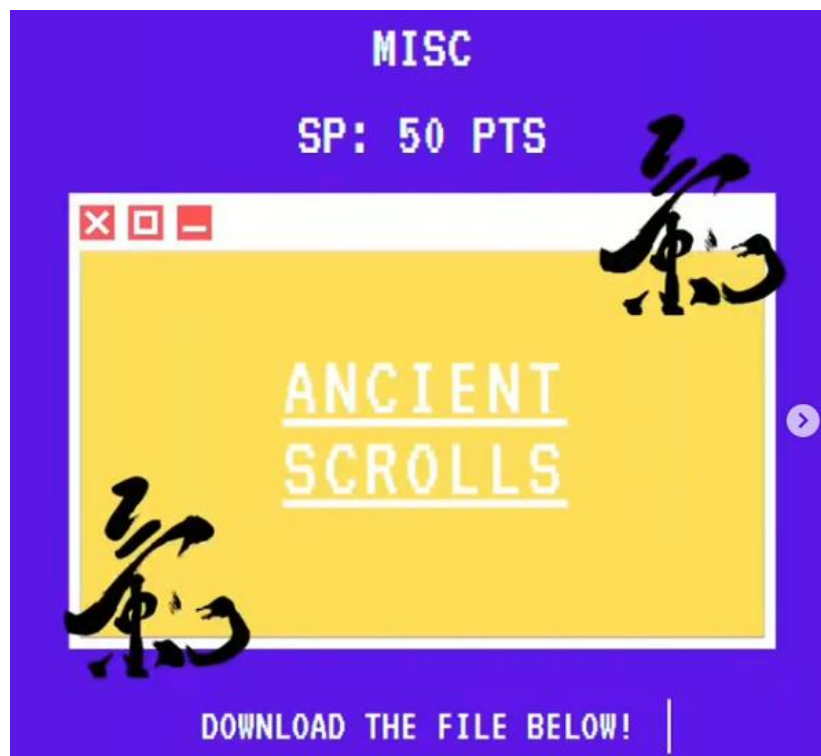
Hasil yang saya dapat berikutnya adalah angka angka aneh dan berdasarkan fungsi magic dari cyberchef, hasil yang saya dapatkan itu berasal dari base58, hex, atau hexdump. Namun setelah mencoba berkali kali saya tidak mendapatkan nya, lalu saya berpikir untuk melakukan reverse lagi baru mencoba satu satu lagi

From_Hex('None')	HACKLABS{mirror_mirror_on_	Valid UTF8
From_Hex('None')	the_wall_who_is_the_1337-	Entropy: 4.41
	est_h4xor_of_them_all?}	

Dan akhirnya saya mendapatkan flagnya, yang ternyata berasa dari hex kemudian hex lagi

HACKLABS{mirror_mirror_on_the_wall_who_is_the_1337-est_h4xor_of_them_all?}

Ancient Scrolls (Misc.)



Challenge di mulai dengan membuka drive Hacklabs yang berisi 3 file, 2 file txt (desc, dan history) dan satu file .rar yang dipassword. Jika melihat ke desc soal

Desc

Hello Players! We meet again.
Last year, Fei Mei, a friend of mine from Shangri-La, gave me a piece of file that contain something from 1000 years ago. She said that it's very special but she couldn't open it because her grandpa, Ip Man, locked the file in 1900s after studying how valuable a file is.

Although the password has been given, it's wrapped with weird chinese letterings and I couldn't understand them at all.
Can you help me?

Hint #1: She convinced me that it's NOT a pure Chinese letterings.

駿啥陰 词鳩喙駁 險 驢 驢

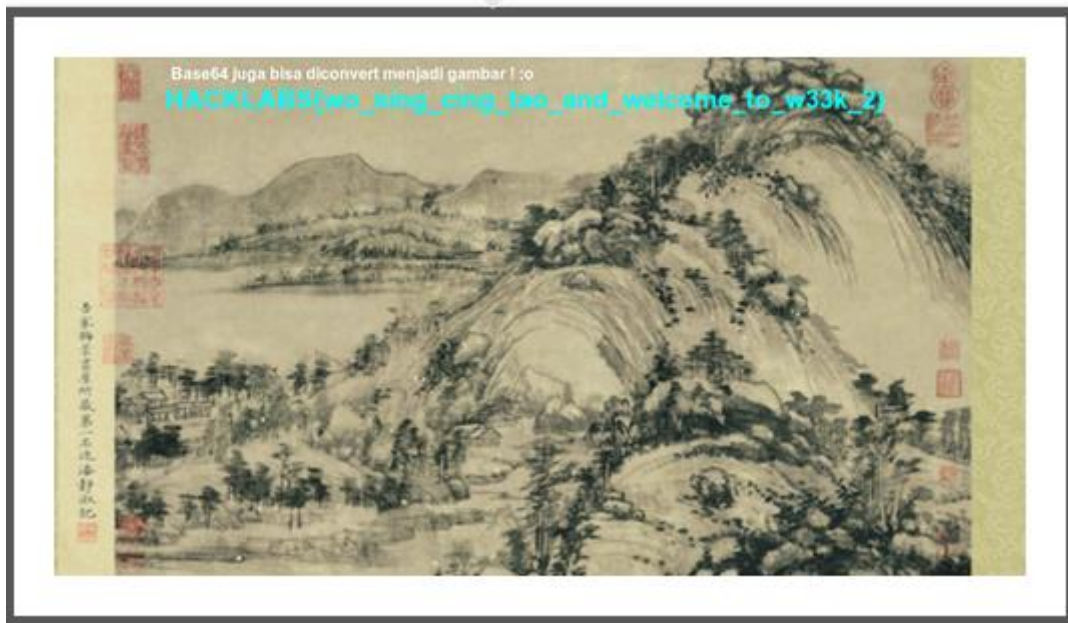
Membaca history dari clue yang diberikan saya pun bingung sehingga harus berdiskusi dengan peserta lainnya yang sudah selesai challenge tersebut, dan saya diberikan clue mengenai

unicode karna hal tersebut berhubungan dengan karakter yang ada. Dan pada akhirnya saya mencari "unicode base" berdasarkan saran peserta lain, dan menemukan base65536

