Table of Contents

[Forensics 2](#_Toc133669809)

[File Signature 2 2](#_Toc133669810)

[Steganography 3](#_Toc133669811)

[Steganography 2 3](#_Toc133669812)

[Steganography 3 4](#_Toc133669813)

[A Thousand Words 5](#_Toc133669814)

[Kuki’s Puzzle 8](#_Toc133669815)

# Forensics

## File Signature 2

Graphical user interface, text, application, Teams

Description automatically generated

Used the previous file, “file.jpeg”

Text

Description automatically generated

Binwalk the jpeg and will get an extracted folder with a file named secret\_msg

Text

Description automatically generated with medium confidence

Used ‘zip2john’ command, extract the password hashes of the zip file to a txt file named ‘gan.txt’.

After that, use ‘john’ to crack the password, which is ‘skr’.

# Steganography

## Steganography 2

Graphical user interface, text, application, Teams

Description automatically generated

I first use exiftool to check inner data, but there’s nothing, and also binwalk. After looking through hint, it let me use online tool. That means online steg decode tool. Additionally, it stated there’s a password,

Graphical user interface, text, application, email

Description automatically generated

Named, skr. And I got the flag.

Text

Description automatically generated

## Steganography 3

Graphical user interface, text, application, Teams

Description automatically generated

A zip file named File.zip downloaded, and unzipped

Text

Description automatically generated

Qr code

Description automatically generatedQr code

Description automatically generated

I opened PPT and import the picture into It, then overlap to the number, then I used Codex, and application for computer scanning QRcode, then I got the flag.

Timeline

Description automatically generated

## A Thousand Words

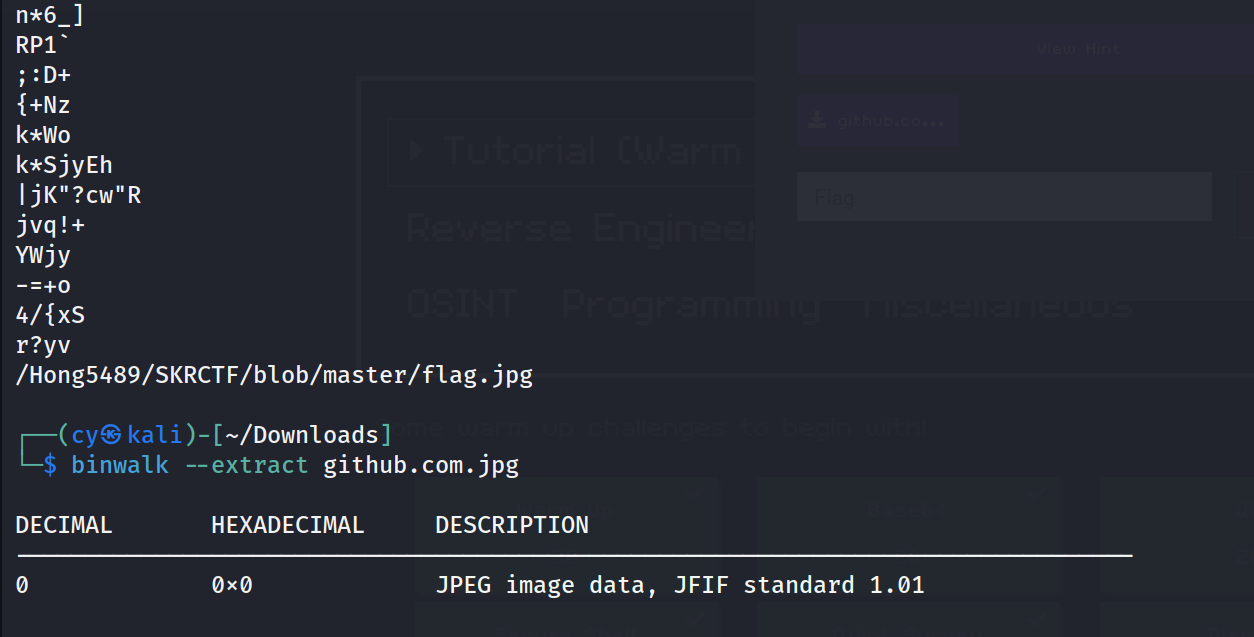
Graphical user interface, application, Teams

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

After downloading the file, I used exiftool and checked there’s some data inside. Then I used strings to see it, firstly I thought was a compressed folder inside, but after extracting, it’s not, so I went back to the question, and thought it may be a repository on GitHub.



Graphical user interface, application, website

Description automatically generated

I went to GitHub, and following the folder name given, which is /Hong5489/SKRCTF/blob/master/flag.jpg, and I got this image. After downloading, I used exiftool and checked there’s data inside the image.

Text

Description automatically generated

Text

Description automatically generated

This is the result, and the equal sign at the end may means it’s a base 64 encryption.

Graphical user interface, text, application

Description automatically generated

I went to cyberchef and found out it’s actually a triple base 64 encrypt, then the file is decrypted.

## Kuki’s Puzzle

Graphical user interface, application, Teams

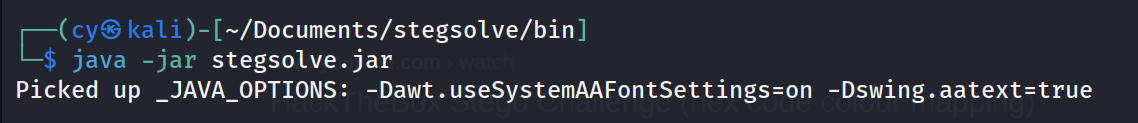
Description automatically generated

After extracting the zip file, I got tons of png files, like 100 of them, it’s obviously impossible to look through on by one, and I don’t is there any other way, so I open the hint, and it said stegsolve. It’s a image analyze tool that was made by java.

Text

Description automatically generated

I used wget to get the stegsolve file and store it into stegsolve.jar.



# Cryptography

## Beware of SHA1rk

Graphical user interface, text, application

Description automatically generated



Based on the title of the question, it stated something like SHA1, it’s an encryption method that can hash the data.

A screenshot of a computer

Description automatically generated



I went to the website that the question stated, and it’s hashes encrypt and decrypt website, so I paste the heshes into it and decrypt it.

## Xtra ObscuRe Service

Graphical user interface, application, Teams

Description automatically generated

Graphical user interface, text, application

Description automatically generated

After looking through the hint, I tried to input lots of A.

Graphical user interface, text, application

Description automatically generated

Then, the flag is out. Based on the flag, we can know the encryption is based on XOR cipher. This kind of cipher is done with lines of key. For example, we can use 1010 as the key, and transfer the text we wanted to ASCII. For instance, the text is 1001, and 1010 + 1001 = 0011. And for decrypt, we can still use the same key to decrypt, this is why it’s not secure.

## Recette Secrete

Graphical user interface, application, Teams

Description automatically generated

Text

Description automatically generated

Used unzip … -d … to extract a zip file to a folder.

Text

Description automatically generated

According to the question, I opened the ‘ingredient’ directory, and cat the ingredient, and I got the part of the flag, and as it says, password is not found,

Can’t solve, TBD.