

BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Kỳ báo cáo: Buổi 3

Tên chủ đề: Steganography & Steganalysis

GVHD: Lê Đức Thịnh

Ngày báo cáo: 15/05/2023

Nhóm: 7

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Nguyễn Bùi Kim Ngân	20520648	20520648@gm.uit.edu.vn
2	Nguyễn Bình Thực Trâm	20520815	20520815@gm.uit.edu.vn
3	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Thực hiện	Thành viên thực hiện	Kết quả tự đánh giá
1	Kịch bản 01	Đã thực hiện tại lớp	Trâm, Kiệt	100%
2	Kịch bản 02	Đã thực hiện tại lớp	Trâm	100%
3	Kịch bản 03	Đã thực hiện tại lớp	Kiệt	100%
4	Kịch bản 04	Tìm flag	Ngân	100%
5	Kịch bản 05	Tìm flag	Ngân	100%
6	Kịch bản 06	Tìm flag	Trâm	100%
7	Kịch bản 07	Tìm flag	Trâm	100%
8	Kịch bản 08	Tìm flag	Kiệt	100%
9	Kịch bản 09	Tìm flag	Kiệt	100%
10	Kịch bản 10	Tìm flag	Kiệt	100%

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành,

Lưu ý: Chỉ ghi Kịch bản thực hành được GVTTH chỉ định phải làm báo cáo

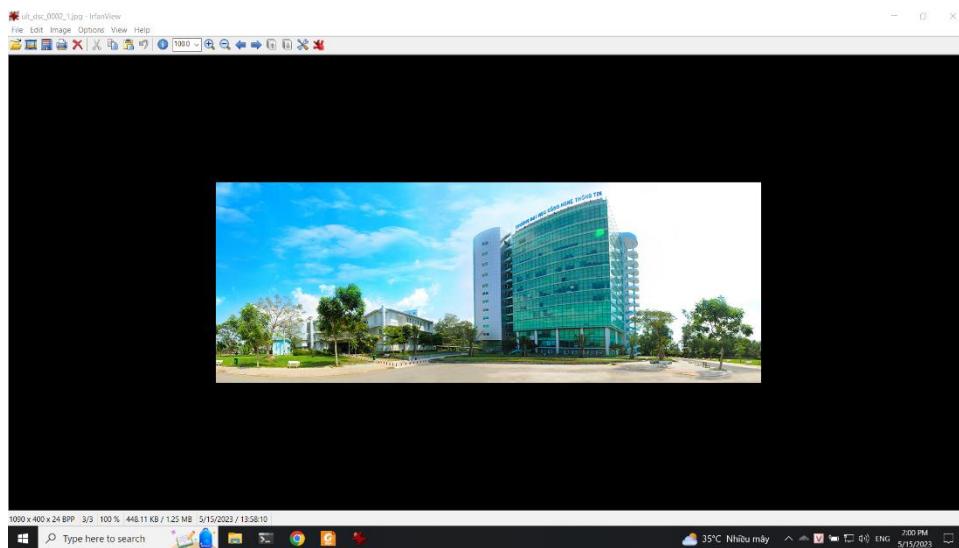
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

(Xem trang kế tiếp)

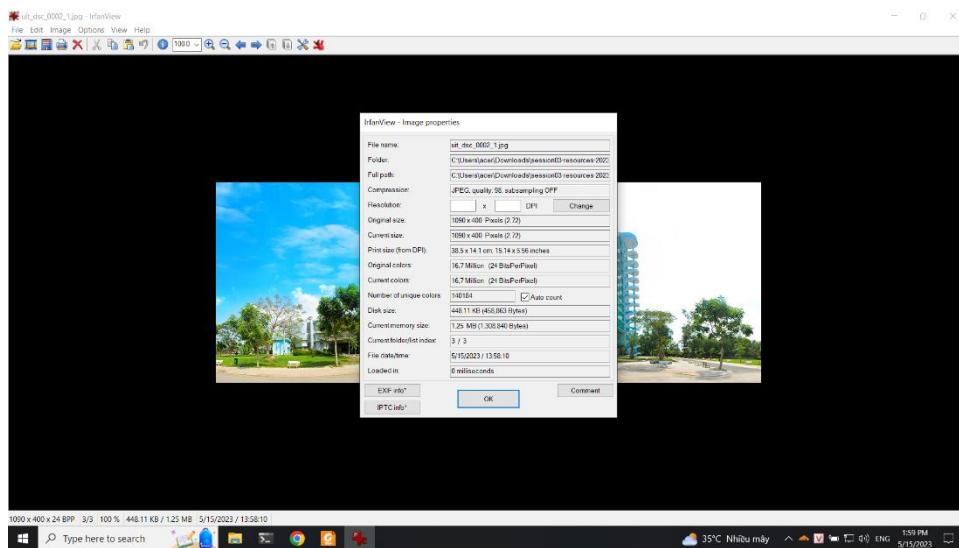
BÁO CÁO CHI TIẾT

1. Kịch bản 01

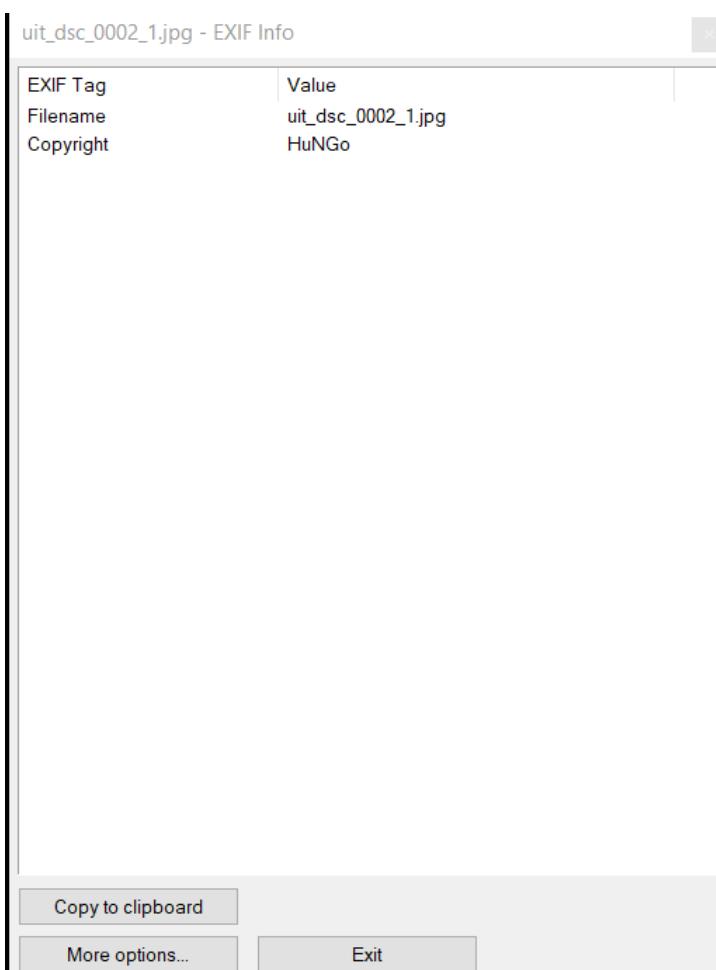
Ảnh 1: uit_dsc_0002_1.jpg



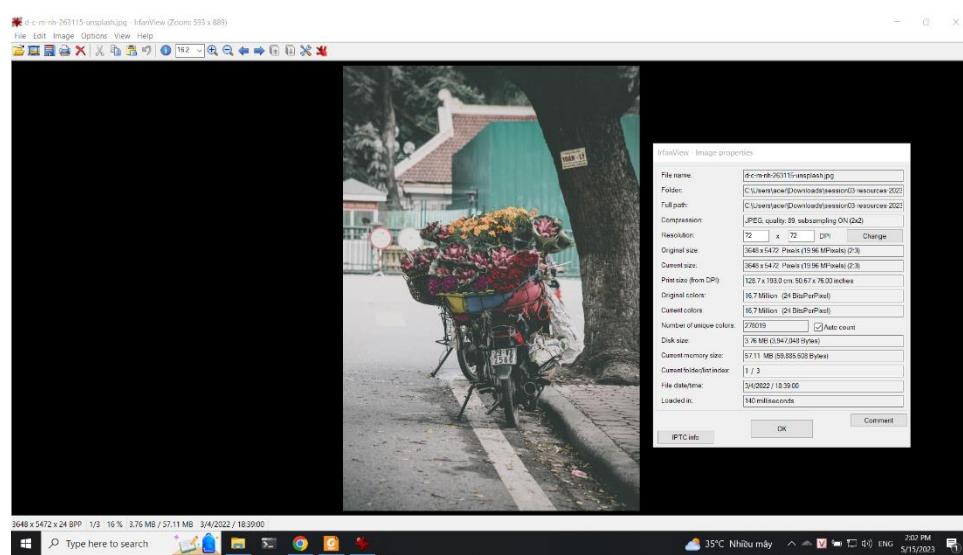
Chọn image -> infor để coi thông tin ảnh