Dengan menggunakan script python, saya menjalankan code seperti berikut :

```
import base65536

a = "𐄂𐄃𐄄𐄅𐄆𐄇𐄈𐄉𐄊𐄋𐄌𐄍𐄎𐄏𐄐𐄑𐄒𐄓𐄔𐄕𐄖𐄗𐄘𐄙𐄚𐄛𐄜𐄝𐄞𐄟𐄠𐄡𐄢𐄣𐄤𐄥𐄦𐄧𐄨𐄩𐄪𐄫𐄬𐄭𐄮𐄯𐄰𐄱𐄲𐄳𐄴𐄵𐄶𐄷𐄸𐄹𐄺𐄻𐄼𐄽𐄾𐄿𐅀𐅁𐅂𐅃𐅄𐅅𐅆𐅇𐅈𐅉𐅊𐅋𐅌𐅍𐅎𐅏𐅐𐅑𐅒𐅓𐅔𐅕𐅖𐅗𐅘𐅙𐅚𐅛𐅜𐅝𐅞𐅟𐅠𐅡𐅢𐅣𐅤𐅥𐅦𐅧𐅨𐅩𐅪𐅫𐅬𐅭𐅮𐅯𐅰𐅱𐅲𐅳𐅴𐅵𐅶𐅷𐅸𐅹𐅺𐅻𐅼𐅽𐅾𐅿𐆀𐆁𐆂𐆃𐆄𐆅𐆆𐆇𐆈𐆉𐆊𐆋𐆌𐆍𐆎𐆏𐆐𐆑𐆒𐆓𐆔𐆕𐆖𐆗𐆘𐆙𐆚𐆛𐆜𐆝𐆞𐆟𐆠𐆡𐆢𐆣𐆤𐆥𐆦𐆧𐆨𐆩𐆪𐆫𐆬𐆭𐆮𐆯𐆰𐆱𐆲𐆳𐆴𐆵𐆶𐆷𐆸𐆹𐆺𐆻𐆼𐆽𐆾𐆿𐇀𐇁𐇂𐇃𐇄𐇅𐇆𐇇𐇈𐇉𐇊𐇋𐇌𐇍𐇎𐇏𐇐𐇑𐇒𐇓𐇔𐇕𐇖𐇗𐇘𐇙𐇚𐇛𐇜𐇝𐇞𐇟𐇠𐇡𐇢𐇣𐇤𐇥𐇦𐇧𐇨𐇩𐇪𐇫𐇬𐇭𐇮𐇯𐇰𐇱𐇲𐇳𐇴𐇵𐇶𐇷𐇸𐇹𐇺𐇻𐇼𐇽𐇾𐇿𐈀𐈁𐈂𐈃𐈄𐈅𐈆𐈇𐈈𐈉𐈊𐈋𐈌𐈍𐈎𐈏𐈐𐈑𐈒𐈓𐈔𐈕𐈖𐈗𐈘𐈙𐈚𐈛𐈜𐈝𐈞𐈟𐈠𐈡𐈢𐈣𐈤𐈥𐈦𐈧𐈨𐈩𐈪𐈫𐈬𐈭𐈮𐈯𐈰𐈱𐈲𐈳𐈴𐈵𐈶𐈷𐈸𐈹𐈺𐈻𐈼𐈽𐈾𐈿𐉀𐉁𐉂𐉃𐉄𐉅𐉆𐉇𐉈𐉉𐉊𐉋𐉌𐉍𐉎𐉏𐉐𐉑𐉒𐉓𐉔𐉕𐉖𐉗𐉘𐉙𐉚𐉛𐉜𐉝𐉞𐉟𐉠𐉡𐉢𐉣𐉤𐉥𐉦𐉧𐉨𐉩𐉪𐉫𐉬𐉭𐉮𐉯𐉰𐉱𐉲𐉳𐉴𐉵𐉶𐉷𐉸𐉹𐉺𐉻𐉼𐉽𐉾𐉿𐊀𐊁𐊂𐊃𐊄𐊅𐊆𐊇𐊈𐊉𐊊𐊋𐊌𐊍𐊎𐊏𐊐𐊑𐊒𐊓𐊔𐊕𐊖𐊗𐊘𐊙𐊚𐊛𐊜𐊝𐊞𐊟𐊠𐊡𐊢𐊣𐊤𐊥𐊦𐊧𐊨𐊩𐊪𐊫𐊬𐊭𐊮𐊯𐊰𐊱𐊲𐊳𐊴𐊵𐊶𐊷𐊸𐊹𐊺𐊻𐊼𐊽𐊾𐊿𐋀𐋁𐋂𐋃𐋄𐋅𐋆𐋇𐋈𐋉𐋊𐋋𐋌𐋍𐋎𐋏𐋐𐋑𐋒𐋓𐋔𐋕𐋖𐋗𐋘𐋙𐋚𐋛𐋜𐋝𐋞𐋟𐋠𐋡𐋢𐋣𐋤𐋥𐋦𐋧𐋨𐋩𐋪𐋫𐋬𐋭𐋮𐋯𐋰𐋱𐋲𐋳𐋴𐋵𐋶𐋷𐋸𐋹𐋺𐋻𐋼𐋽𐋾𐋿𐌀𐌁𐌂𐌃𐌄𐌅𐌆𐌇𐌈𐌉𐌊𐌋𐌌𐌍𐌎𐌏𐌐𐌑𐌒𐌓𐌔𐌕𐌖𐌗𐌘𐌙𐌚𐌛𐌜𐌝𐌞𐌟𐌠𐌡𐌢𐌣𐌤𐌥𐌦𐌧𐌨𐌩𐌪𐌫𐌬𐌭𐌮𐌯𐌰𐌱𐌲𐌳𐌴𐌵𐌶𐌷𐌸𐌹𐌺𐌻𐌼𐌽𐌾𐌿𐍀𐍁𐍂𐍃𐍄𐍅𐍆𐍇𐍈𐍉𐍊𐍋𐍌𐍍𐍎𐍏𐍐𐍑𐍒𐍓𐍔𐍕𐍖𐍗𐍘𐍙𐍚𐍛𐍜𐍝𐍞𐍟𐍠𐍡𐍢𐍣𐍤𐍥𐍦𐍧𐍨𐍩𐍪𐍫𐍬𐍭𐍮𐍯𐍰𐍱𐍲𐍳𐍴𐍵𐍶𐍷𐍸𐍹𐍺𐍻𐍼𐍽𐍾𐍿𐎀𐎁𐎂𐎃𐎄𐎅𐎆𐎇𐎈𐎉𐎊𐎋𐎌𐎍𐎎𐎏𐎐𐎑𐎒𐎓𐎔𐎕𐎖𐎗𐎘𐎙𐎚𐎛𐎜𐎝𐎞𐎟𐎠𐎡𐎢𐎣𐎤𐎥𐎦𐎧𐎨𐎩𐎪𐎫𐎬𐎭𐎮𐎯𐎰𐎱𐎲𐎳