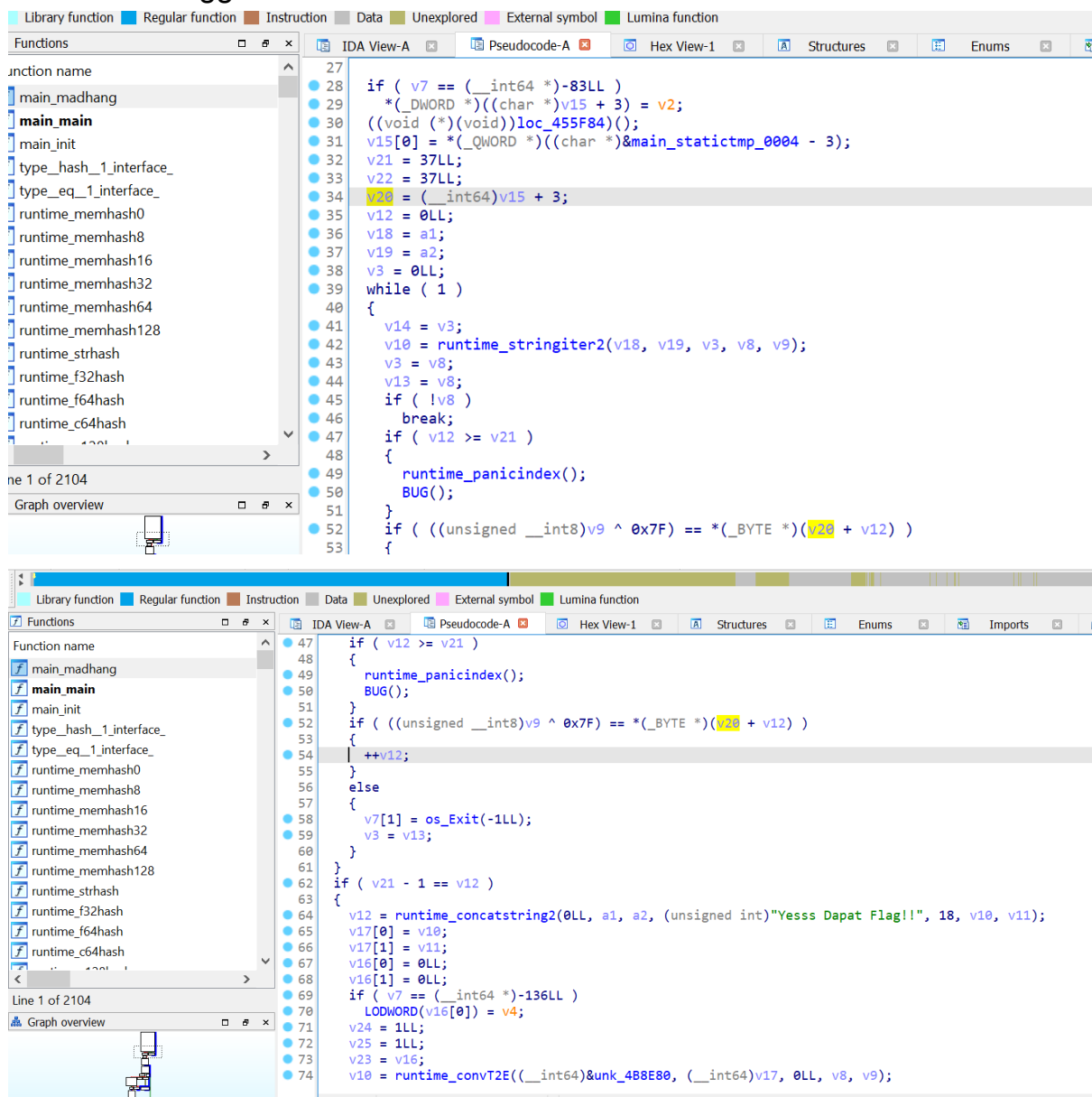


Writeup Bebas Mang

Fejka  
Maskirovka  
Kisanak

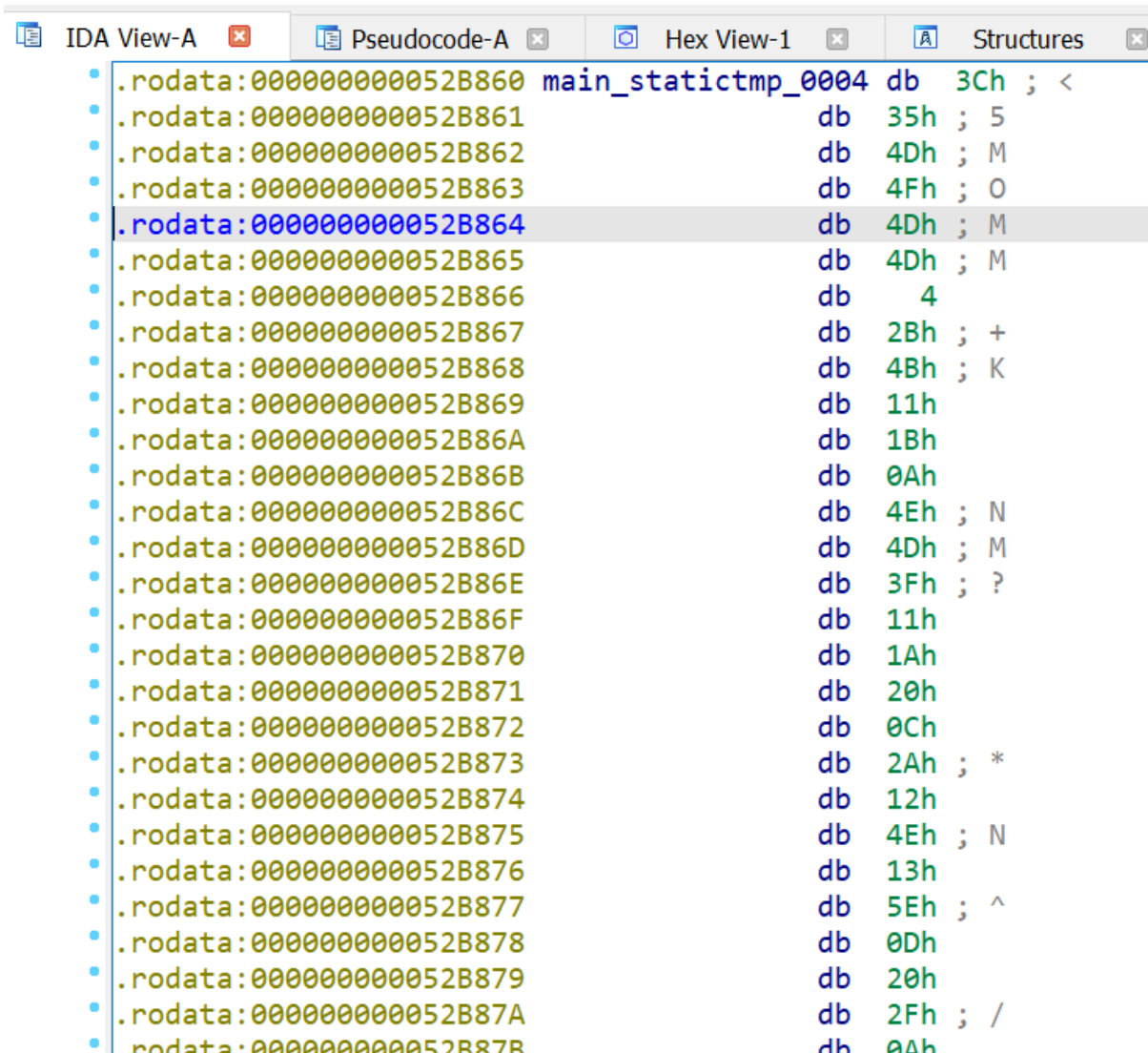
# Rev Madhang

Untuk soal madhang ini, kita diberikan sebuah executable dan langsung saja kita buka menggunakan ida.



