

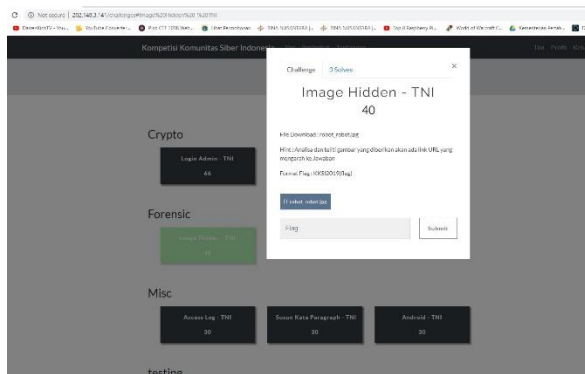


**NAMA TIM : [Broken of Jarvis - TNI]**

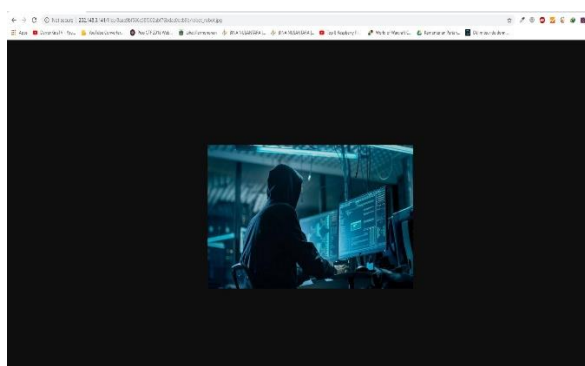
<b>Ketua Tim</b>	
1.	Teuku Rizliansyah
<b>Member</b>	
1.	Achmad Irvan Z
2.	Agung Saputra Chair Lages
3.	Achmad Wahyudi