𐎴𐎵𐎶𐎷𐎸𐎹𐎺𐎻𐎼𐎽𐎾𐎿𐏀𐏁𐏂𐏃𐏄𐏅𐏆𐏇𐏈𐏉𐏊𐏋𐏌𐏍𐏎𐏏𐏐𐏑𐏒𐏓𐏔𐏕𐏖𐏗𐏘𐏙𐏚𐏛𐏜𐏝𐏞𐏟𐏠𐏡𐏢𐏣𐏤𐏥𐏦𐏧𐏨𐏩𐏪𐏫𐏬𐏭𐏮𐏯𐏰𐏱𐏲𐏳𐏴𐏵𐏶𐏷𐏸𐏹𐏺𐏻𐏼𐏽𐏾𐏿𐐀𐐁𐐂𐐃𐐄𐐅𐐆𐐇𐐈𐐉𐐊𐐋𐐌𐐍𐐎𐐏𐐐𐐑𐐒𐐓𐐔𐐕𐐖𐐗𐐘𐐙𐐚𐐛𐐜𐐝𐐞𐐟𐐠𐐡𐐢𐐣𐐤𐐥𐐦𐐧𐐨𐐩𐐪𐐫𐐬𐐭𐐮𐐯𐐰𐐱𐐲𐐳𐐴𐐵𐐶𐐷𐐸𐐹𐐺𐐻𐐼𐐽𐐾𐐿𐑀𐑁𐑂𐑃𐑄𐑅𐑆𐑇𐑈𐑉𐑊𐑋𐑌𐑍𐑎𐑏𐑐𐑑𐑒𐑓𐑔𐑕𐑖𐑗𐑘𐑙𐑚𐑛𐑜𐑝𐑞𐑟𐑠𐑡𐑢𐑣𐑤𐑥𐑦𐑧𐑨𐑩𐑪𐑫𐑬𐑭𐑮𐑯𐑰𐑱𐑲𐑳𐑴𐑵𐑶𐑷𐑸𐑹𐑺𐑻𐑼𐑽𐑾𐑿𐒀𐒁𐒂𐒃𐒄𐒅𐒆𐒇𐒈𐒉𐒊𐒋𐒌𐒍𐒎𐒏𐒐𐒑𐒒𐒓𐒔𐒕𐒖𐒗𐒘𐒙𐒚𐒛𐒜𐒝𐒞𐒟𐒠𐒡𐒢𐒣𐒤𐒥𐒦𐒧𐒨𐒩𐒪𐒫𐒬𐒭𐒮𐒯𐒰𐒱𐒲𐒳𐒴𐒵𐒶𐒷𐒸𐒹𐒺𐒻𐒼𐒽𐒾𐒿𐓀𐓁𐓂𐓃𐓄𐓅𐓆𐓇𐓈𐓉𐓊𐓋𐓌𐓍𐓎𐓏𐓐𐓑𐓒𐓓𐓔𐓕𐓖𐓗𐓘𐓙𐓚𐓛𐓜𐓝𐓞𐓟𐓠𐓡𐓢𐓣𐓤𐓥𐓦𐓧𐓨𐓩𐓪𐓫𐓬𐓭𐓮𐓯𐓰𐓱𐓲𐓳𐓴𐓵𐓶𐓷𐓸𐓹𐓺𐓻𐓼𐓽𐓾𐓿𐔀𐔁𐔂𐔃𐔄𐔅𐔆𐔇𐔈𐔉𐔊𐔋𐔌𐔍𐔎𐔏𐔐𐔑𐔒𐔓𐔔𐔕𐔖𐔗𐔘𐔙𐔚𐔛𐔜𐔝𐔞𐔟𐔠𐔡𐔢𐔣𐔤𐔥𐔦𐔧𐔨𐔩𐔪𐔫𐔬𐔭𐔮𐔯𐔰𐔱𐔲𐔳𐔴𐔵𐔶𐔷𐔸𐔹𐔺𐔻𐔼𐔽𐔾𐔿𐕀𐕁𐕂𐕃𐕄𐕅𐕆𐕇𐕈𐕉𐕊𐕋𐕌𐕍𐕎𐕏𐕐𐕑𐕒𐕓𐕔𐕕𐕖𐕗𐕘𐕙𐕚𐕛𐕜𐕝𐕞𐕟𐕠𐕡𐕢𐕣𐕤𐕥𐕦𐕧𐕨𐕩𐕪𐕫𐕬𐕭𐕮𐕯𐕰𐕱𐕲𐕳𐕴𐕵𐕶𐕷𐕸𐕹𐕺𐕻𐕼𐕽𐕾𐕿𐖀𐖁𐖂𐖃𐖄𐖅𐖆𐖇𐖈𐖉𐖊𐖋𐖌𐖍𐖎𐖏𐖐𐖑𐖒𐖓𐖔𐖕𐖖𐖗𐖘𐖙𐖚𐖛𐖜𐖝𐖞𐖟𐖠𐖡𐖢𐖣𐖤𐖥𐖦𐖧𐖨𐖩𐖪𐖫𐖬𐖭𐖮𐖯𐖰𐖱𐖲𐖳𐖴𐖵𐖶𐖷𐖸𐖹𐖺𐖻𐖼𐖽𐖾𐖿𐗀𐗁𐗂𐗃𐗄𐗅𐗆𐗇𐗈𐗉𐗊𐗋𐗌𐗍𐗎𐗏𐗐𐗑𐗒𐗓𐗔𐗕𐗖𐗗𐗘𐗙𐗚𐗛𐗜𐗝𐗞𐗟𐗠𐗡𐗢𐗣𐗤𐗥𐗦𐗧𐗨𐗩𐗪𐗫𐗬𐗭𐗮𐗯𐗰𐗱𐗲𐗳𐗴𐗵𐗶𐗷𐗸𐗹𐗺𐗻𐗼𐗽𐗾𐗿𐘀𐘁𐘂𐘃𐘄𐘅𐘆𐘇𐘈𐘉𐘊𐘋𐘌𐘍𐘎𐘏𐘐𐘑𐘒𐘓𐘔𐘕𐘖𐘗𐘘𐘙𐘚𐘛𐘜𐘝𐘞𐘟𐘠𐘡𐘢𐘣𐘤𐘥𐘦𐘧𐘨𐘩𐘪𐘫𐘬𐘭𐘮𐘯𐘰𐘱𐘲𐘳𐘴𐘵𐘶𐘷𐘸𐘹𐘺𐘻𐘼𐘽𐘾𐘿𐙀𐙁𐙂𐙃𐙄𐙅𐙆𐙇𐙈𐙉𐙊𐙋𐙌𐙍𐙎𐙏𐙐𐙑𐙒𐙓𐙔𐙕𐙖𐙗𐙘𐙙𐙚𐙛𐙜𐙝𐙞𐙟𐙠𐙡𐙢𐙣𐙤𐙥𐙦𐙧𐙨𐙩𐙪𐙫𐙬𐙭𐙮𐙯𐙰𐙱𐙲𐙳𐙴𐙵𐙶𐙷𐙸𐙹𐙺𐙻𐙼𐙽𐙾𐙿𐚀𐚁𐚂𐚃𐚄𐚅𐚆𐚇𐚈𐚉𐚊𐚋𐚌𐚍𐚎𐚏𐚐𐚑𐚒𐚓𐚔𐚕𐚖𐚗𐚘𐚙𐚚𐚛𐚜𐚝𐚞𐚟𐚠𐚡𐚢𐚣𐚤𐚥𐚦𐚧𐚨𐚩𐚪𐚫𐚬𐚭𐚮𐚯𐚰𐚱𐚲𐚳𐚴𐚵𐚶𐚷𐚸𐚹𐚺𐚻𐚼𐚽𐚾𐚿𐛀𐛁𐛂𐛃𐛄𐛅𐛆𐛇𐛈𐛉𐛊𐛋