Challenge Security (**CTFlearn**)

Name: Rimas Alharbi

Months: June-July

Supervised: Eng. Fahad Alsadda And Ms. Reeman Alharbi

1. Overall Summary

This document provides a comprehensive summary of the cybersecurity challenges I am working on as part of my learning and skill development in the field of security. These challenges cover a wide range of attack and defense techniques that are essential. The primary goal is to strengthen my practical knowledge in identifying vulnerabilities, exploiting them responsibly in a controlled environment, and applying appropriate defensive measures. Each challenge is designed to simulate real-world scenarios using a safe and isolated lab environment, ensuring ethical practice. The outcomes of these exercises will enhance my ability to conduct security assessments and respond effectively to potential threats.

2. Study Progress

2.1 Forensics 101 Challenge (easy Level)

1. First, visit this site. "https://mega.nz/#!OHohCbTa!wbg60PARf4u6E6juuvK9-aDRe_bgEL937VO01EImM7c"
2. Download the image, create a file named CTF and rename for ex:
3. Write in terminal "cd CTF" Go into the folder named CTF that exists in the current directory.
4. Write in terminal "exiftool Forensics\ 101.jpeg"Use exiftool to extract metadata from the file named Forensics 101.jpeg
5. Write in terminal "strings Forensics\ 101.jpeg "Use strings Extract readable text (ASCII strings) from inside the image file Forensics 101.jpeg
6. Well done we have found the flag.

Screenshot:

