Nama Tim : USER2
Nama Sekolah : Smk Negeri 1 Lahat

AES biasalah

Apa dampak Key jika tidak dirahasiakan ?

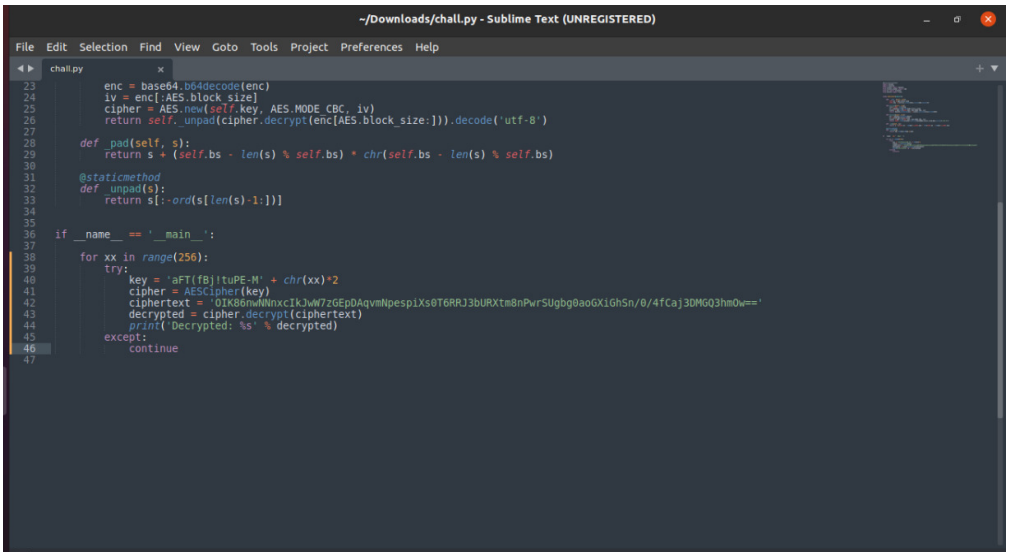
- Dampaknya akan lebih mudah untuk di brute force
  kami menemukan sebuah key di file chall.py

```
if __name__ == '__main__':

    xx = urandom(1)
    key = b'aFT(fBj!tuPE-M' + xx*2
    print(key)
    cipher = AESCipher(key.decode())
```

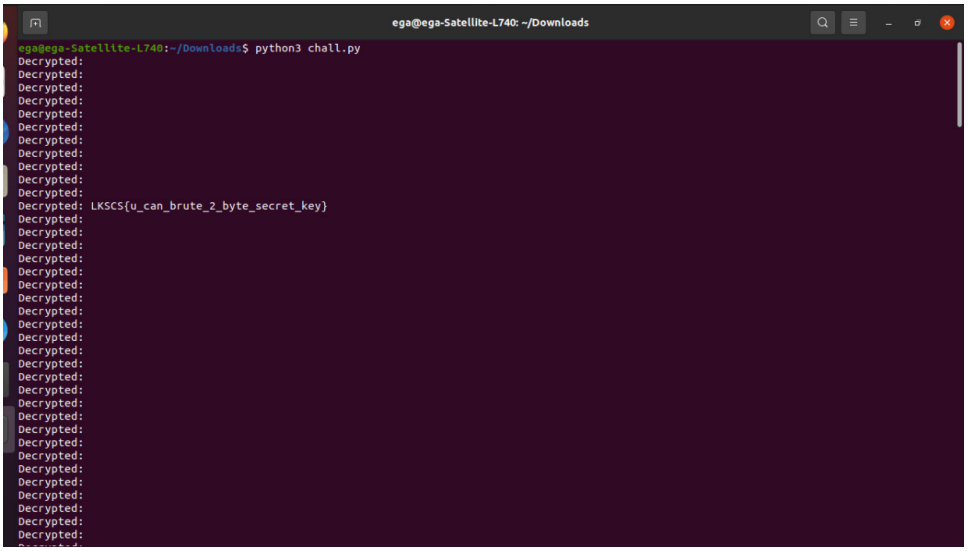
Key yang dibutuhkan untuk melakukan enkripsi pada soal ini berjumlah 16 byte / 16 Karakter

- Dibawah ini adalah isi dari file chall.py yang di berikan. disana kami menemukan sebuah key dan kami lakukan enskrip yang menghasilkan sebuah chipertext , dan sesuai dengan chipertext tersebut kami deskrip , disini kami menggunakan tools pycrypto.

  Setelah itu lalu kami ubah File chall.py yang seharusnya berfungsi untuk enskrip kami ubah agar bisa men deskrip chipertext



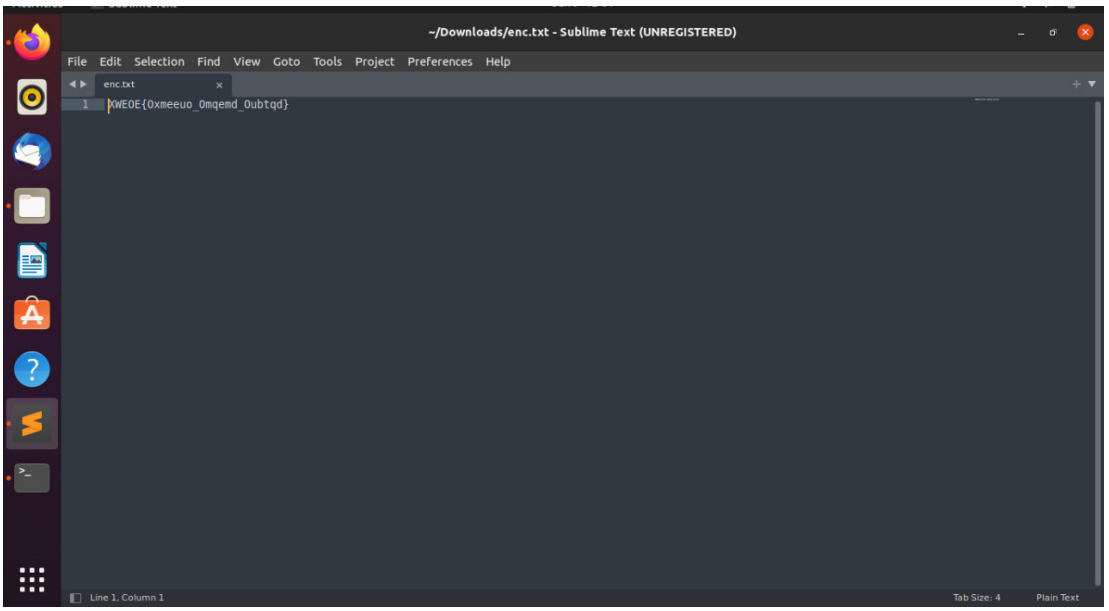
Setelah mengedit file lalu kami jalankan Program/tools tersebut di terminal, dengan cara :



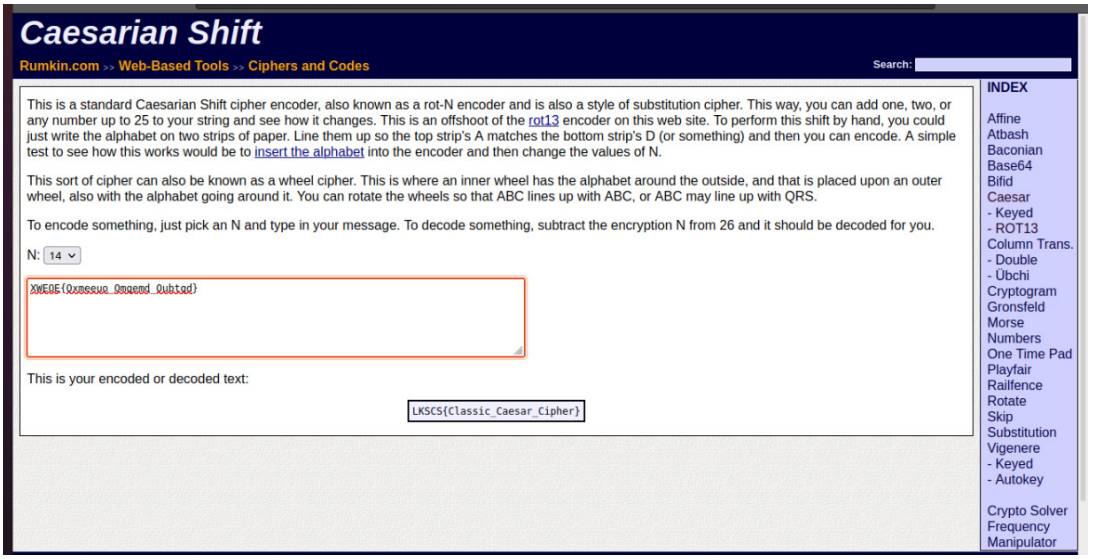
Disana ditemukan sebuah flag untuk menjawab Soal di AES biasalah.
Flag : LKSCS{u_can_brute_2_byte_secret_key}

Caesar Chiper

-Ini adalah isi dari file yang di berikan.