𐛌𐛍𐛎𐛏𐛐𐛑𐛒𐛓𐛔𐛕𐛖𐛗𐛘𐛙𐛚𐛛𐛜𐛝𐛞𐛟𐛠𐛡𐛢𐛣𐛤𐛥𐛦𐛧𐛨𐛩𐛪𐛫𐛬𐛭𐛮𐛯𐛰𐛱𐛲𐛳𐛴𐛵𐛶𐛷𐛸𐛹𐛺𐛻𐛼𐛽𐛾𐛿𐜀𐜁𐜂𐜃𐜄𐜅𐜆𐜇𐜈𐜉𐜊𐜋𐜌𐜍𐜎𐜏𐜐𐜑𐜒𐜓𐜔𐜕𐜖𐜗𐜘𐜙𐜚𐜛𐜜𐜝𐜞𐜟𐜠𐜡𐜢𐜣𐜤𐜥𐜦𐜧𐜨𐜩𐜪𐜫𐜬𐜭𐜮𐜯𐜰𐜱𐜲𐜳𐜴𐜵𐜶𐜷𐜸𐜹𐜺𐜻𐜼𐜽𐜾𐜿𐝀𐝁𐝂𐝃𐝄𐝅𐝆𐝇𐝈𐝉𐝊𐝋𐝌𐝍𐝎𐝏𐝐𐝑𐝒𐝓𐝔𐝕𐝖𐝗𐝘𐝙𐝚𐝛𐝜𐝝𐝞𐝟𐝠𐝡𐝢𐝣𐝤𐝥𐝦𐝧𐝨𐝩𐝪𐝫𐝬𐝭𐝮𐝯𐝰𐝱𐝲𐝳𐝴𐝵𐝶𐝷𐝸𐝹𐝺𐝻𐝼𐝽𐝾𐝿𐞀𐞁𐞂𐞃𐞄𐞅𐞆𐞇𐞈𐞉𐞊𐞋𐞌𐞍𐞎𐞏𐞐𐞑𐞒𐞓𐞔𐞕𐞖𐞗𐞘𐞙𐞚𐞛𐞜𐞝𐞞𐞟𐞠𐞡𐞢𐞣𐞤𐞥𐞦𐞧𐞨𐞩𐞪𐞫𐞬𐞭𐞮𐞯𐞰𐞱𐞲𐞳𐞴𐞵𐞶𐞷𐞸𐞹𐞺𐞻𐞼𐞽𐞾𐞿𐟀𐟁𐟂𐟃𐟄𐟅𐟆𐟇𐟈𐟉𐟊𐟋𐟌𐟍𐟎𐟏𐟐𐟑𐟒𐟓𐟔𐟕𐟖𐟗𐟘𐟙𐟚𐟛𐟜𐟝𐟞𐟟𐟠𐟡𐟢𐟣𐟤𐟥𐟦𐟧𐟨𐟩𐟪𐟫𐟬𐟭𐟮𐟯𐟰𐟱𐟲𐟳𐟴𐟵𐟶𐟷𐟸𐟹𐟺𐟻𐟼𐟽𐟾𐟿𐠀𐠁𐠂𐠃𐠄𐠅𐠆𐠇𐠈𐠉𐠊𐠋𐠌𐠍𐠎𐠏𐠐𐠑𐠒𐠓𐠔𐠕𐠖𐠗𐠘𐠙𐠚𐠛𐠜𐠝𐠞𐠟𐠠𐠡𐠢𐠣𐠤𐠥𐠦𐠧𐠨𐠩𐠪𐠫𐠬𐠭𐠮𐠯𐠰𐠱𐠲𐠳𐠴𐠵𐠶𐠷𐠸𐠹𐠺𐠻𐠼𐠽𐠾𐠿𐡀𐡁𐡂𐡃𐡄𐡅𐡆𐡇𐡈𐡉𐡊𐡋𐡌𐡍𐡎𐡏𐡐𐡑𐡒𐡓𐡔𐡕𐡖𐡗𐡘𐡙𐡚𐡛𐡜𐡝𐡞𐡟𐡠𐡡𐡢𐡣𐡤𐡥𐡦𐡧𐡨𐡩𐡪𐡫𐡬𐡭𐡮𐡯𐡰𐡱𐡲𐡳𐡴𐡵𐡶𐡷𐡸𐡹𐡺𐡻𐡼𐡽𐡾𐡿𐢀𐢁𐢂𐢃𐢄𐢅𐢆𐢇𐢈𐢉𐢊𐢋𐢌𐢍𐢎𐢏𐢐𐢑𐢒𐢓𐢔𐢕𐢖𐢗𐢘𐢙𐢚𐢛𐢜𐢝𐢞𐢟𐢠𐢡𐢢𐢣𐢤𐢥𐢦𐢧𐢨𐢩𐢪𐢫𐢬𐢭𐢮𐢯𐢰𐢱𐢲𐢳𐢴𐢵𐢶𐢷𐢸𐢹𐢺𐢻𐢼𐢽𐢾𐢿𐣀𐣁𐣂𐣃𐣄𐣅𐣆𐣇𐣈𐣉𐣊𐣋𐣌𐣍𐣎𐣏𐣐𐣑𐣒𐣓𐣔𐣕𐣖𐣗𐣘𐣙𐣚𐣛𐣜𐣝𐣞𐣟𐣠𐣡𐣢𐣣𐣤𐣥𐣦𐣧𐣨𐣩𐣪𐣫𐣬𐣭𐣮𐣯𐣰𐣱𐣲𐣳𐣴𐣵𐣶𐣷𐣸𐣹𐣺𐣻𐣼𐣽𐣾𐣿𐤀𐤁𐤂𐤃𐤄𐤅𐤆𐤇𐤈𐤉𐤊𐤋𐤌𐤍𐤎𐤏𐤐𐤑𐤒𐤓𐤔𐤕𐤖𐤗𐤘𐤙𐤚𐤛𐤜𐤝𐤞𐤟𐤠𐤡𐤢𐤣𐤤𐤥𐤦𐤧𐤨𐤩𐤪𐤫𐤬𐤭𐤮𐤯𐤰𐤱𐤲𐤳𐤴𐤵𐤶𐤷𐤸𐤹𐤺𐤻𐤼𐤽𐤾𐤿𐥀𐥁𐥂𐥃𐥄𐥅𐥆𐥇𐥈𐥉𐥊𐥋𐥌𐥍𐥎𐥏𐥐𐥑𐥒𐥓𐥔𐥕𐥖𐥗𐥘𐥙𐥚𐥛𐥜𐥝𐥞𐥟𐥠𐥡𐥢𐥣𐥤𐥥𐥦𐥧𐥨𐥩𐥪𐥫𐥬𐥭𐥮𐥯𐥰𐥱𐥲𐥳𐥴𐥵𐥶𐥷𐥸𐥹𐥺𐥻𐥼𐥽𐥾𐥿𐦀𐦁𐦂𐦃𐦄𐦅𐦆𐦇𐦈𐦉𐦊𐦋𐦌𐦍𐦎𐦏𐦐𐦑𐦒𐦓𐦔𐦕𐦖𐦗𐦘𐦙𐦚𐦛𐦜𐦝𐦞𐦟𐦠𐦡𐦢𐦣𐦤𐦥𐦦𐦧𐦨𐦩𐦪𐦫𐦬𐦭𐦮𐦯𐦰𐦱𐦲𐦳𐦴𐦵𐦶𐦷𐦸𐦹𐦺𐦻𐦼𐦽𐦾𐦿𐧀𐧁𐧂𐧃𐧄𐧅𐧆𐧇𐧈𐧉𐧊𐧋𐧌𐧍𐧎𐧏𐧐𐧑𐧒𐧓𐧔𐧕𐧖𐧗𐧘𐧙𐧚𐧛𐧜𐧝𐧞𐧟𐧠𐧡𐧢𐧣𐧤