**PRACTICAL CHALLENGE + REPORT TEMPLATE**

MATA LOMBA CTF

|  |  |
| --- | --- |
| Metadata | |
| **Tanggal** | 24 april (24 april 2024) 2024 |
| **Nama Sekolah** | SMK TARUNA BANGSA |
| **Disusun Oleh** | Abdurrohman Al Fathi |

[**Overview 3**](#_qi0kabt9y8zu)

[**PERATURAN PRACTICAL CHALLENGE 4**](#_nl3xncq73803)

[Disclaimer 4](#_kg1ow44z0792)

[Peraturan Pengerjaan 4](#_w960werhw1i8)

[Kategori Challenge 4](#_ppc0salvkhlz)

[Durasi Pengerjaan 4](#_tbf70tv4ugh7)

[Cara Dokumentasi 5](#_f4trfmpephcw)

[Cara duplikasi dokumen pada google docs: 5](#_8l6p7fsj8nzk)

[Link Submit Laporan 6](#_pa3kcmhk9y1)

[Index Penilaian 6](#_5flbjo9xw55a)

[**THE CHALLENGES 7**](#_eghtk1euypi6)

WEB EXPLOITATION [8](#_ceamtmjzzlvc)

[1. Task 1 - Kue Admin 8](#_xiyhwtru0hhd)

[2. Task 2 - Konsolog 8](#_qew61orjurdn)

[3. Task 3 - Mr.Robot 8](#_h9v9e0d1ptuk)

DIGITAL FORENSICS [9](#_3ay0qq1pz7gr)

[1. Task 1 - Manipulasi Kepala 9](#_7sp6h4bicot8)

[2. Task 2 - OpenMe! 9](#_y7pn8qdm6fib)

[2. Task 3 - Garmbar Bagus 9](#_y7pn8qdm6fib)

REVERSE ENGINEERING [10](#_da2tzff4hkkb)

[1. Task 1 - Perbandingan](#_j11meydsta99) [11](#_cy1lvp5iyzzs)

[KRIPTOGRAFI 13](#_mbpqer1kt35s)

[1. Task 1 - Kode CIP Vigenere 13](#_kot1g8nowzva)

[2. Task 2 - Eks OR 13](#_9w9u7yk3kq57)

[STEGANOGRAPHY 16](#_49lqktickvzf)

[1. Task 1 - Exifme 1](#_kot1g8nowzva)7

[2. Task 2 - Awas Jebakan 1](#_9w9u7yk3kq57)7

3[. Task 3 - Kiu AR 1](#_9w9u7yk3kq57)7

# **Overview**

Dokumen ini berisi seluruh challenge dari mata lomba CTF Cybersecurity. Dalam challenge ini akan disediakan sejumlah 12 Challenge yang akan diselesaikan dalam waktu yang ditentukan untuk seluruh peserta secara individu. Dokumen ini menjadi laporan untuk menjawab seluruh challenge yang diberikan kepada seluruh peserta.

# **PERATURAN PRACTICAL CHALLENGE**

## **Disclaimer**

Peserta akan menemukan bentuk flag dengan format **LKS\_CTF{}** yang nantinya akan juri mention untuk format menjawabnya.

Silahkan dikerjakan sebisa mungkin karena durasi pengerjaan **4 Jam** dengan berbagai macam tipe **mind-blowing** challenge untuk problem solving skills.

## **Peraturan Pengerjaan**

1. Peserta mengerjakan challenge secara fleksibel.
2. Pengerjaan dan lampiran jawaban wajib pada dokumen ini.
3. Dilarang mencontek dari dokumentasi orang lain.
4. Tidak ada bantuan hint dari panitia atau juri, diharapkan peserta dapat memecahkan masalah pada exam secara mandiri.

## **Kategori Challenge**

1. Web Exploitation
2. Digital Forensics
3. Reverse Engineering
4. Cryptography
5. Steganography

## **Durasi Pengerjaan**

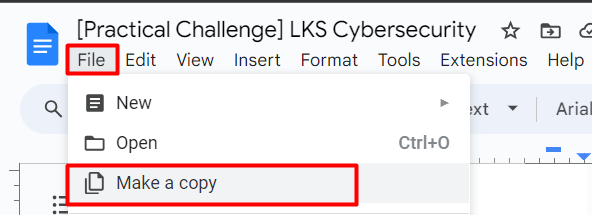
Pengerjaan challenge ini memiliki durasi **4 Jam** dari mulai lomba Cybersecurity dimulai higga selesai.

## **Cara Dokumentasi**

Silahkan untuk melakukan copy pada dokumen challenge ini dan dikerjakan pada **Google Docs** peserta masing-masing.

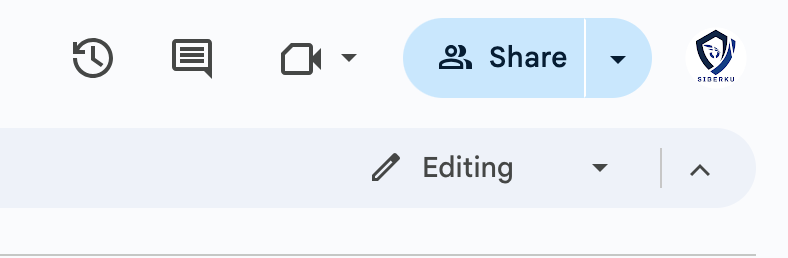
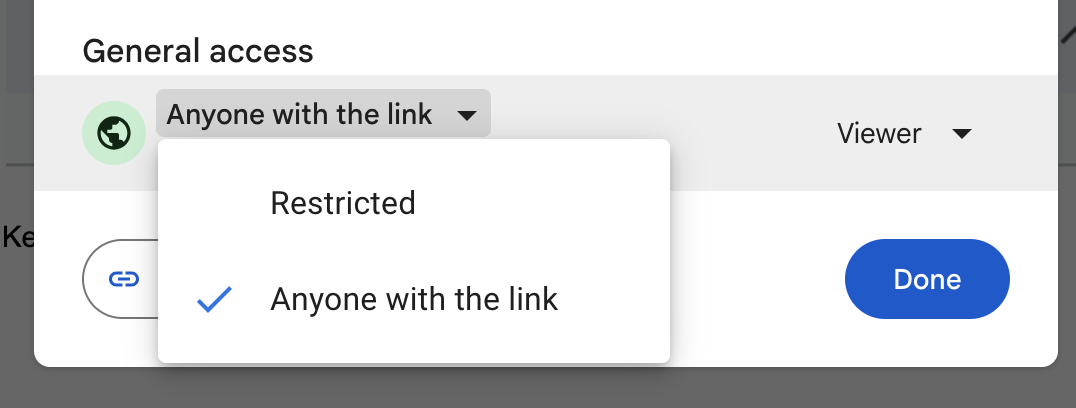
### **Cara duplikasi dokumen pada google docs:**

1. Buka pada bagian **File** kemudian pilih **Make a copy**.



1. Dokumen akan ter-duplikasi pada **google docs** peserta, dan peserta dapat langsung mengerjakannya.
2. Format nama file untuk dokumen masing-masing peserta adalah berikut:

|  |
| --- |
| Nama Sekolah \_ CYBERSECURITY \_ CTF  *Example: SMK 1 BEKASI\_CYBERSECURITY\_CTF* |

1. Diharapkan peserta memastikan bahwa dokumen dapat diakses secara public. Pilih pada bagian **Share**.
2. Kemudian, pada **General Access**, pilih opsi **Anyone With The Link**.

