

**[ONLINE - PENYISIHAN]**

**TNI - JAKARTA**

**Nama Team : IoT**

**Ketua Team**

Didit Dwi Aftianto

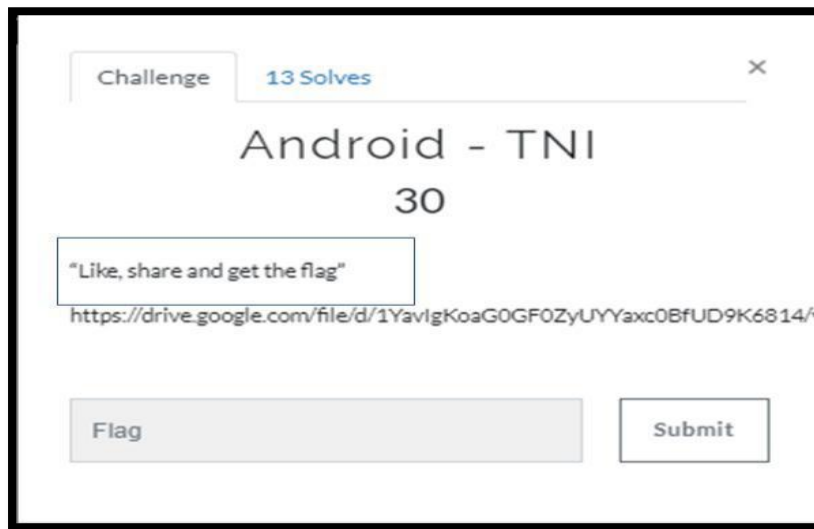
**Anggota**

Rusly Tomagola  
Abdullah Iksan  
Zaenudin

3 November 2019

# KKSI KOMPETISI KOMUNITAS SIBER INDONESIA

## Android-TNI



Download :

<https://drive.google.com/file/d/1YavIgKoaG0GF0ZyUYyaxc0BfUD9K6814/view>

Diberikan sebuah file APK bernama `_KKSI_.apk`, selanjutnya melakukan verifikasi file `_KKSI_.apk`

\$ `file _KKSI_.apk`

`_KKSI_.apk`: Zip archive data, at least v2.0 to extract

APK memang hanya sebuah arsip berbentuk ZIP dan format dasarnya adalah JAR. Tetapi isi sebenarnya dari arsip .zip disusun sedemikian rupa untuk menjadi aplikasi yang sebenarnya karena didalamnya tersimpan berbagai macam file.

Banyak cara untuk membuka file tersebut.

# KKSI

## KOMPETISI KOMUNITAS SIBER INDONESIA

Langkah 1, membuka dengan menggunakan **apktool** (a tool for reengineering Android apk files)

```
Apktool v2.4.0 - a tool for reengineering Android apk files
with smali v2.2.6 and baksmali v2.2.6
Copyright 2014 Ryszard Wiśniewski <brut.all@gmail.com>
Updated by Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
  -advance,--advanced    prints advance information.
  -version,--version      prints the version then exits
usage: apktool if|install-framework [options] <framework.apk>
  -p,--frame-path <dir>  Stores framework files into <dir>.
  -t,--tag <tag>         Tag frameworks using <tag>.
usage: apktool d[ecode] [options] <file_apk>
  -f,--force             Force delete destination directory.
  -o,--output <dir>      The name of folder that gets written. Default is apk.out
  -p,--frame-path <dir>  Uses framework files located in <dir>.
  -r,--no-res            Do not decode resources.
  -s,--no-src            Do not decode sources.
  -t,--frame-tag <tag>   Uses framework files tagged by <tag>.
usage: apktool b[uild] [options] <app_path>
  -f,--force-all        Skip changes detection and build all files.
  -o,--output <dir>      The name of apk that gets written. Default is dist/name.apk
  -p,--frame-path <dir>  Uses framework files located in <dir>.

For additional info, see: http://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali
```