𐧥𐧦𐧧𐧨𐧩𐧪𐧫𐧬𐧭𐧮𐧯𐧰𐧱𐧲𐧳𐧴𐧵𐧶𐧷𐧸𐧹𐧺𐧻𐧼𐧽𐧾𐧿𐨀𐨁𐨂𐨃𐨄𐨅𐨆𐨇𐨈𐨉𐨊𐨋𐨌𐨍𐨎𐨏𐨐𐨑𐨒𐨓𐨔𐨕𐨖𐨗𐨘𐨙𐨚𐨛𐨜𐨝𐨞𐨟𐨠𐨡𐨢𐨣𐨤𐨥𐨦𐨧𐨨𐨩𐨪𐨫𐨬𐨭𐨮𐨯𐨰𐨱𐨲𐨳𐨴𐨵𐨶𐨷𐨹𐨺𐨸𐨻𐨼𐨽𐨾𐨿𐩀𐩁𐩂𐩃𐩄𐩅𐩆𐩇𐩈𐩉𐩊𐩋𐩌𐩍𐩎𐩏𐩐𐩑𐩒𐩓𐩔𐩕𐩖𐩗𐩘𐩙𐩚𐩛𐩜𐩝𐩞𐩟𐩠𐩡𐩢𐩣𐩤𐩥𐩦𐩧𐩨𐩩𐩪𐩫𐩬𐩭𐩮𐩯𐩰𐩱𐩲𐩳𐩴𐩵𐩶𐩷𐩸𐩹𐩺𐩻𐩼𐩽𐩾𐩿𐪀𐪁𐪂𐪃𐪄𐪅𐪆𐪇𐪈𐪉𐪊𐪋𐪌𐪍𐪎𐪏𐪐𐪑𐪒𐪓𐪔𐪕𐪖𐪗𐪘𐪙𐪚𐪛𐪜𐪝𐪞𐪟𐪠𐪡𐪢𐪣𐪤𐪥𐪦𐪧𐪨𐪩𐪪𐪫𐪬𐪭𐪮𐪯𐪰𐪱𐪲𐪳𐪴𐪵𐪶𐪷𐪸𐪹𐪺𐪻𐪼𐪽𐪾𐪿𐫀𐫁𐫂𐫃𐫄𐫅𐫆𐫇𐫈𐫉𐫊𐫋𐫌𐫍𐫎𐫏𐫐𐫑𐫒𐫓𐫔𐫕𐫖𐫗𐫘𐫙𐫚𐫛𐫜𐫝𐫞𐫟𐫠𐫡𐫢𐫣𐫤𐫦𐫥𐫧𐫨𐫩𐫪𐫫𐫬𐫭𐫮𐫯𐫰𐫱𐫲𐫳𐫴𐫵𐫶𐫷𐫸𐫹𐫺𐫻𐫼𐫽𐫾𐫿𐬀𐬁𐬂𐬃𐬄𐬅𐬆𐬇𐬈𐬉𐬊𐬋𐬌𐬍𐬎𐬏𐬐𐬑𐬒𐬓𐬔𐬕𐬖𐬗𐬘𐬙𐬚𐬛𐬜𐬝𐬞𐬟𐬠𐬡𐬢𐬣𐬤𐬥𐬦𐬧𐬨𐬩𐬪𐬫𐬬𐬭𐬮𐬯𐬰𐬱𐬲𐬳𐬴𐬵𐬶𐬷𐬸𐬹𐬺𐬻𐬼𐬽𐬾𐬿𐭀𐭁𐭂𐭃𐭄𐭅𐭆𐭇𐭈𐭉𐭊𐭋𐭌𐭍𐭎𐭏𐭐𐭑𐭒𐭓𐭔𐭕𐭖𐭗𐭘𐭙𐭚𐭛𐭜𐭝𐭞𐭟𐭠𐭡𐭢𐭣𐭤𐭥𐭦𐭧𐭨𐭩𐭪𐭫𐭬𐭭𐭮𐭯𐭰𐭱𐭲𐭳𐭴𐭵𐭶𐭷𐭸𐭹𐭺𐭻𐭼𐭽𐭾𐭿𐮀𐮁𐮂𐮃𐮄𐮅𐮆𐮇𐮈𐮉𐮊𐮋𐮌𐮍𐮎𐮏𐮐𐮑𐮒𐮓𐮔𐮕𐮖𐮗𐮘𐮙𐮚𐮛𐮜𐮝𐮞𐮟𐮠𐮡𐮢𐮣𐮤𐮥𐮦𐮧𐮨𐮩𐮪𐮫𐮬𐮭𐮮𐮯𐮰𐮱𐮲𐮳𐮴𐮵𐮶𐮷𐮸𐮹𐮺𐮻𐮼𐮽𐮾𐮿𐯀𐯁𐯂𐯃𐯄𐯅𐯆𐯇𐯈𐯉𐯊𐯋𐯌𐯍𐯎𐯏𐯐𐯑𐯒𐯓𐯔𐯕𐯖𐯗𐯘𐯙𐯚𐯛𐯜𐯝𐯞𐯟𐯠𐯡𐯢𐯣𐯤𐯥𐯦𐯧𐯨𐯩𐯪𐯫𐯬𐯭𐯮𐯯𐯰𐯱𐯲𐯳𐯴𐯵𐯶𐯷𐯸𐯹𐯺𐯻𐯼𐯽𐯾𐯿𐰀𐰁𐰂𐰃𐰄𐰅𐰆𐰇𐰈𐰉𐰊𐰋𐰌𐰍𐰎𐰏𐰐𐰑𐰒𐰓𐰔𐰕𐰖𐰗𐰘𐰙𐰚𐰛𐰜𐰝𐰞𐰟𐰠𐰡𐰢𐰣𐰤𐰥𐰦𐰧𐰨𐰩𐰪𐰫𐰬𐰭𐰮𐰯𐰰𐰱𐰲𐰳𐰴𐰵𐰶𐰷𐰸𐰹𐰺𐰻𐰼𐰽𐰾𐰿𐱀𐱁𐱂𐱃𐱄𐱅𐱆𐱇𐱈𐱉𐱊𐱋𐱌𐱍𐱎𐱏𐱐𐱑𐱒𐱓𐱔𐱕𐱖𐱗𐱘𐱙𐱚𐱛𐱜𐱝𐱞𐱟𐱠𐱡𐱢𐱣𐱤𐱥𐱦𐱧𐱨𐱩𐱪𐱫𐱬𐱭𐱮𐱯𐱰𐱱𐱲𐱳𐱴𐱵𐱶𐱷𐱸𐱹𐱺𐱻𐱼𐱽𐱾𐱿𐲀𐲁𐲂𐲃𐲄𐲅𐲆𐲇𐲈𐲉𐲊𐲋𐲌𐲍𐲎𐲏𐲐𐲑𐲒𐲓𐲔𐲕𐲖𐲗𐲘𐲙𐲚𐲛𐲜𐲝𐲞𐲟𐲠𐲡𐲢𐲣𐲤𐲥𐲦𐲧𐲨𐲩𐲪𐲫𐲬𐲭𐲮𐲯𐲰𐲱𐲲𐲳𐲴𐲵𐲶𐲷𐲸𐲹𐲺𐲻𐲼𐲽𐲾𐲿𐳀𐳁𐳂𐳃𐳄𐳅𐳆𐳇𐳈𐳉𐳊𐳋𐳌𐳍𐳎𐳏𐳐𐳑𐳒𐳓𐳔𐳕𐳖𐳗𐳘𐳙𐳚𐳛𐳜𐳝𐳞𐳟𐳠𐳡𐳢𐳣𐳤𐳥𐳦𐳧𐳨𐳩𐳪𐳫𐳬𐳭𐳮𐳯𐳰𐳱𐳲𐳳𐳴
```