Intinya, program dijalankan dengan cara `./madhang <flagnya>` dan jika flagnya benar, maka akan muncul string `Yesss Dapat Flag!!`. Yang perlu kita perhatikan adalah ada komparasi dimana `v9` yang sepertinya inputan akan di XOR dengan `0x7F` dan akan dibandingkan dengan `v20`. `V20` sendiri merujuk

kepada v15 yang memanggil main\_statictmp\_0004. Kita lihat isi dari main\_statictmp\_0004



```
.rodata:000000000052B860 main_statictmp_0004 db 3Ch ; <
.rodata:000000000052B861 db 35h ; 5
.rodata:000000000052B862 db 4Dh ; M
.rodata:000000000052B863 db 4Fh ; O
.rodata:000000000052B864 db 4Dh ; M
.rodata:000000000052B865 db 4Dh ; M
.rodata:000000000052B866 db 4
.rodata:000000000052B867 db 2Bh ; +
.rodata:000000000052B868 db 4Bh ; K
.rodata:000000000052B869 db 11h
.rodata:000000000052B86A db 1Bh
.rodata:000000000052B86B db 0Ah
.rodata:000000000052B86C db 4Eh ; N
.rodata:000000000052B86D db 4Dh ; M
.rodata:000000000052B86E db 3Fh ; ?
.rodata:000000000052B86F db 11h
.rodata:000000000052B870 db 1Ah
.rodata:000000000052B871 db 20h
.rodata:000000000052B872 db 0Ch
.rodata:000000000052B873 db 2Ah ; *
.rodata:000000000052B874 db 12h
.rodata:000000000052B875 db 4Eh ; N
.rodata:000000000052B876 db 13h
.rodata:000000000052B877 db 5Eh ; ^
.rodata:000000000052B878 db 0Dh
.rodata:000000000052B879 db 20h
.rodata:000000000052B87A db 2Fh ; /
.rodata:000000000052B87B db 0Ah
```

Nah kita coba kumpulkan bytes2 dalam main\_statictmp\_0004 tadi dan tiap bytesnya kita xor dengan 0x7f. Maka dengan script berikut ini:

```
a =
['3C', '35', '4D', '4F', '4D', '4D', '04', '2B', '4B', '11', '1B', '0A',
'4E', '4D', '3F', '11', '1A', '20', '0C', '2A', '12', '4E', '13', '5E', '
0D', '20', '2F', '0A', '4F', '4F', '4F', '4F', '33', '33', '33', '02', '7
5']
for i in a:
    print(chr(int(i, 16) ^ 0x7f), end="")
```

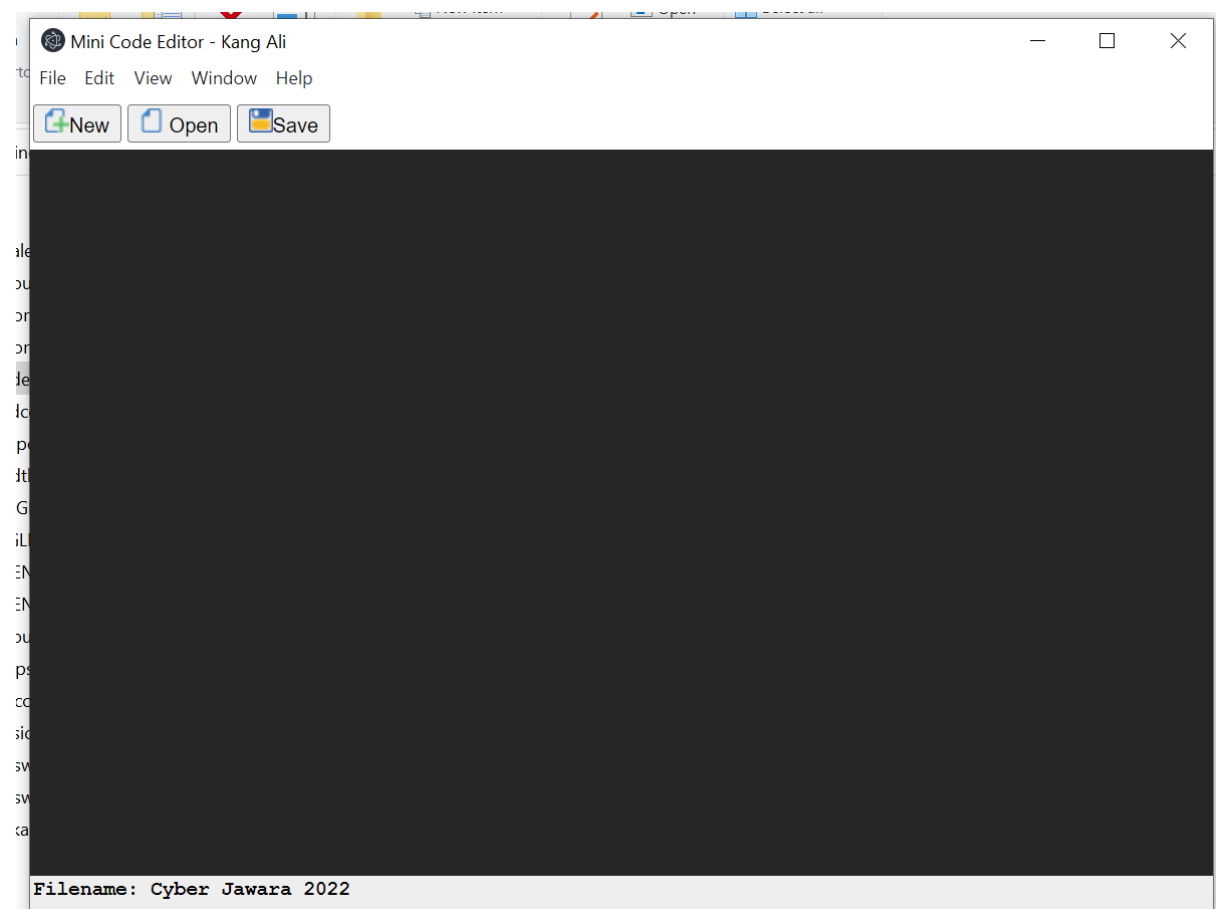
Bisa kita dapatkan flagnya

```
$ python3 solve.py  
CJ2022{T4ndu12@ne_sUm1l!r_Pu0000LLL}
```