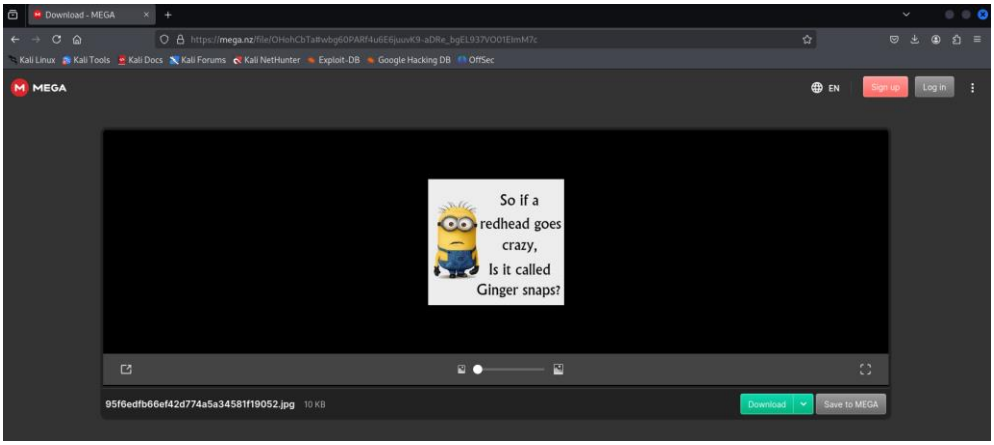

Figure 1

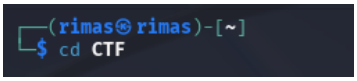

Figure 2

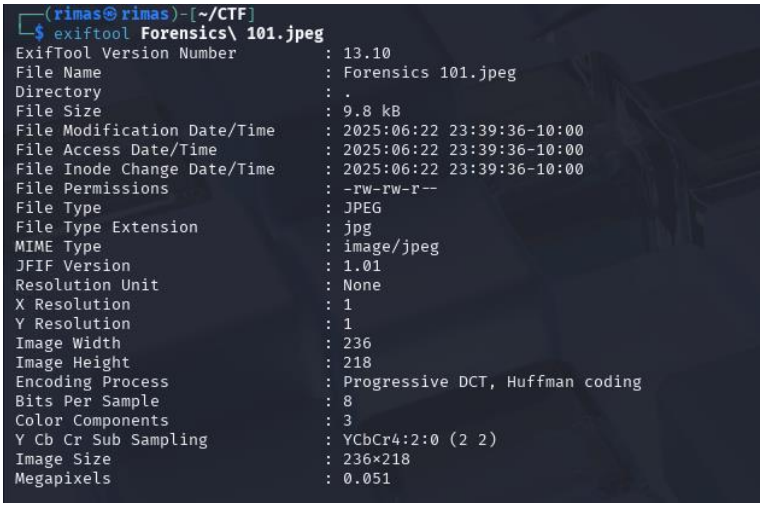

Figure 3

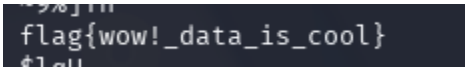

Figure 4

Figure 5

2.2 Taking LS Challenge (easy Level)

1. First, visit this site. https://mega.nz/#!mCgBjZgB!_FtmAm8s_mpsHr7KWv8GYUzhbThNn0I8cHMBi4fJQp8
2. Download the ZIP File.
3. Write in Terminal “unzip The\ Flag.zip” To open the ZIP file.
4. Write in Terminal “cd The\ Flag” Go into the folder named The Flag that exists in the current directory.
5. Write in Terminal “ls -la” to lists all files and folders, including hidden ones, with detailed information.
6. Take the file highlighted in a different color because it is the hidden file.
7. Repeat step 2 in ThePassword' file
8. Repeat step 2
9. Write in Terminal “cat ThePassword.txt” to Display the contents of a file in the terminal.
10. Well done we have found the password and go to The flag PDF and write the password.

Screenshot:

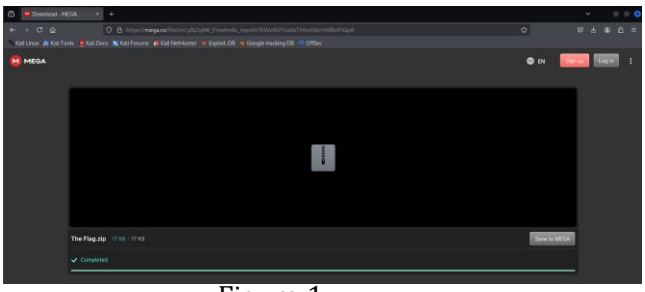

Figure 1

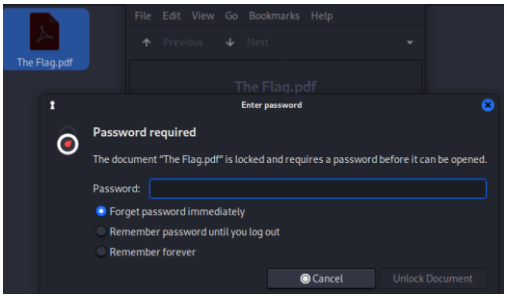

Figure 2

```
┌──(rimas㉿rimas)-[~/Challengs/Taking _LS]
└─$ unzip The\ Flag.zip
Archive:  The Flag.zip
   creating: The Flag/
  inflating: The Flag/.DS_Store
   creating: __MACOSX/
   creating: __MACOSX/The Flag/
  inflating: __MACOSX/The Flag/._.DS_Store
   creating: The Flag/.ThePassword/
  inflating: The Flag/.ThePassword/ThePassword.txt
  inflating: The Flag/The Flag.pdf
  inflating: __MACOSX/The Flag/._The Flag.pdf

┌──(rimas㉿rimas)-[~/Challengs/Taking _LS]
└─$ cd The\ Flag

┌──(rimas㉿rimas)-[~/Challengs/Taking _LS/The Flag]
└─$ ls
'The Flag.pdf'

┌──(rimas㉿rimas)-[~/Challengs/Taking _LS/The Flag]
└─$ ls -la
total 40
drwxr-xr-x 3 rimas rimas  4096 Oct 30  2016  .
drwxrwxr-x 4 rimas rimas  4096 Jun 24 22:48  ..
-rw-r--r-- 1 rimas rimas  6148 Oct 30  2016  .DS_Store
-rw-r--r-- 1 rimas rimas 16647 Oct 30  2016 'The Flag.pdf'
drwxr-xr-x 2 rimas rimas  4096 Oct 30  2016  .ThePassword
```

Figure 3

```
┌──(rimas㉿rimas)-[~/Challengs/Taking _LS/The Flag]
└─$ cd .ThePassword

┌──(rimas㉿rimas)-[~/Challengs/Taking _LS/The Flag/.ThePassword]
└─$ ls
ThePassword.txt

┌──(rimas㉿rimas)-[~/Challengs/Taking _LS/The Flag/.ThePassword]
└─$ cat ThePassword.txt
Nice Job!  The Password is "Im The Flag".
```