Flagnya dapat terlihat!

HACKLABS{wo_sing_cing_tao_and_welcome_to_w33k_2}

Keyless v2 (Crypto)



```
#!/usr/bin/python3

flag = "REDACTED"
key = "REDACTED"
keyIndex = 0
enc = ""

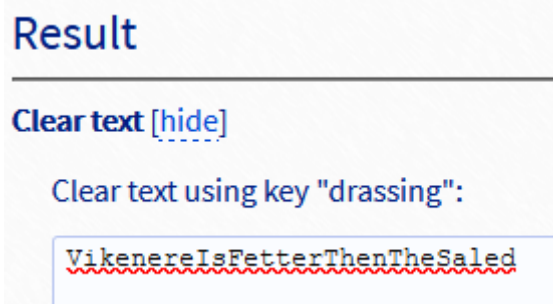
for c in flag:
    if ord(c) >= ord('A') and ord(c) <= ord('Z'):
        enc += chr( (( ord(c) - ord('A') + (ord(key[keyIndex]) - ord('a')) ) % 26) + ord('A'))
    elif ord(c) >= ord('a') and ord(c) <= ord('z'):
        enc += chr( (( ord(c) - ord('a') + (ord(key[keyIndex]) - ord('a')) ) % 26) + ord('a'))
    else:
        enc += c

    keyIndex += 1
    if keyIndex == len(key):
        keyIndex = 0

print(enc)
#YzkwfmeKljFwlbrxWyefLprYdcev
```

Dengan melihat file yang diberikan di link drive yang terlampir pada caption, saya mengetahui bahwa cryptography yang digunakan adalah **Vigenere Cipher**, hal ini dikarenakan adanya key yang berulang-ulang, contoh key = abc, dan plain textnya = hacklabs, maka keynya akan menjadi "abcabcab".

Kemudian karna tidak adanya clue untuk key nya, maka saya menggunakan online solver [link](#) dan berhasil mendapatkan string yang saya pikir merupakan flagnya, namun setelah dicek lagi itu merupakan flagnya



Karna plain textnya memiliki typo begitu juga dengan keynya, maka saya mencoba jika keynya dirubah huruf “a”nya sehingga menjadi **dressing**. Dan saat itulah flag nya muncul.

The image shows a web interface for a Vigenere Decoder tool. On the left, there is a search bar with the text "e.g. type random" and a "GO" button. Below it, the results section shows "Vigenere" with a tag "DRESSING" and a list of related items: "VigenereIsBetterThanTheSalad", "Vigenere Cipher - dCode", and "Tag(s) : Poly-Alphabetic Cipher". There are also social media share icons. On the right, the "VIGENERE DECODER" section has a "VIGENERE CIPHERTEXT" input field containing "YzkwfmeLjFw1brxwyefLprydcev". Below this are "PARAMETERS" for "PLAINTEXT LANGUAGE" (set to English) and "ALPHABET" (set to ABCDEFGHIJKLMNOPQRSTUVWXYZ). An "AUTOMATIC DECRYPTION" button is present. At the bottom, the "DECRYPTION METHOD" is set to "KNOWING THE KEY/PASSWORD: DRESSING".

HACKLABS{VigenerelsBetterThanTheSalad}

Catch The Ride (OSINT)



Dari challenge yang diberikan, saya hanya diberikan 2 file saja yaitu 1 file deskripsi soal yang berisikan kata kata seperti berikut :

Catch The Ride (Medium)

Interpol mencurigai seorang bernama Mang Oleh, dan Interpol ingin menyadap rumah Mang Oleh, namun hal itu tidak bisa dilakukan sembarangan karna Mang Oleh sering menghabiskan waktunya di rumah dan hanya pergi ketika hari Kamis pagi-pagi sekali ke london, dan ketika Interpol menggunakan drone untuk memantau, drone tersebut dirusak orang dan hanya satu foto yang dapat direcover, dapatkan kamu membantu interpol mencari tahu kapan kereta pertama berangkat?