**Flag = CJ2022{T4ndu12@ne\_sUm1l!r\_Pu0000LLL}**

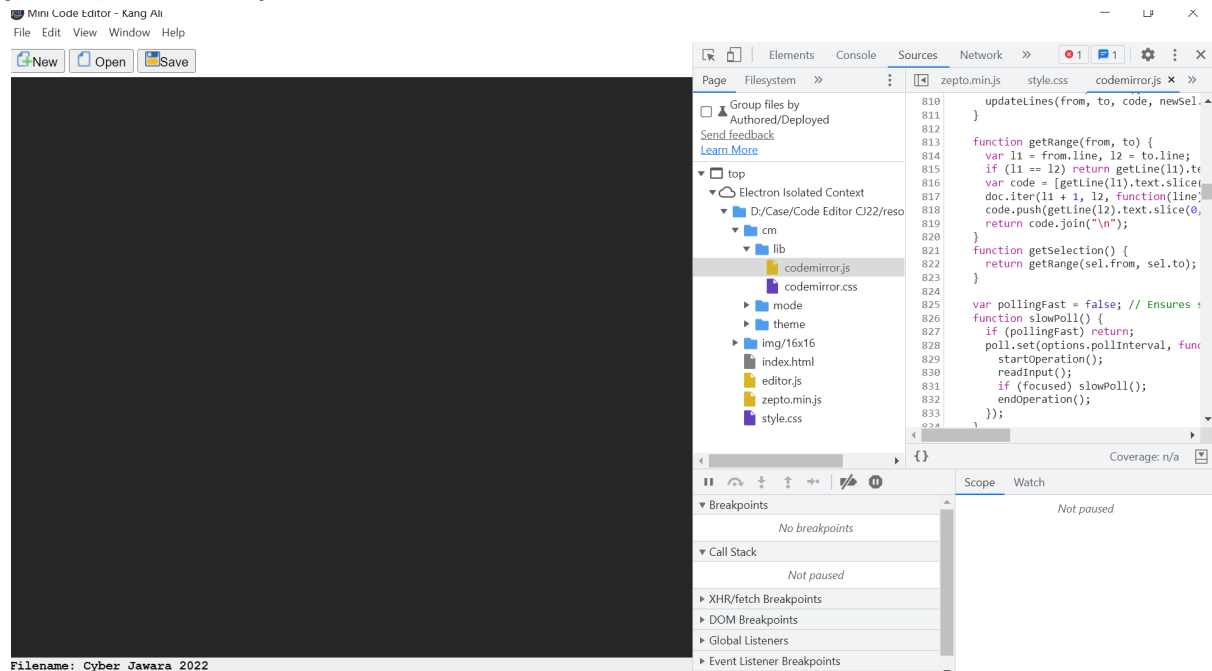
### Aplikasi Apa tuh?