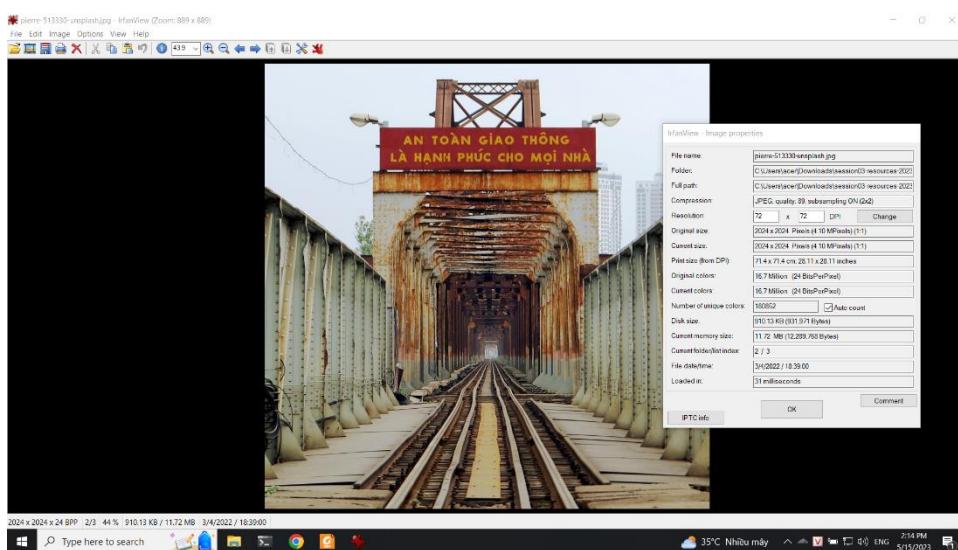
Kiểm tra exif infor thì ta có được thông tin Copyright là HuNGo



Ảnh 2 Ở đây ta không thấy thông tin về exif infor



Ảnh 3 không có exif



Kích bản 1b

Giấu file

JPHS for WIndows - Freeware version BETA test rev 0.5

Exit Open jpeg Hide Seek Save jpeg Save jpeg as Pass phrase Options Help About

Input jpeg file

Directory C:\Users\acer\Downloads\session03-resources-20230515T061939Z-001\s
 Filename 2009_miss_gsu.jpg
 Filesize 113 Kb Width 320 pixels Height 445 pixels
 Approximate max capacity 17 Kb recommended limit 11 Kb

Hidden file

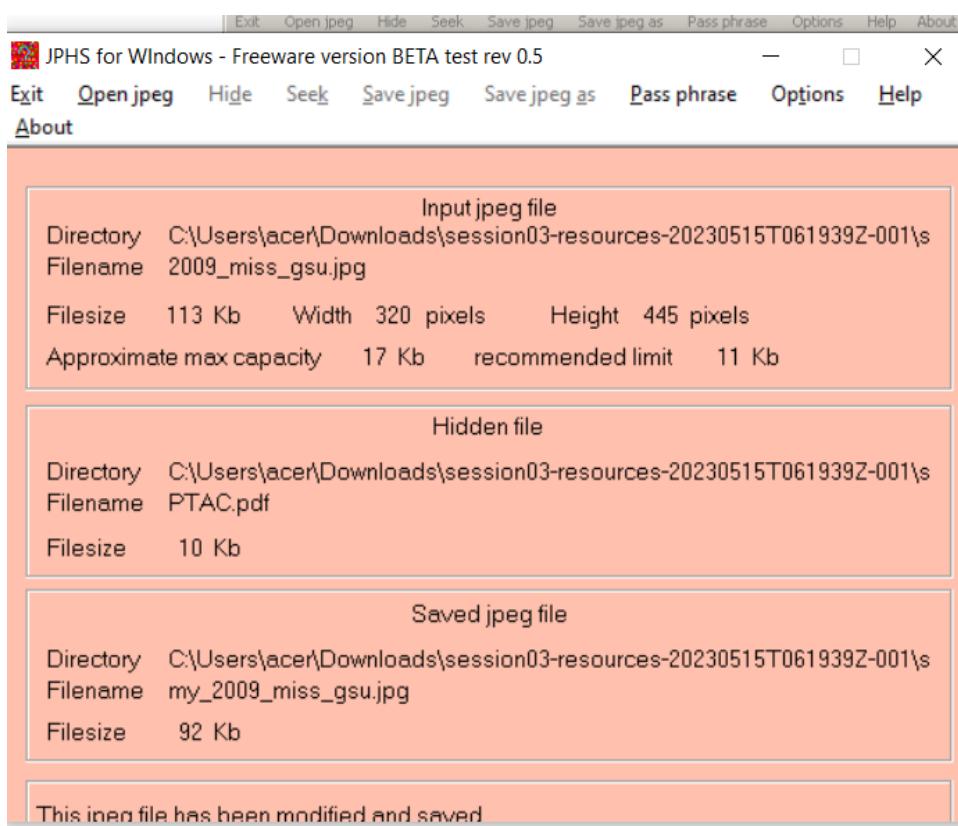
Directory C:\Users\acer\Downloads\session03-resources-20230515T061939Z-001\s
 Filename PTAC.pdf
 Filesize 10 Kb

Saved jpeg file

Directory
 Filename
 Filesize Kb

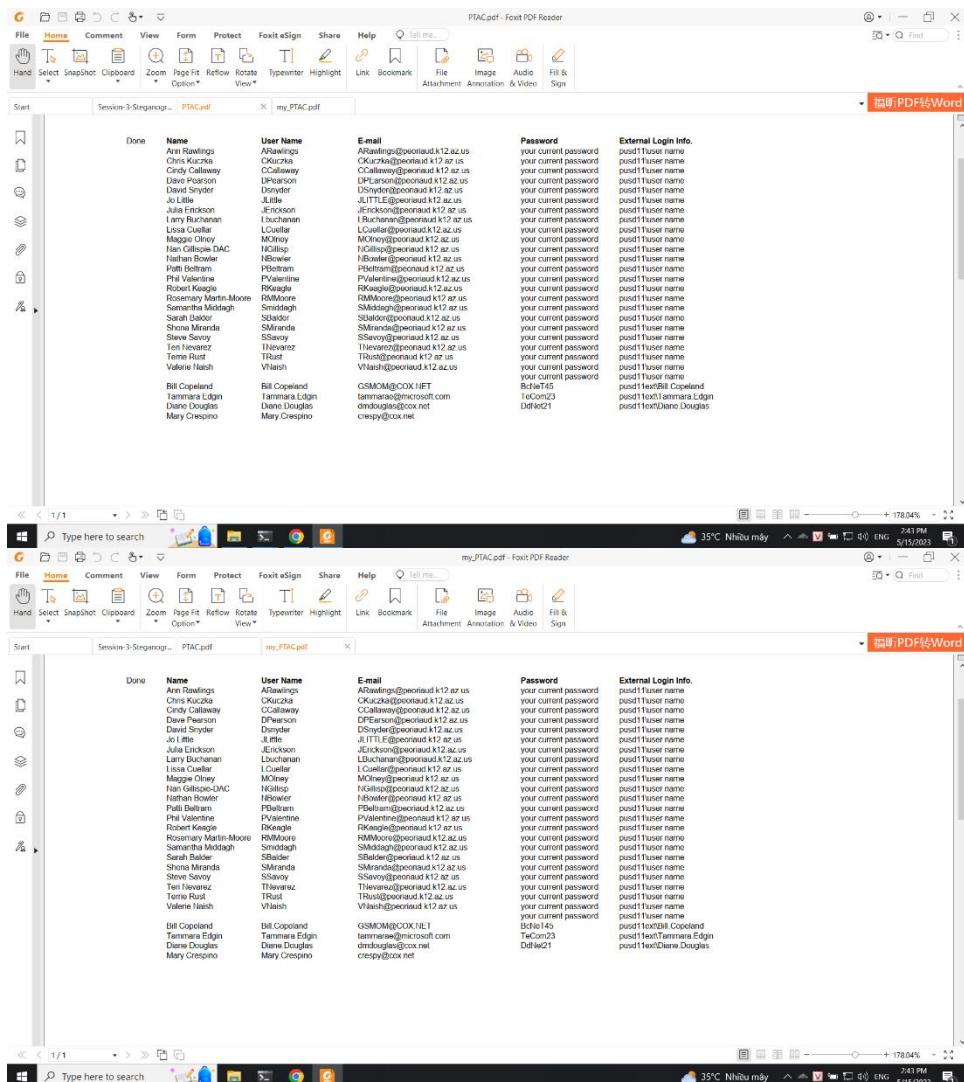
This jpeg file has been modified but not saved.

Lưu file



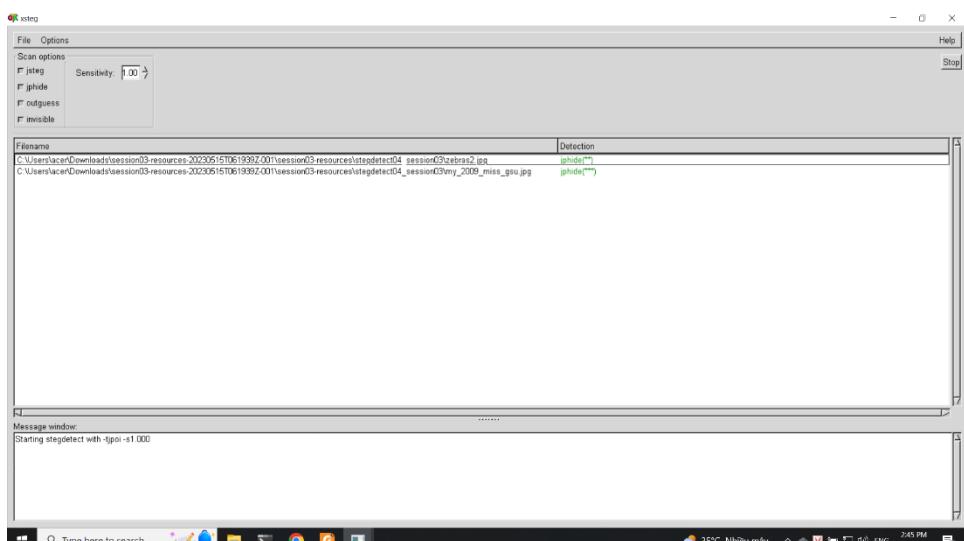
Kiểm tra thì nội dung thông đổi

Steganography & Steganalysis



Kịch bản 1c

Thực hiện xem thông tin bằng file xsteg



Có được password là together



```
PowerShell 7.3.4
PS C:\Users\acer\Downloads\session03-resources-20230515T061939Z-001\session03-resources\stegdetect04_session03> ./stegbreak.exe -r rules.ini -f MedDict.DIC
Extracted 1 files...
zebras2.jpg : johndelv5{(together)
Processed 1 files, found 1 embeddings.
Time: 4 seconds: Cracks: 68607, 17151.8 c/s
```

Mở file và seek password

JPHS for WIndows - Freeware version BETA test rev 0.5

Exit Open jpeg Hide Seek Save jpeg Save jpeg as Pass phrase Options Help About

Input jpeg file

Directory C:\Users\acer\Downloads\session03-resources-20230515T061939Z-001\session03-resources\stegdetect04_session03>

Filename zebras2.jpg

Filesize 90 Kb Width 640 pixels Height 480 pixels

Approximate max capacity 14 Kb recommended limit 9 Kb

Hidden file

Directory C:\Users\acer\Downloads\session03-resources-20230515T061939Z-001\session03-resources\stegdetect04_session03>

Filename filehide.pdf

Filesize 13 Kb

Saved jpeg file

Directory

Filename

Filesize Kb

This jpeg file already contains a hidden file.