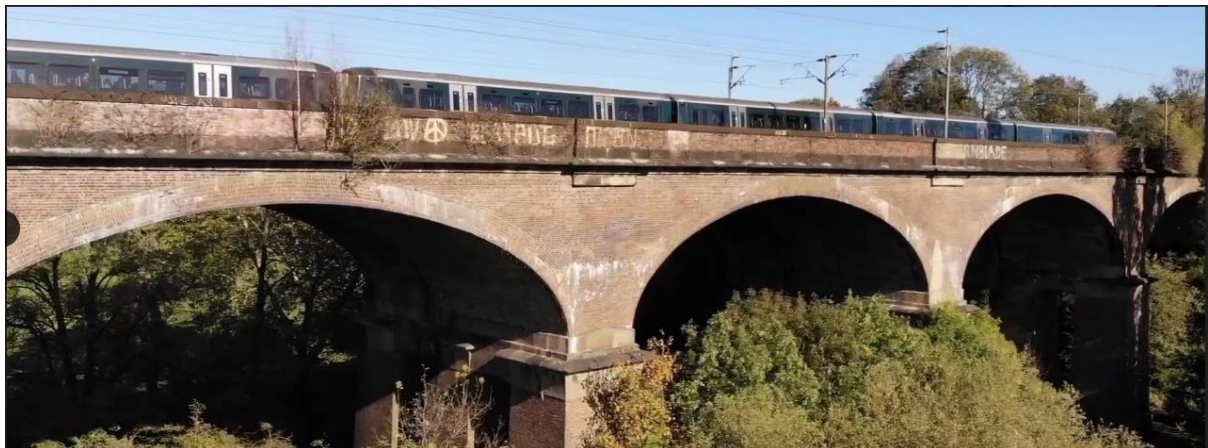
```
format flag = HACKLABS{stationName_nameofRailwayService_firstTrainTime(hh:mm)}
```

Hint 1 = Railway Servicesnya singkatan aja

Hint 2 = Railway Servicesnya ditemukan pada tahun 1833 di Bristol

note : flagnya untuk yang didalam bracket huruf kecil semuanya

Dan 1 file gambar yang seperti berikut :



Setelah melakukan reverse image, saya tidak menemukan tempat yang begitu mirip dan saya terpikirkan untuk mengecek metadata dari foto tersebut, dan saya melihat sesuatu yang menarik dan itu merupakan gps.

Property	Value
Description	
Title	
Subject	
Rating	☆☆☆☆☆
Tags	51.5110464,-0.3433982
Comments	
Origin	
Authors	Odading Mang Oleh
Date taken	
Program name	
Date acquired	
Copyright	
Image	

Dan setelah mengecek gps tersebut di googlemaps, saya menemukan tempat yang sesuai dengan foto tersebut, yaitu Whancliffe Viaduct, lalu berdasarkan lokasi tersebut, saya menemukan stasiun terdekat dari foto tersebut yaitu **Hanwell** sehingga saya yakin bahwa stasiun tersebut adalah stasiun keberangkatan pelaku, lalu saya pun lanjut mencari **railway services** dari stasiun tersebut, berdasarkan https://en.wikipedia.org/wiki/Hanwell_railway_station maka bisa dipastikan **railway services** pada stasiun Hanwell merupakan **Great Western Railway** yang disingkat **GWR**, terakhir adalah mencari tahu kapan kereta pertama dari Hanwell berangkat ke London, karna stasiun yang menerima kedatangan dari Hanwell adalah London Paddington jadi saya memperkecil pencarian dengan keyword "Hanwell to London Paddington first train" dan mendapatkan hasil

The first train from Hanwell to London Paddington departs at 05:41 .

Train operators: TfL Rail

Fastest route: 14 m

Distance: 7 miles (11 km)

www.thetrainline.com > Train Times

[Trains Hanwell to London Paddington | Cheap Tickets ...](#)

Dan parameter terakhir dari flag sudah didapatkan yaitu **05:41** sehingga flag dari challenge ini adalah

HACKLABS{hanwell_gwr_05:41}

Pokemon Go! (Misc.)



Challenge ini diawali dengan download file bernama games.zip yang ada pada drive dari HackLabs,

Desc

Himaru and Tsubasa love to play Pokemon Go!. They have been a fan of the game since a year ago and have joined the Online Community.

One day, the mysterious 'taskmaster' gave them a mini-game. If they can find the secret message from the given file, they will win a Legendary Pokemon!

Help them to uncover the secret messages from the file!

Hint #1: The file is encrypted with unknown password.

I think we should try "brute-force" method that is related to the challenge (?).

Hint #2: Have you ever heard of esoteric languages?

It's a custom-made for sure!

karna file tersebut dipassword, dan saya tidak tahu passwordnya karna itu saya mencari password list yang berhubungan dengan pokemon. Dan karna menggunakan script tidak bisa dilakukan bruteforce, maka saya mencoba menggunakan JohnTheRipper untuk melakukan bruteforce password Zip tersebut.

```
root@pacife:~/Downloads# john --wordlist=pokemon.txt hasil
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
delibird (games.zip/pokemon_go_easter_egg.txt)
1g 0:00:00:00 DONE (2020-10-15 18:56) 16.66g/s 12016p/s 12016c/s 12016C/s abomas
now..zygarde
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@pacife:~/Downloads# john hasil --show
games.zip/pokemon_go_easter_egg.txt:delibird:pokemon_go_easter_egg.txt:games.zip
:games.zip

1 password hash cracked, 0 left
root@pacife:~/Downloads#
```

Dan dari hasil command di atas, saya berhasil mendapatkan password dari games.zip tersebut yaitu pokemone bernama delibird. Dan kemudian setelah berhasil mengextract text file bernama pokemon_go_easter_egg.txt dan membukanya saya menemukan bahasa dari pikachu karna hanya berisi pika pi pika dsb.

[illegible]

Lalu saya mencari “pikachu language decoder” di teman terbaik semua orang yaitu, Google. Dan hasil dari decoder tersebut adalah link seperti di bawah ini

<https://docs.google.com/document/d/1uj1LgGjUi8OhgZFhbA49qeX3YiO3l0d7Lx6uJZmD5Cs>

dan hasil dari link diatas adalah mengarah ke suatu document google yang mengarahkan lagi ke link berikutnya



Dan qr code tersebut mengarah lagi ke link

https://mega.nz/file/pFAVEGcC#E5OjHOloXGxhoYetnCliamySIO8i3Q8_CTU3WCWOYDI

dan pada akhirnya saya perlu untuk mendownload file bernama pikapika.exe yang di dalamnya ada fake flag dan juga real flag

```
#H#####%/%/%/%%{#####V#####((//**
###A#####%/%/%/%%P#####R##_#####((//**
#####C#####%B/%/%/%%I#####3#####C#####((//**
#####K##A#####K#####V#####U#####(///
###&%&%#L#####4#####_#####T###((//
###&%/%%,&(((#####T#####5#####E###(((
#####%/%&,,,&#####C#####1#####_####
###((( (%%,,,,&#####H##_#####:3}%
##(((((&,,,&#####U#####%#%
GOOD BYE, TERMINATING ...
HACKLABS{m1sc_1s_F00n_but_1s_th1s_the_fl4g?}
```

Dan setelah mencoba kedua flag tersebut, ditemukan bahwa real flagnya adalah

HACKLABS{PIK4TCHU_15_V3RY_CUTE__:3}

How Hot It Is (OSINT)