Figure 4

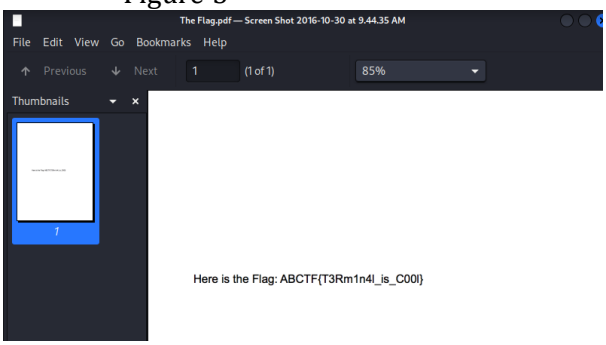

Figure 5

2.3 What could this be? (Medium Level)

1. First, visit this site. https://mega.nz/#!SDQkUYQZ!b1Fu7iZ_wGiNX0aOjez95_74TYDCnLb3YSQfRzs0J-o
2. Download the what_can_this_be .txt.
3. So you can see it is a JSfuck
4. Go to https://jsfuck.com/
5. Copy and paste and run the text to the site to find out the flag.
6. The flag (flag{5uch_j4v4_5crip7_much_w0w})

Screenshot:

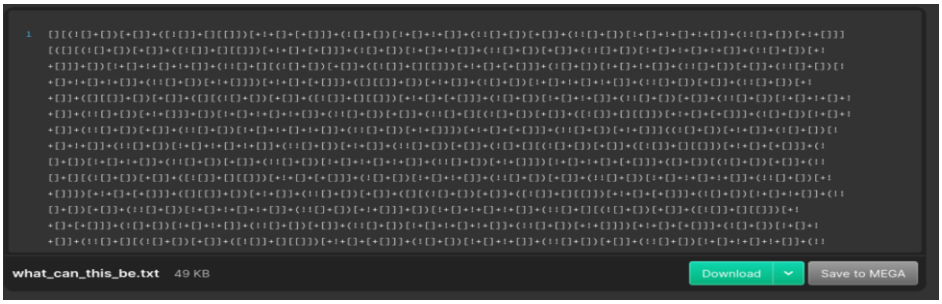

Figure 1

Figure 2

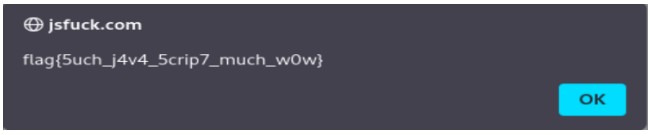

Figure 3

2.4 Substitution Cipher (Medium Level)

1. First, visit this site. https://mega.nz/#!iCBz2IIL!B7292dJSx1PGXoWhd9oFLk2g0NFqGApBaItI_2Gsp9w Figure it out for me, will ya?
2. Download the Substitution .txt.
3. You can go to this site to Analyze the speech and solve the problem yourself. I solved it myself, then I used a site to solve the codes because of the time like https://legacy.cryptool.org/en/cto/frequency-analysis.
4. The site that solves https://www.guballa.de/substitution-solver
5. Copy and paste and run the text to the site to find out the flag.
6. The flag it is (flag{IFONLYMODERNCRYPTOWASLIKETHIS})

Screenshot:

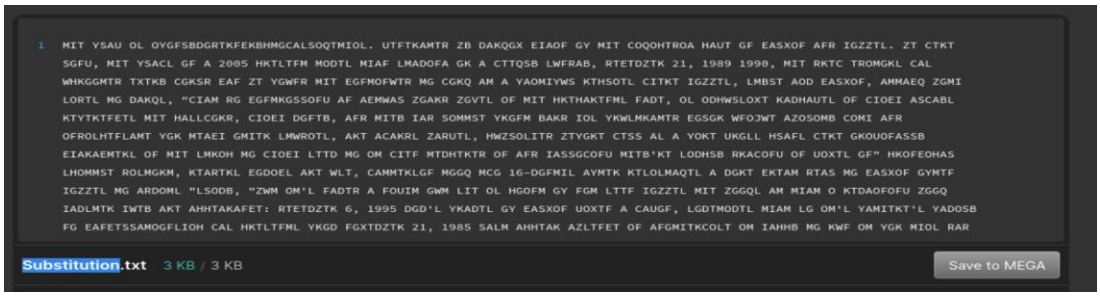

Figure 1

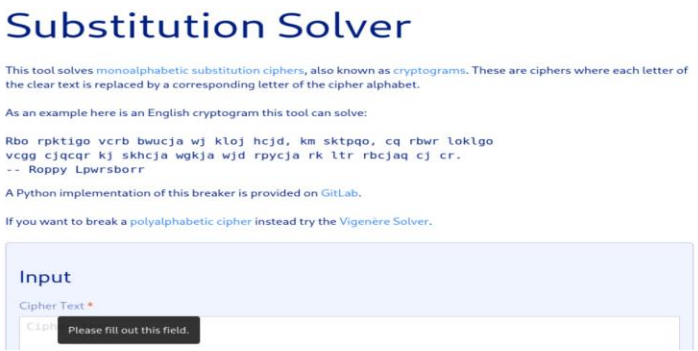

Figure 2

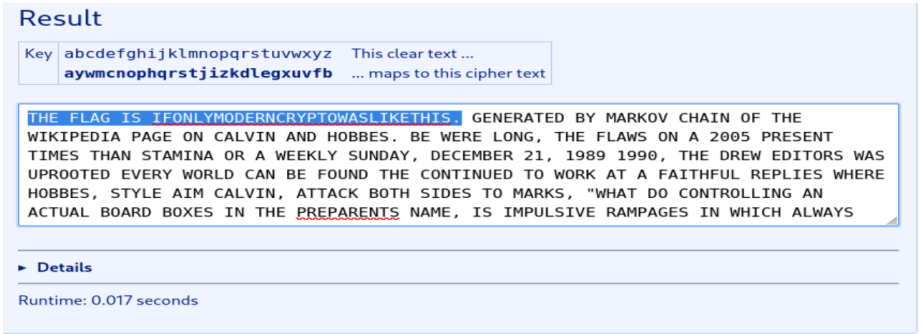

Figure 3

2.5 The adventures of Boris Ivanov. Part 1. (Medium Level)

1. First, visit this site. https://mega.nz/#!HfAHmKQb!zg6EPqfwes1bBDCjx7-ZFR_0O0-GtGg2Mrn56l5LCkE
2. Download the Boris_Ivanov_1 .jpg.
3. Write in Terminal “sudo -s” starts a new shell with root privileges, allowing you to run commands as the root user without switching users completely.
4. Write in Terminal “cd Downloads” Change into the Downloads directory from the current location.
5. Write in Terminal “ls” List the files and folders in the current directory.
6. Write in Terminal “file Boris_Ivanov_1.jpg” tell me the type of the file.
7. Write in Terminal “java -jar stegsolve.jar” To Run the StegSolve tool using Java.
8. Open the Image Boris_Ivanov_1.jpg from File.
9. And go to analyse and go to stereogram solver and change the offset to 102.

Screenshot:

Figure 1

Figure 2

Figure 3

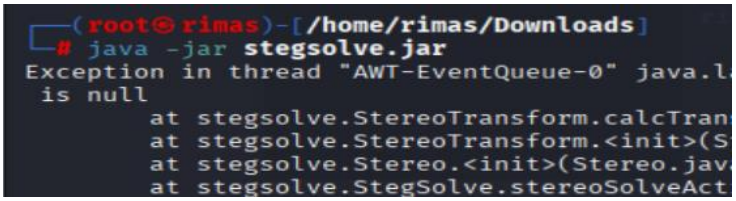

Figure 4

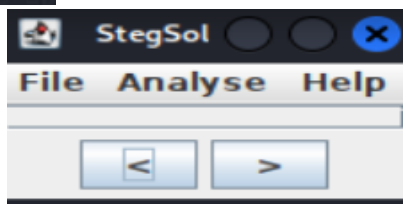

Figure 5

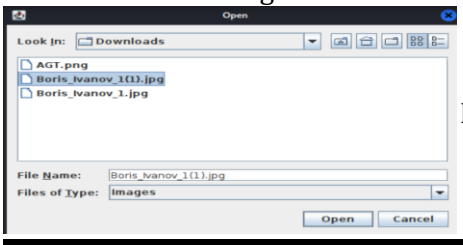

Figure 6

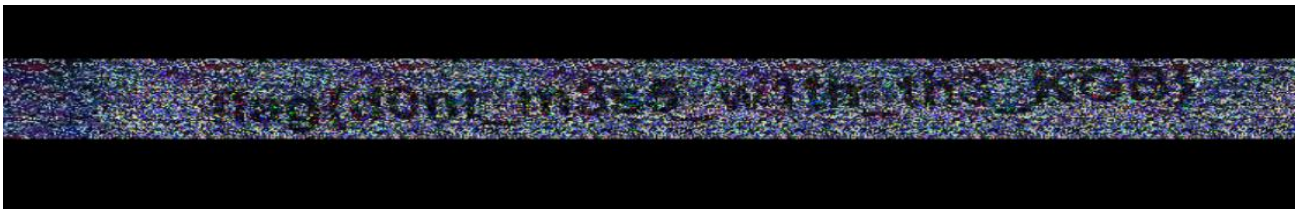

Figure 7

2.6 PIN (Medium Level)

1. First, visit this site. https://mega.nz/file/PXYjCKCY#F2gcs83XD6RxjOR-FNWGQZpyvUFvDbuT-PTnqRhBPGQ
2. Download the rev1 file.
3. Write in Terminal “cd Downloads” Change into the Downloads directory from the current location.
4. Write in Terminal “ls” List the files and folders in the current directory.
5. Write in Terminal “chmod +x rev1” is used in Linux to make the file rev1 executable, so you can run it like a program or script.
6. Write in Terminal “./rev1” try to run a file and write the PIN.
7. Write in Terminal “r2 -AA rev1” This command opens the file rev1 in Radare2 (r2) and performs deep automatic analysis.
8. In Radare2, write ood This reopens the file in debug mode, allowing you to step through the program during execution.
9. Write pdf @main This command disassembles and displays the instructions inside the main function.
10. Write pdf @sym.cek This shows the disassembly of the cek function, which contains the logic used to check the correct PIN.
11. From analyzing the function, identify the correct PIN value (e.g., 333333) and use it to run the file successfully.

Screenshot:

Figure 1

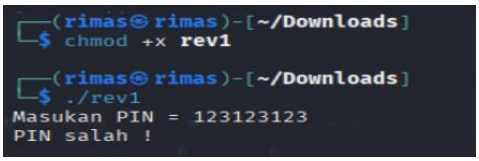

Figure 2

Figure 3

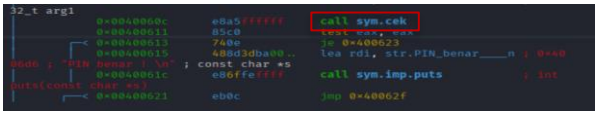

Figure 4

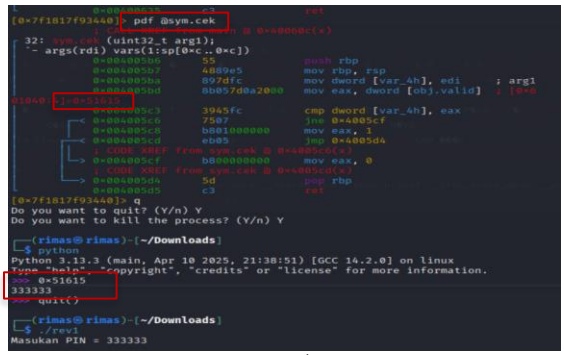

Figure 5

2.7 Calculat3 M3. (Hard Level)

1. First, visit this site. http://web.ctflearn.com/web7/.
2. I right-clicked anywhere on the page and chose Inspect to open Developer Tools.
3. I entered a basic expression in the calculator, for example: 9 * 9, then clicked the "=" button to calculate.
4. I went to the Network tab to monitor requests sent by the calculator.
5. I looked at the first network request that appeared in the list after I clicked "="
6. I clicked on that request to see the expression, then go to header then resend and go to the body.
7. I modified the expression to: expression=;ls — trying to test for command injection.
8. I clicked on send the expression and clicked the new state and go to the response and see the flag.

Screenshot:

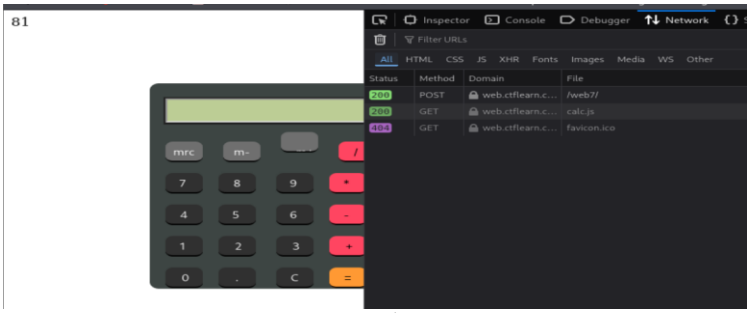

Figure 1

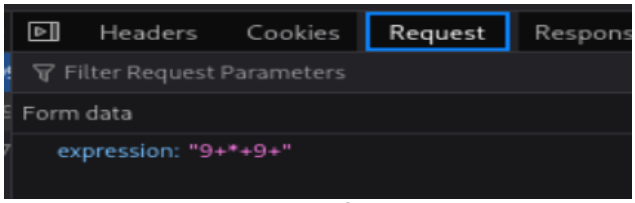

Figure 2

Figure 3

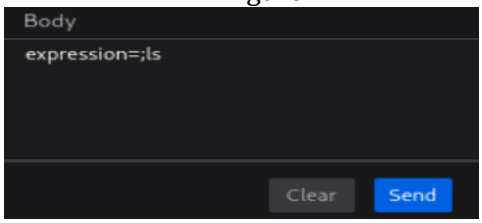

Figure 4

Figure 5

2.8 Corrupted File. (Hard Level)

1. First, visit this site. https://mega.nz/#!OKxByZyT!vaabCJRG5D9zAUp7drTekcA5pszu67r_TbQMtxEzqGE
2. Download the unopenable .gif.
3. Write in Terminal “file unopenable.gif” tell me the type of the file.
4. Write in Terminal “hexdump -C unopenable.gif | head -n 5” This shows the first few lines of the file in hex. The first 6 bytes of a real .gif file.
5. Write in Terminal “echo -ne '\x47\x49\x46\x38\x39\x61' > fixed.gif” This creates a new file called fixed.gif and writes the correct .gif header to it.
6. Write in Terminal “tail -c +2 unopenable.gif >> fixed.gif” corrupted file starting from the second byte and appends it to the new file fixed.gif.
7. Write in Terminal “identify fixed.gif” uses ImageMagick to show detailed information about the image.
8. Write in Terminal “convert fixed.gif frames_%02d.png” split the animated GIF into separate PNG images.
9. Go to Downloads file and see the image, see the text in image, go to the https://www.base64decode.org/
10. Decode the text “ZmxhZ3tnMWZfb3JfajFmfq==”
11. See the flag.

Screenshot:

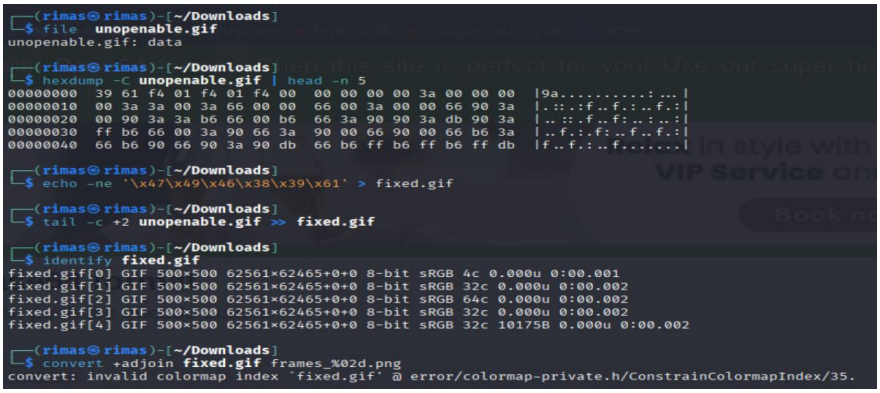

Figure 1

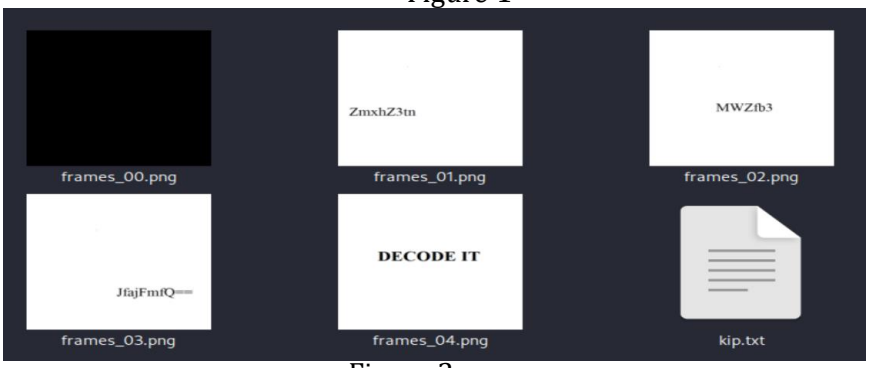

Figure 2

Figure 3

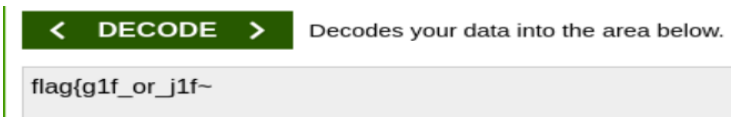

Figure 4