Lưu file xuất dạng pdf

The Secret Recipe

The secret is out! Finally, you can make your own Coca-Cola with the recipe below. I have never tried it, so if you decide to give it a try, please email me and let me know how it turns out. I'm anxious to hear how the real thing is homemade!

Ingredients:

- 1 oz. Citric Acid
- 3 oz. Carbonation
- 1 oz. Ext. Vanilla
- 1 Qt. Lime juice
- 2 1/2 qt. Syrup
- 30 lbs. Sugar
- 4 qt. Water
- 2 1/2 gal. Water
- Caramel sufficient

Flavoring:

- 80 Oz Orange
- 40 Oz Lemon
- 120 Oz Lemon
- 20 Oz Mandarin
- 40 Oz Nutmeg
- 40 Oz Neroli
- 1 Qt. Alcohol

Directions:

Mix Caffeine Acid and Lime juice. 1 Qt. Carbonator add vanilla and flavoring when cold. Let stand for 24 hours.

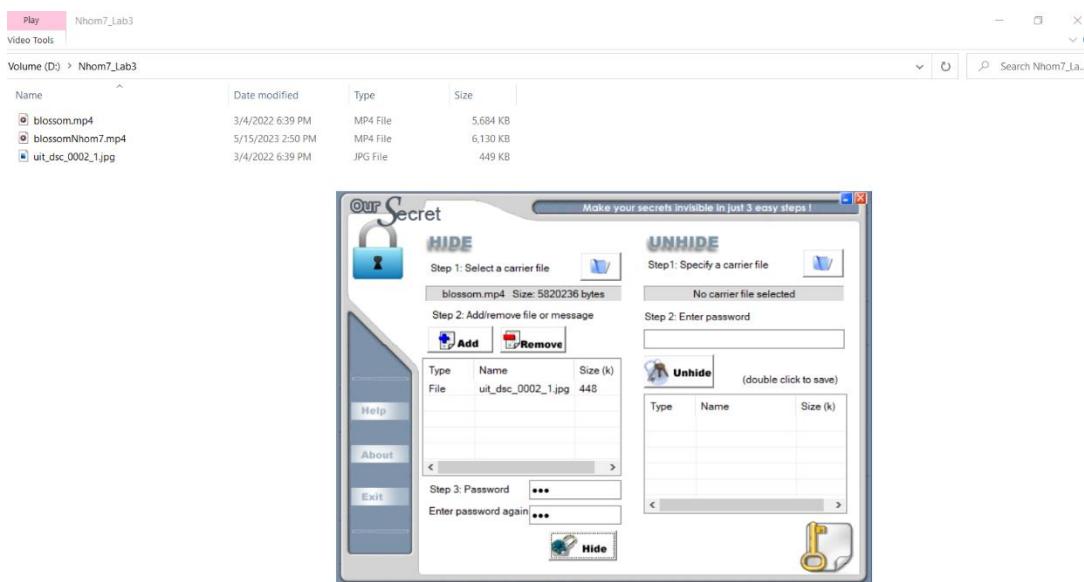
Some Notes on Preparing The Coca Cola Formula

- It takes 1 oz. of syrup mixed with carbonated water to make a 6.5 oz. serving of Coca-Cola.
- "I.E. Cocai" means fluid extract of coca (the plant that produces cocaine), however the recipe does not contain cocaine.
- The original Coca-Cola formula, which was in the possession of Frank Robinson's great-grandson, indicates that 10 pounds of coffee beans are required to flavor 30 gallons of syrup. It is also believed that the plant with leaves and flowers leaves were used to prepare the coffee. The basis on some of Pemberton's writings that indicate some coca plants were too bitter (that was because of cocaine).
- The coffee in Coca-Cola comes from the kola nut, yet kola nuts are not mentioned in the above Coca-Cola formula. This was because the company for using kola nuts was for their caffeine content. Pemberton had previously worked for another company, which was a company that derived their caffeine from kola nuts. (Pemberton had previously praised the German firm Merck of producing a superior form of the stimulant from kola nut.)

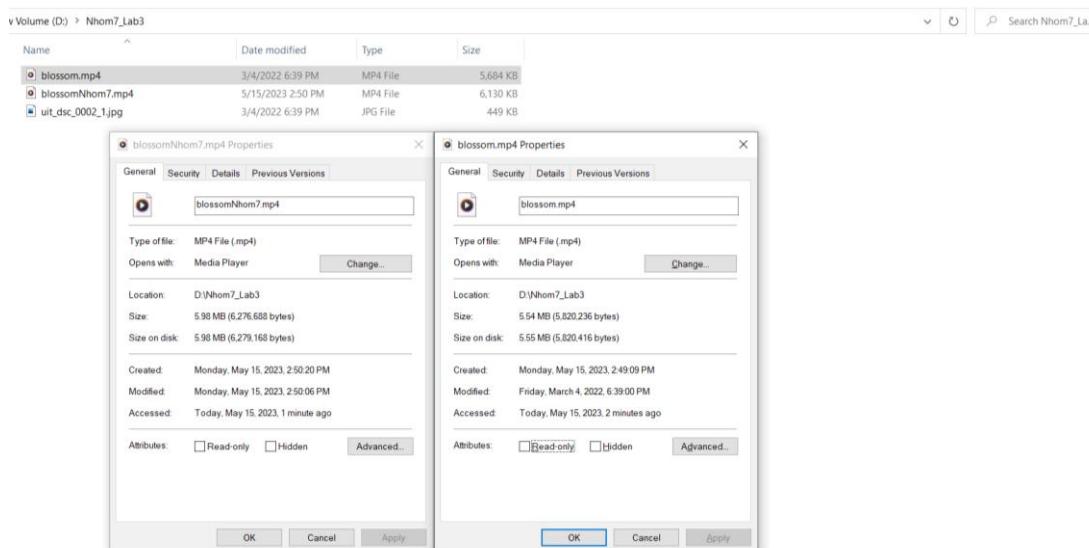
(http://www.angelfire.com/m2/CokeRoom/secretrecipe/)

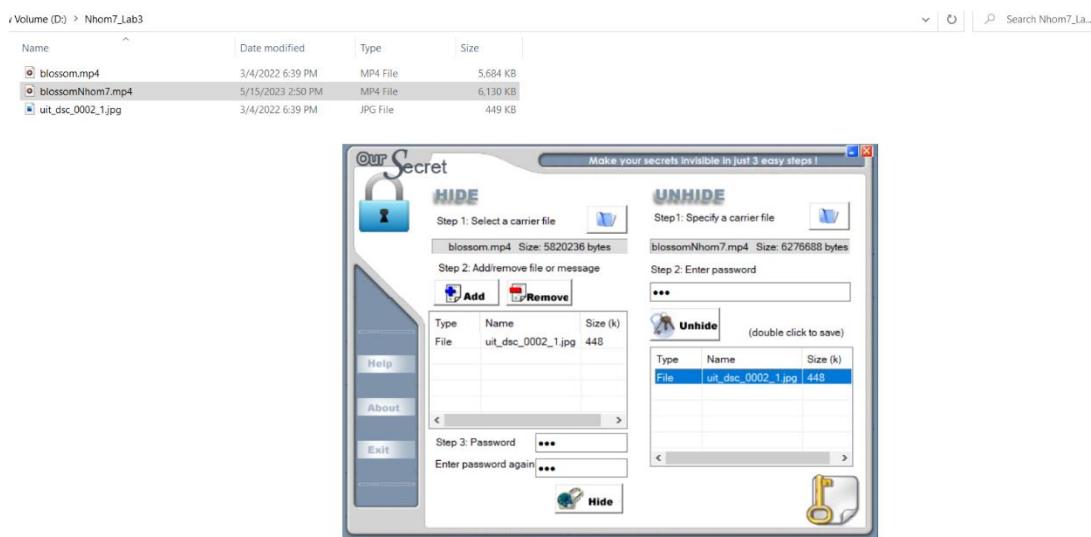
2. Kịch bản 02

- Sử dụng công cụ Our secret để thực hiện giấu ảnh uit_dsc_0002_1.jpg vào tập tin mp4, mật khẩu là E81