Dari link yang diberikan kita mendapatkan gambar satelit dan juga deskripsi soal, seperti yang terlampir di bawah :

```
How Hot Is It? (Med-Hard)
Chunny merupakan ahli Geologi, namun dia butuh bantuan kalian untuk mengecek Brightness Temperature (Channel 21/22) dari
foto yang terlampir karena Chunny harus segera pergi ke suatu tempat lain pada tanggal 28 September kemarin, dapatkah kalian
membantu Chunny mendapatkan berapa derajat Brightness Temperature (Channel 21/22)nya agar ia tidak ditegur oleh atasannya?
format flag : ubah spasi menjadi '_'

Hint 1 : it has been said, its in the past
Hint 2 : you know it is a satellite image right?
Hint 3 : use Terra and Aqua / MODIS layers
```

Dan berdasarkan dari deskripsi challenge tersebut, kita tahu bahwa foto tersebut diambil tanggal 28 September, dan foto tersebut adalah foto satelit, jadi kita bisa mencari menggunakan keyword "View satellite past image" dan mendapatkan link berikut : <https://medium.com/@thegeospatialnews/how-to-get-old-satellite-images-on-google-maps-f11b2fad17b4>

Dari link di atas, kita dapat menggunakan gambar *satellite* dari NASA yang dapat diakses dari link ini : worldview.earthdata.nasa.gov/ dan mencari dimana gunung Krakatau berada, setelah itu dengan layer yang ada kita dapat melakukan filter sesuai dari clue yaitu Terra and Aqua / MODIS Layers, dan kita memilih yang versi *day and night* kemudian kita dapat melihat suhu temperatur dari Krakatau.

Fires and Thermal An... [1]	
03:20	
Latitude	-6.101 °
Longitude	105.425 °
Brightness Temperature (Channel 21/22)	325 Kelvin
Brightness Temperature (Channel 31)	304.3 Kelvin
Fire Radiative Power	16.8 MW
Detection Confidence	78 %
Day/Night Flag	Daytime Fire
Along-Scan Pixel Size	1 km

Dan dari deskripsi challenge juga, kita hanya perlu melihat ke “Brightness Temperature (Channel 21/22)” yaitu sebesar 325K, dan itulah flag yang kita cari.

Flag: HACKLABS{325_Kelvin}

Money Heist v2 (OSINT)

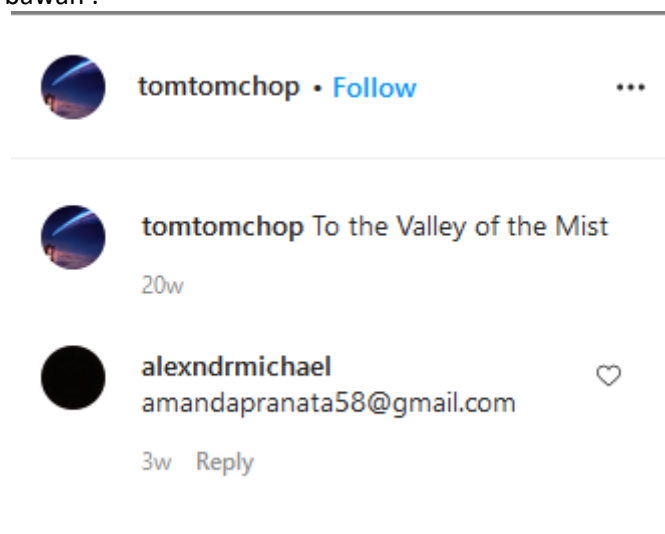


Money Heist v2, Where is She? (Easy - Med)

Masih ingatkah kalian dengan perempuan yang merupakan ketua kelompok Dali? Interpol kembali memburunya dan sebagai salah satu dari gerakan Dali, kamu harus lebih dahulu menemukan perempuan ini, dan clue yang kamu punya hanya radio comm dari markas kepolisian.

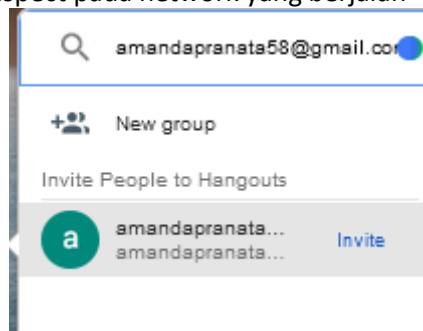
Hint 1 : email ID

Dari deskripsi challenge yang diberikan kita tahu bahwa itu berhubungan dengan email ID, dan file yang lainnya kita mendapatkan file pdf yang terlihat kosong, namun ketika menggunakan read aloud atau merubah background dari pdf tersebut, sebetulnya terdapat percakapan antara 2 orang yang akan mengarahkan kita ke akun instagram TomTomChop, dan dari akun tersebut kita dapat menemukan suatu email amandapranata58@gmail.com seperti terlihat di bawah :

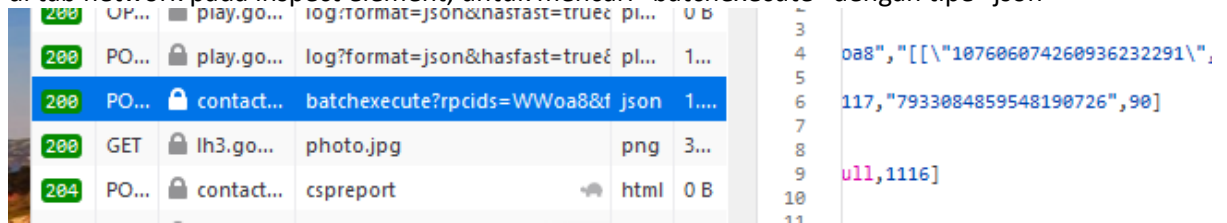


Dan dengan cara memanfaatkan google hangout kita dapat mendapatkan Google ID, terdapat cara lain jika kalian mencari "Gmail ID OSINT" tapi saya hanya membahas satu cara saja.

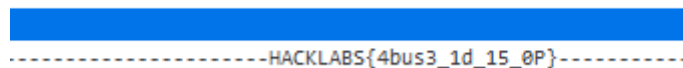
Pertama kita perlu memasukkan email dari target kita ke dalam form *Google Hangout*, kemudian kita melakukan inspect pada network yang berjalan



Kedua kita menghover mouse kita ke atas foto dari amandapranata tersebut dan kita cek lagi di tab network pada inspect element, untuk mencari "batchexecute" dengan tipe "json"



Dan voila! Kita mendapatkan Google IDnya, yaitu **107606074260936232291** selanjutnya, berdasarkan challenge kita perlu mencari di mana keberadaan terakhir dari email tersebut, artinya berhubungan dengan maps, lalu kita perlu memasukkan url seperti berikut : <https://www.google.com/maps/contrib/107606074260936232291> untuk mengakses apa yang telah direview oleh email tersebut, dan kita dapat melihat bahwa email tersebut mereview satu tempat yaitu gunung Rinjani, dan diantara simbol "-" terdapat string yang merupakan flag kita



Dan akhirnya kita mendapatkan flag kita.

HACKLABS{4bus3_1d_15_0P}