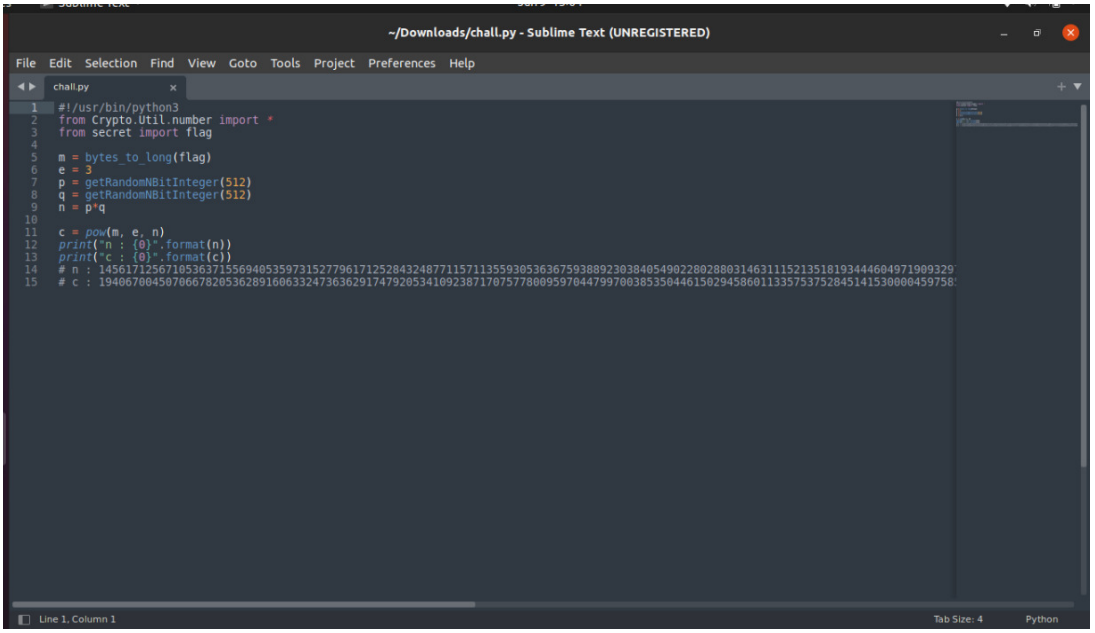
-Setelah itu dideskrip kan menggunakan website
http://rumkin.com/tools/cipher/caesar.php
-Berdasarkan soal yang telah dikerjakan ciri khas flag diawali dengan LKSCS. Jadi setelah di coba pergeseran dari 0 sampai 25 maka ditemukan angka yang cocok dengan ciri khas flag yaitu angka 14 atur N menjadi = 14 , dan paste isi file enc.txt



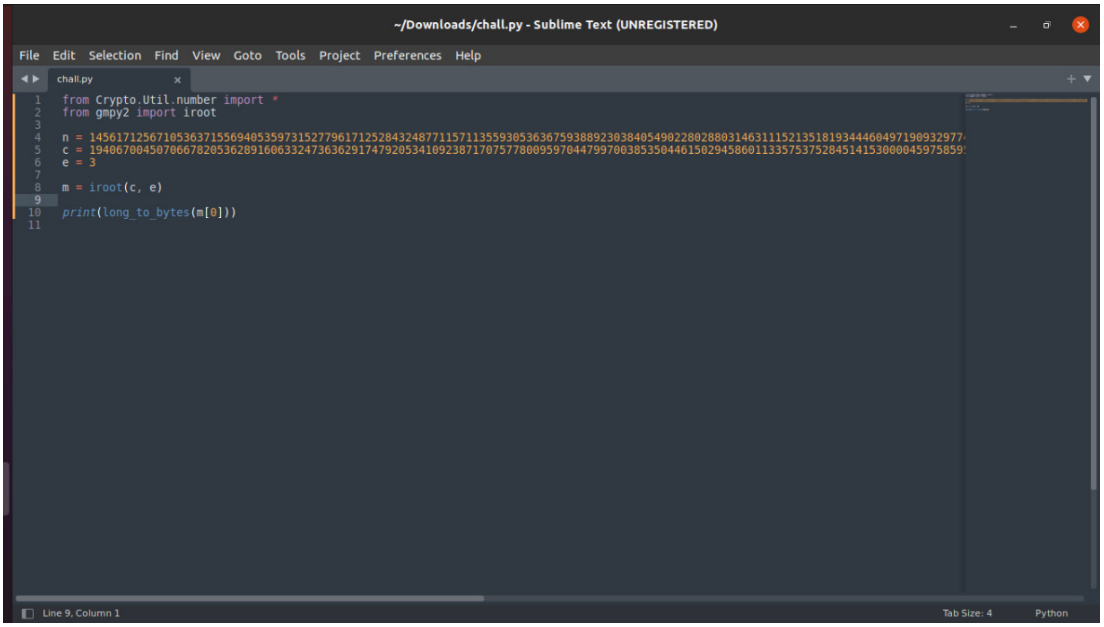
Flag : LKSCS{Classic_Caesar_Cipher}

RSA Small e

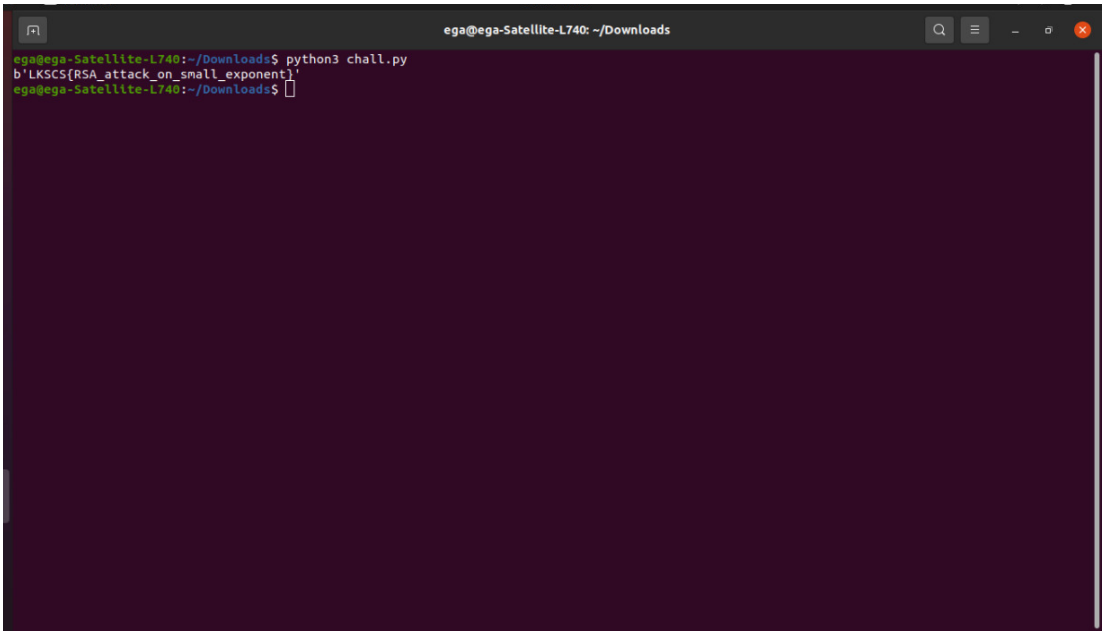
-Ini adalah isi file chall.py disana telah diberitahu nilai n dan c.



-Setelah nilai n dan c diketahui selanjutnya membuat program untuk mencari flag dengan tools gmpy2 dengan fungsi iroot.