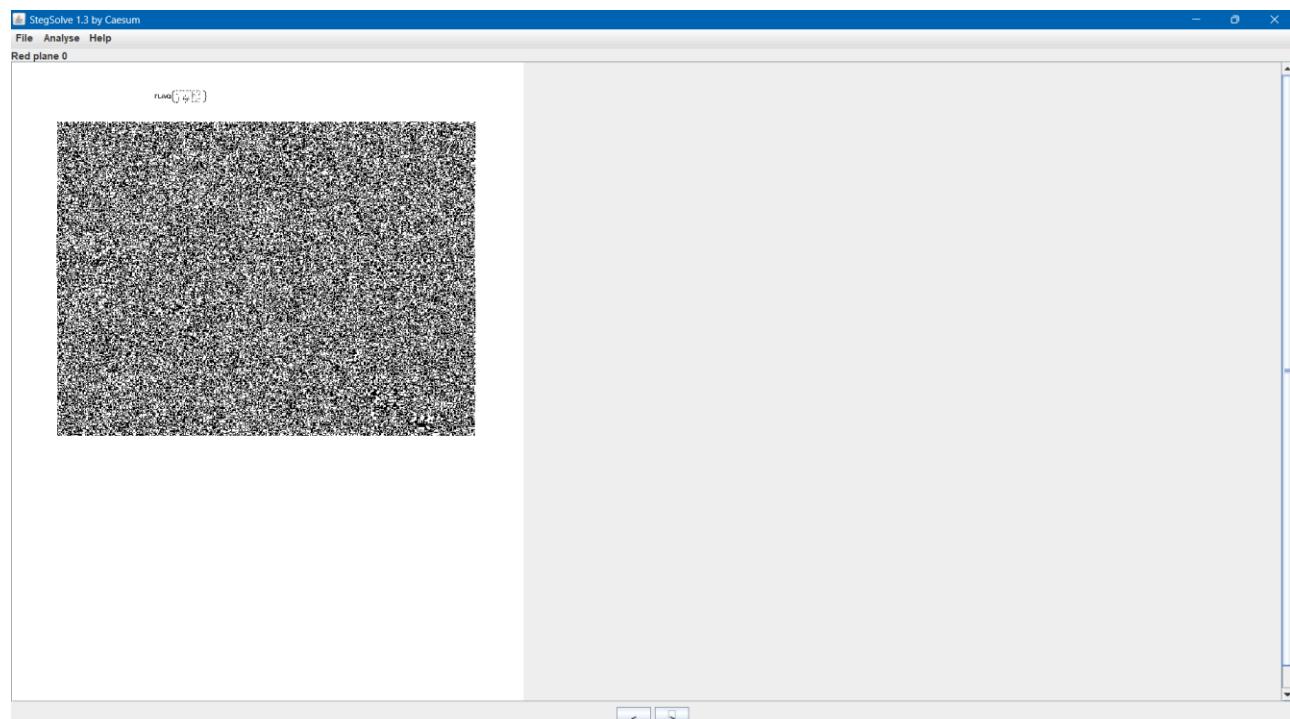
File mp4 sau khi chèn tập tin blossomNhóm7 có tăng dung lượng hơn so với file gốc





3. Kịch bản 03

Đầu tiên thực hiện mở file, sau đó thử hiện chỉnh sửa gam màu plane đến Red plane 0, ta thấy có đoạn thông điệp flag



Thực hiện giải mã theo chữ nổi và ta có được thông điệp bên dưới

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	x		x x x			x	x x			x		x x			
64										x		x		x	x
32	x									x x			x x		
16					x					x x x			x		
8	x		x			x		x	x						
4	x		x x x x			x		x				x x x			
2	x			x			x		x		x x				
1 x			x						x x x x						
	14		12	21	6	12				57	19	71	53		
	12:14		21/6/2012							53711947					
										711957					

⇒ Số seri sẽ là : 53711947/711957

4. Kịch bản 04

Dùng strings để tìm lấy các chuỗi từ file star-wars.jpg

```
strings star-wars.jpg
```

Tìm được chuỗi nhị phân đáng ngờ gồm 54 bit

10011010101010101010111010100110101010101110101010011110

Theo đề bài thì John Bramblitt là một họa sĩ mù do đó em nghĩ đến sẽ chuyển chuỗi trên theo ngôn ngữ Braille

Tham khảo <https://www.wikihow.com/Read-Braille>

Trong ngôn ngữ Braille thì mỗi chữ được thể hiện bởi 6 điểm → 6 bit và xếp theo thứ tự từ trên xuống và từ trái qua

100110

11

01

00

101010

10

01

10

101010

10

01

10

111010

10

11

10

100110

11

01

00

101010

10

01

10

101110

11

01

10

101010

10

01

10

011110

01

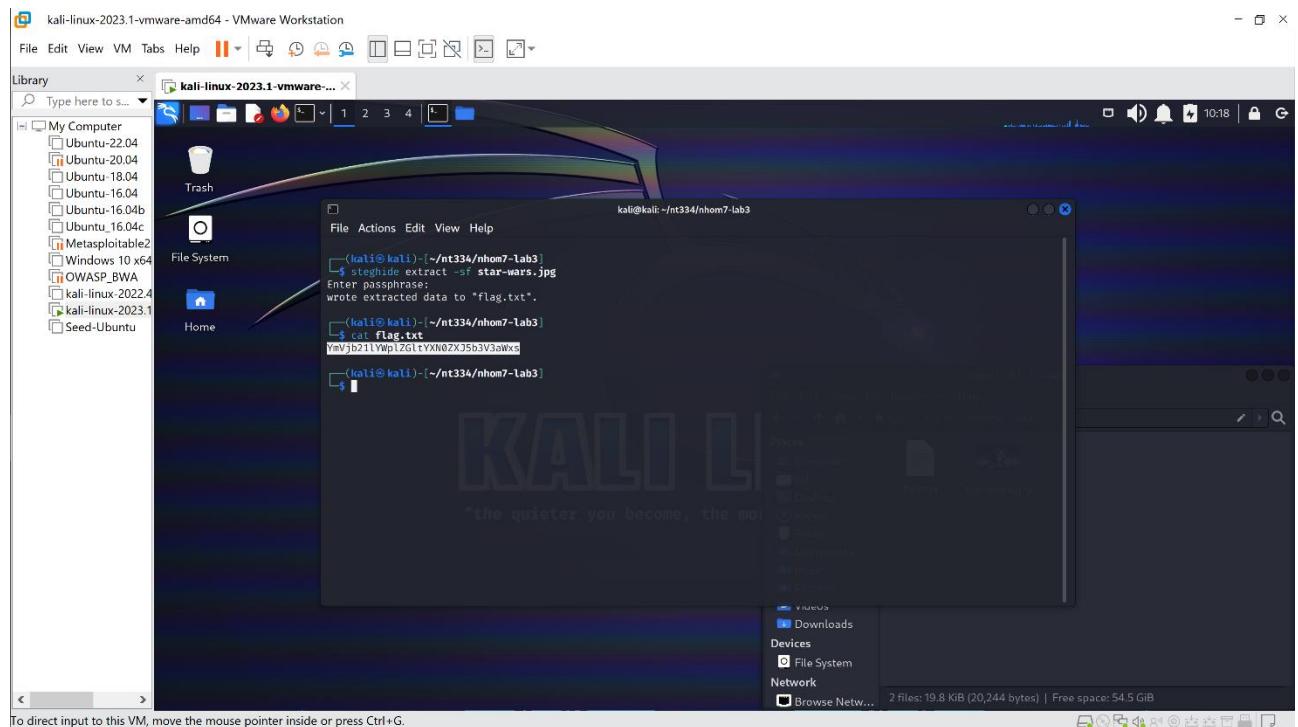
11

10

Dùng công cụ decoder để dịch lại các ký tự trên <https://www.dcode.fr/braille-alphabet>

Có được chuỗi là: doordonot Chuỗi này có khả năng là một key nào đó.

Tiếp tục dùng công cụ steghide để trích xuất file ẩn từ star-wars.jpg, với pass là chuỗi “doordonot”



Từ nội dung của file trích xuất được, giải mã base64 tìm được flag
becomeajedimasteryouwill

The screenshot shows the CyberChef interface with the following details:

- Operations:** A sidebar with various conversion tools like To Base64, From Base64, To Hex, etc.
- Recipe:** Set to "From Base64" with the alphabet set to "A-Za-z0-9+=". The "Remove non-alphabet chars" checkbox is checked, while "Strict mode" is unchecked.
- Input:** Contains the Base64 string: YmVjb21lYwpIZGltYXN0ZXJ5b3V3awxs.
- Output:** Shows the extracted message: becomeajedimasteryouwill.
- Buttons:** STEP, BAKE!, Auto Bake.

5. Kích bản 5

Tài nguyên bài này là một file khá lớn nên có khả năng cao chứa file ẩn ở trong. Dùng tool stegbreak tìm file ẩn theo wordlist rockyou.txt