**IMAGE HIDDEN – TNI**

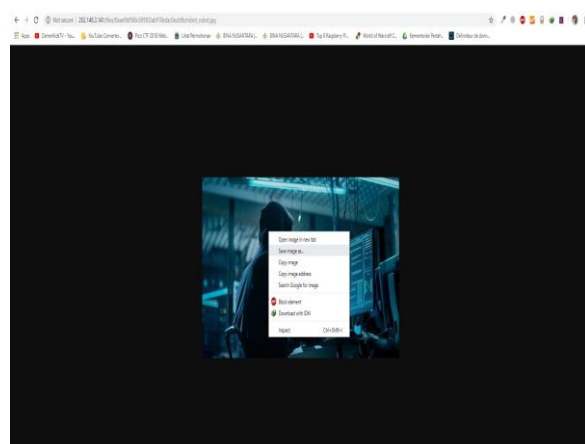
1



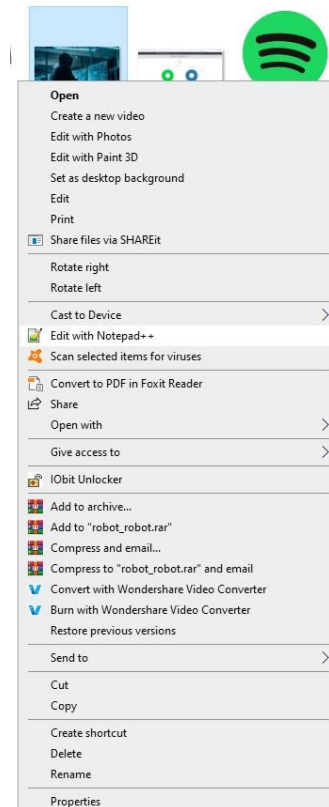
2



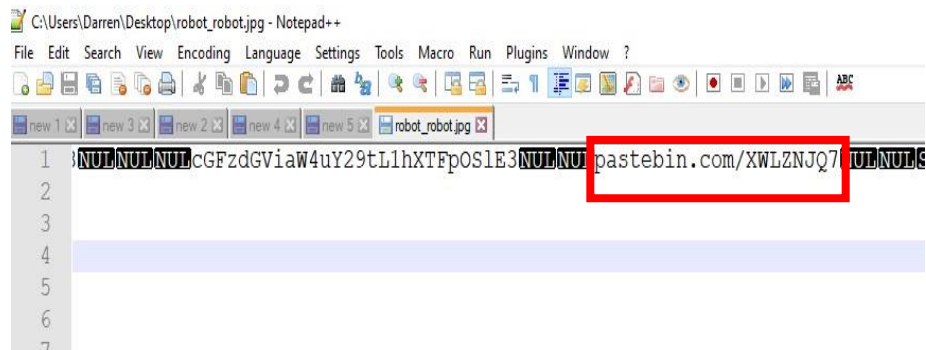
3



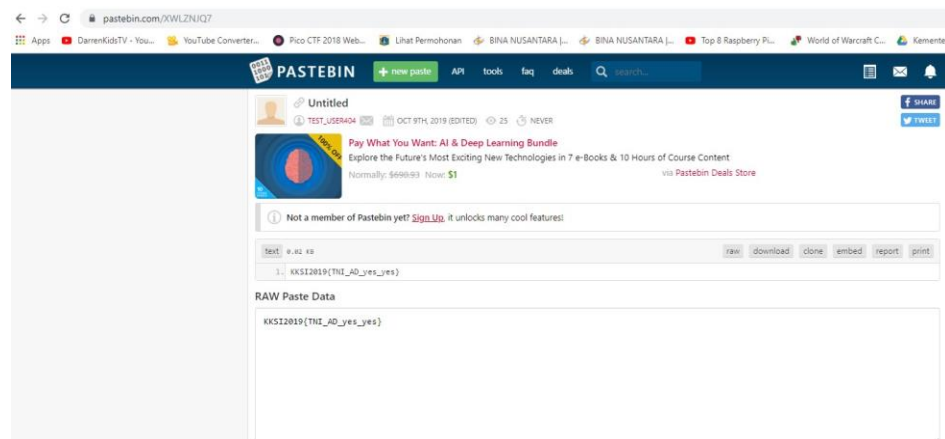
4



5



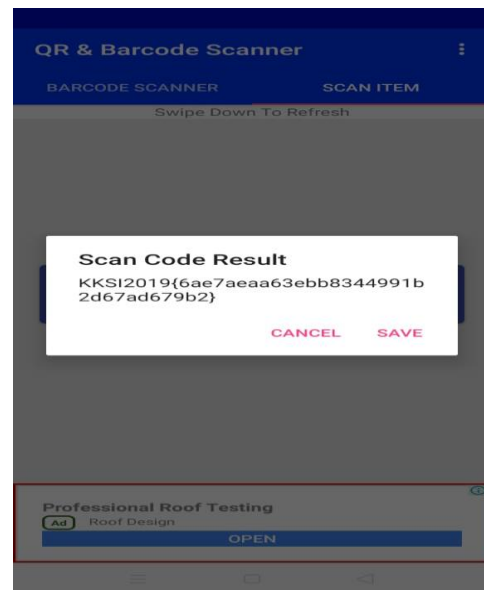
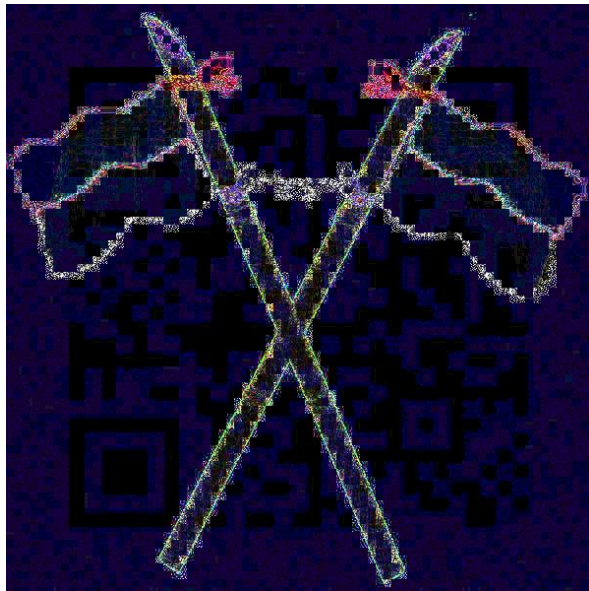
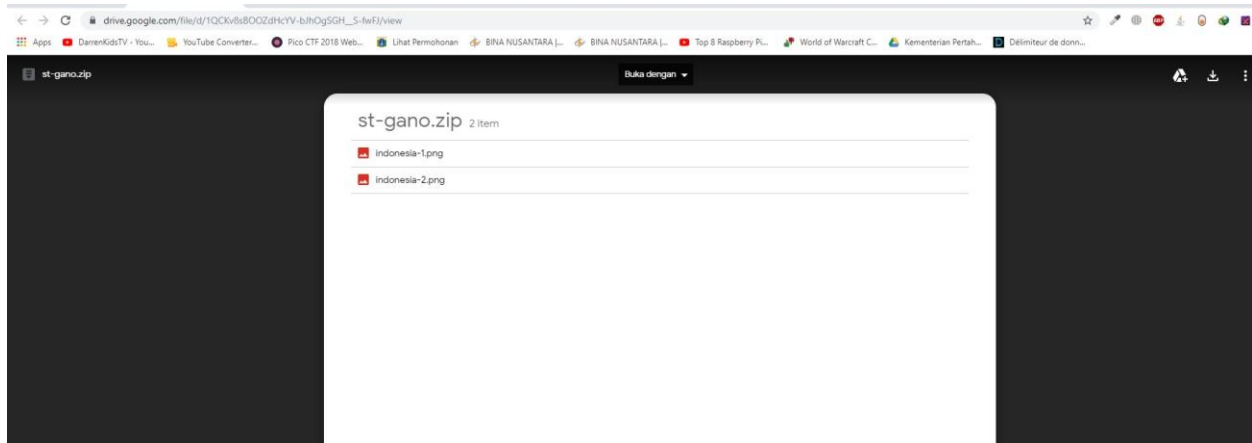
6