## **Link Submit Laporan**

Silahkan submit URL Google Docs laporan kamu apabila sudah selesai mengerjakan seluruh challenge pada link berikut: <https://forms.gle/Zauoa8oAV5Yqg9mW9> (tanggal 24 April 2024)

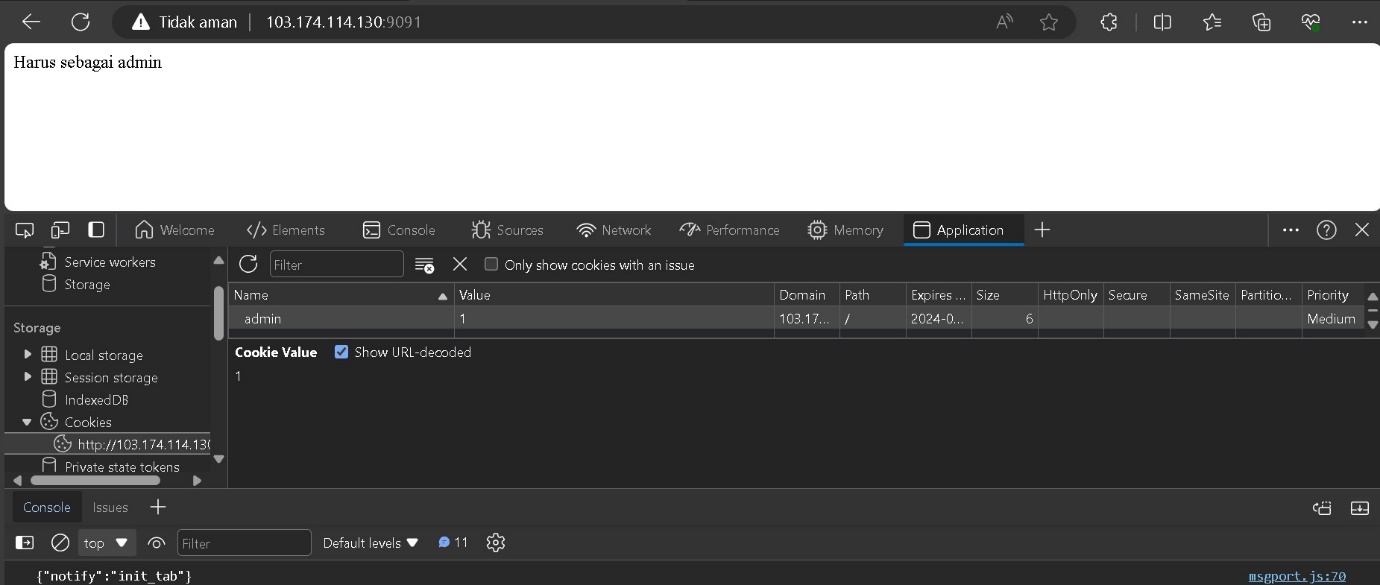
## **Index Penilaian**

1. Akumulasi persentase dari setiap kategori challenge.
2. Kecepatan pengerjaan dan ketepatan submit challenge pertama kali.
3. Kejelasan pada dokumentasi.

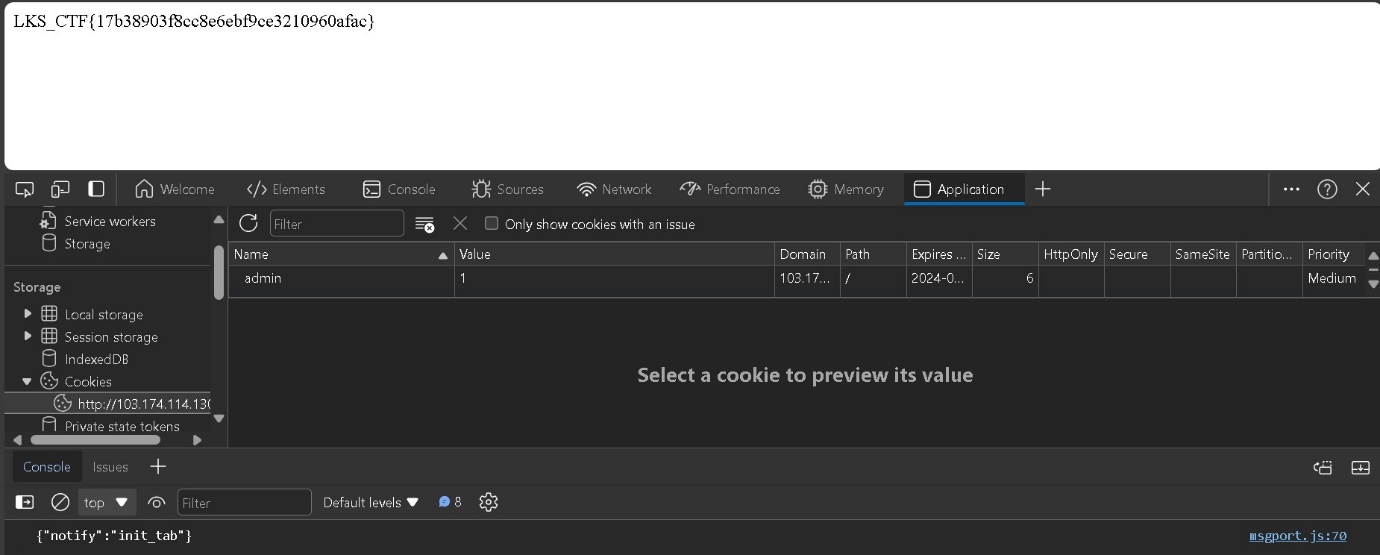
# 

# **WEB EXPLOITATION**

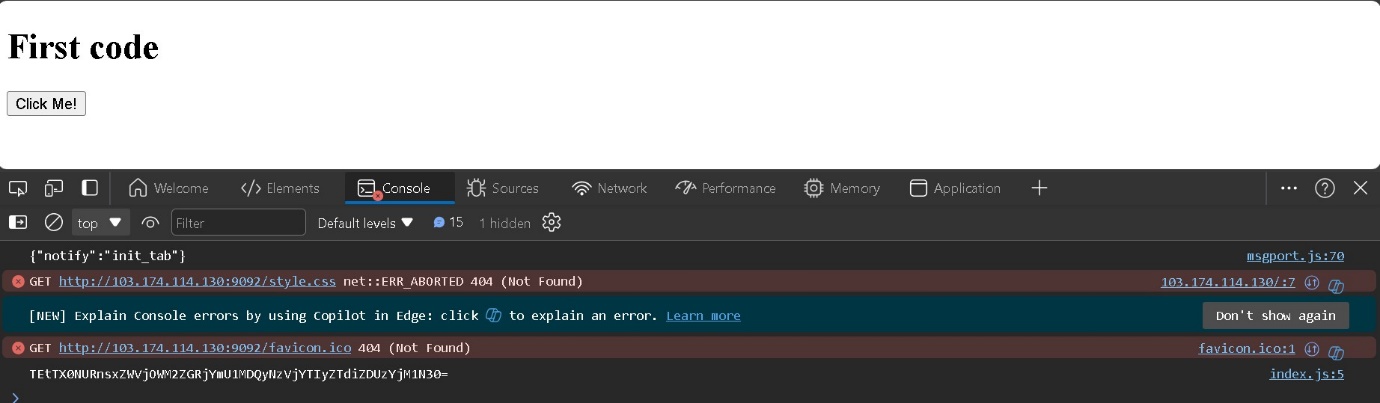
TASK-1 > pada halaman awal web hanya terdapat “ harus sebagai admin”



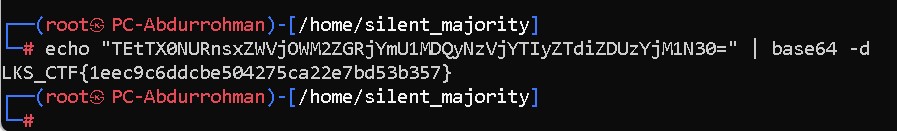
Setelah di edit pada cookiesnya dan direfresh terdapat flagnya pada TASK-1



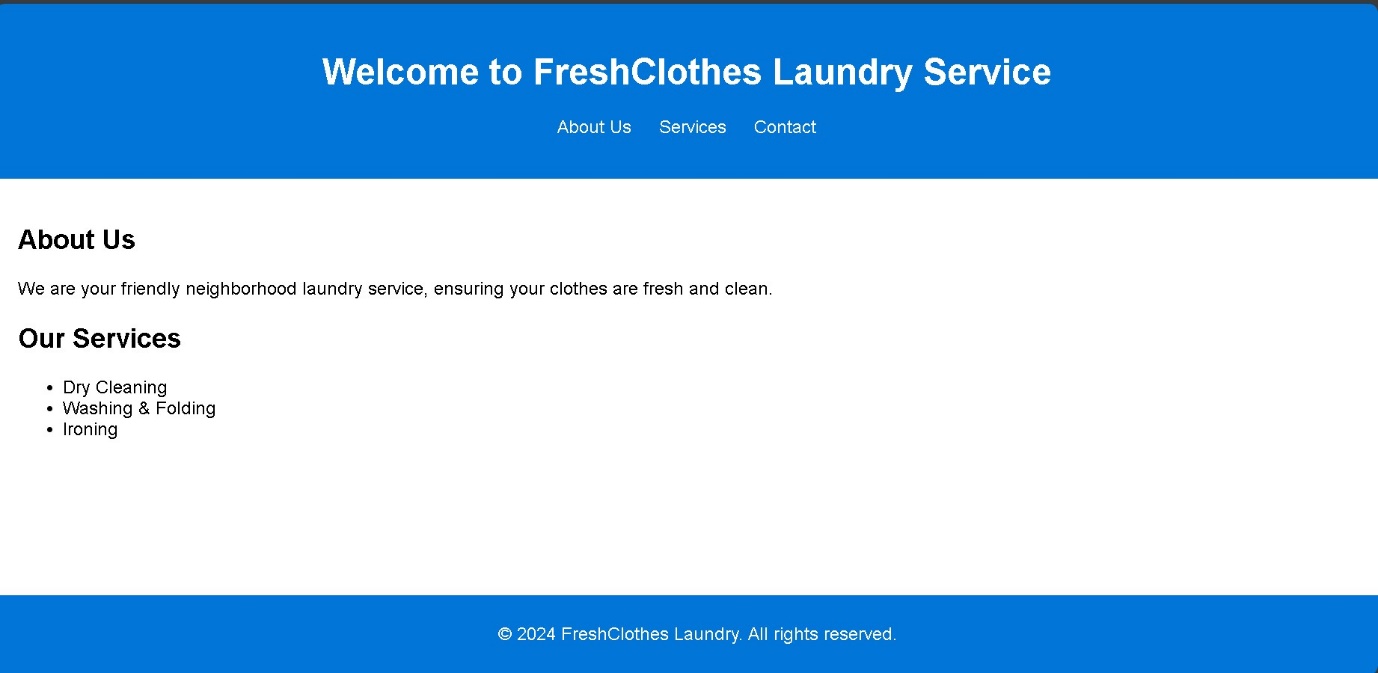
TASK-2 > Pada halaman awal web terdapat tombol klik “CLICK ME” setelah diklik dan dicek pada bagian console terdapat text ter enkripsi



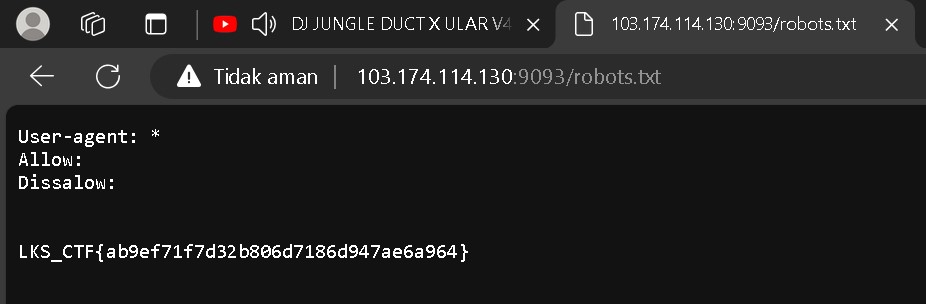
Dan setelah didecrypt dengan decoder tipe enkripsi base64 terdapat flag pada TASK-2



TASK-3 > pada halaman awal web hanya terdapat index.html



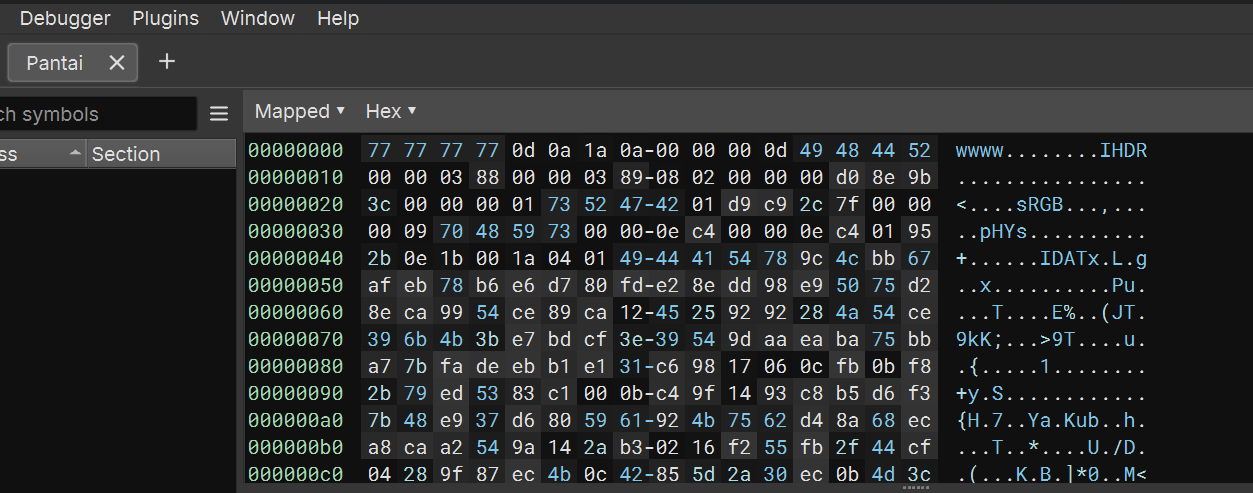
Setelah diubah pada belakang urlnya/path terdapat flag pada TASK-3