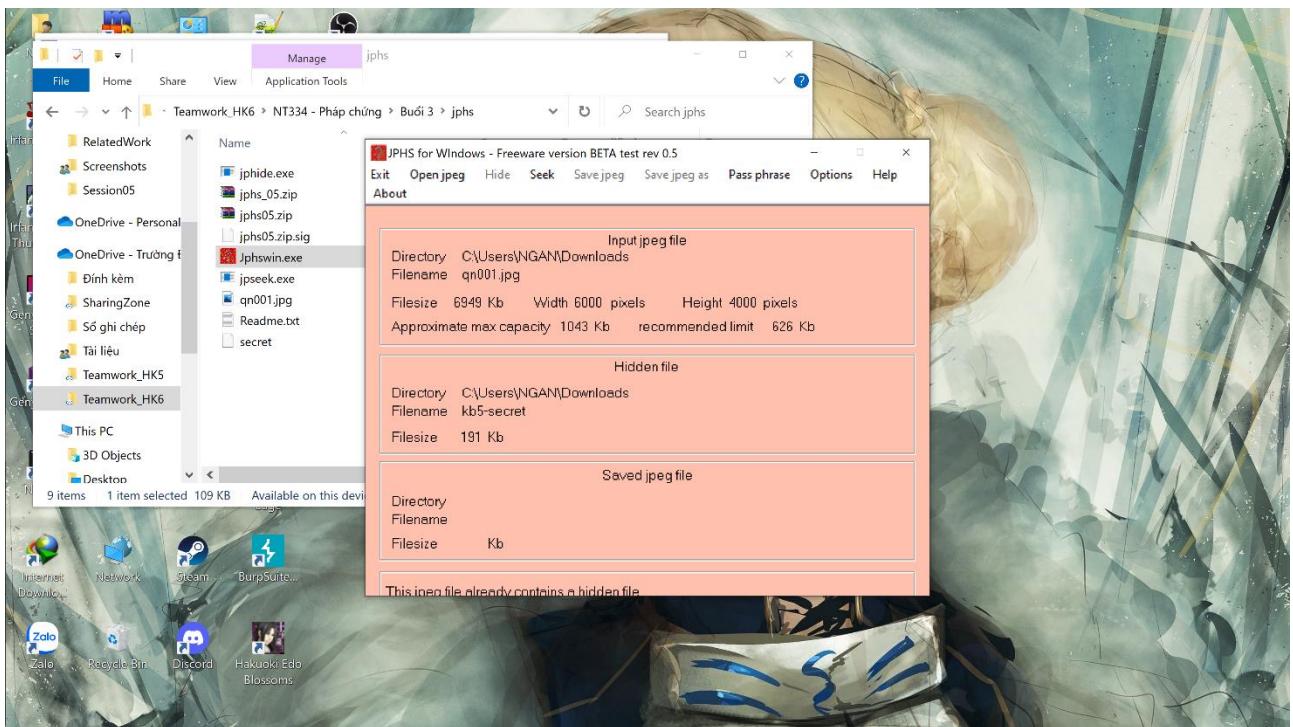
```

PS C:\Users\acer\Downloads\session03-resources-nhombay\session03-resources\stegdetect04_session03> ./stegbreak.exe -r rules.ini -f ./rockyou.txt .\qn001.jpg
Corrupt JPEG data: bad Huffman code
Loaded 1 files
\qn001.jpg [jphide[v5]()]
Decrypted 1 files, found 1 embeddings.
Time: 1 seconds: Cracks: 4751, 4751.0 c/s
PS C:\Users\acer\Downloads\session03-resources-nhombay\session03-resources\stegdetect04_session03>

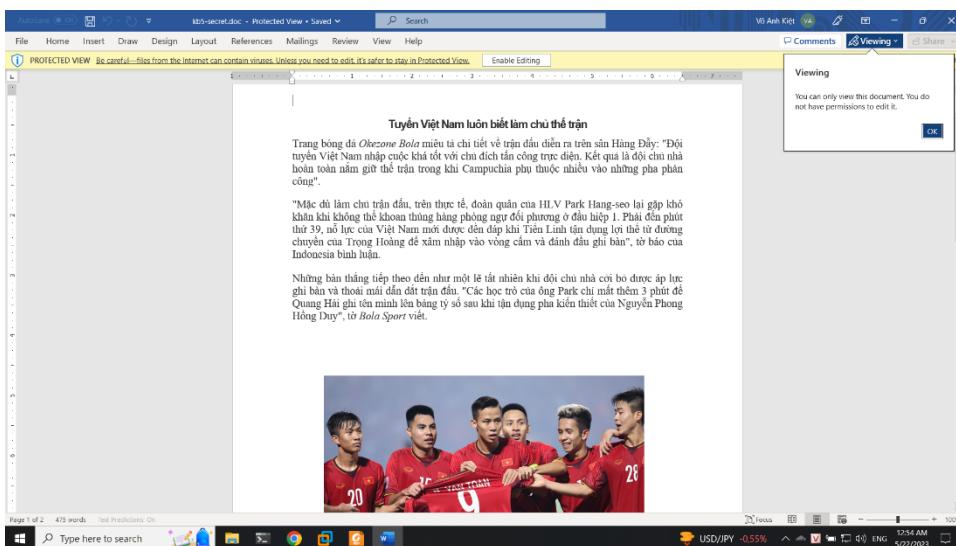
```

Kết quả cho thấy có 1 file được nhúng trong ảnh.

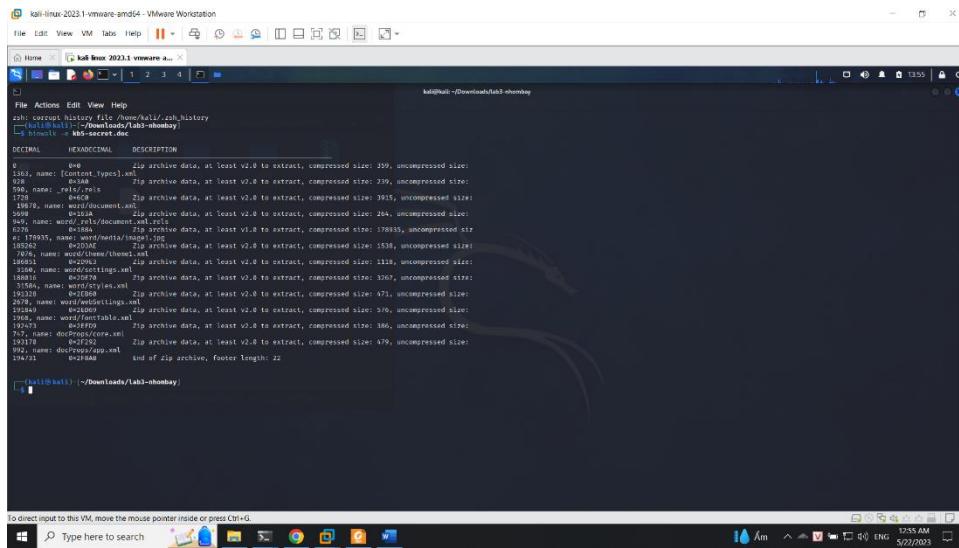
Dùng tool JPHS để lấy file đó. Chọn file input là qn001.jpg, output đặt tên là kb5-secret, để trống passphrase



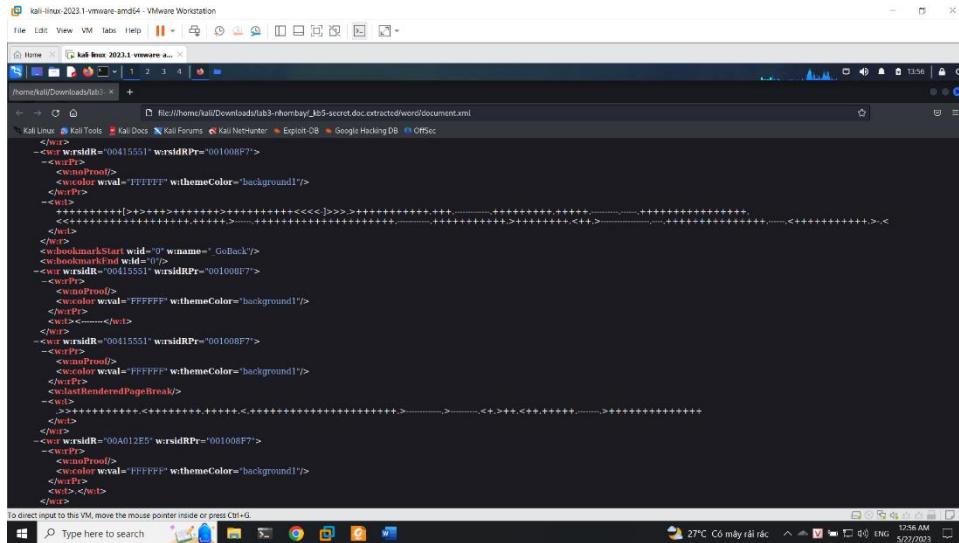
Chuyển tên file lấy được thành file doc



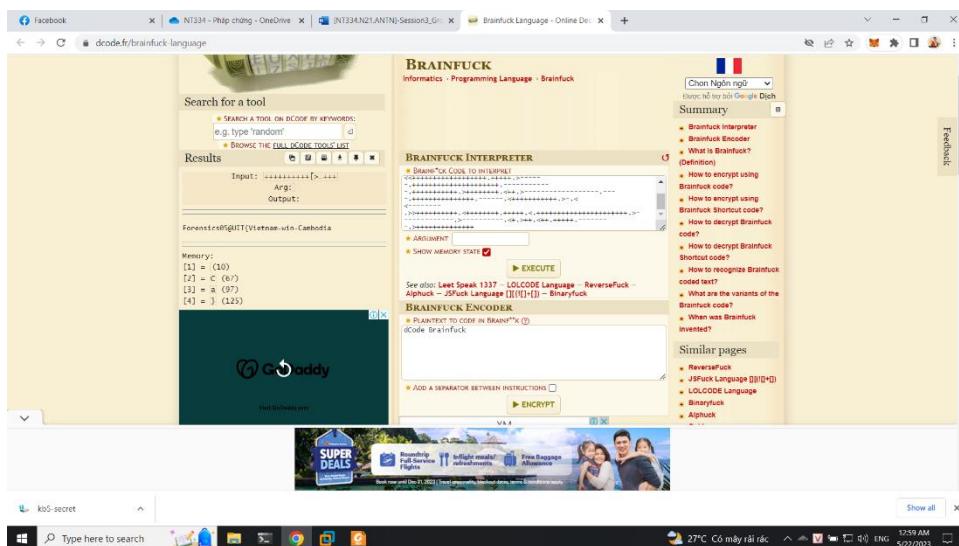
Ta không thấy gì đó đặc biệt, ta sử dụng binwalk để xem



Thấy một thông tin trong file _embedded.doc.extracted/word/document.xml có dạng ngôn ngữ brainfuck