Untuk soal ini, kita diberikan file msi (windows installer). Awalnya kami berpikir bahwa ketika melakukan instalasi terdapat proses background mencurigakan yang berjalan, maka kami menggunakan procmon untuk memonitor namun hasilnya nihil. Karena itu, kami menganalisis folder hasil instalasi program tersebut.



Pada program exe yang terinstall, tombol2 tersebut tidak bereaksi apapun

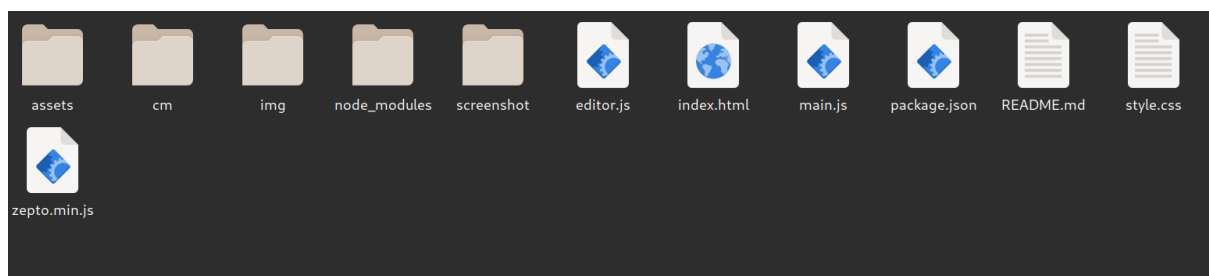
ketika ditekan. Namun pada opsi view terdapat toggle developer tools yang jika dipilih hasilnya seperti ini.



Ada nama2 file yang mengindikasikan bahwa ini merupakan electron app (sebenarnya bisa dilihat dari icon exenya juga cuma ga sadar, oh well.). Karena itu, kami menggunakan referensi ini untuk mereverse electron app.

<https://www.doyler.net/security-not-included/reverse-electron-apps-eversecme-et>

Setelah menginstall asar dengan command `npm install -g asar`, kami mengekstrak file app.asar yang ada pada folder `/resources/` hasilnya adalah terekstrak file2 baru.



Setelah mengenumerasi sesaat, kami menemukan flagnya pada folder screenshot berbentuk file png.