\$ **apktool d \_KKSI\_.apk -o androtni/**

```
I: Using Apktool 2.4.0 on _KKSI_.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/dontukulesto/Library/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

setelah selesai mendecode file **\_KKSI\_.apk** tersebut, maka dapat dilihat pada folder **androtni** yang berisikan **1188 direktori** dan **17399 berkas**.

Tidak ada informasi tambahan pada soal, hanya "**Like, share and get the flag**" dan itu akan kita jadikan sebagai kata kunci pencarian didalam folder dan file dengan menggunakan perintah **grep** pada direktori kerja **androtni** dengan beberapa tambahan perintah.

- n        untuk menampilkan nomer line pada kata yang dicari.
- r        untuk mencari didalam folder.
- .        adalah direktori kerja.

# KKSI

## KOMPETISI KOMUNITAS SIBER INDONESIA

Dimulai dari kata kunci pertama "**Like**"

```
$ grep -nr "like*" . | more
```

tidak ada hasil yang sesuai keinginan

```
$ grep -nr "share*" . | more
```

```
./res/values-zh/strings.xml:37: <string name="shareSiteSubject">网站分享</string>
./res/values-uk/strings.xml:17: <string name="abc_shareactionprovider_share_with">Надіслати через</string>
./res/values-uk/strings.xml:18: <string name="abc_shareactionprovider_share_with_application">Поділитися через додаток %s</string>
./res/values-uk/strings.xml:64: <string name="shareContentSubject">Get this cool Android App</string>
./res/values-sr/strings.xml:17: <string name="abc_shareactionprovider_share_with">Дели са</string>
./res/values-sr/strings.xml:18: <string name="abc_shareactionprovider_share_with_application">Делење са апликацијом %s</string>
./res/values-sr/strings.xml:64: <string name="shareContentSubject">Get this cool Android App</string>
./res/raw/configuration.xml:38: <shareExtraLink>KKSI2019{7093571a3d4d9f735126b252a332eb6a}</shareExtraLink>
./res/values-pa/strings.xml:17: <string name="abc_shareactionprovider_share_with">ਸਿ ਤੁ ਤ ਸੰ ਝ ਭੇ</string>
./res/values-pa/strings.xml:18: <string name="abc_shareactionprovider_share_with_application">%s ਤੁ ਤ ਸੰ ਝ ਭੇ</string>
./res/values-si/strings.xml:17: <string name="abc_shareactionprovider_share_with">සමඟ බෙදා හරින්න</string>
./res/values-si/strings.xml:18: <string name="abc_shareactionprovider_share_with_application">%s සමඟ බෙදා හරින්න</string>
./res/values-b+sr+Latn/strings.xml:17: <string name="abc_shareactionprovider_share_with">Deli sa</string>
./res/values-b+sr+Latn/strings.xml:18: <string name="abc_shareactionprovider_share_with_application">Deljenje sa aplikacijom %s</string>
```

kata kunci "**share**" tersebut membuahkan hasil meskipun harus sangat teliti membacanya.

```
./res/raw/configuration.xml:38:
```

```
<shareExtraLink>KKSI2019{7093571a3d4d9f735126b252a332eb6a}
</s
```

```
hareExtraLink>
```

kalimat tersebut terdapat pada subdirektori **res** yaitu **raw** dengan namafile **configuration.xml** dan terletak pada line **38**

Langkah 2, membuka file dengan **7-Zip**.

x adalah perintah untuk mengeluarkan file

-o adalah nama direktori untuk hasil keluar file

```
$ 7za x _KKSI_.apk -oandroidtni/
```

```
7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=utf8,Utf16=on,HugeFiles=on,64 bits,4 CPUs x64)
```

```
Scanning the drive for archives:
1 file, 14265377 bytes (14 MiB)
```

```
Extracting archive: _KKSI_.apk
```

```
---
Path = _KKSI_.apk
Type = zip
Physical Size = 14265377
```

```
Everything is Ok
```

```
Files: 1110
Size: 28705148
Compressed: 14265377
```



# KKSI

## KOMPETISI KOMUNITAS SIBER INDONESIA

\$ grep -nr "share\*" . | more

```
Binary file ./resources.arsc matches
Binary file ./res/anim/abc_popup_enter.xml matches
Binary file ./res/anim/abc_grow_fade_in_from_bottom.xml matches
Binary file ./res/anim/abc_shrink_fade_out_from_bottom.xml matches
Binary file ./res/anim/abc_popup_exit.xml matches
./res/raw/configuration.xml:38: <shareExtraLink>KKSI2019{7093571a3d4d9f735126b252a332eb6a}</shareExtraLink>
./META-INF/MANIFEST.MF:249:Name: res/drawable-hdpi/abc_ab_share_pack_mtrl_alpha.9.png
./META-INF/MANIFEST.MF:441:Name: res/drawable-hdpi/outline_share_black_24.png
./META-INF/MANIFEST.MF:519:Name: res/drawable-mdpi/abc_ab_share_pack_mtrl_alpha.9.png
./META-INF/MANIFEST.MF:603:Name: res/drawable-mdpi/abc_ic_menu_share_mtrl_alpha.png
./META-INF/MANIFEST.MF:630:Name: res/drawable-xhdpi/abc_ic_menu_share_mtrl_alpha.png
./META-INF/MANIFEST.MF:899:Name: res/drawable-hdpi/abc_ic_menu_share_mtrl_alpha.png
./META-INF/MANIFEST.MF:950:Name: res/drawable-mdpi/outline_share_black_24.png
./META-INF/MANIFEST.MF:1152:Name: res/drawable-xxhdpi/outline_share_black_24.png
./META-INF/MANIFEST.MF:1528:Name: res/drawable-xhdpi/abc_ab_share_pack_mtrl_alpha.9.png
./META-INF/MANIFEST.MF:1693:Name: res/drawable-hdpi/ic_share_black_24dp.png
./META-INF/MANIFEST.MF:1836:Name: res/drawable-mdpi/ic_share_black_24dp.png
./META-INF/MANIFEST.MF:1945:Name: res/drawable-xxxhdpi/outline_share_black_24.png
./META-INF/MANIFEST.MF:2315:Name: res/drawable-xhdpi/ic_share_black_24dp.png
./META-INF/MANIFEST.MF:2387:Name: res/drawable-xxhdpi/abc_ic_menu_share_mtrl_alpha.png
./META-INF/MANIFEST.MF:2483:Name: res/drawable-xxxhdpi/ic_share_black_24dp.png
./META-INF/MANIFEST.MF:2729:Name: res/drawable-xhdpi/outline_share_black_24.png
./META-INF/MANIFEST.MF:2795:Name: res/drawable-xxxhdpi/abc_ic_menu_share_mtrl_alpha.png
./META-INF/MANIFEST.MF:3075:Name: res/drawable-xxhdpi/abc_ab_share_pack_mtrl_alpha.9.png
./META-INF/MANIFEST.MF:3338:Name: res/drawable-xxhdpi/ic_share_black_24dp.png
./META-INF/ANDROID_ID._SF:251:Name: res/drawable-hdpi/abc_ab_share_pack_mtrl_alpha.9.png
./META-INF/ANDROID_ID._SF:443:Name: res/drawable-hdpi/outline_share_black_24.png
./META-INF/ANDROID_ID._SF:521:Name: res/drawable-mdpi/abc_ab_share_pack_mtrl_alpha.9.png
./META-INF/ANDROID_ID._SF:605:Name: res/drawable-mdpi/abc_ic_menu_share_mtrl_alpha.png
./META-INF/ANDROID_ID._SF:632:Name: res/drawable-xhdpi/abc_ic_menu_share_mtrl_alpha.png
./META-INF/ANDROID_ID._SF:901:Name: res/drawable-hdpi/abc_ic_menu_share_mtrl_alpha.png
./META-INF/ANDROID_ID._SF:952:Name: res/drawable-mdpi/outline_share_black_24.png
./META-INF/ANDROID_ID._SF:1154:Name: res/drawable-xxhdpi/outline_share_black_24.png
./META-INF/ANDROID_ID._SF:1530:Name: res/drawable-xhdpi/abc_ab_share_pack_mtrl_alpha.9.png
./META-INF/ANDROID_ID._SF:1695:Name: res/drawable-hdpi/ic_share_black_24dp.png
./META-INF/ANDROID_ID._SF:1838:Name: res/drawable-mdpi/ic_share_black_24dp.png
./META-INF/ANDROID_ID._SF:1947:Name: res/drawable-xxxhdpi/outline_share_black_24.png
./META-INF/ANDROID_ID._SF:2317:Name: res/drawable-xhdpi/ic_share_black_24dp.png
./META-INF/ANDROID_ID._SF:2389:Name: res/drawable-xxhdpi/abc_ic_menu_share_mtrl_alpha.png
./META-INF/ANDROID_ID._SF:2485:Name: res/drawable-xxxhdpi/ic_share_black_24dp.png
./META-INF/ANDROID_ID._SF:2731:Name: res/drawable-xhdpi/outline_share_black_24.png
./META-INF/ANDROID_ID._SF:2797:Name: res/drawable-xxxhdpi/abc_ic_menu_share_mtrl_alpha.png
./META-INF/ANDROID_ID._SF:3077:Name: res/drawable-xxhdpi/abc_ab_share_pack_mtrl_alpha.9.png
./META-INF/ANDROID_ID._SF:3340:Name: res/drawable-xxhdpi/ic_share_black_24dp.png
Binary file ./classes2.dex matches
Binary file ./classes.dex matches
Binary file ./lib/armeabi-v7a/libmodpdfium.so matches
Binary file ./lib/arm64-v8a/libmodpdfium.so matches
```

FLAG : KKSI2019{7093571a3d4d9f735126b252a332eb6a}

# KKSI KOMPETISI KOMUNITAS SIBER INDONESIA

## Crypto

### OBFUS-TNI

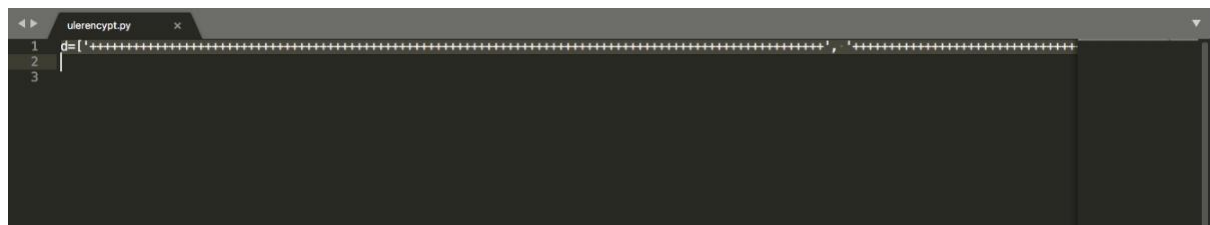
Can Python code be Protected

Download file di

[https://drive.google.com/open?id=1S3XTZ8ZKJIG\\_TfFOCycctLE5CIK4EFS9G](https://drive.google.com/open?id=1S3XTZ8ZKJIG_TfFOCycctLE5CIK4EFS9G)

Format Flag : KKSI2019{flag}

Setelah di download dan di buka dengan arsip manager terdapat 1 buah script python yang terproteksi dalam 1 line agar sulit dibaca.



Ketika di jalankan akan muncul sebuah pesan error

*File "main.py", line 8*

*print "KKSI 2019 - TNI ANGKATAN DARAT"*

*SyntaxError: Missing parentheses in call to 'print'*



# KKSI KOMPETISI KOMUNITAS SIBER INDONESIA

Mencoba untuk merapihkan kode tersebut secara manual juga tetap akan muncul pesan error tersebut.

```
523 '+++++',
524 '+++++',
525 '+++++',
526 '+++++',
527 '+++++',
528 '+++++',
529 '+++++',
530 '+++++',
531 '+++++',
532 '+++++',
533 '+++++',
534 '+++++',
535 '+++++',
536 '+++++',
537 '+++++',
538 '+++++',
539 '+++++',
540 '+++++',
541 '+++++',
542 '+++++',
543 '+++++',
544 '+++++'];
545 exec(''.join([chr(len(i)) for i in d]))
546
547
```

Mencoba merapihkan dengan Stream Editor yang ada pada linux untuk melakukan pergantian teks manipulasi tanpa harus membukanya.

Dengan perintah sebagai berikut:

**\$ cat ulerencypt.py | sed 's/exec/print/' | python**

Hasil dari perintah tersebut:

```
from datetime import datetime

KKSI = [75, 75, 83, 73, 50, 48, 49, 57, 123, 101, 55, 98, 102, 52, 100, 100, 53, 49, 97, 101, 53, 57, 99, 97]
TNIAD = [49, 53, 54, 101, 102, 55, 52, 56, 99, 48, 100, 49, 48, 48, 56, 57, 99, 125]

def main():
    print "KKSI 2019 - TNI ANGKATAN DARAT"
    input = raw_input("Cek Waktu: ").strip()
    merdeka = ""
    for i in TNIAD:
        merdeka += chr(i)

    if input == merdeka:
        indonesia = ""
        for i in KKSI:
            indonesia += chr(i)
        print indonesia
    else:
        print datetime.now()

if __name__ == '__main__':
    main()
```

Setelah mendapatkan kode asli dari script python yang terproteksi, jika kembali kepada pesan error pada line 8 yang muncul sebelum kode tersebut dirapihkan, maka terlihat jelas ada beberapa fungsi yang salah dalam penulisan.



# KKSI

## KOMPETISI KOMUNITAS SIBER INDONESIA

```
1 from datetime import datetime
2
3 KKSI = [75, 75, 83, 73, 50, 48, 49, 57, 123, 101, 55, 98, 102, 52, 100, 100, 53, 49, 97, 101, 53, 57, 99, 97]
4 TNIAD = [49, 53, 54, 101, 102, 55, 52, 56, 99, 48, 100, 49, 48, 48, 56, 57, 99, 125]
5
6
7 def main():
8     print "KKSI 2019 - TNI ANGKATAN DARAT"
9     input = raw_input("Cek Waktu: ").strip()
10    merdeka = ""
11    for i in TNIAD:
12        merdeka += chr(i)
13
14    if input == merdeka:
15        indonesia = ""
16        for i in KKSI:
17            indonesia += chr(i)
18        print indonesia
19
20    else:
21        print datetime.now()
22
23
24
25 if __name__ == '__main__':
26     main()
27
```

setelah script tersebut dirapihkan maka fungsi-fungsi pemanggilan kode python tersebut berjalan sempurna.

```
1 from datetime import datetime
2
3 KKSI = [75, 75, 83, 73, 50, 48, 49, 57, 123, 101, 55, 98, 102, 52, 100, 100, 53, 49, 97, 101, 53, 57, 99, 97]
4 TNIAD = [49, 53, 54, 101, 102, 55, 52, 56, 99, 48, 100, 49, 48, 48, 56, 57, 99, 125]
5
6
7 def main():
8     print "KKSI 2019 - TNI ANGKATAN DARAT"
9     input = raw_input("Cek Waktu: ").strip()
10
11    merdeka = ""
12    indonesia = ""
13
14    if input == "merdeka":
15        for i in TNIAD:
16            merdeka += chr(i)
17        print merdeka
18    elif input == "indonesia":
19        for i in KKSI:
20            indonesia += chr(i)
21        print indonesia
22    else:
23        print datetime.now()
24
25 if __name__ == '__main__':
26     main()
27
```

jika menginputkan kata **merdeka**, maka fungsi pemanggilan akan mendecode charcode yang berada dalam **TNIAD**, jika menginputkan kata **indonesia**, maka fungsi pemanggilan akan mendecode charcode yang berada dalam **KKSI**.



# KKSI KOMPETISI KOMUNITAS SIBER INDONESIA

**\$ python ulerencypt.py**

KKSI 2019 - TNI ANGKATAN DARAT  
Cek Waktu: indonesia  
KKSI2019{e7bf4dd51ae59ca

**\$ python ulerencypt.py**

KKSI 2019 - TNI ANGKATAN DARAT  
Cek Waktu: merdeka  
156ef748c0d10089c}

FLAG : **KKSI2019{e7bf4dd51ae59ca156ef748c0d10089c}**

# KKSI

## KOMPETISI KOMUNITAS SIBER INDONESIA

### REVERSING

#### Bongkar Password - TNI

Diberikan sebuah file binary bernama **rev\_word** dengan hasil verifikasi nya

**rev\_word: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=a3357176a9630f7e655d9b11e041d96c4e87f688, not stripped**

ELF binary-format yang diberikan menggunakan arsitektur 64-bit, agar dapat di jalankan maka harus merubah modenya dengan **chmod a+x rev\_word**. Ketika program dijalankan mengeluarkan sebuah pesan:

```
$ ./rev_word
```

Flag: ./rev\_word [Cari Dulu Ya :D]

Selanjutnya melakukan analisa statis terhadap binary ELF tersebut dengan **gdb**

```
$ gdb -q rev_word
```

Selanjutnya melakukan **disassembly** pada fungsi **main**

```
add pdbs pdisas main
Dump of assembler code for function main:
0x00000000000000c0 <+0v>: push rbp
0x00000000000000c1 <+1v>: mov rbp, rsp
0x00000000000000c4 <+4v>: sub rsp, 0x30
0x00000000000000c8 <+8v>: mov DWORD PTR [rbp-0x24], edi
0x00000000000000cb <+11v>: mov QWORD PTR [rbp-0x30], rsi
0x00000000000000cf <+15v>: mov rax, QWORD PTR fs:0x28
0x00000000000000d8 <+24v>: mov QWORD PTR [rbp-0x8], rax
0x00000000000000dc <+28v>: xor eax, eax
0x00000000000000de <+30v>: cmp QWORD PTR [rbp-0x24], 0x2
0x00000000000000e2 <+34v>: je 0x909 <main+73>
0x00000000000000e4 <+36v>: mov rax, QWORD PTR [rbp-0x30]
0x00000000000000e8 <+40v>: mov rax, QWORD PTR [rax]
0x00000000000000eb <+43v>: mov rsi, rax
0x00000000000000ee <+46v>: lea rdi, [rip+0x173] # 0xa68
0x00000000000000f5 <+53v>: mov eax, 0x0
0x00000000000000fa <+58v>: call 0x650 <printf@plt>
0x00000000000000ff <+63v>: mov eax, 0x1
0x00000000000000904 <+68v>: jmp 0x9c1 <main+257>
0x00000000000000909 <+73v>: mov BYTE PTR [rbp-0x15], 0x45
0x0000000000000090d <+77v>: mov BYTE PTR [rbp-0x14], 0x27
0x00000000000000911 <+81v>: mov BYTE PTR [rbp-0x13], 0x74
0x00000000000000915 <+85v>: mov BYTE PTR [rbp-0x12], 0x25
0x00000000000000919 <+89v>: mov BYTE PTR [rbp-0x11], 0x64
0x0000000000000091d <+93v>: mov BYTE PTR [rbp-0x10], 0x42
0x00000000000000921 <+97v>: mov BYTE PTR [rbp-0xf], 0x58
0x00000000000000925 <+101v>: mov BYTE PTR [rbp-0xe], 0x5f
0x00000000000000929 <+105v>: mov BYTE PTR [rbp-0xd], 0x24
0x0000000000000092d <+109v>: mov BYTE PTR [rbp-0xc], 0x26
0x00000000000000931 <+113v>: mov BYTE PTR [rbp-0xb], 0x27
0x00000000000000935 <+117v>: mov BYTE PTR [rbp-0xa], 0x2f
0x00000000000000939 <+121v>: mov BYTE PTR [rbp-0x9], 0x0
0x0000000000000093d <+125v>: mov rax, QWORD PTR [rbp-0x30]
0x00000000000000941 <+129v>: add rax, 0x8
0x00000000000000945 <+133v>: mov rax, QWORD PTR [rax]
0x00000000000000948 <+136v>: mov rdi, rax
0x0000000000000094b <+139v>: call 0x7bc <xor>
0x00000000000000950 <+144v>: mov QWORD PTR [rbp-0x20], rax
0x00000000000000954 <+148v>: mov rdx, QWORD PTR [rbp-0x20]
0x00000000000000958 <+152v>: lea rax, [rbp-0x15]
```

# KKSI

## KOMPETISI KOMUNITAS SIBER INDONESIA

pada instruksi **lea** (Load Effective Address) merupakan destinasi pemanggilan kode yang harus diinputkan dengan memanggil fungsi **xor** yang menyimpan sebuah kode, dengan kata lain jika ingin menjalankan program **ELF** tersebut harus serta menginputkan kode yang benar terdapat pada instruksi **mov** yang merupakan instruksi untuk menyalin kode ke tujuan yang diinputkan tanpa mempengaruhi sumbernya.

```
0x0000000000000909 <+73>:  mov    BYTE PTR [rbp-0x15],0x45
0x000000000000090d <+77>:  mov    BYTE PTR [rbp-0x14],0x27
0x0000000000000911 <+81>:  mov    BYTE PTR [rbp-0x13],0x74
0x0000000000000915 <+85>:  mov    BYTE PTR [rbp-0x12],0x25
0x0000000000000919 <+89>:  mov    BYTE PTR [rbp-0x11],0x64
0x000000000000091d <+93>:  mov    BYTE PTR [rbp-0x10],0x42
0x0000000000000921 <+97>:  mov    BYTE PTR [rbp-0xf],0x58
0x0000000000000925 <+101>: mov    BYTE PTR [rbp-0xe],0x5f
0x0000000000000929 <+105>: mov    BYTE PTR [rbp-0xd],0x24
0x000000000000092d <+109>: mov    BYTE PTR [rbp-0xc],0x26
```

```
0x0000000000000941 <+129>: add     rax,0x8
0x0000000000000943 <+133>: mov     rax,QWORD PTR [rbp-0x4],0x27
0x0000000000000948 <+136>: mov     rdi,rax
0x000000000000094b <+139>: call    0x75c <__xchg>
0x0000000000000950 <+144>: mov     QWORD PTR [rbp-0x20],rax
0x0000000000000954 <+148>: mov     rdx,QWORD PTR [rbp-0x20]
0x0000000000000958 <+152>: lea     rax,[rbp-0x15]
0x000000000000095c <+156>: mov     rsi,rdx
0x000000000000095f <+159>: mov     rdi,rax
0x0000000000000962 <+162>: call    0x832 <cmp>
0x0000000000000967 <+167>: test    eax,eax
0x0000000000000969 <+169>: je      0x977 <main+183>
0x000000000000096b <+171>: lea     rdi,[rip+0x112] # 0xa84
0x0000000000000972 <+178>: call    0x630 <puts@plt>
0x0000000000000977 <+183>: mov     rdx,QWORD PTR [rbp-0x20]
0x000000000000097b <+187>: lea     rax,[rbp-0x15]
0x000000000000097f <+191>: mov     rsi,rdx
0x0000000000000982 <+194>: mov     rdi,rax
0x0000000000000985 <+197>: call    0x832 <cmp>
0x000000000000098a <+202>: test    eax,eax
0x000000000000098c <+204>: je      0x99c <main+220>
0x000000000000098e <+206>: lea     rdi,[rip+0x10b] # 0xaa0
0x0000000000000995 <+213>: call    0x630 <puts@plt>
0x000000000000099a <+218>: jmp     0x9a8 <main+232>
0x000000000000099c <+220>: lea     rdi,[rip+0x10d] # 0xab0
0x00000000000009a3 <+227>: call    0x630 <puts@plt>
0x00000000000009a8 <+232>: mov     rax,QWORD PTR [rbp-0x20]
0x00000000000009ac <+236>: mov     rdi,rax
0x00000000000009af <+239>: call    0x620 <free@plt>
0x00000000000009b4 <+244>: mov     QWORD PTR [rbp-0x20],0x0
0x00000000000009b8 <+252>: mov     eax,0x0
0x00000000000009bc <+257>: mov     rcx,QWORD PTR [rbp-0x8]
0x00000000000009c5 <+261>: xor     rcx,QWORD PTR fs:0x28
0x00000000000009ce <+270>: je      0x9d5 <main+277>
0x00000000000009d0 <+272>: call    0x640 <__stack_chk_fail@plt>
0x00000000000009d5 <+277>: leave
0x00000000000009d6 <+278>: ret

End of assembler dump.
gdb-peda$ x/s 0xa68
Flag: %s [Cari Dulu Ya :D]\n"
gdb-peda$
```



Analisa selanjutnya dilakukan pada fungsi **xor** yang digunakan untuk mengenkripsi kode yang tersimpan pada memory tersebut. Instruksi **XOR** menghubungkan dua nilai menggunakan logika eksklusif **OR**.

```
gdb-peda$ pdisas xor
Dump of assembler code for function xor:
0x00000000000007bc <+0>:  push    rbp
0x00000000000007bd <+1>:  mov     rbp, rsp
0x00000000000007c0 <+4>:  sub     rsp, 0x20
0x00000000000007c4 <+8>:  mov     QWORD PTR [rbp-0x18], rdi
0x00000000000007c8 <+12>: mov     rax, QWORD PTR [rbp-0x18]
0x00000000000007cc <+16>: mov     rdi, rax
0x00000000000007cf <+19>: call    0x78a <len>
0x00000000000007d4 <+24>: add     eax, 0x1
0x00000000000007d7 <+27>: cdq     q
0x00000000000007d9 <+29>: mov     esi, 0x1
0x00000000000007de <+34>: mov     rdi, rax
0x00000000000007e1 <+37>: call    0x660 <calloc@plt>
0x00000000000007e6 <+42>: mov     QWORD PTR [rbp-0x8], rax
0x00000000000007ea <+46>: mov     DWORD PTR [rbp-0xc], 0x0
0x00000000000007f1 <+53>: jmp     0x81b <xor+95>
0x00000000000007f3 <+55>: mov     eax, DWORD PTR [rbp-0xc]
0x00000000000007f6 <+58>: movsxd  rdx, eax
0x00000000000007f9 <+61>: mov     rax, QWORD PTR [rbp-0x18]
0x00000000000007fd <+65>: add     rax, rdx
0x0000000000000800 <+68>: movzxb  ecx, BYTE PTR [rax]
0x0000000000000803 <+71>: mov     eax, DWORD PTR [rbp-0xc]
0x0000000000000806 <+74>: movsxd  rdx, eax
0x0000000000000809 <+77>: mov     rax, QWORD PTR [rbp-0x8]
0x000000000000080d <+81>: add     rax, rdx
0x0000000000000810 <+84>: xor     ecx, 0x16
0x0000000000000813 <+87>: mov     edx, ecx
0x0000000000000815 <+89>: mov     BYTE PTR [rax], dl
0x0000000000000817 <+91>: add     DWORD PTR [rbp-0xc], 0x1
0x000000000000081b <+95>: mov     rax, QWORD PTR [rbp-0x18]
0x000000000000081f <+99>: mov     rdi, rax
0x0000000000000822 <+102>: call    0x78a <len>
0x0000000000000827 <+107>: cmp     DWORD PTR [rbp-0xc], eax
0x000000000000082a <+110>: jl      0x7f3 <xor+55>
0x000000000000082c <+112>: mov     rax, QWORD PTR [rbp-0x8]
0x0000000000000830 <+116>: leave
0x0000000000000831 <+117>: ret
End of assembler dump.
gdb-peda$
```

Pada instruksi **xor** terdapat **ecx (EXTENDED COUNT REGISTER)** dari hasil disassemble diketahui akan melakukan looping dan melakukan xor pada setiap looping-nya dengan nilai 0x16

**0x0000000000000810 <+84>: xor ecx,0x16**



# KKSI KOMPETISI KOMUNITAS SIBER INDONESIA

Untuk mendapatkan flag, kita dapat melakukan xor ulang terhadap nilai diatas dengan nilai 0x16 setiap byte-nya.

```
Python 2.7.17 (default, Oct 19 2019, 23:36:22)
[GCC 9.2.1 20191008] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> flag = []
>>> for i in '\x45\x27\x74\x25\x64\x42\x58\x5f\x24\x26\x27\x2f' :
...     flag.append(chr(ord(i) ^ 0x16))
...
>>> print "".join(flag)
S1b3rTNI2019
>>>
```

Menghasilkan sebuah kalimat **S1b3rTNI2019**, setelah itu dimasukkan menjadi sebuah jawaban flag.

```
gdb-peda$ r S1b3rTNI2019
Starting program: /root/Downloads/rev_word S1b3rTNI2019
Hore Ternyata ini Flag Nya
This Key : 22
[Inferior 1 (process 7040) exited normally]
Warning: not running
gdb-peda$
```

FLAG : **KKSI2019{S1b3rTNI2019}**