Decode ra ta được thông tin



Forensics05@UIT{Vietnam-win-Cambodia}

6. Kịch bản 6

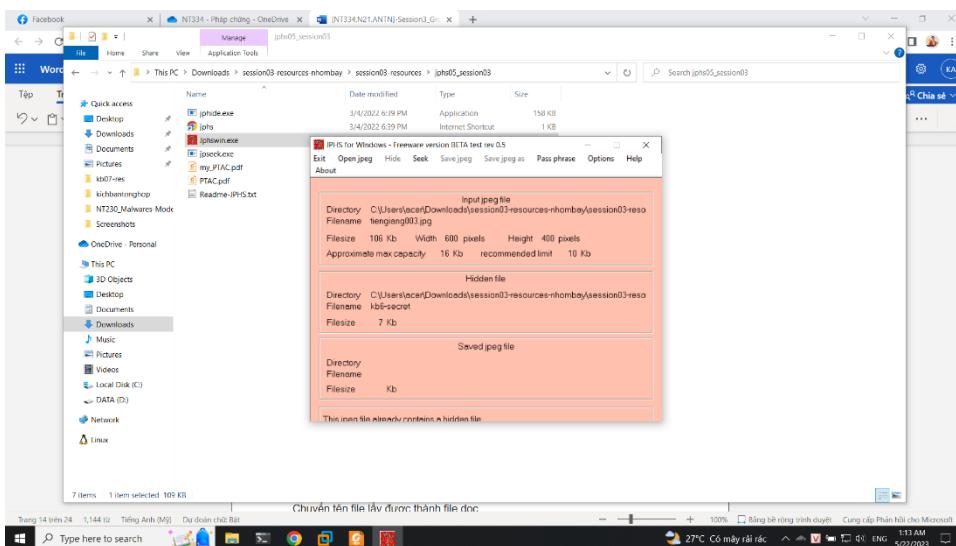
Đầu tiên ta thấy được có một file được nhúng trong ảnh

```

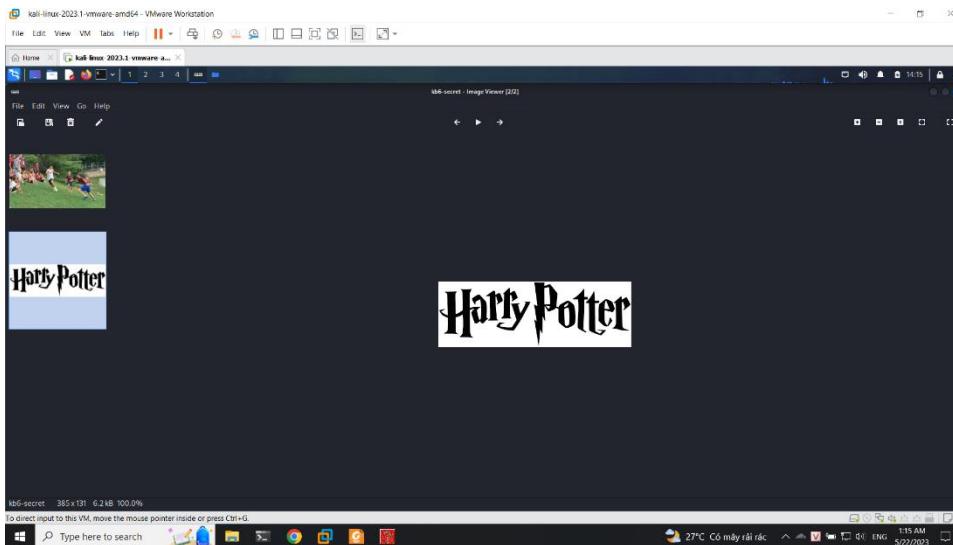
PowerShell 7.3.4
PS C:\Users\acer\Downloads\session03-resources-nhombay\session03-resources\stegdetect04_session03> .\stegbreak.exe -r
rules.ini -f .\rockyou.txt .\tiengiang003.jpg
Loaded 1 files...
.\tiengiang003.jpg : jphide[v5]()
Processed 1 files, found 1 embeddings.
Time: 1 seconds: Cracks: 4751, 4751.0 c/s
PS C:\Users\acer\Downloads\session03-resources-nhombay\session03-resources\stegdetect04_session03>

```

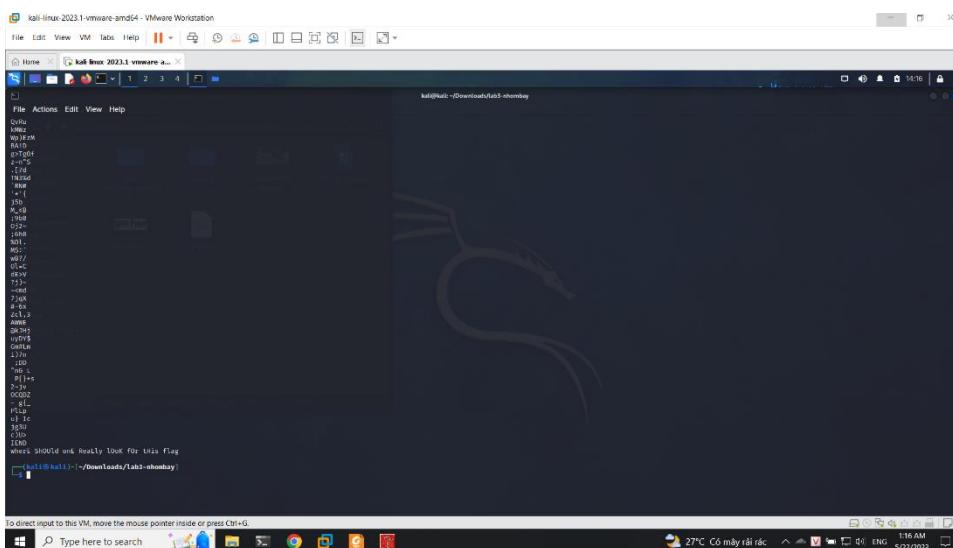
Sử dụng JPHS để trích xuất



Đưa file xuất ra thì ta thấy đây là định dạng file png



Sử dụng strings để xem thông tin bên trong



Dự đoán đây là mã hoá Bacon Cipher, vậy ta sẽ thực hiện code để chuyển chuỗi thành A B với A là chữ thường và B là in

```

File Edit Selection View Go Run ... ← → Search
cau6.py x
C:\>Users>acer>Downloads>session03-resources-nhombay>session03-resources>kichbantonghop> cau6.py
1 # string input
2 string = "wherE ShOuld one ReallY looK foR thiS flag"
3
4 # change the string to A and B, A match the normal letter and B match the capital letter, and the space character keeping it
5 for i in range(len(string)):
6     if string[i] == " ":
7         string = string[:i] + " " + string[i+1:]
8     elif string[i].isupper():
9         string = string[:i] + "B" + string[i+1:]
10    else:
11        string = string[:i] + "A" + string[i+1:]
12
13 # print the string
14 print(string)

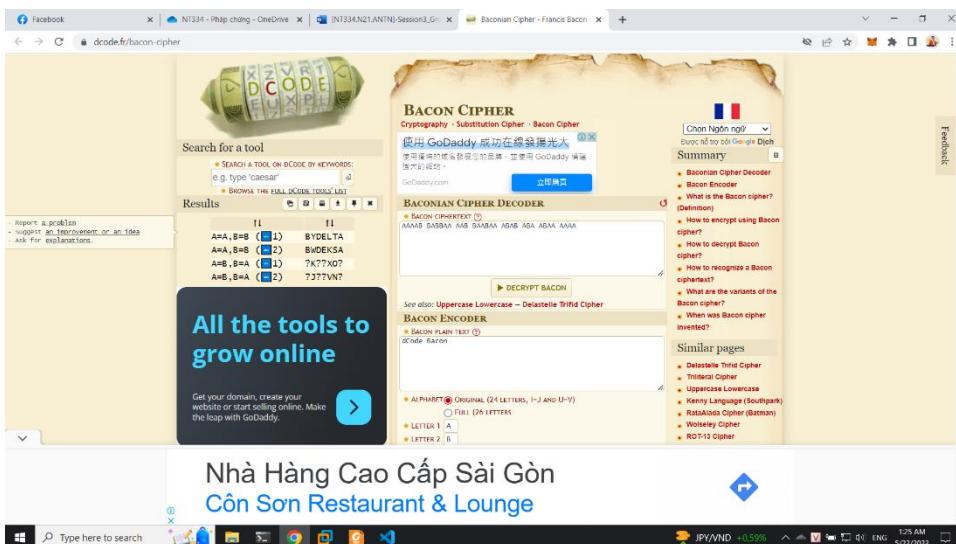
```

Thực hiện chạy thì ta có được kết quả

```
PS C:\Users\acer\Downloads\session03-resources-nhombay\session03-resources\kichbantonghop> python cau6.py
AAAAB BABAA AAB BAABAA ABAB ABA ABAA AAAA
PS C:\Users\acer\Downloads\session03-resources-nhombay\session03-resources\kichbantonghop> |
```