### Write UP POC :

Diberikan Soal tentang Forensic gambar dengan nama robot\_robot.jpg, setelah kita download kemudian open with dengan menggunakan notepad++ editor, setelah itu ada kalimat yang aneh yaitu pastebin.com/XWLZNJQ7, copy kan url tersebut ke browser, kemudian didapatkan flag : **KXS12019{TNI\_AD\_yes\_yes}**.

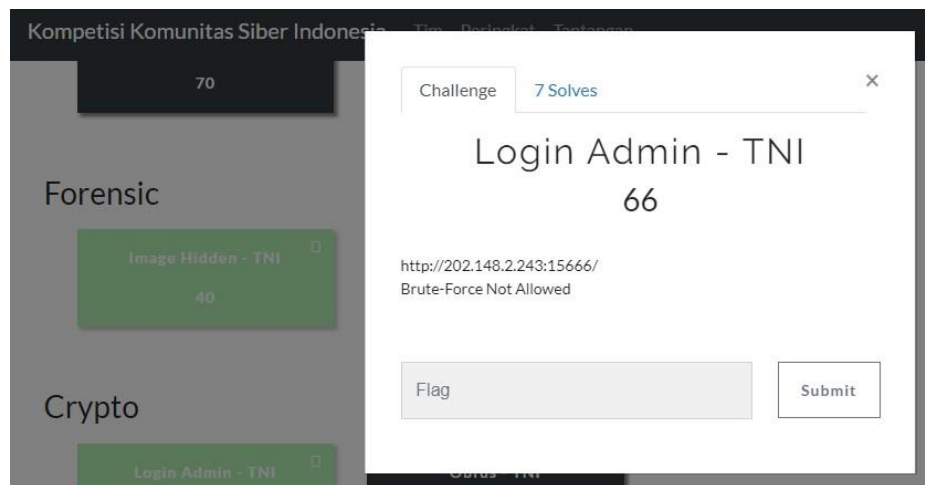
## STGANO – TNI



### Write UP POC :

Diberikan Soal tentang Forensic gambar tentang Stgano, dengan langkah-langkahnya yaitu menggabungkan (combine) gambar indonesia-1.png dan indonesia-2.png, setelah menggabungkan gambar tersebut didapatkan sebuah barcode yang tersembunyi, setelah discan menggunakan aplikasi barcode didapatkan flag : **KKS12019{6ae7aeaa63ebb8344991b2d67ad679b2}**.

## LOGIN ADMIN – TNI



## Admin login

Username :  Password :





## C:\> deobfuscate javascript

This tool is designed to assist analysts in deobfuscating malicious Javascripts. It does not interpret HTML so any HTML must be removed in order to properly deobfuscate the code. The script must also be free of syntax errors for proper results. Blackhole landing pages and exploit kits employ obfuscation in order to hide the intent of the code while decreasing the likelihood of detection. When scripts are packed, the original code becomes data and the visible code is the deobfuscation routine. During execution the data is unpacked by the routine and the result is a string that must be evaluated as code in order to execute. This deobfuscation tool works by returning that string of code rather than evaluating it. It is then beautified for easy reading. Many thanks to the folks at jsbeautifier.org for sharing the code that makes deobfuscated Javascript pretty again. You can visit their site by clicking [here](#). **NOTE** - Code analyzed by this tool will execute in your browser. This tool is only designed to intercept calls made to the eval() and write() functions which are commonly used as the final function in malicious Javascripts. Some malicious scripts may not employ these functions and may therefore infect your browser..

```
if (document.forms[0].username.value == "tni-kuat" && document.forms[0].password.value == "bersama-rakyat")  
document.location = "ragagljglagjaljglajglajglajss.php"
```

KKSI2019{TNI-KUAT-7fc56270e7a70fa81a5935b72eacbe29-BERSAMA-RAKYAT}

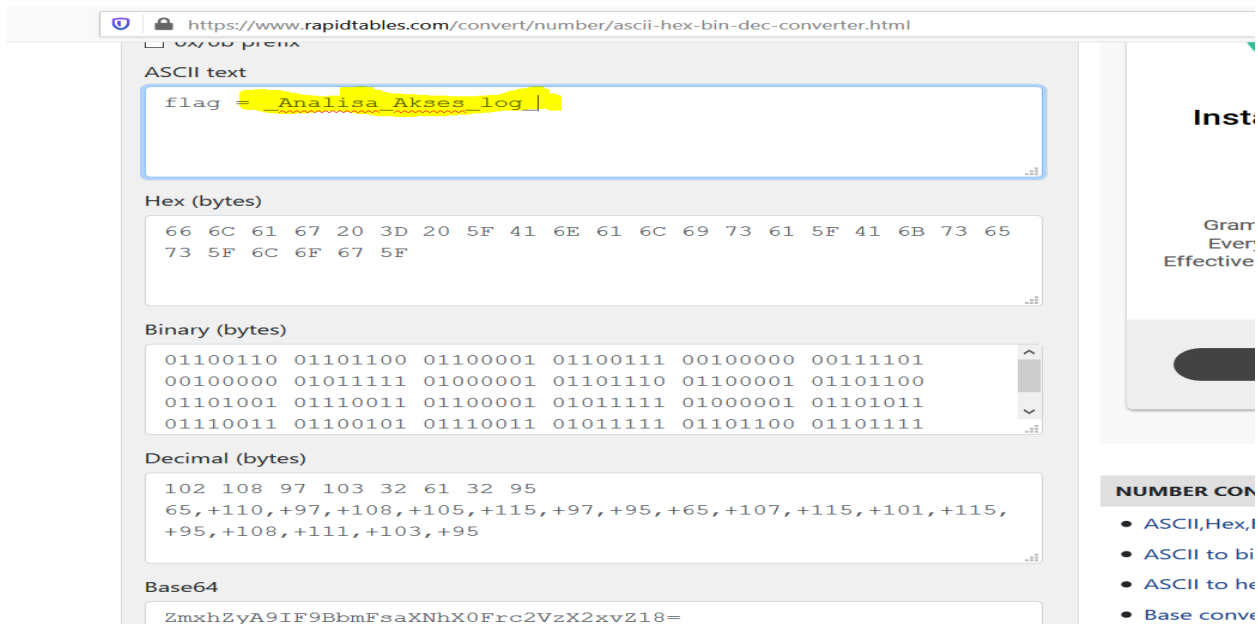
### Write UP POC :

Diberikan Soal tentang Login Admin dengan ip <http://202.148.2.243:15666> yang tertera Username dan Password, kemudian kami inspect element pada browser didapatkan source javascript, kemudian javascript tersebut di decrypt dengan tools online menggunakan deobfuscate javascript, kemudian didapatkan link php dan didapatkan flag : **KKSI2019{TNI-KUAT-7fc56270e7a70fa81a5935b72eacbe29-BERSAMA-RAKYAT}**.

## MISC

### ACCESS LOG – TNI

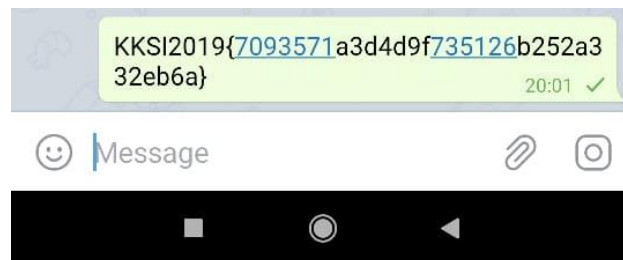
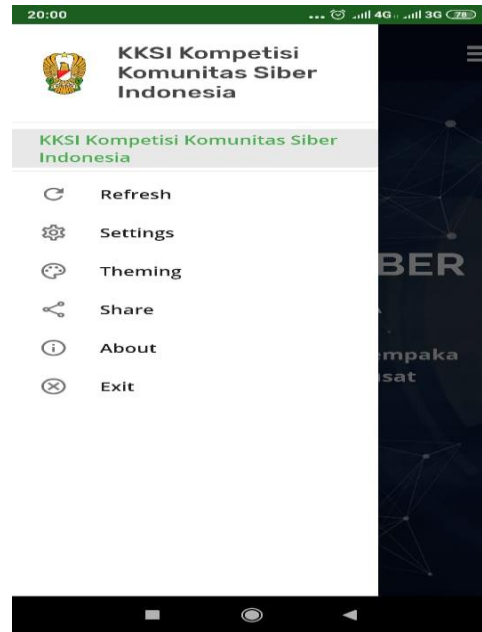
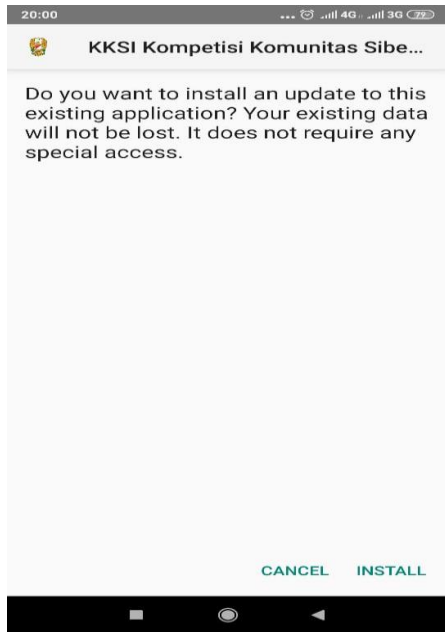
```
access - Notepad
File Edit Format View Help
page=register.php" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2019:03:39:05 -0400] "GET /fdsfsda HTTP/1.1" 404 501 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2019:03:39:05 -0400] "GET /fdsfsda HTTP/1.1" 404 501 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2019:03:39:46 -0400] "GET /mutillidae/index.php?page=client-side-control-challenge.php HTTP/1.1" 200 9197
"http://192.168.32.134/mutillidae/index.php?page=user-info.php&username='%2bunion%2ball%2bselect%2bi,String.fromCharCode(102,%2b108,%2b97,%2b103,%2b32,%2b61,%2b32,%2b95,%2b65,%2b10,%2b97,%2b108,%2b105,%2b115,%2b97,%2b95,%2b65,%2b107,%2b115,%2b101,%2b115,%2b95,%2b108,%2b111,%2b103,%2b95),3%2b--+&password=&user-info-php-submit-button=View Account Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2019:03:40:09 -0400] "GET /mutillidae/index.php?page=user-info.php HTTP/1.1" 200 8874
"http://192.168.32.134/mutillidae/index.php?page=client-side-control-challenge.php" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2019:03:40:13 -0400] "GET /mutillidae/index.php?page=user-info.php&username=fdsda&password=fdsda&user-info-php-submit-
button=View+Account+Details HTTP/1.1" 200 8944 "http://192.168.32.134/mutillidae/index.php?page=user-info.php" "Mozilla/5.0 (Windows NT 6.3;
WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2019:03:40:18 -0400] "GET /mutillidae/webservices/soap/ws-hello-world.php HTTP/1.1" 200 1968
"http://192.168.32.134/mutillidae/index.php?page=user-info.php&username=fdsda&password=fdsda&user-info-php-submit-button=View+Account+Details"
"Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2019:03:40:23 -0400] "GET /mutillidae/index.php?page=user-info.php&username=fdsda&password=fdsda&user-info-php-submit-
button=View+Account+Details HTTP/1.1" 200 8974 "http://192.168.32.134/mutillidae/index.php?page=user-
info.php&username=fdsda&password=fdsda&user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2019:03:40:25 -0400] "GET /mutillidae/index.php?page=user-info.php&username=fdsda&password=&user-info-php-submit-
button=View+Account+Details HTTP/1.1" 200 8974 "http://192.168.32.134/mutillidae/index.php?page=user-
info.php&username=fdsda&password=fdsda&user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
Ln 110, Col 419 100% Unix (LF) UTF-8
```



### Write UP POC :

Diberikan Soal tentang analisa LOG serangan dengan nama file access.log, setelah dianalisa didapatkan file menggunakan Decimal, kemudian kita decrypt ke ASCII text dan didapatkan flag : KKS12019{ \_Analisa\_Akses\_log }.

## ANDROID – TNI



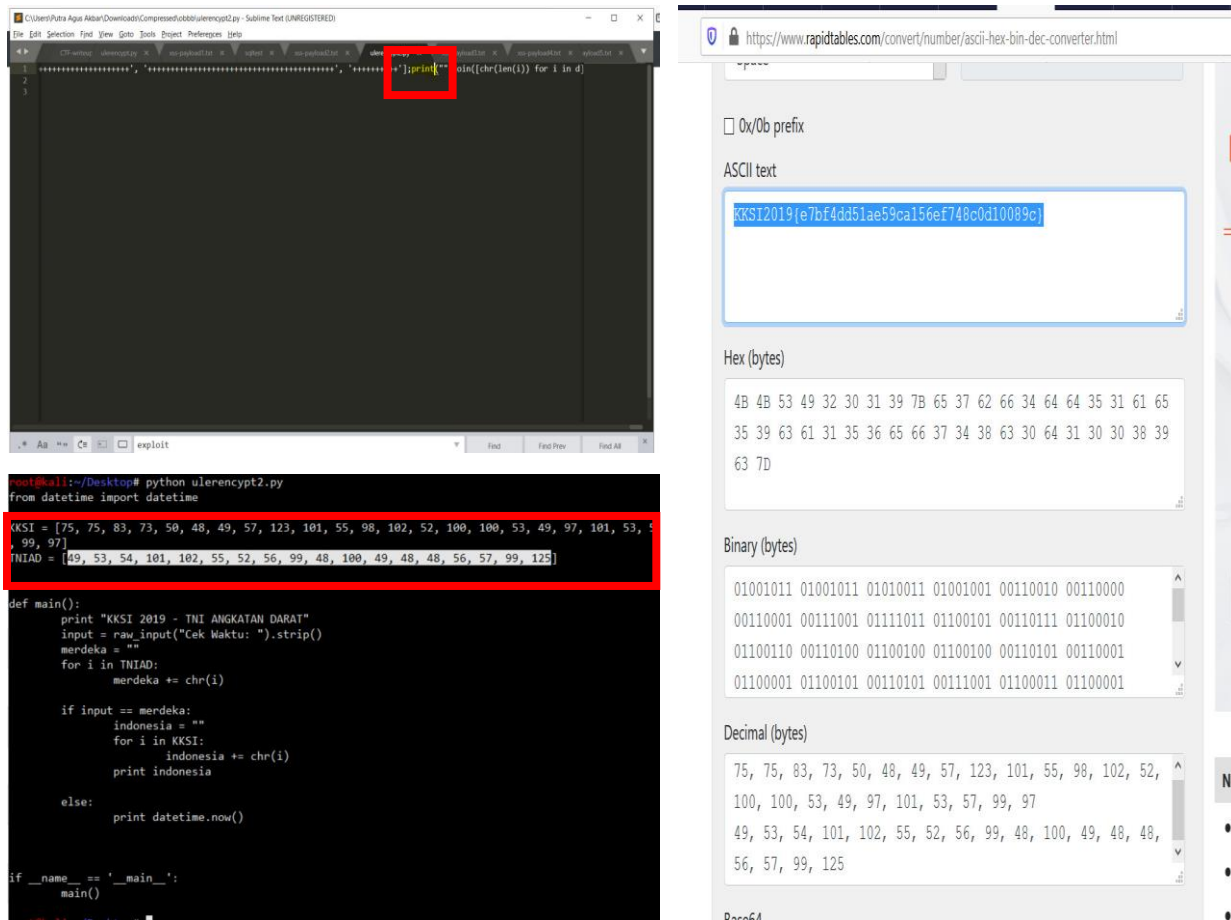
### Write UP POC :

Diberikan soal \_KKSII\_.apk, caranya adalah dengan instalasi .apk tersebut kemudian setelah selesai diinstal sentuh icon share (bebas share dimana, kami contohkan di telegram) setelah itu didapatkan flag : **KKSII2019{7093571a3d4d9f735126b252a332eb6a}**.



## CRYPTO

### OBFUS –TNI



The image shows two side-by-side screenshots. The left screenshot is a Sublime Text editor window titled 'C:\Users\Putra Agus Albar\Downloads\Compressed\obfus\ulerencypt2.py - Sublime Text (UNREGISTERED)'. It displays a Python script with a red box highlighting the line `print(chr(i) for i in d)`. Below the editor, a terminal window shows the execution of `python ulerencypt2.py`, which outputs the flag `KKSI2019{e7bf4dd51ae59ca156ef748c0d10089c}`. The right screenshot is a web browser window showing the URL `https://www.rapidtables.com/convert/number/ascii-hex-bin-dec-converter.html`. It displays the conversion of the flag from decimal to ASCII text, with the result `KKSI2019{e7bf4dd51ae59ca156ef748c0d10089c}` highlighted in the ASCII text field.

```
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()
```

ASCII text  
KKSI2019{e7bf4dd51ae59ca156ef748c0d10089c}

Hex (bytes)  
4B 4B 53 49 32 30 31 39 7B 65 37 62 66 34 64 64 35 31 61 65  
35 39 63 61 31 35 36 65 66 37 34 38 63 30 64 31 30 30 38 39  
63 7D

Binary (bytes)  
01001011 01001011 01010011 01001001 00110010 00110000  
00110001 00111001 01111011 01100101 00110111 01100010  
01100110 00110100 01100100 01100100 00110101 00110001  
01100001 01100101 00110101 00111001 01100011 01100001

Decimal (bytes)  
75, 75, 83, 73, 50, 48, 49, 57, 123, 101, 55, 98, 102, 52,  
100, 100, 53, 49, 97, 101, 53, 57, 99, 97  
49, 53, 54, 101, 102, 55, 52, 56, 99, 48, 100, 49, 48, 48,  
56, 57, 99, 125

#### Write UP POC :

Diberikan persoalan mengenai bahasa pemrograman python, langkah-langkahnya adalah kita edit file `ulerencypt.py`, kemudian cari kata `exec` dan diganti dengan `print`, setelah itu save. Setelah itu jalankan file yang telah diedit tersebut, tampak ada angka di `KKSI` dan `TNIAD`, setelah itu di konvert dari desimal ke ASCII text menggunakan `rapidtables.com` dan didapatkan flag : **KKSI2019{e7bf4dd51ae59ca156ef748c0d10089c}**.