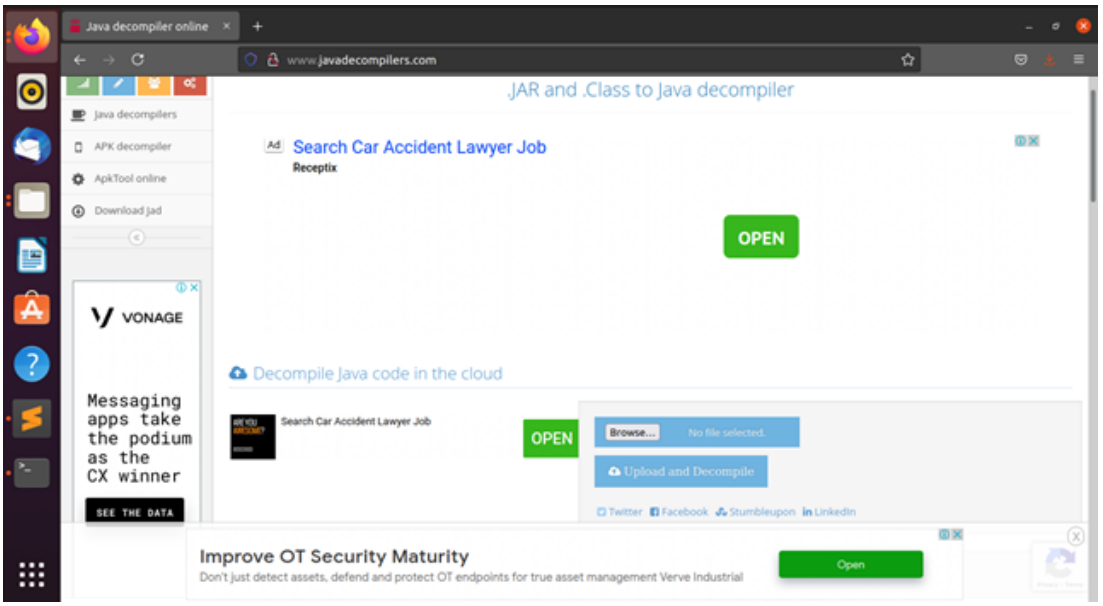
-Berikut adalah hasil run dari program yang dibuat mencari flag.



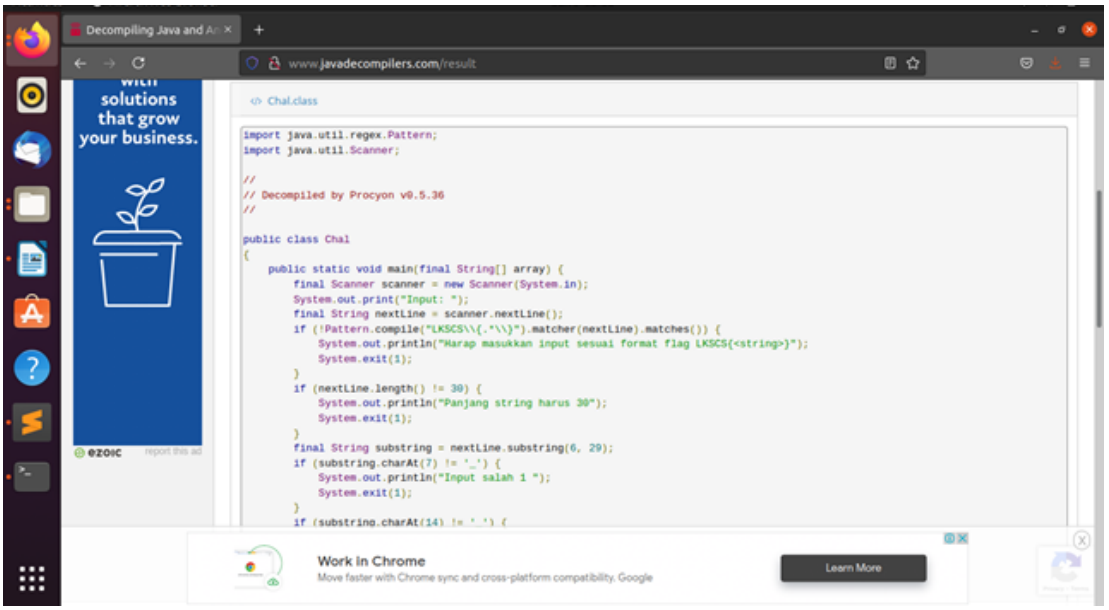
Flag :LKSCS{RSA_attack_on_small_exponent}

Jawa

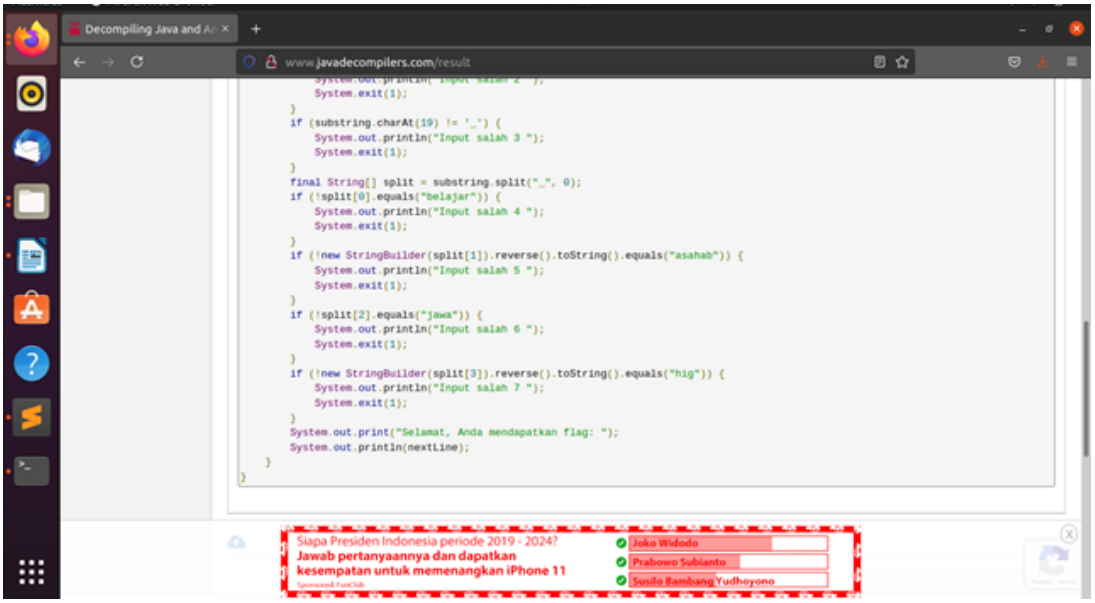
-Setelah mendownload file Chal.class yg diberikan di deskripsi soal selanjutny buka website javadecompilers.com untuk decompile file Chal.class
-Kemudian pilih menu browse untuk memasukkan file Chal.class ke website tersebut
-Lalu pilih menu Upload and Decompile untuk melakukan decompile pada file Chal.class



-Setelah di decompile maka akan tampil sebagai berikut:



-Dari hasil decompile tersebut terlihat sesuatu yg mencurigakan seperti terdapat kata “Harap masukkan input sesuai format flag LKSCS{<string>}
“ dan tanda “_”
-Lalu sesuatu yg mencurigakan juga terdapat di program berikut:

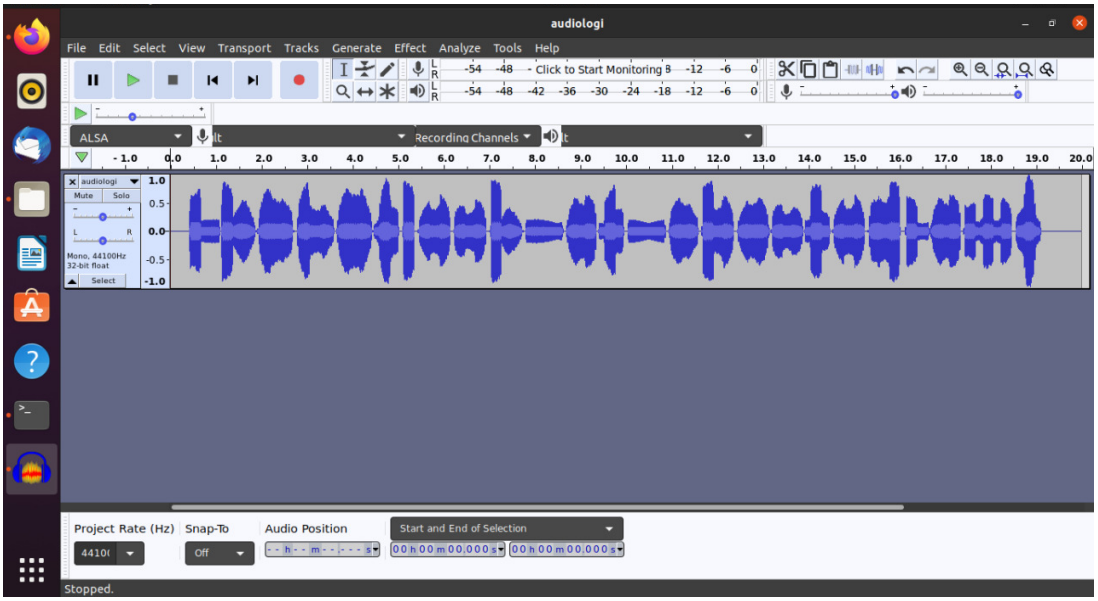


-Di program tersebut terdapat kata yg mencurigakan seperti belajar,asahab,jawa,dan hig
-Seperti yang diketahui kata asahab dan hig itu terbalik jika katanya diurutkan dari belakang maka akan menjadi bahasa dan gih
-Jika semua yang mencurigakan itu kita hubungkan maka akan merangkai sebuah kata LKSCS{belajar_bahasa_jawa_gih}

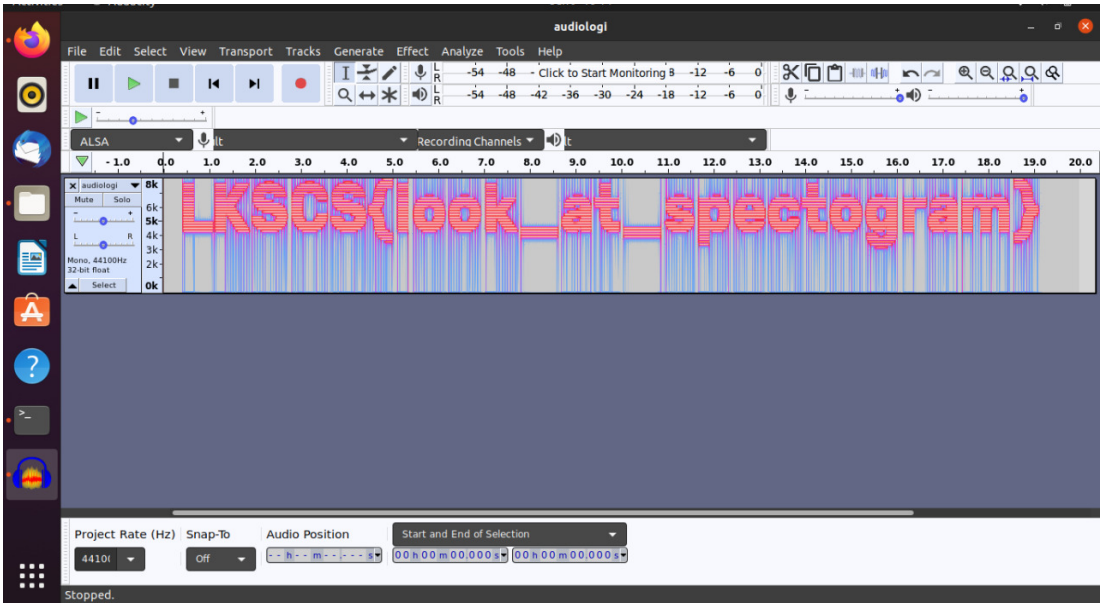
Flag : LKSCS{belajar_bahasa_jawa_gih}

Audiology

-Buka file audiologi.wav menggunakan tool audacity dan ini adalah tampilan dari file nya.



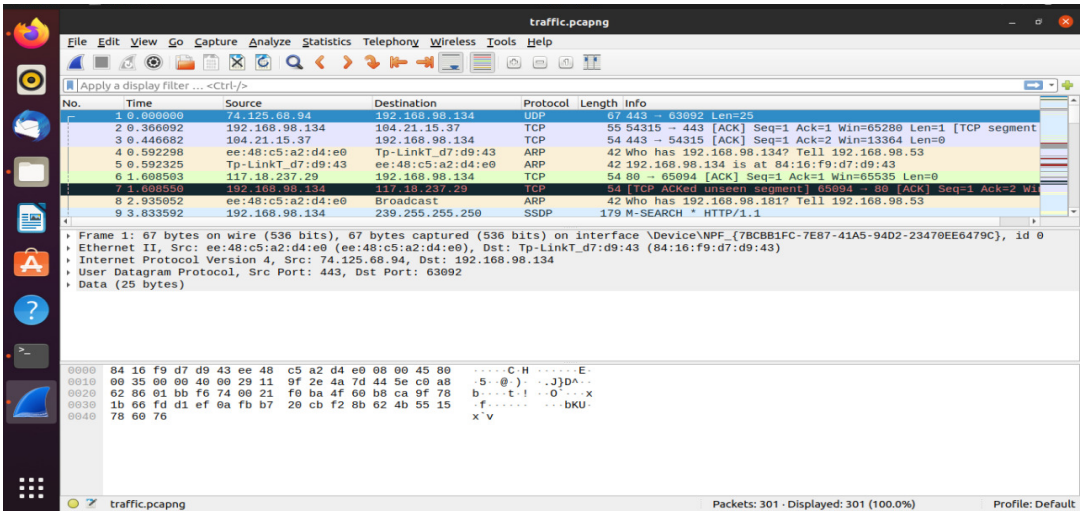
-Setelah file di buka pilih menu audiologi lalu pilih spectrogram.
Dan berikut adalah hasilnya.



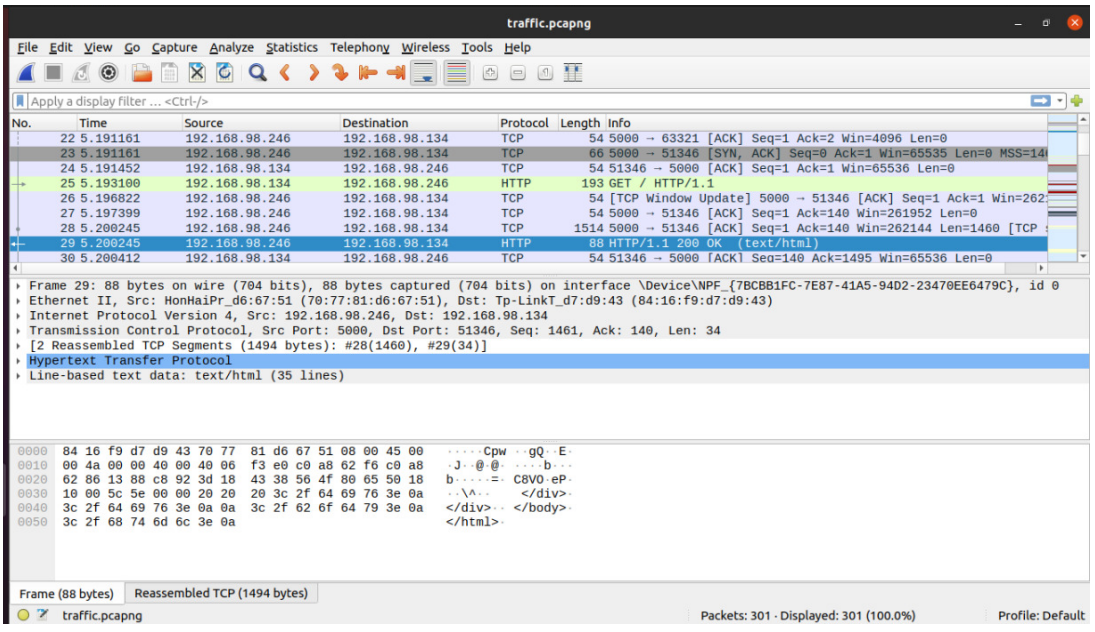
Flag : LKSCS{look_at_spectogram}

Capture The Traffic

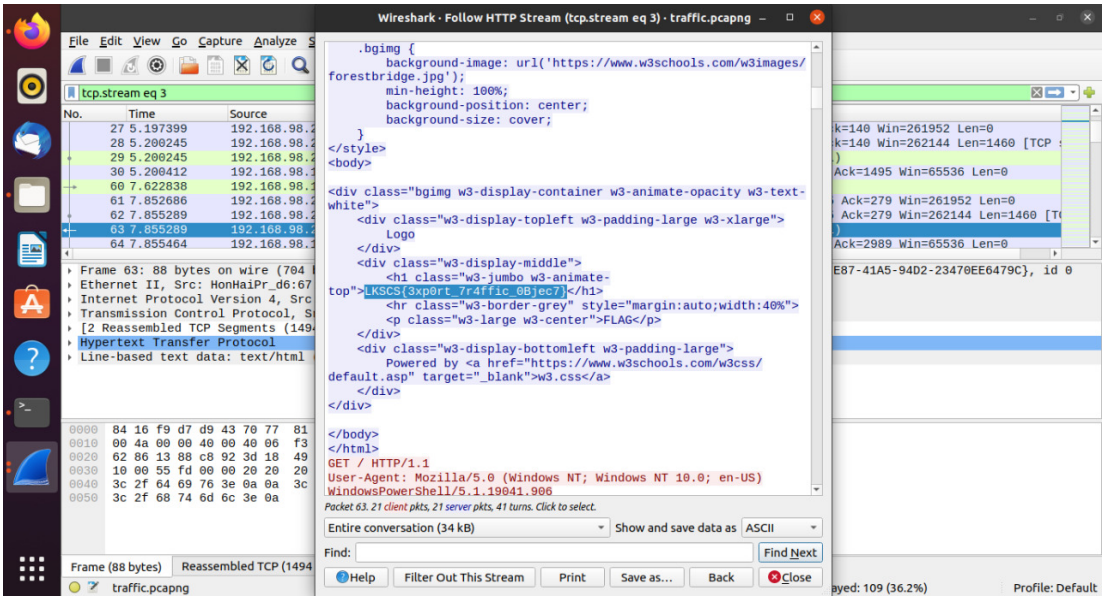
-Buka file traffic.pcapng di tool wireshark



-Cari protocol HTTP lalu klik kanan pilih menu follow lalu pilih menu HTTP stream.



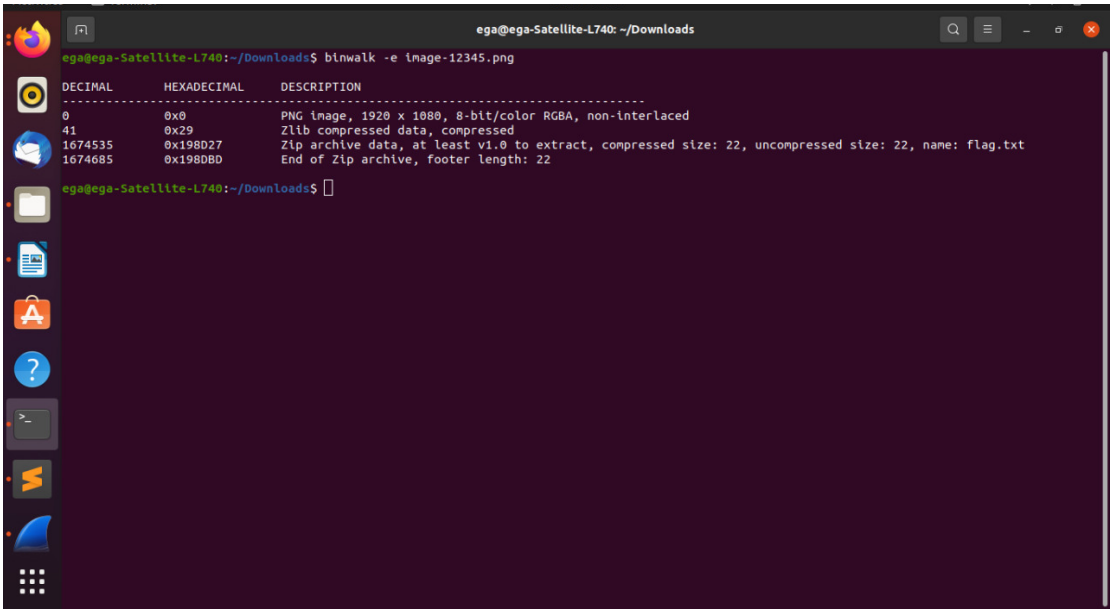
-Setelah muncul seperti digambar maka cari flag nya.



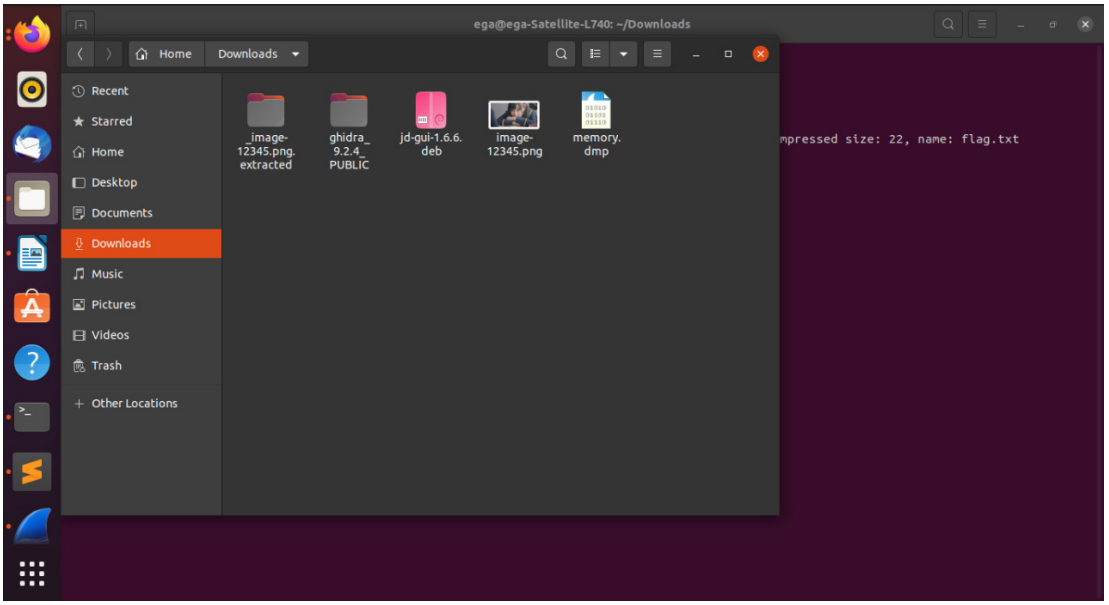
Flag:LKSCS{3xp0rt_7r4ffic_0Bjec7}

Hidden File

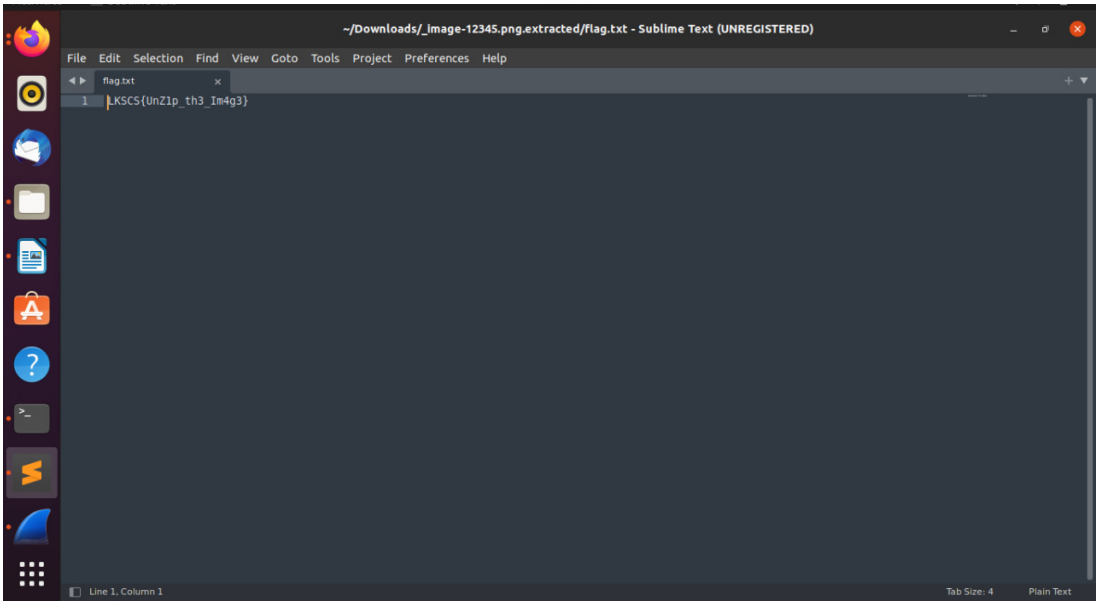
-Ekstrak image -12345.png dengan menggunakan binwalk seperti gambar berikut :



-Setelah di ekstrak maka akan muncul folder baru hasil dari ekstrak image-12345.png yang tadi.



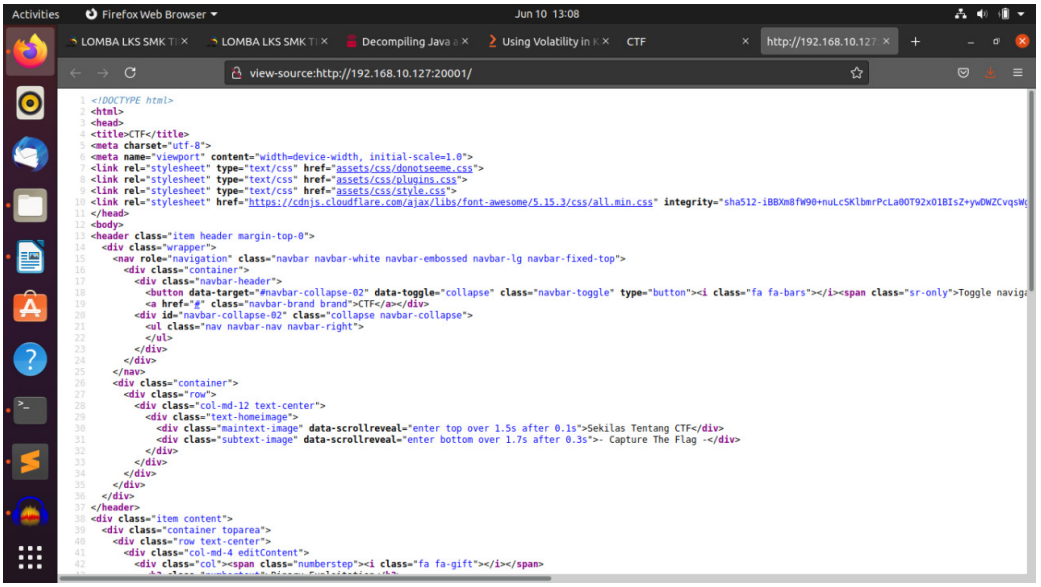
-Di dalam folder hasil ekstrak image-12345.png tadi terdapat flag.txt yang mempunyai isi berikut:



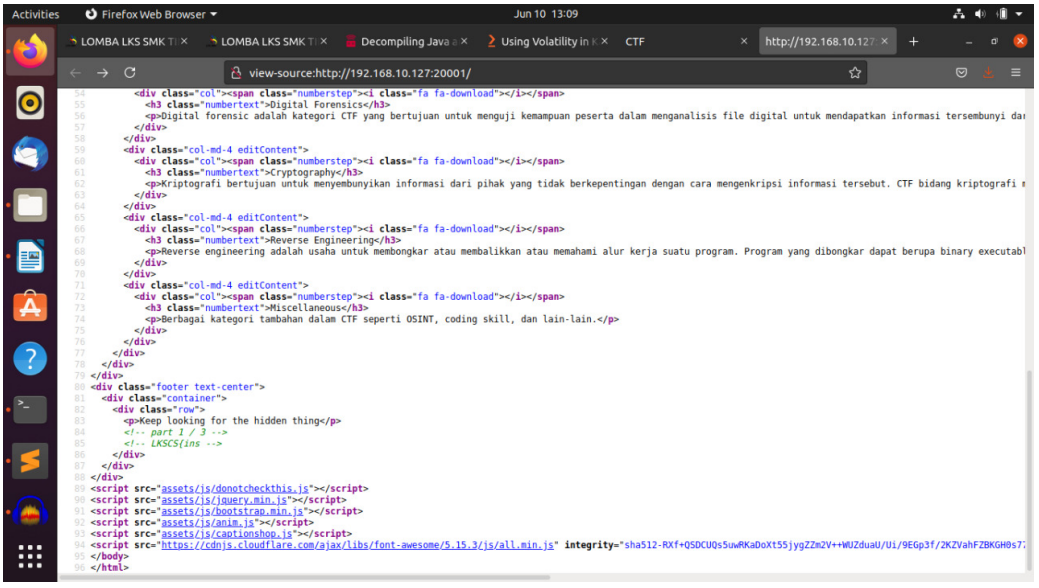
Flag:{UnZ1p_th3_1m4g3}

Know Your HTML

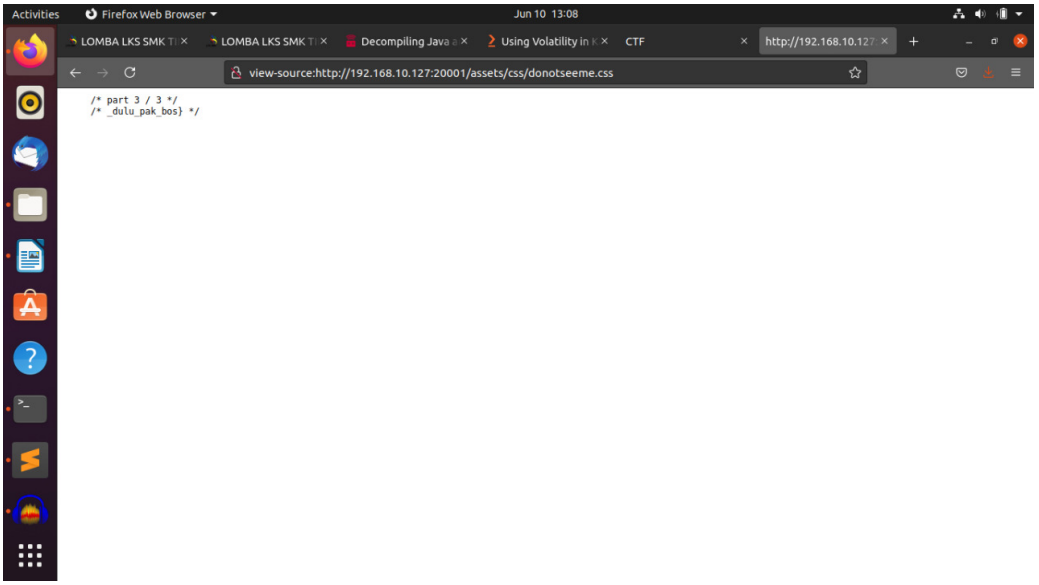
-Buka link server yang diberikan lalu inspect web tersebut sehingga menghasilkan tampilan sebagai berikut.



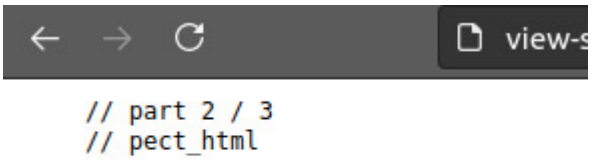
-Jika discroll ke bawah akan ketemu kata-kata seperti "part 1 / 3" dan "LKSCS{ins" yang artinya itu adalah part 1 dari 3 part flag yg terpisah.kita dapat mencari part lainnya dengan mengklik link yang terdapat pada fungsi href.



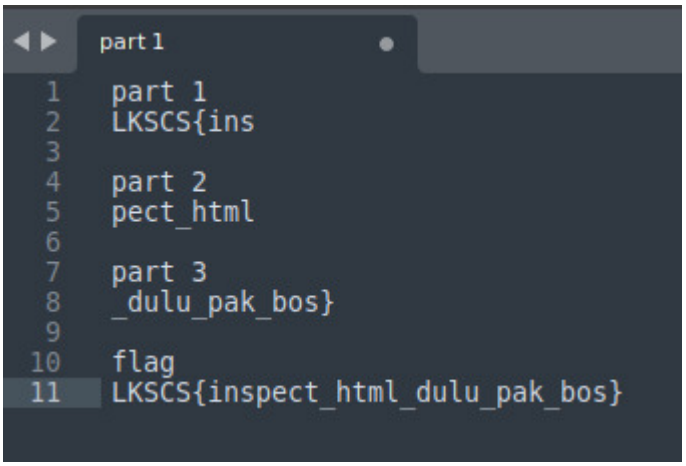
-Setelah diselidiki part 3 flag yang terdapat di href="assets/css/donotseeme.css"
-Berikut adalah tampilan dari href="assets/css/donotseeme.css":



-Part 3 berada di src="assets/js/donotcheckthis.js" dan berikut ini adalah tampilan setelah meng-klik src="assets/js/donotcheckthis.js"



-Setelah 3 part telah diketahui waktunya kita mengurutkan flagny sesuai urutan dari part 1 sampai part 3.berikut adalah hasilnya.



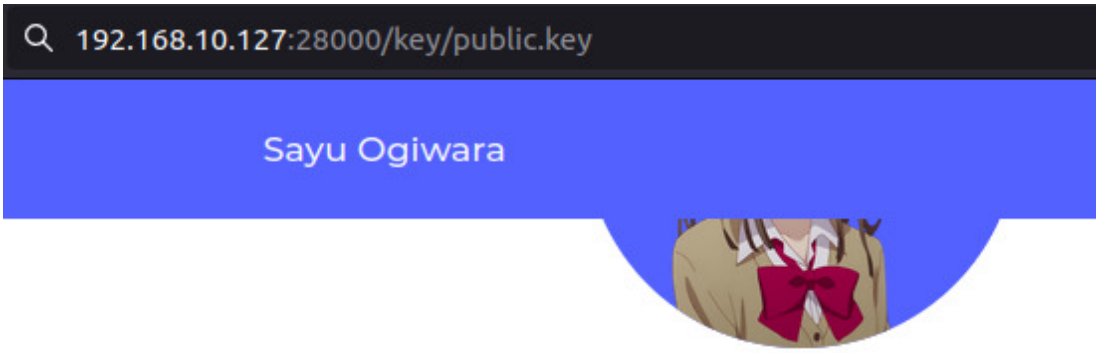
Flag : LKSCS{inspect_html_dulu_pak_bos}

Sayu's Blog

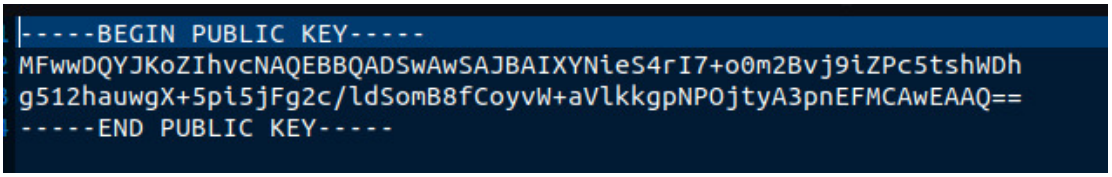
-Buka link yg tertera di deskripsi soal lalu inspect element disana ada note mengenai public.key

```
<!DOCTYPE html>
    <html lang="en">
    <head>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">
        <link rel="icon" href="/favicon.ico" type="image/x-icon">

        <!-- ===== CSS ===== -->
        <link rel="stylesheet" href="assets/css/styles.css">

        <!-- ===== BOX ICONS ===== -->
        <link href='https://cdn.jsdelivr.net/npm/boxicons@2.0.5/css/boxicons.min.css' rel='stylesheet'>

        <!-- ----------------TODO: remove this---------------  -->
        <!--  <link href="/key/public.key" rel='public-key'>   -->
        <!-- ------------TODO: move keys from public---------  -->

        <title>Sayur</title>
    </head>
    <body>
        <!--===== HEADER =====-->
        <header class="l-header">
            <nav class="nav bd-grid">
                <div>
                    <a href="#" class="nav__logo">Sayu Ogiwara</a>
                </div>

                <div class="nav__menu" id="nav-menu">
                    <ul class="nav__list">
                        <li class="nav__item"><a href="#home" class="nav__link active">Home</a></li>
                        <li class="nav__item"><a href="#about" class="nav__link">About</a></li>
                        <li class="nav__item"><a href="#skills" class="nav__link">Skills</a></li>
                        <li class="nav__item"><a href="#portfolio" class="nav__link">Portfolio</a></li>
                        <li class="nav__item"><a href="#contact" class="nav__link">Contact</a></li>
                        <li class="nav__item"><a href="/admin" class="nav__link">Admin</a></li>
                    </ul>
                </div>

                <div class="nav__toggle" id="nav-toggle">
```

-Tambahkan /key/public.key di link website nya.

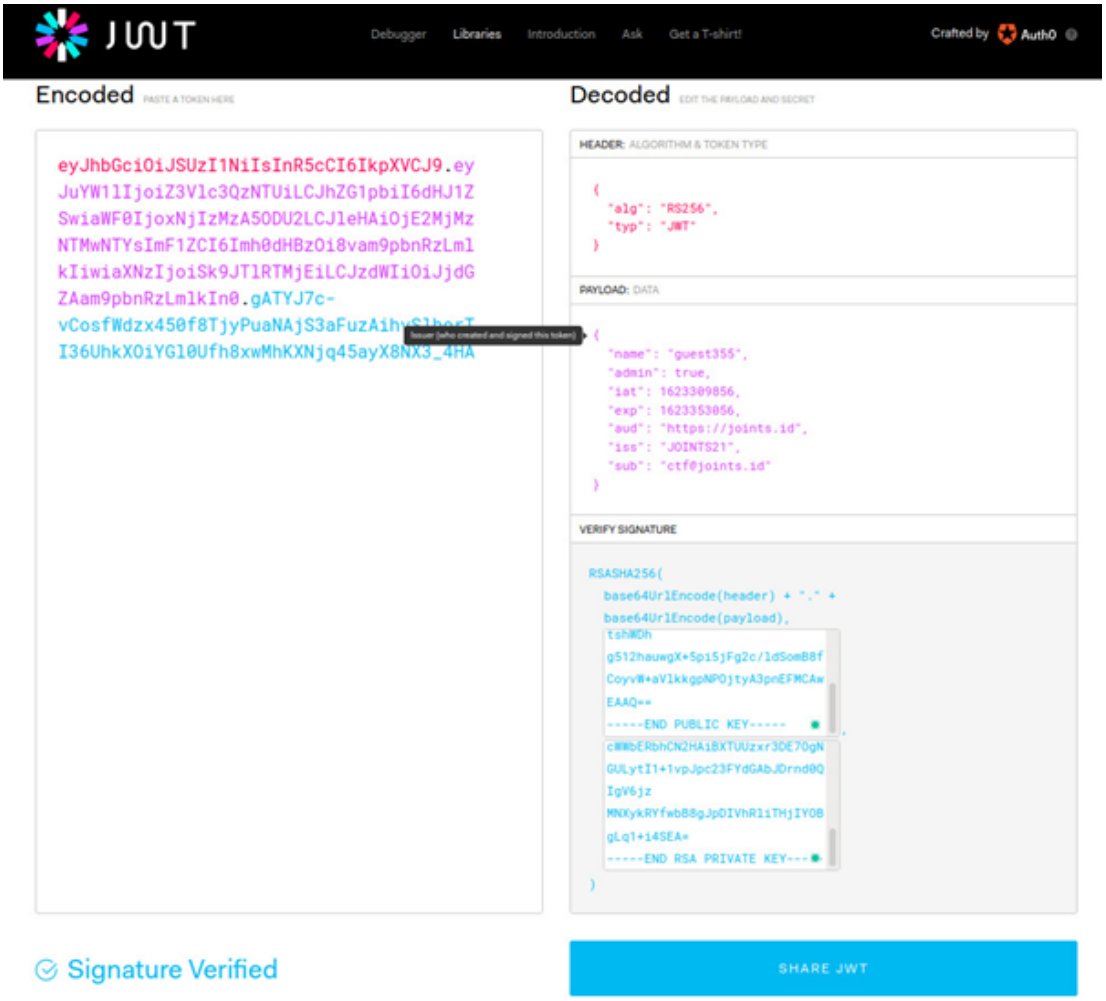


-Berikut ini adalah tampilan public.key



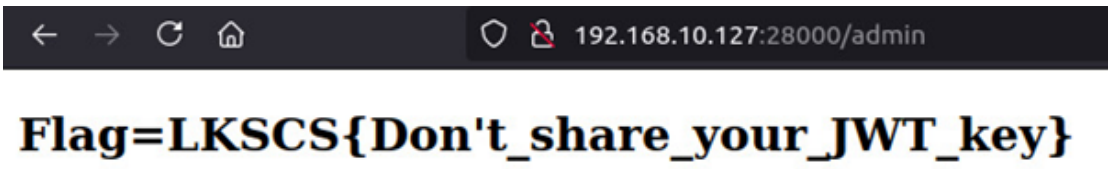
-Kemudian cari private.key dengan menambahkan /key/private.key di akhir link

-Kemudian decode private key tadi seperti berikut:



-Lakukan seperti digambar dulu sebelum membuka link 192.168.10.127:28000/admin

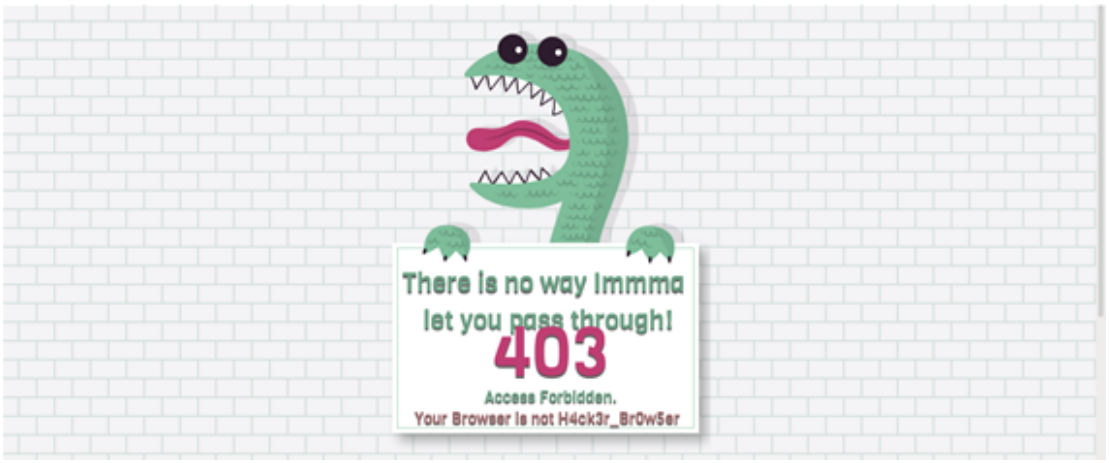
-Terakhir buka link 192.168.10.127:28000/admin seperti berikut:



Flag : LKSCS{Don’t_share_your_JWT_key}

Invalid browser

-Berikut adalah tampilan dari http://192.168.10.127:27900/rsvp

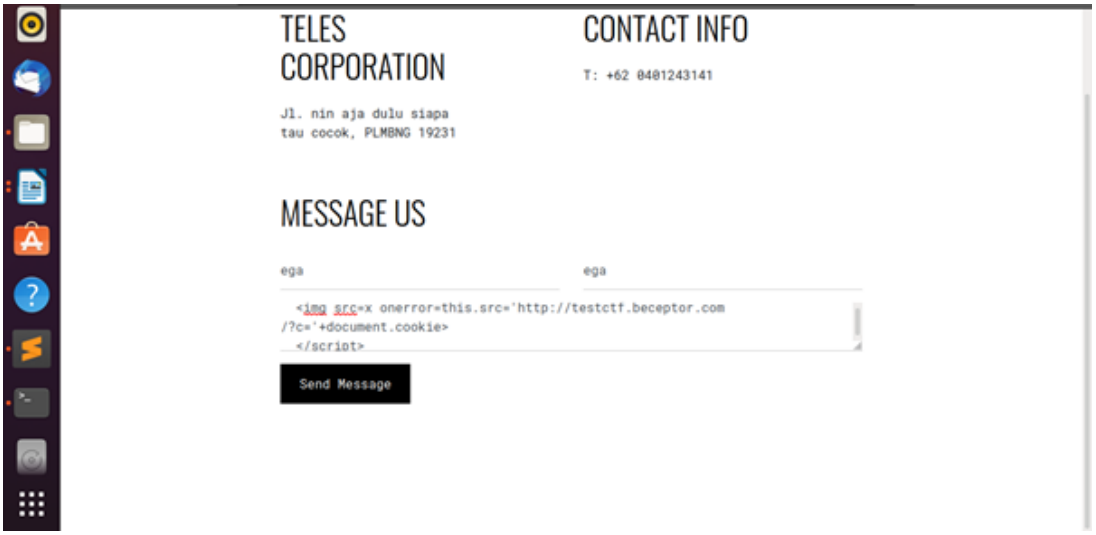


-Untuk mencari flag cukup jalankan “curl --user-agent "H4ck3r_Br0w5er" 192.168.10.127:27900/rsvp” di terminal seperti berikut:

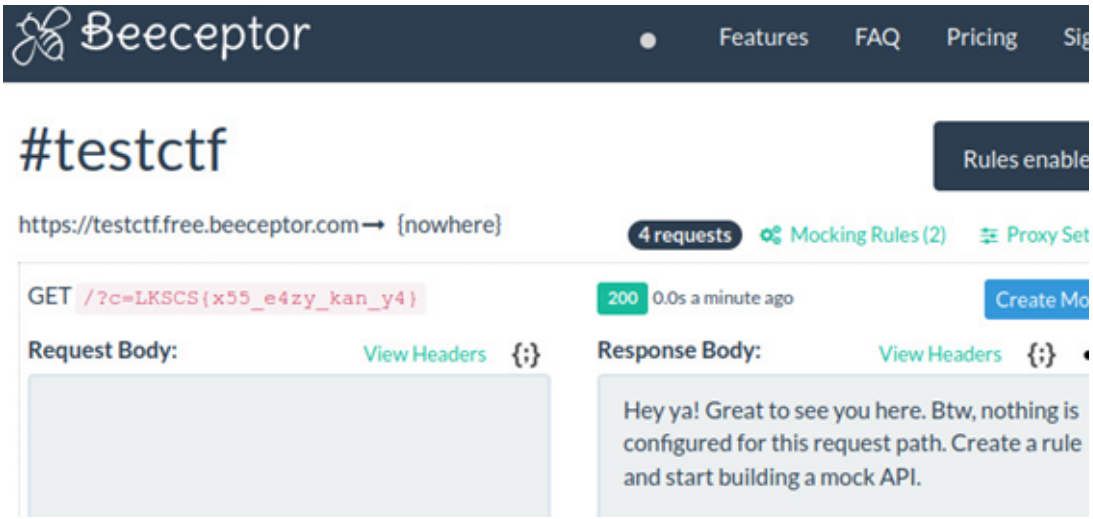
Flag : LKSCS{u53r_4gen7_wh1teli5t}

Form Feedback

-Buka link yg berikan di deskripsi.pada bagian message isi script untuk mencuri cookie seperti gambar berikut.



-Berikut ini adalah tampilan setelah berhasil mendapatkan cookie.



Virus Program

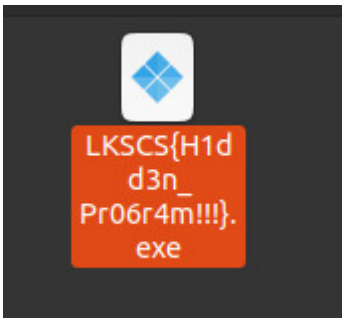
-Pertama scan file memory.dmp

```
ega@ega-Satellite-L740:~$ cd Downloads
ega@ega-Satellite-L740:~/Downloads$ volatility --profile=Win7SP1x86 pstree -f memory.dmp
Volatility Foundation Volatility Framework 2.6.1
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x90030030:wininit.exe                              460    392      4     88 2021-06-03 17:51:35 UTC+0000
. 0x90095030:services.exe                            556    460      7    191 2021-06-03 17:51:35 UTC+0000
.. 0x9036c2b8:svchost.exe                           1280    556     17    361 2021-06-03 17:51:47 UTC+0000
.. 0x901ebc70:svchost.exe                            912    556     21    397 2021-06-03 17:51:47 UTC+0000
... 0x9032dd20:audiodg.exe                          1092    912      5    131 2021-06-03 17:51:47 UTC+0000
.. 0x903c89e0:spoolsv.exe                           1432    556     15    309 2021-06-03 17:51:47 UTC+0000
.. 0x9c08fd20:taskhost.exe                          1744    556     10    174 2021-06-03 17:51:48 UTC+0000
.. 0x9c036030:svchost.exe                           1576    556      9    221 2021-06-03 17:51:48 UTC+0000
.. 0x901be770:svchost.exe                            812    556      7    247 2021-06-03 17:51:47 UTC+0000
.. 0x903da1f8:svchost.exe                           1460    556     20    323 2021-06-03 17:51:47 UTC+0000
.. 0x90307030:svchost.exe                            948    556     24    495 2021-06-03 17:51:47 UTC+0000
... 0x9c0c0030:dwm.exe                              1888    948      5    100 2021-06-03 17:51:48 UTC+0000
.. 0x90313030:svchost.exe                            976    556     15    321 2021-06-03 17:51:47 UTC+0000
.. 0x901ac030:VBoxService.ex                         744    556     12    152 2021-06-03 17:51:47 UTC+0000
.. 0x90347940:svchost.exe                           1148    556      6    120 2021-06-03 17:51:47 UTC+0000
.. 0x901a2030:svchost.exe                            680    556     13    369 2021-06-03 17:51:46 UTC+0000
.. 0x90311330:svchost.exe                           1016    556     29    706 2021-06-03 17:51:47 UTC+0000
.. 0x84f36d20:SearchIndexer.                        2324    556     13    611 2021-06-03 17:51:56 UTC+0000
... 0x9c253d20:SearchProtocol                       2408   2324      7    278 2021-06-03 17:51:56 UTC+0000
... 0x9c25ed20:SearchFilterHo                       2428   2324      6     88 2021-06-03 17:51:56 UTC+0000
. 0x900ac1a0:lsm.exe                                 580    460     10    152 2021-06-03 17:51:36 UTC+0000
. 0x9009a770:lsass.exe                               564    460     10    481 2021-06-03 17:51:36 UTC+0000
 0x867eb030:csrss.exe                                400    392     12    362 2021-06-03 17:51:34 UTC+0000
 0x83f2f4a0:System                                     4      0    113    474 2021-06-03 17:51:32 UTC+0000
. 0x8508c020:smss.exe                                316      4      2     34 2021-06-03 17:51:32 UTC+0000
 0x90024030:csrss.exe                                452    444     12    231 2021-06-03 17:51:35 UTC+0000
. 0x9c15bcf8:conhost.exe                            2536    452      2     53 2021-06-03 17:51:58 UTC+0000
. 0x9c32e4f8:conhost.exe                            3116    452      2     53 2021-06-03 17:52:21 UTC+0000
 0x9004bd20:winlogon.exe                             508    444      5    123 2021-06-03 17:51:35 UTC+0000
 0x9c0b7d20:explorer.exe                            1964   1872     34    849 2021-06-03 17:51:48 UTC+0000
. 0x9c185030:VBoxTray.exe                            708   1964     15    156 2021-06-03 17:51:50 UTC+0000
. 0x9c0b4d20:livekd.exe                             3108   1964      5     65 2021-06-03 17:52:21 UTC+0000
.. 0x9c303030:kd.exe                                3144   3108      2     28 2021-06-03 17:52:25 UTC+0000
```

-Di bagian bawah terdapat file dengan awalan "LKSCS{H1dd3n_P"

```
. 0x9c185030:VBoxTray.exe                            708   1964     15    156 2021-06-03 17:51:50 UTC+0000
. 0x9c0b4d20:livekd.exe                             3108   1964      5     65 2021-06-03 17:52:21 UTC+0000
.. 0x9c303030:kd.exe                                3144   3108      2     28 2021-06-03 17:52:25 UTC+0000
. 0x9c27e1e8:LKSCS{H1dd3n_P                         2524   1964      4     38 2021-06-03 17:51:57 UTC+0000
.. 0x9c279d20:LKSCS{H1dd3n_P                        2560   2524      5    101 2021-06-03 17:51:59 UTC+0000
```

-Jika kita ekstrak maka akan menghasilkan file sebagai berikut.



Flag :LKSCS{H1dd3n_Pr06r4m!!!}.exe