AAAAB BABAA AAB BAABAA ABAB ABA ABAA AAAA

Thực hiện decode



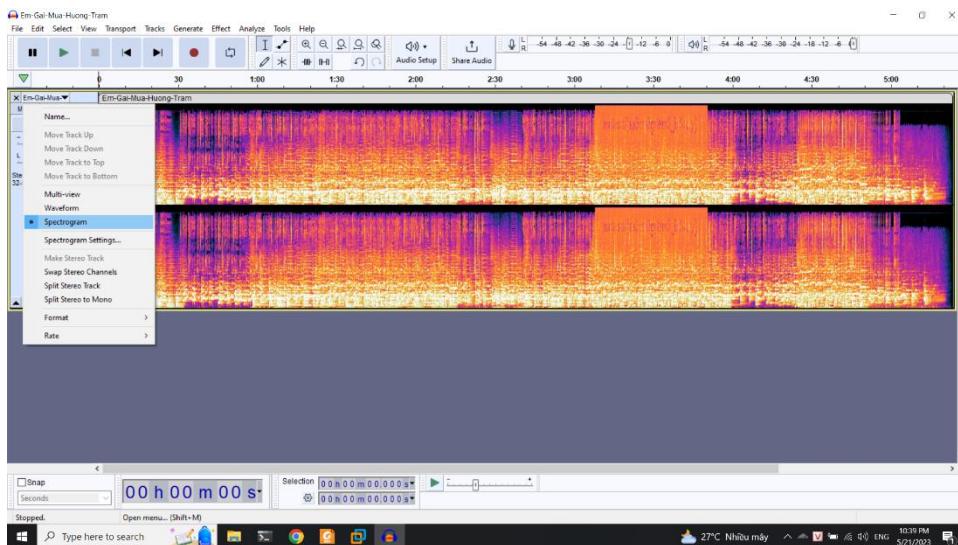
Ta có được flag là BYDELTA

7. Kịch bản 7

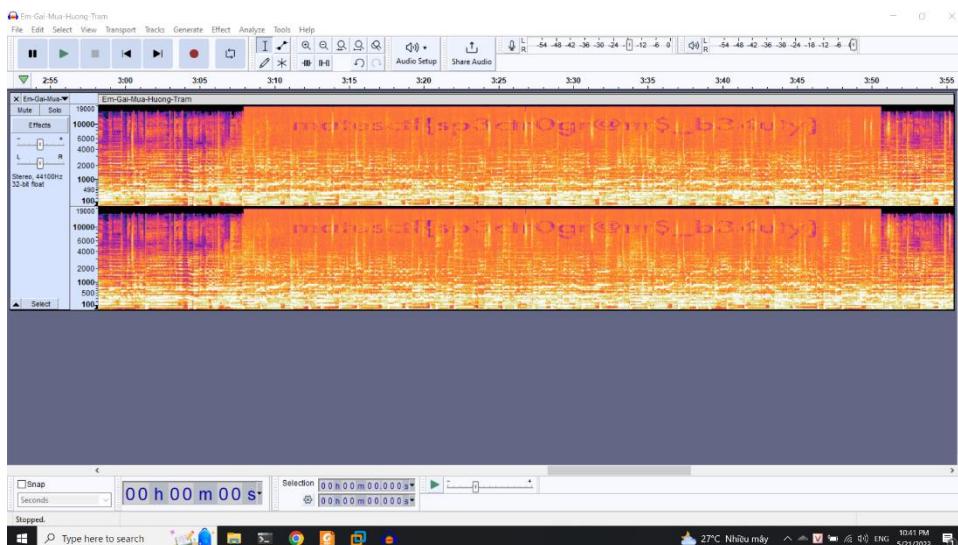
Đầu tiên ta tải phần mềm: <https://www.audacityteam.org/download/>

Tiếp theo mở file lên và chọn định dạng spectrogram

Steganography & Steganalysis



Mở lớn phần đậm lên thì ta thấy thông tin flag

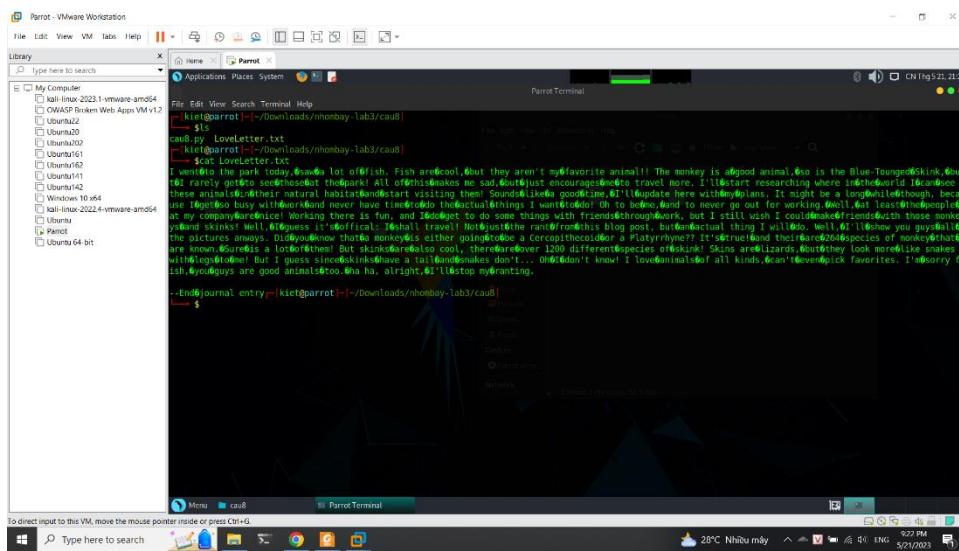


matesctf{sp3ctr0gr@m\$_b34uty}

8. Kịch bản 8

Đầu tiên ở file này ta thấy thông tin dấu cách không chính xác, nó không phải dấu thông thường

Steganography & Steganalysis



Thực hiện code python để giải mã (giải thích code trong phần comment của chương trình). Chương trình sẽ thực hiện lấy cái thông tin ở phần dấu cách các ký tự đặc biệt, đánh dấu là 1 (đánh dấu 0 với dấu cách thông thường) và thực hiện chuyển đổi thành dev và xử lý unhexlify với dec truyền vào và in kết quả

```

File Edit Selection View Go Run ...
Search

cau8.py x
C:\Users\acer\Downloads> session03-resources-nhombay> session03-resources> kichbantonghop> cau8.py > ...
1 # import library
2 import binascii
3
4 # declare variable
5 binary_string= ""
6
7 # open file
8 with open("LoveLetter.txt","r") as file:
9
10    # read file
11    for character in file.read():
12
13        # if character is space, add 0 to binary_string
14        if character == ' ':
15            binary_string = binary_string + "0"
16
17        # if character is not space, add 1 to binary_string
18        if ord(character) == 160:
19            binary_string = binary_string + "1"
20
21    # convert to binary_string format
22 bin_format = '0b' + binary_string
23
24    # convert to decimal format
25 dec_format = int(bin_format, 2)
26
27    # convert to hex format and print
28 result = binascii.unhexlify('%x' % dec_format)
29 print(result)
```

Ta có được flag

```
PS C:\Users\acer\Downloads\session03-resources-nhombay\session03-resources\kichba
ntonghop> python cau8.py
b'FLAG-3b6f70fcf070009561f5276fe98fc9c6'
PS C:\Users\acer\Downloads\session03-resources-nhombay\session03-resources\kichba
ntonghop> |
```

FLAG-3b6f70fcf070009561f5276fe98fc9c6

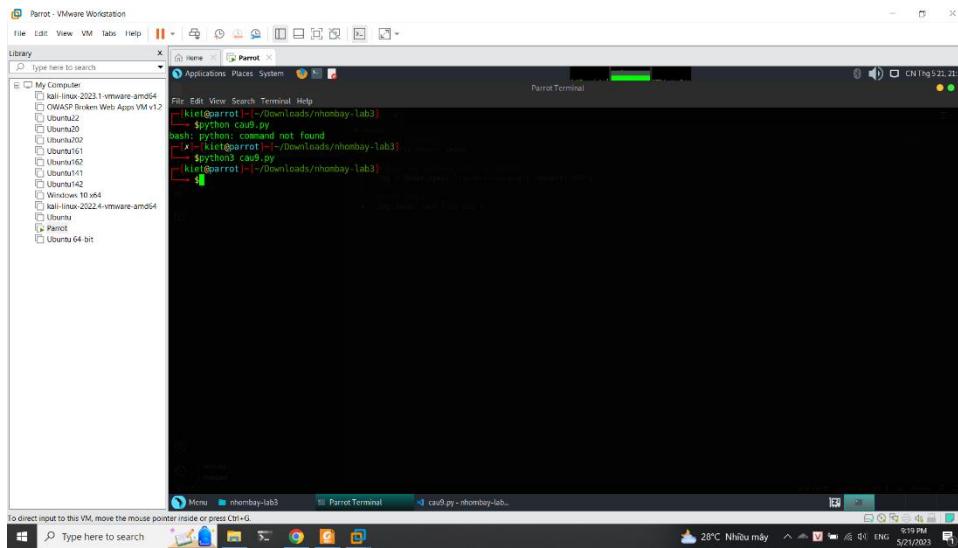
9. Kịch bản 9

Ở bài này ta sẽ thực hiện code python để thực hiện giải mã lấy flag bằng việc chuyển mã màu sang rgb

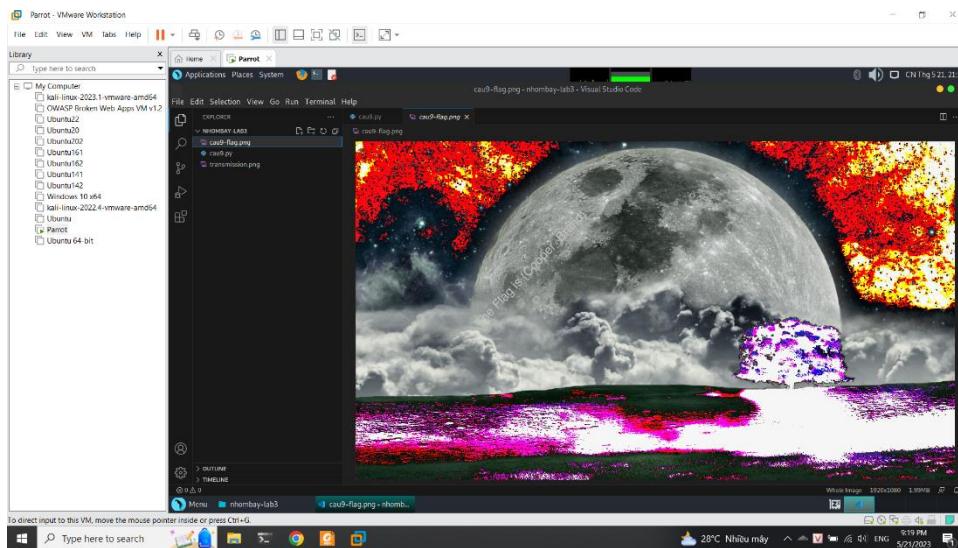
```
File Edit Selection View Go Run Terminal Help
cau9.py - nhombay-lab3 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
cau9.py
1 import
2 from PIL import Image
3
4 # Open the picture with rgb color
5 img = Image.open('transmission.png').convert('RGB')
6
7 #Save image
8 img.save('cau9-Tflag.png')
```