# 

# **DIGITAL FORENSIC**

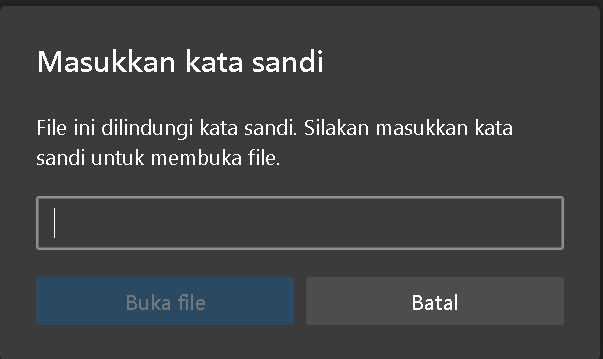
Pada tampilan awal file ketika dibuka menggunakan binaryninja/hxd pada headernya masih tertera “wwww”



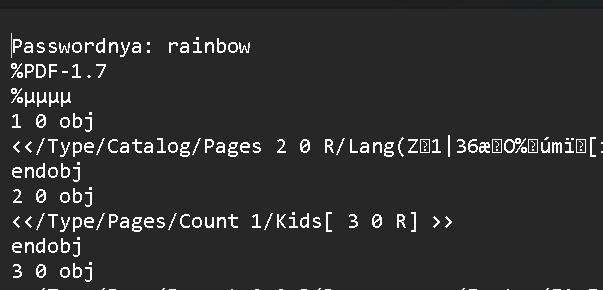
Setelah kita samakan headernya dengan foto mekar.png dari wwww jadi ‰PNG dan diubah format filenya dengan menambahkan .png pada belakang file lalu kita open dan kita gabungkan flag yang terdapat pada kedua foto tersebut terdapat flag pada TASK-1



TASK-2 > pada tampilan awal disaat mencoba membuka file ternyata terkunci



Setelah diubah format filenya menjadi .txt dan dibuka terdapat password yang dapat kita masukan untuk membuka file openme.pdf



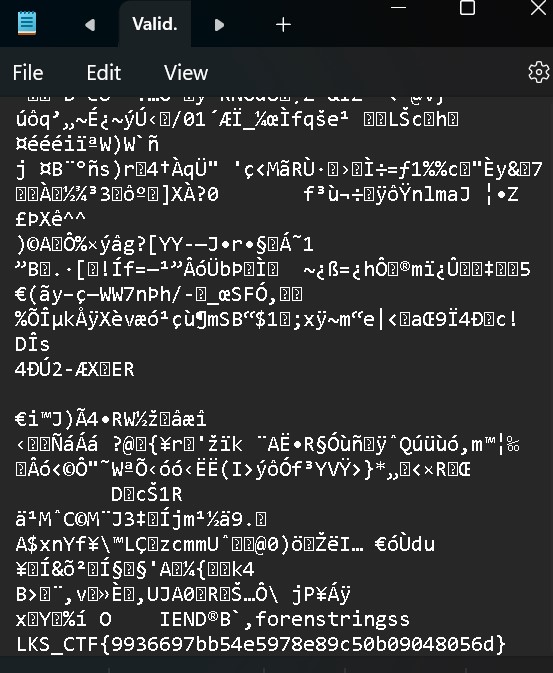
Setelah dibuka terdapat flag pada TASK-2



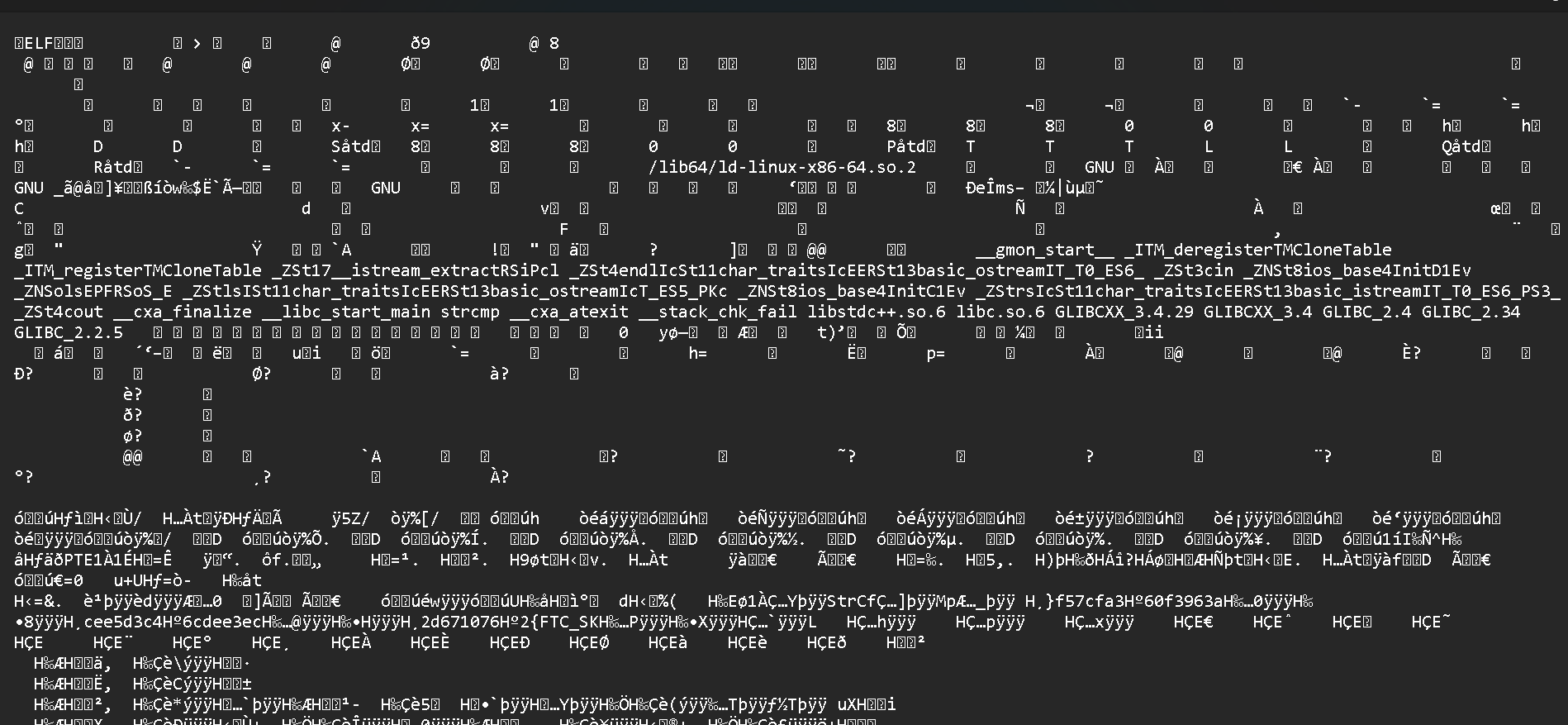
TASK-3 > pada tampilan awal file Valid.png hanya berisi gambar berikut



Setelah dibuka menggunakan notepad/binaryninja/hxd terdapat flag pada TASK-3

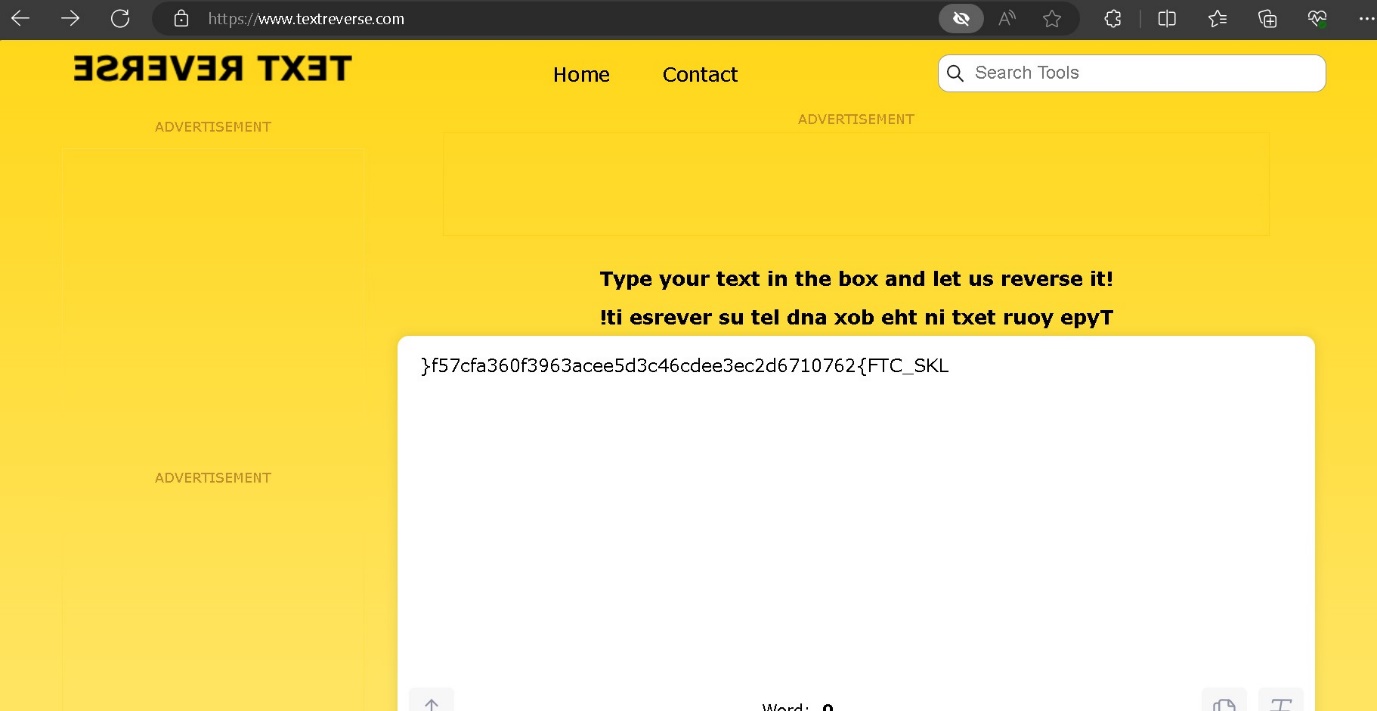


# **REVERSE ENGINEERING**

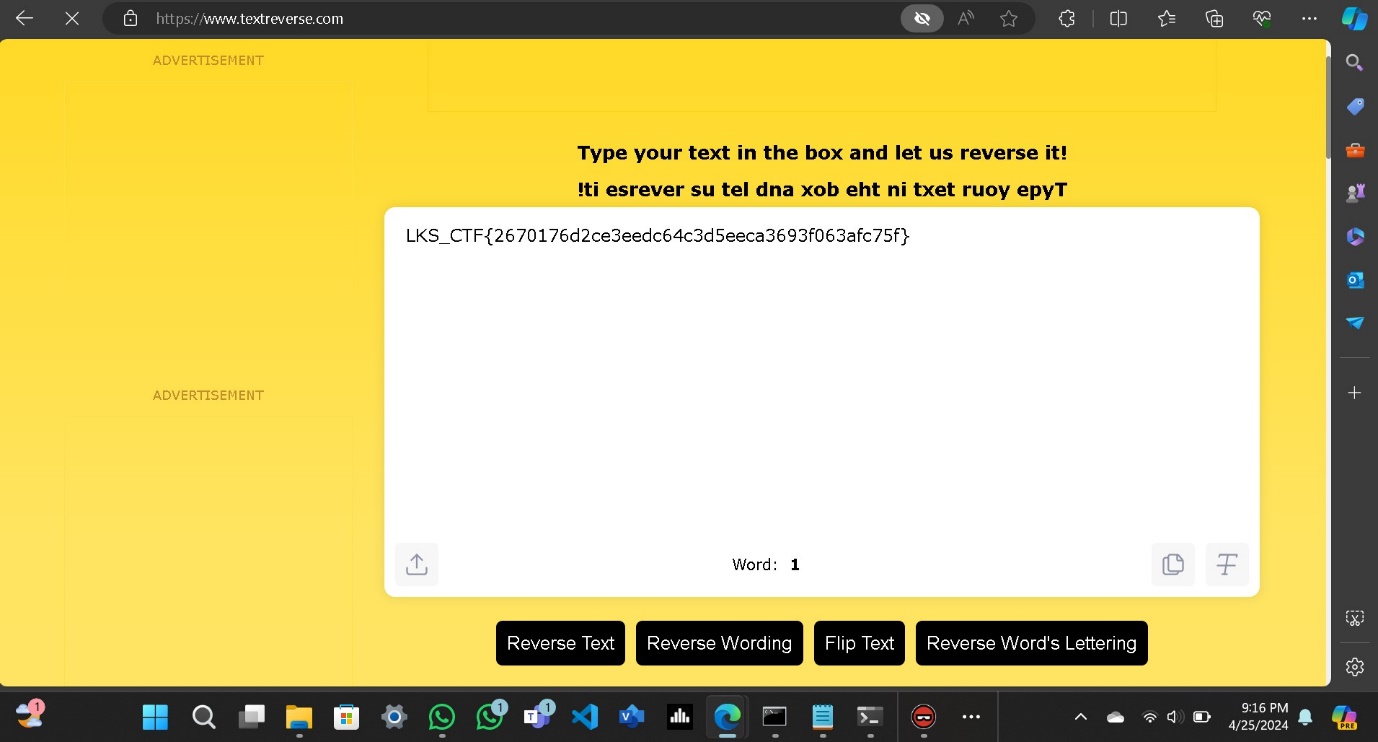
TASK-1 > Pada tampilan awal file berisi kode string berikut   


Setelah dibuka file /perbandingan dibuka dengan binaryninja dan discroll terdapat flag yang masih ke reverse textnya



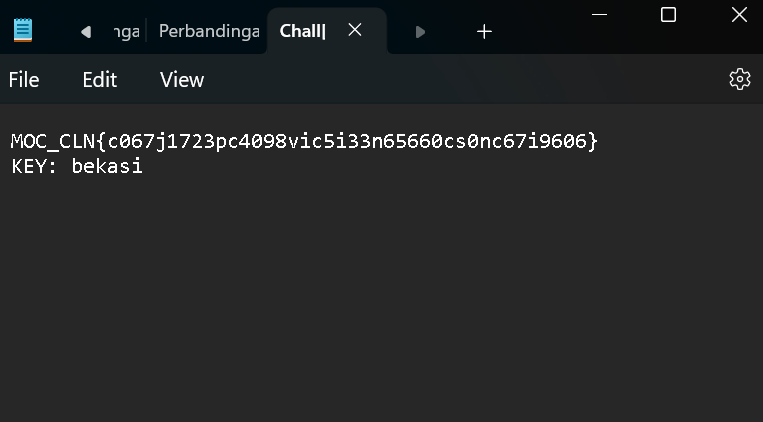
Lalu kita reverse textnya  


Setelah direverse textny terdapat flag pada TASK-1

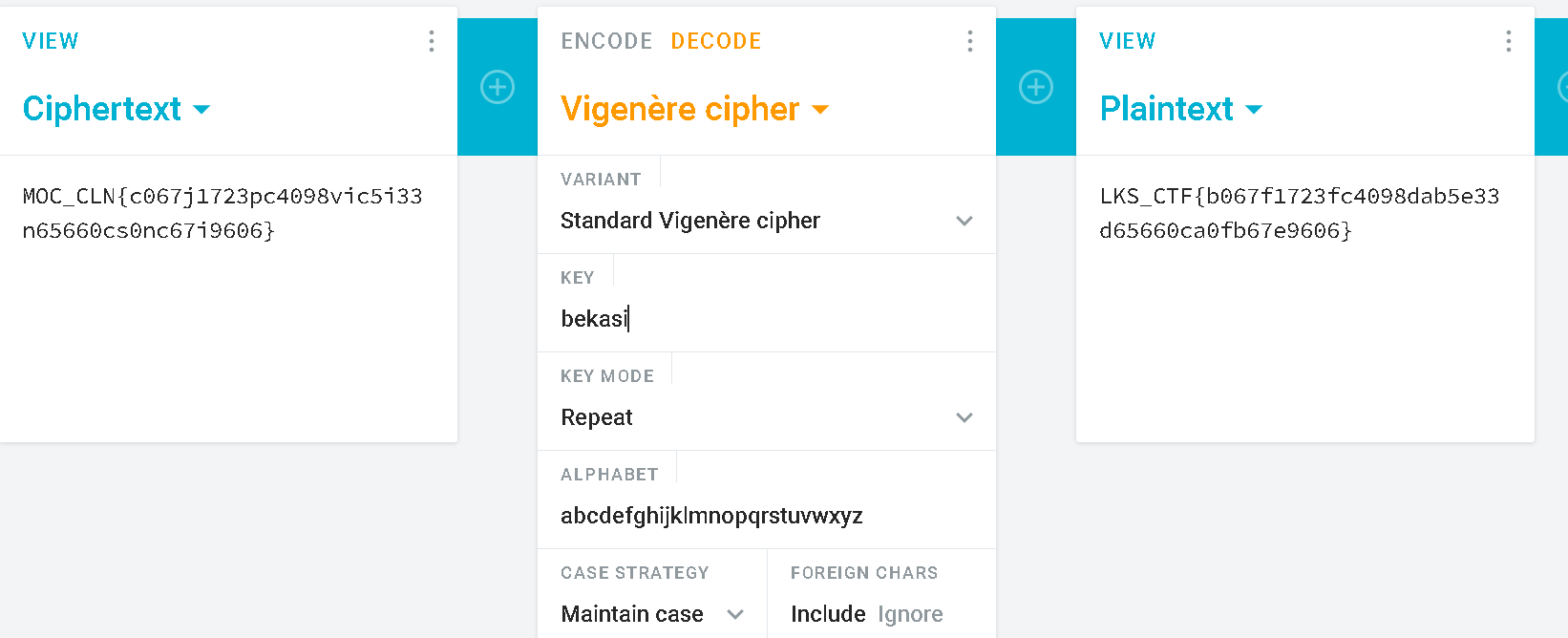


# **CRYPTOGRAPHY**

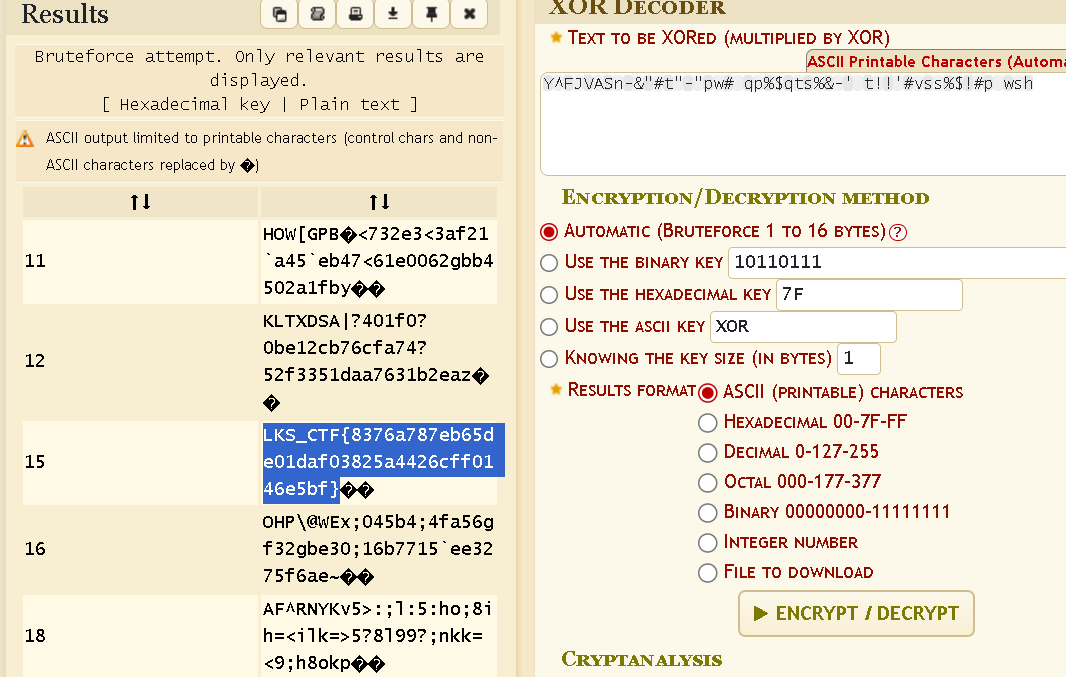
TASK-1 > pada tampilan awal file terdapat text terenkripsi kode cip vignere dengan key:bekasi



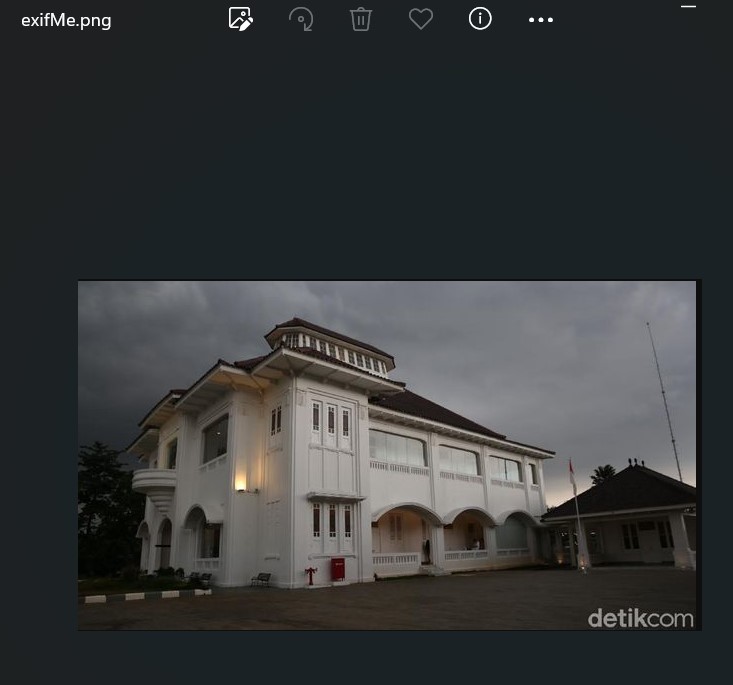
Setelah di decrypt dengan decryptor terdapat flag pada TASK-1

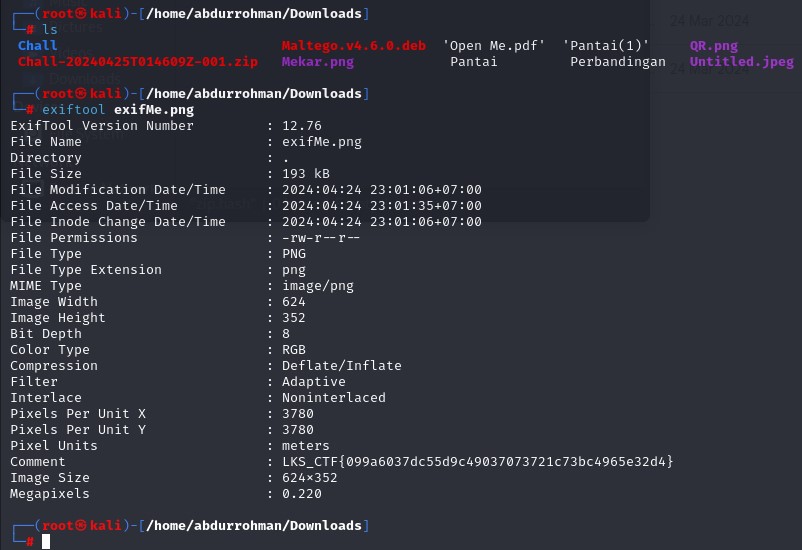


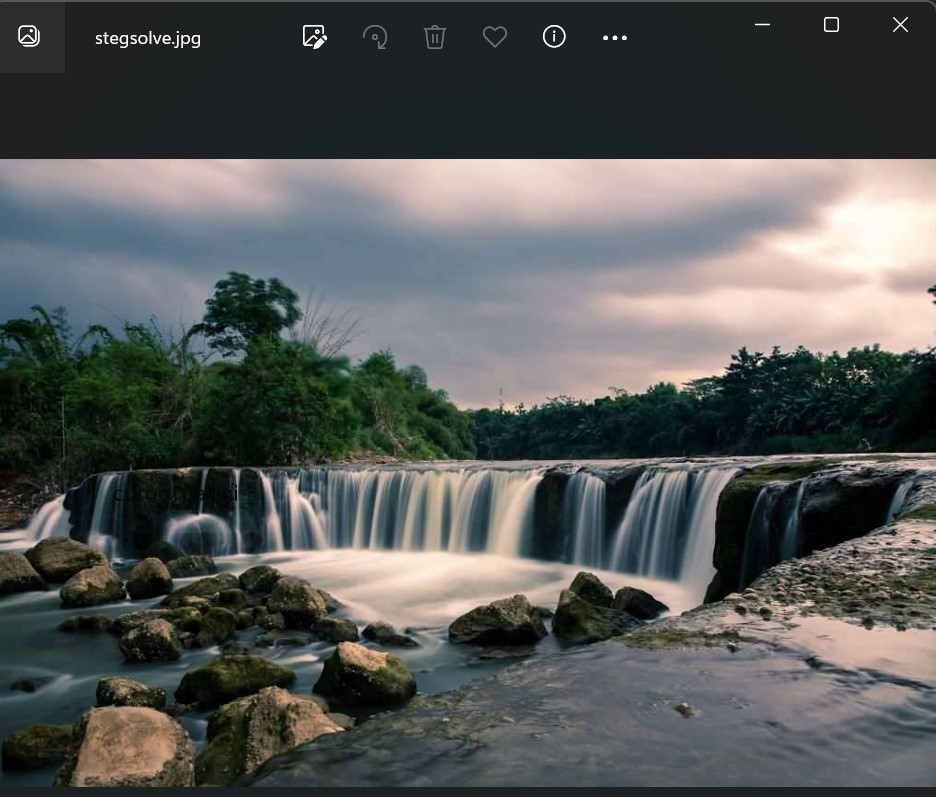
TASK-2 > terdapat text ternkripsi pada tampilan awal setelah didecrypt menggunakan decryptor xor terdapat flag pada TASK-2



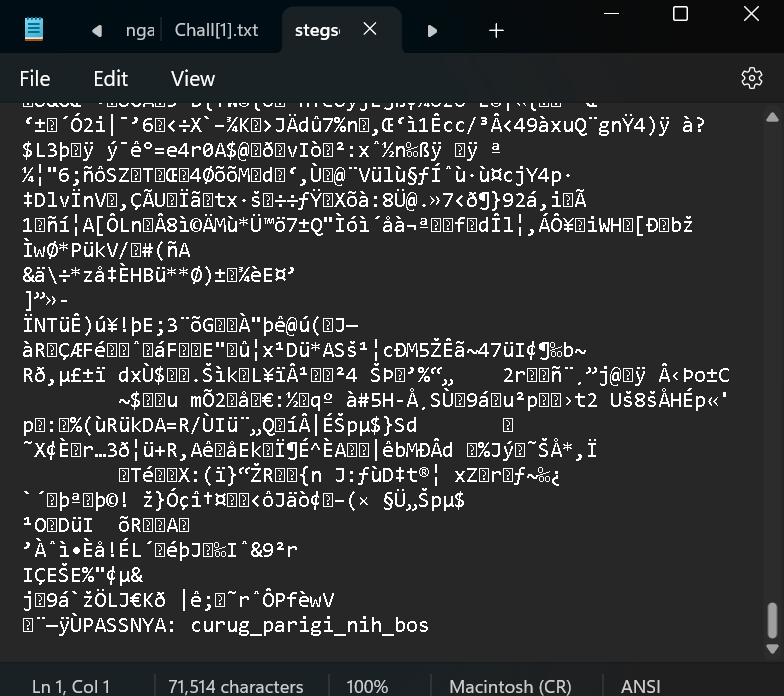
# **STEGANOGRAPHY**

TASK-1 > pada tampilan awal hanya terdapat gambar berikut  


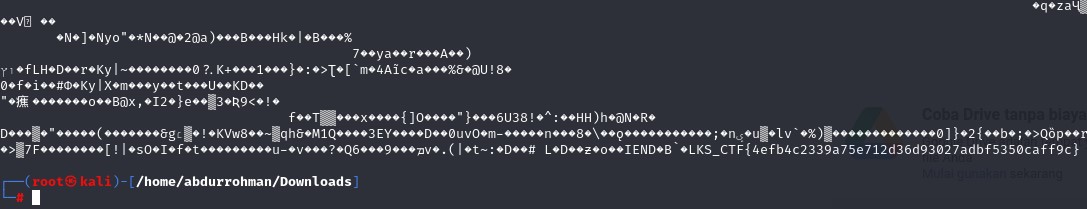
Setelah di cek menggunakan exiftool terdapat flag pada TASK-1  


TASK-2 > pada tampilan awal file stegsolve.png hanya terdapat gambar Berikut

Setelah format file stegsolve,png diubah menjadi stegsolve.txt kita scroll terdapat kunci untuk membuka file gatcha.zip



Sekarang kita buka file terdapat gatcha.png setelah kita ubah format filenya /metode cat pada bagian paling bawah terdapat flag



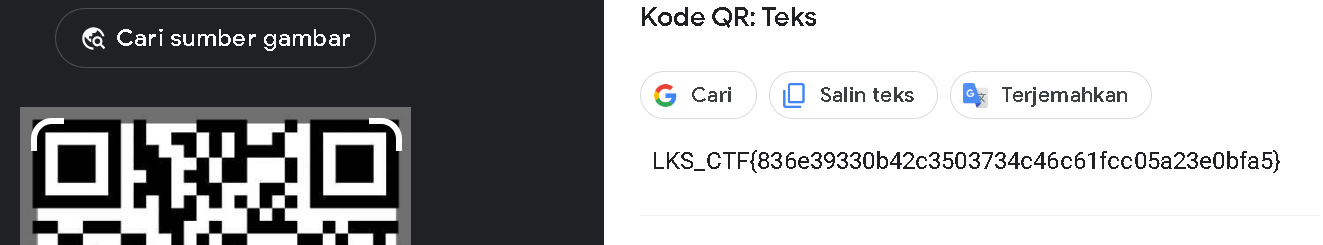
TASK-3 > terdapat file QR dalam keadaan sudah teredit



Setelah kita edit menggunakan photoeditor



Dan kita scan dengan search engine terdapat flag pada TASK-3



## **WEB EXPLOITATION**

### **TASK 1 - KUE ADMIN**

Tugas Anda adalah untuk memotong kue yang disediakan menggunakan "pisau admin". Kue ini merupakan sebuah analogi untuk sebuah website yang rentan terhadap serangan yang memanfaatkan kelemahan sistem administrasi. Anda diminta untuk menemukan celah keamanan di dalam website tersebut dan menggunakan "pisau admin" untuk memanfaatkannya.

**Endpoint**: <http://103.174.114.130:9091/>

***Dokumentasi, Jawaban dan Pembahasan:***

### **TASK 2 - KONSOLOG**

Tantangan "Konsolog" mengharuskan peserta untuk menemukan sebuah flag yang tersembunyi di dalam suatu pesan atau respon yang diberikan oleh website target. Peserta perlu melakukan eksplorasi dan analisis menyeluruh terhadap website tersebut untuk menemukan tempat di mana flag disembunyikan.

**Endpoint:** <http://103.174.114.130:9092/>

***Dokumentasi, Jawaban dan Pembahasan:***

### **TASK 3 - MR.ROBOT**

Tantangan "Mr.Robot" mengajak peserta untuk menemukan sebuah kunci yang tersembunyi di dalam website target. Peserta perlu melakukan eksplorasi menyeluruh terhadap halaman web dan mengidentifikasi cara untuk menemukan kunci tersebut tanpa adanya petunjuk yang spesifik.

**Endpoint:** <http://103.174.114.130:9093/index.html>

***Dokumentasi, Jawaban dan Pembahasan:***

### 

## **DIGITAL FORENSICS**

### **TASK 1 - MANIPULASI KEPALA**

Tantangan "Manipulasi Kepala" menantang peserta untuk membantu tim forensik dalam memperbaiki sebuah file yang mencurigakan. Peserta diminta untuk melakukan analisis dan manipulasi terhadap bagian-bagian tertentu dari file tersebut.

**Challenge:** <https://drive.google.com/drive/folders/1TfO24HEmoaqZ-GNN7b5kLXv_z_ISp4rj?usp=sharing>

***Dokumentasi, Jawaban dan Pembahasan:***

### **TASK 2 - OPENME!**

Tantangan "OpenMe!" meminta Anda untuk menemukan password yang mengunci sebuah file PDF. Anda harus mencari dan menemukan password tersebut untuk membuka file PDF tersebut dan mengungkap isinya.

**Challenge:** <https://drive.google.com/drive/folders/1DnluBiiz8VYD_OrqHRX6EPmr70IT0IaS?usp=sharing>

***Dokumentasi, Jawaban dan Pembahasan:***

### **TASK 3 - GAMBAR BAGUS**

Temukan flag yang tersembunyi di dalam sebuah gambar yang diberikan. Anda perlu memeriksa setiap detail gambar dengan cermat dan mencari tahu di mana flag tersebut disembunyikan.

**Challenge:** <https://drive.google.com/drive/folders/1h17GGtekwDjPvoBEzF2T_9PrlgHN2ARK?usp=sharing>

***Dokumentasi, Jawaban dan Pembahasan:***

## **REVERSE ENGINEERING**

### **TASK 1 - PERBANDINGAN**

Tantangan "Perbandingan" meminta Anda untuk menemukan password utama yang akan memberikan akses ke flag yang tersembunyi. Anda perlu melakukan pencarian teliti dan analisis yang mendalam untuk mengungkap password tersebut.

**Challenge:** <https://drive.google.com/drive/folders/1VRqIXr00ayhsdBzAv6yOFHbzZF1lD7i_?usp=sharing>

***Dokumentasi, Jawaban dan Penjelasan***

## **CRYPTOGRAPHY**

### **TASK 1 - KODE CIP VIGENERE**

Bantu intelijen dalam memecahkan sebuah kode chiper yang menggunakan metode Vigenere. Anda akan diberikan teks terenkripsi yang perlu diuraikan menggunakan pengetahuan tentang teknik chiper Vigenere. Dengan menggunakan kecerdasan dan ketelitian Anda, Anda akan memecahkan teka-teki ini dan mengungkap pesan yang tersembunyi di dalamnya.

**Challenge:** <https://drive.google.com/drive/folders/1J4YTqe10iMho79nKyIjoKqxtQRC8HuHn?usp=sharing>

***Dokumentasi, Jawaban dan Penjelasan***

### **TASK 2 - EKS OR**

Bantu intelijen dalam memecahkan sebuah enkripsi yang tidak diketahui. Anda akan diberikan teks terenkripsi yang perlu diuraikan menggunakan pengetahuan dan keterampilan kriptografi Anda. Dengan analisis yang teliti dan pemecahan teka-teki yang cerdas, Anda akan mencoba mengungkap pesan yang tersembunyi di dalamnya.

|  |
| --- |
| **XOR** |
| Y^FJVASn-&"#t"-"pw# qp%$qts%&-' t!!'#vss%$!#p wsh |

***Dokumentasi, Jawaban dan Penjelasan***

### 

## **STEGANOGRAPHY**

### **TASK 1 - EXIFME!**

Temukan flag yang tersembunyi dalam sebuah file yang diberikan. Lakukan pencarian dan analisis pada metadata file tersebut menggunakan pengetahuan dan keterampilan Anda. Dengan teliti mengeksplorasi setiap detail yang tersedia, Anda akan berusaha untuk menemukan flag yang disembunyikan di dalamnya.

**Challenge:** <https://drive.google.com/drive/folders/10jbDqoqi1F8wgdJLlxM0y-lBez7dUaTe?usp=sharing>

***Dokumentasi, Jawaban dan Penjelasan:***

### **TASK 2 - AWAS JEBAKAN**

Temukan teka-teki yang tersembunyi dalam sebuah gambar. Dalam gambar tersebut, terdapat petunjuk atau kode yang akan membawa Anda menuju gacha atau hadiah spesial. Dengan cermat memeriksa setiap detail gambar, Anda akan mencoba untuk mengungkap teka-teki yang tersembunyi di dalamnya.

**Challenge:**

<https://drive.google.com/drive/folders/1OjIqW8uOZ516j7r9qs-pJTDJGHa_fSnE?usp=sharing>

***Dokumentasi, Jawaban dan Penjelasan:***

### **TASK 3 - KIU AR**

Baca sebuah teks atau pesan yang tersembunyi di dalam gambar yang diberikan.

**Challenge:** <https://drive.google.com/drive/folders/1Wb7IllBjZyGAafZOatJoiXYvkdyCbQWy?usp=sharing>

***Dokumentasi, Jawaban dan Penjelasan:***