/\*\*

This Challenge Tribute To

*Pak Iwan Sumantri*

Dedication for Cyber Jawara

CJ2022{Tribut3\_to\_P4k\_lw@n\_So3ma4ntr!}

\*/

**Flag = CJ2022{Tribut3\_to\_P4k\_lw@n\_So3ma4ntr!}**

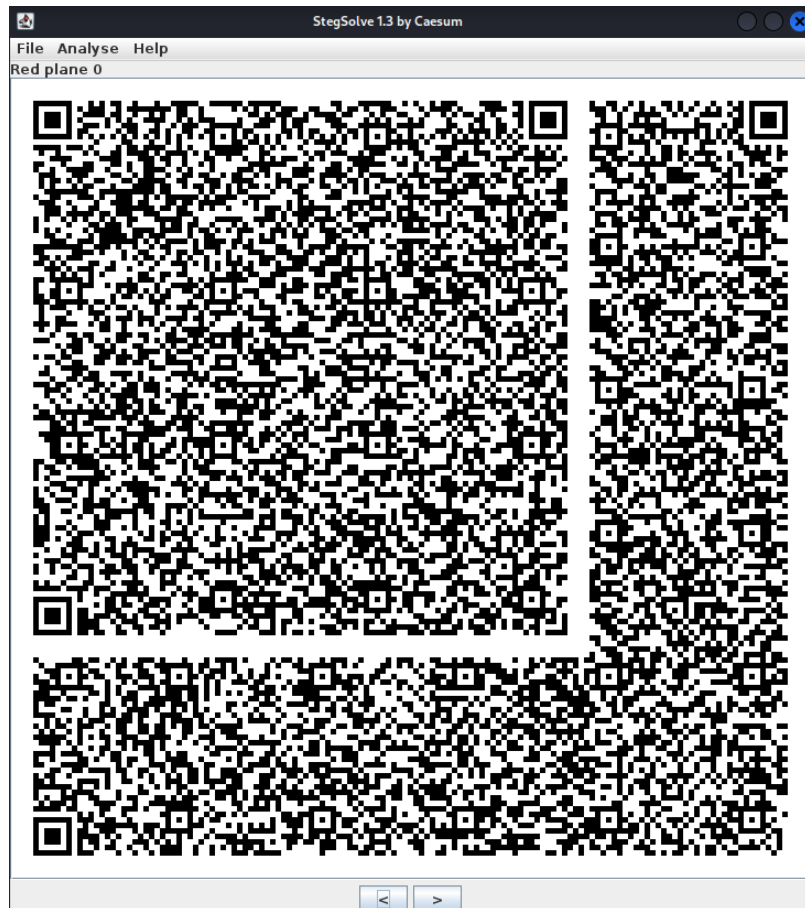
Misc

**Kui R Kode?**

Untuk soal ini, kita diberikan gambar barcode, namun ketika discan langsung terdapat binary yg jika ditranslate mengatakan bahwa bukan di situ flagnya.

```
zbarimg Kui R Kode.png
QR-Code:01000111 01100001 01101000 01101111 01101000 01101011 01100001 01100011 01100001 00100000 01100001 01
1101110 00100000 01110011 01100101 01110000 01110101 01110000 01110101 01101110 01100101 00100000 01100101 01
1100100 01100001 01101000 00100000 01110011 01100001 01101101 01100001 00100000 01000001 01100010 01101001 01
1100001 00100000 01000001 01110010 01101010 01110101 01101110 01100001 00101110 00100000 01010011 01100001 01
1100100 01101001 01101110 01110100 01100101 01101110 00100000 01000001 01100010 01101001 01101101 01100001 01
1101011 01100001 01101100 01101001 01101000 00100000 01010101 01110100 01100001 01110010 01101001 00100000 01
1100111 01101011 01101001 01101110 01100111 00100000 01101011 01100101 01110010 01100001 01101010 01100001 01
0101100 00100000 01110000 01100001 01110011 00100000 01101110 01101001 01101011 01110101 00100000 01000001 01
1100001 01101011 01110101 00100000 01110100 01100001 01110011 01100101 01101000 00100000 01110000 01100101 01
1100001 01100100 01100001 01101000 01100001 01101100 00100000 01000001 01100010 01101001 01101101 01100001 01
0100000 01101110 01101001 01101011 01100001 01101000 00100000 01101011 01100001 01101100 01101001 01100001 01
1100100 01100001 01110010 01101001 00100000 01110000 01110101 01110100 01110010 01101001 00100000 01000110 01
1100001 00100000 01110100 01101001 01100100 01100001 01101011 00100000 01100001 01100100 01100001 00100000 01
110111 01100001 01101110 00101110
scanned 1 barcode symbols from 1 images in 0.4 seconds
```

Maka kami menggunakan stegsolve untuk mencari barangkali ada clue2 tersembunyi ketika warnanya dishift. Dan benar saja kita menemukan ini:



Rupanya ada QR kecil yang tersisip dalam Qr besarnya. Langsung saja kita save dan scan qr kecilnya.



```
!- $ zbarimg inner.png
QR-Code:Gatotkaca arab kalian sepupune engkang gadah sama Abimayu putra Arjuna. Sawijining dinten Abimayu nikah kalih Utari putra sangking kerajaan Wirata, pa
aka. Padahal Abimayu sampun nikah kalian Sitisundari putri Saka Kresna.Sitisundari engkang diitipne teng istana Gatotkaca mireng nek Abimayu nikah maleh. Pa
alabendana, ngajak Abimayu wangsul. Hal niku damel Utari cemburu. Abimayu kepeksan matur nek mpun sesomah kecobo kalian utari. Mulai benjeng Arjuna badhe mati
ndana nemono Gatotkaca, CJ2022W0ng_j00wo_oJo_il4n9_J0wO_N3 ngaturake sikape Abimayu. Nanging malah diseneni, amergi kewanen nyampuri urusane sepupune iku. Gat
he Kalabendana. Senajan kelakun niku wau mboten sengaja, nanging damel Paklike mati saknalika.
scanned 1 barcode symbols from 1 images in 0.11 seconds
```

Namun karena kurawalnya hilang, maka kita wrap sendiri dengan {.\*}

**Flag = CJ2022{W0ng\_j00wo\_oJo\_il4n9\_J0wO\_N3}**