Thực hiện chạy code

Steganography & Steganalysis



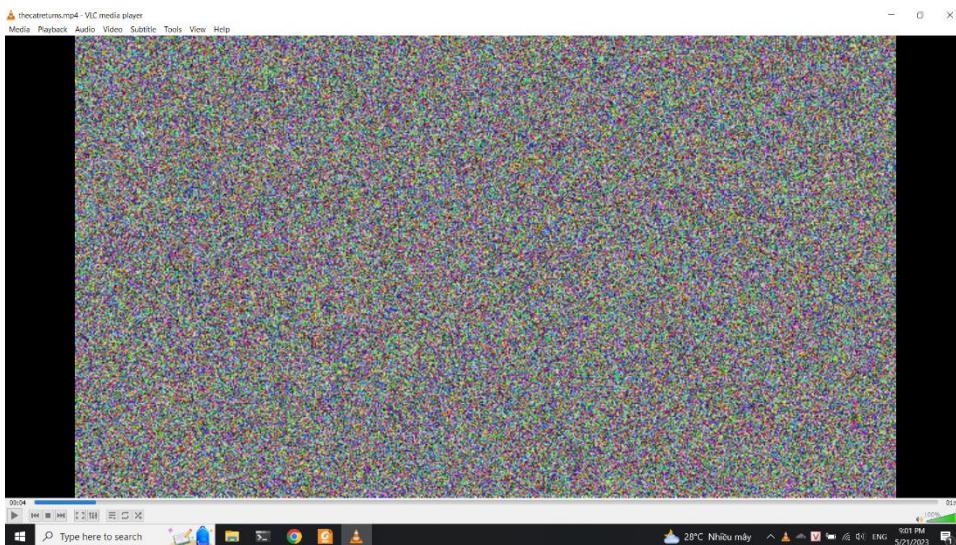
Ta có được flag



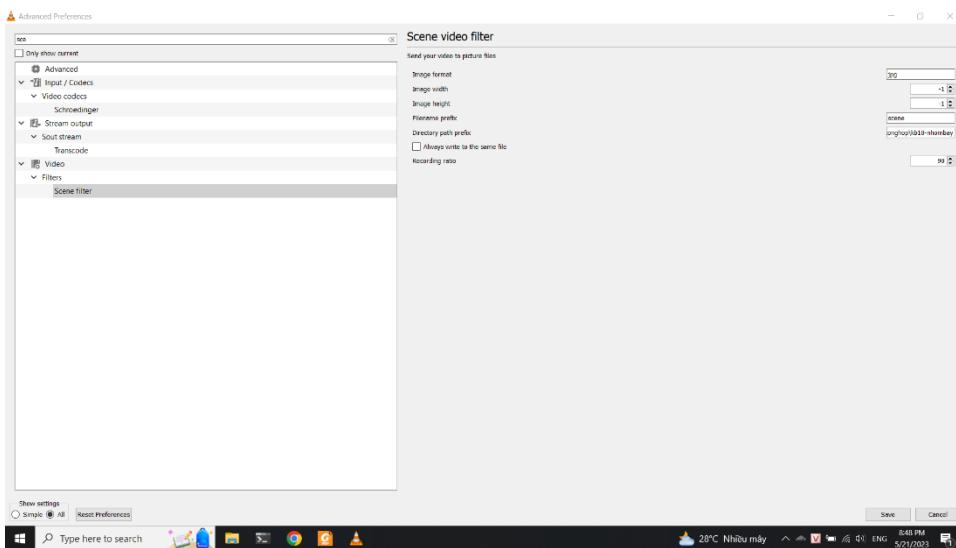
{Cooper_Brand}

10. Kịch bản 10

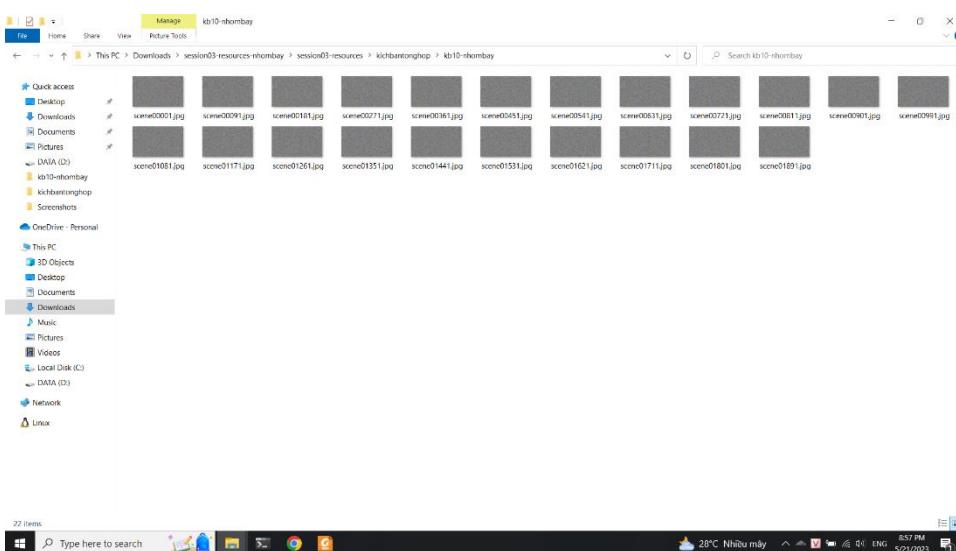
Đầu tiên ta sẽ sử dụng VLC tạo ra các frame cho video



Ta sẽ thực hiện cấu hình như bên dưới, sau khi cấu hình xong ta lưu lại và tắt vlc

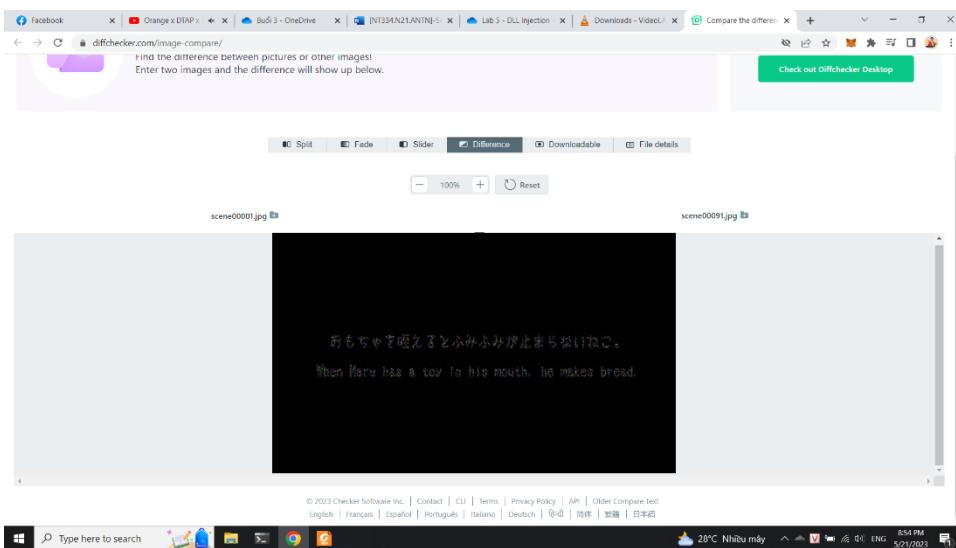


Tiếp tục thực hiện mở lại video để cắt thành các frame

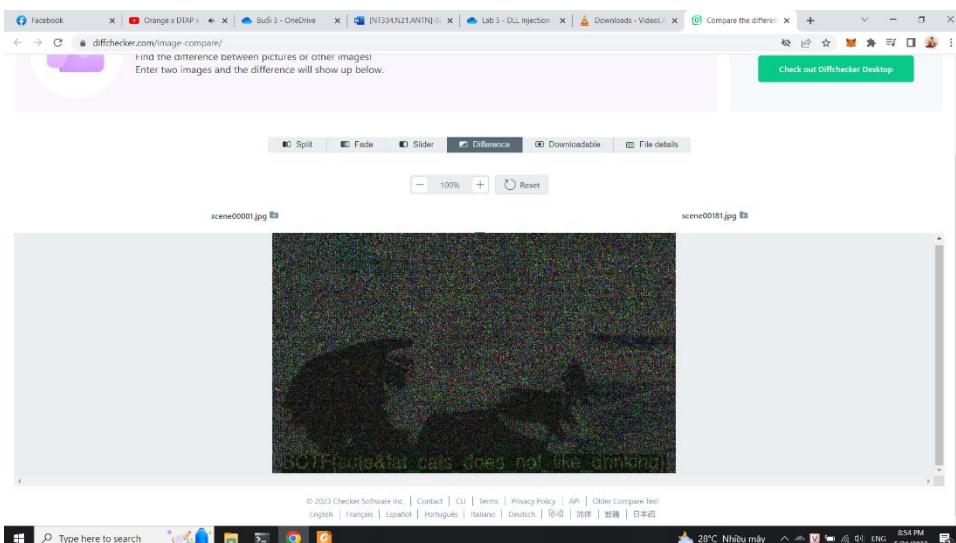


Dùng tool <https://www.diffchecker.com/> để thực hiện kiểm tra

Ở ảnh 1 và ảnh 91 thì ta thấy thông tin là 1 gợi ý



Ở ảnh 1 và ảnh 181 thì thấy được flag



BCTF{cute&fat_cats_does_not_like_drinking}

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.DOCX** và **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)** – cỡ **chữ 13**. **Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

Ví dụ: [NT101.H11.1]-Session1_Group3.

- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT