

# BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Kỳ báo cáo: Buổi 03 (Session 03)

Tên chủ đề: Steganography & Steganalysis

GVHD: Đoàn Minh Trung

Ngày báo cáo: 08/04/2024

Nhóm: 07

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.O21.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Đình Bảo Long	21522303	<a href="mailto:21522303@gm.uit.edu.vn">21522303@gm.uit.edu.vn</a>
2	Nguyễn Tân Phát	21522447	<a href="mailto:21522447@gm.uit.edu.vn">21522447@gm.uit.edu.vn</a>
3	Ngô Minh Thiên	21522623	<a href="mailto:21522623@gm.uit.edu.vn">21522623@gm.uit.edu.vn</a>
4	Đào Vĩnh Thịnh	21522632	<a href="mailto:2152632@gm.uit.edu.vn">2152632@gm.uit.edu.vn</a>

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Kịch bản 01(a,b,c)	100%
2	Kịch bản 02	100%
3	Kịch bản 03	100%
4	Kịch bản 04	100%
5	Kịch bản 05	100%
6	Kịch bản 06	100%
7	Kịch bản 07	100%
8	Kịch bản 08	100%
9	Kịch bản 09	100%
10	Kịch bản 10	100%

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành,

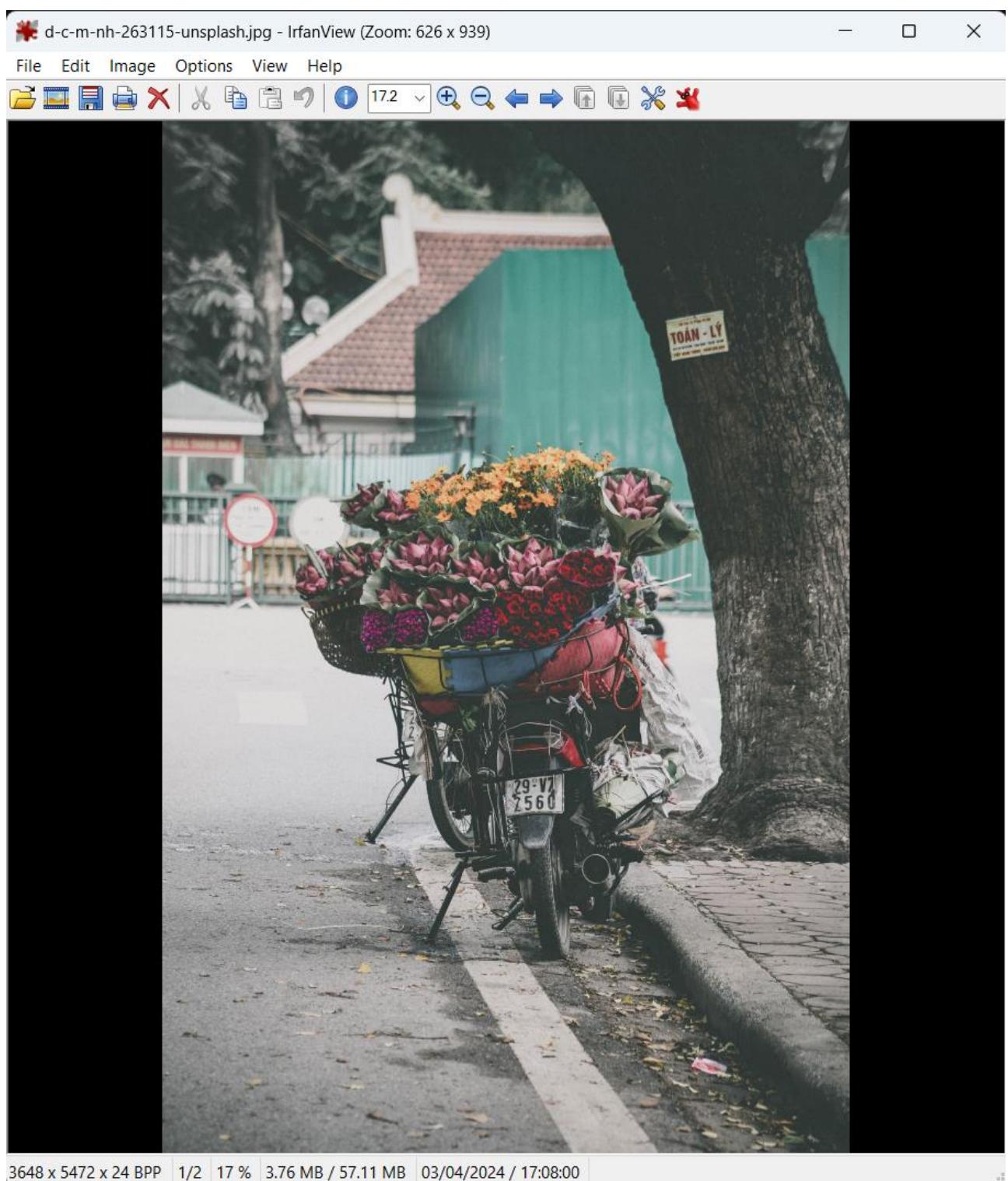
# BÁO CÁO CHI TIẾT

## Kịch bản 01-a. Thực hiện phân tích thông tin tập tin ảnh

- Tài nguyên thực hiện, nằm trong thư mục kb-01-a
- Yêu cầu: Cung cấp các thông tin chi tiết liên quan tới các bức ảnh trên bằng phần mềm IrfanView

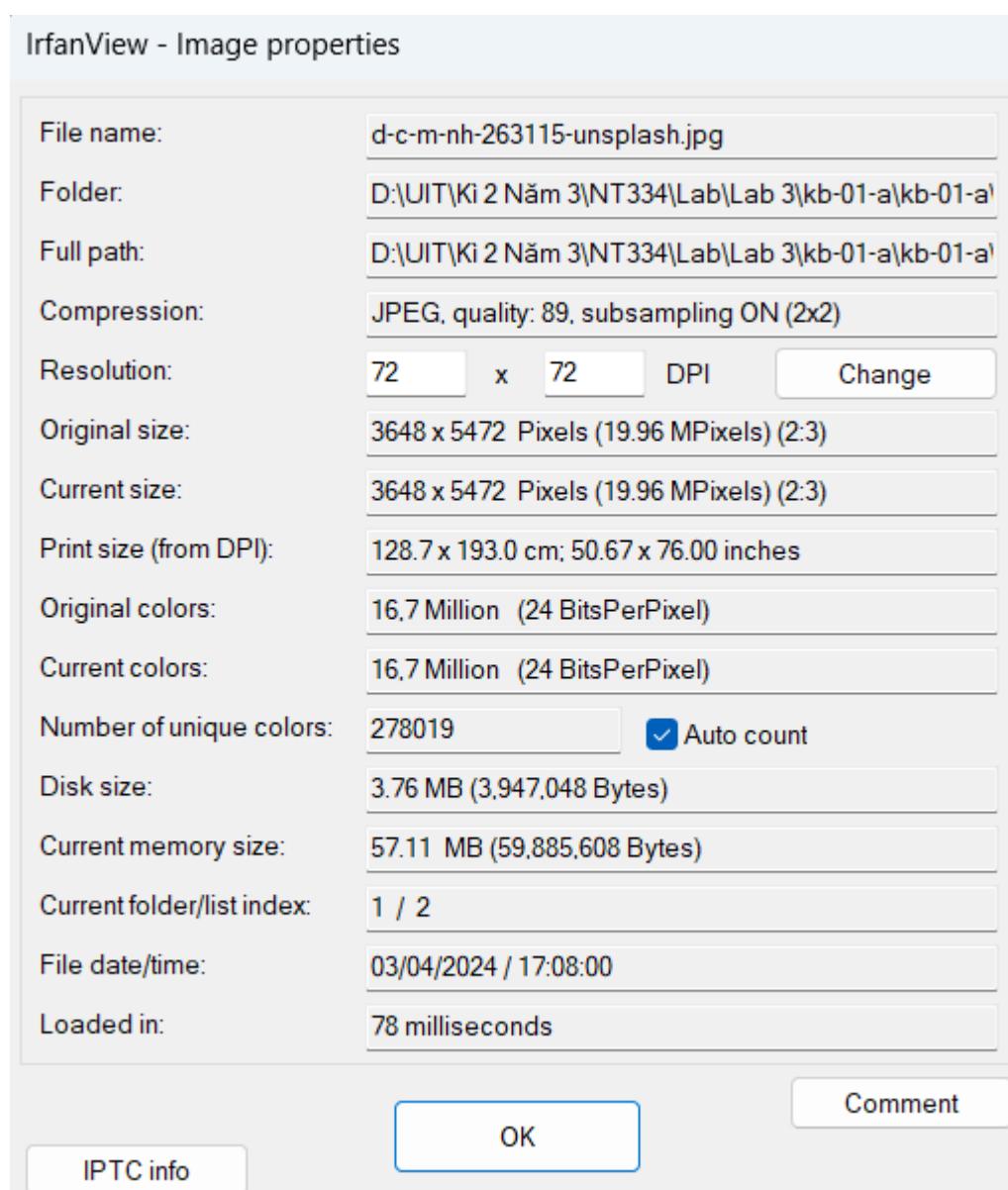
Đáp án:

Đầu tiên ta kiểm tra ảnh d-c-m-nh-263115-unsplash.jpg



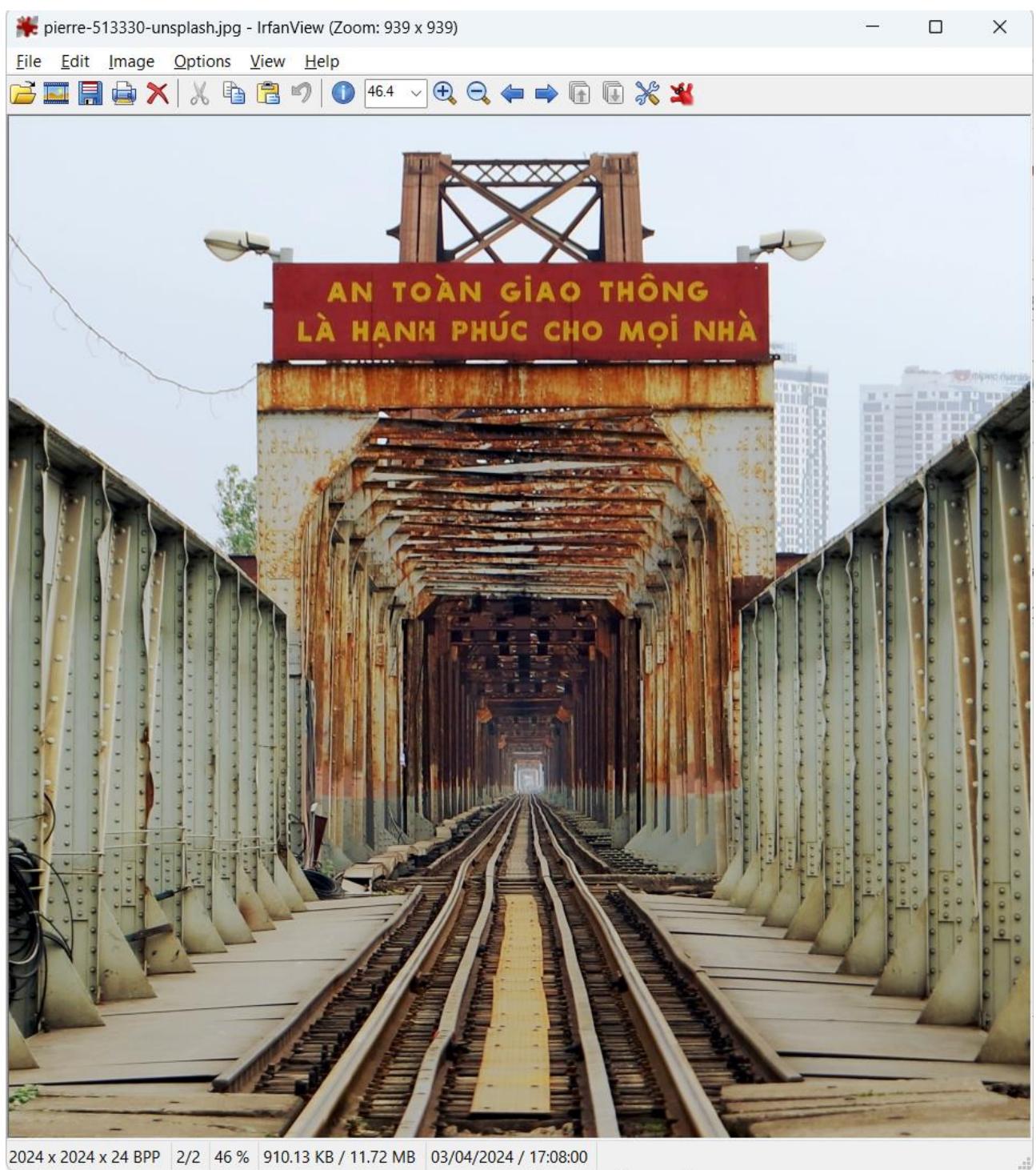
3648 x 5472 x 24 BPP | 1/2 | 17 % | 3.76 MB / 57.11 MB | 03/04/2024 / 17:08:00

Chọn Image → Information

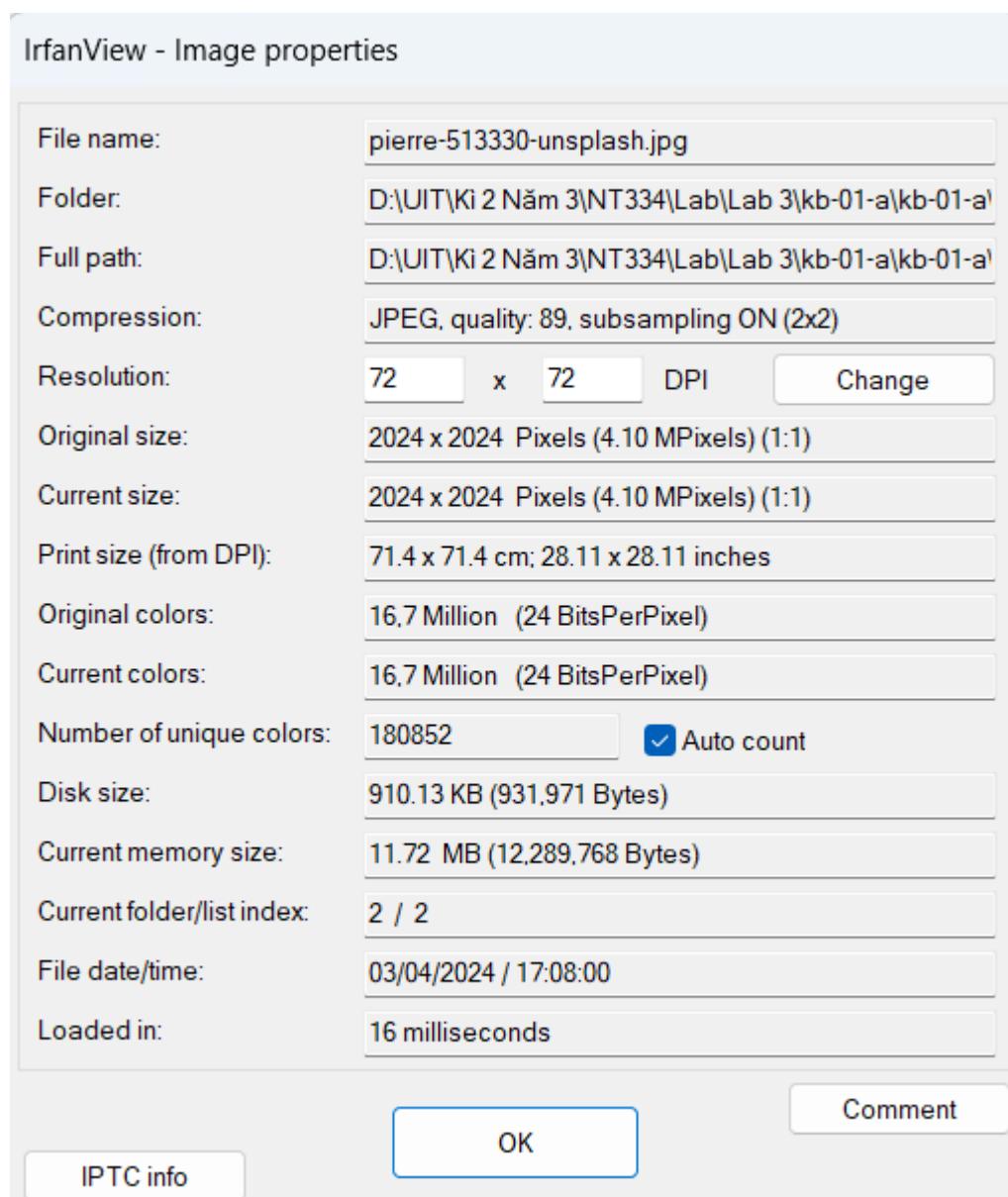


Ảnh này không có thông tin EXIF để chiết xuất.

Tương tự mở ảnh pierre-513330-unsplash.jpg và phân tích



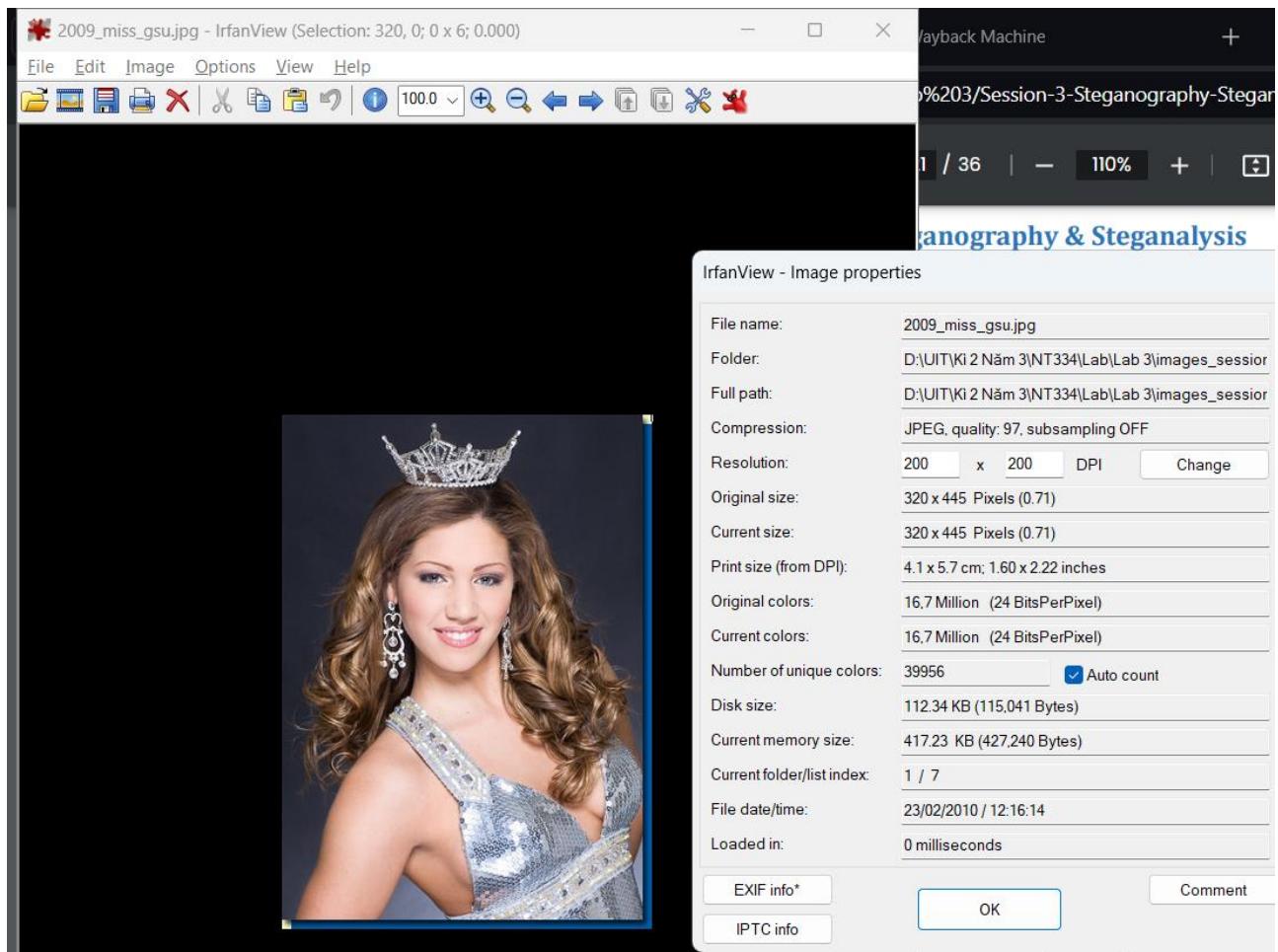
Thông tin của ảnh.



Ảnh này cũng không có thông tin EXIF để chiết xuất.

a. Kịch bản 01-b: Giấu tin và giải mã thông tin trong ảnh

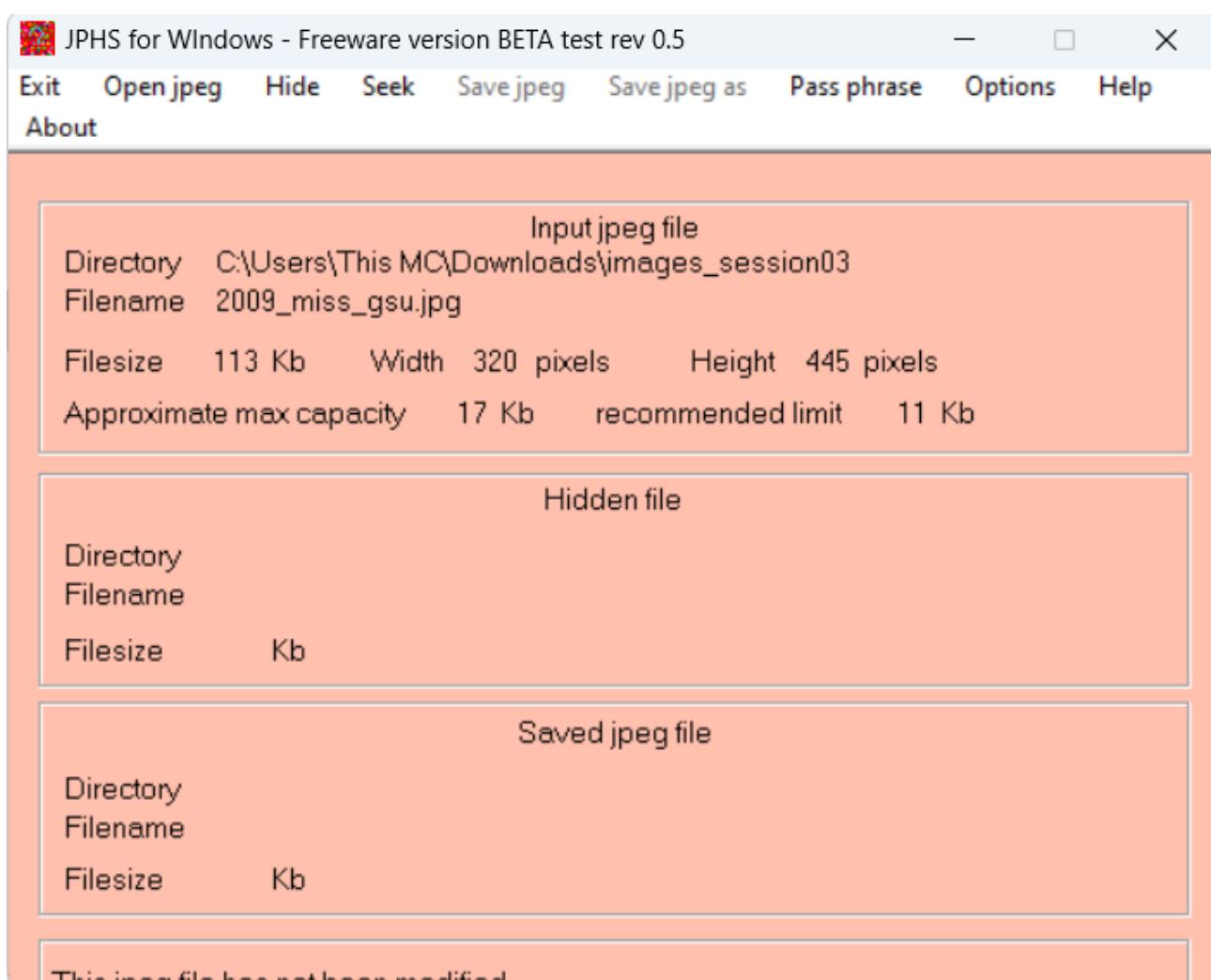
Tài nguyên ảnh trong file nén images\_session03.zip (Ảnh: 2009\_miss\_gsu.jpg)



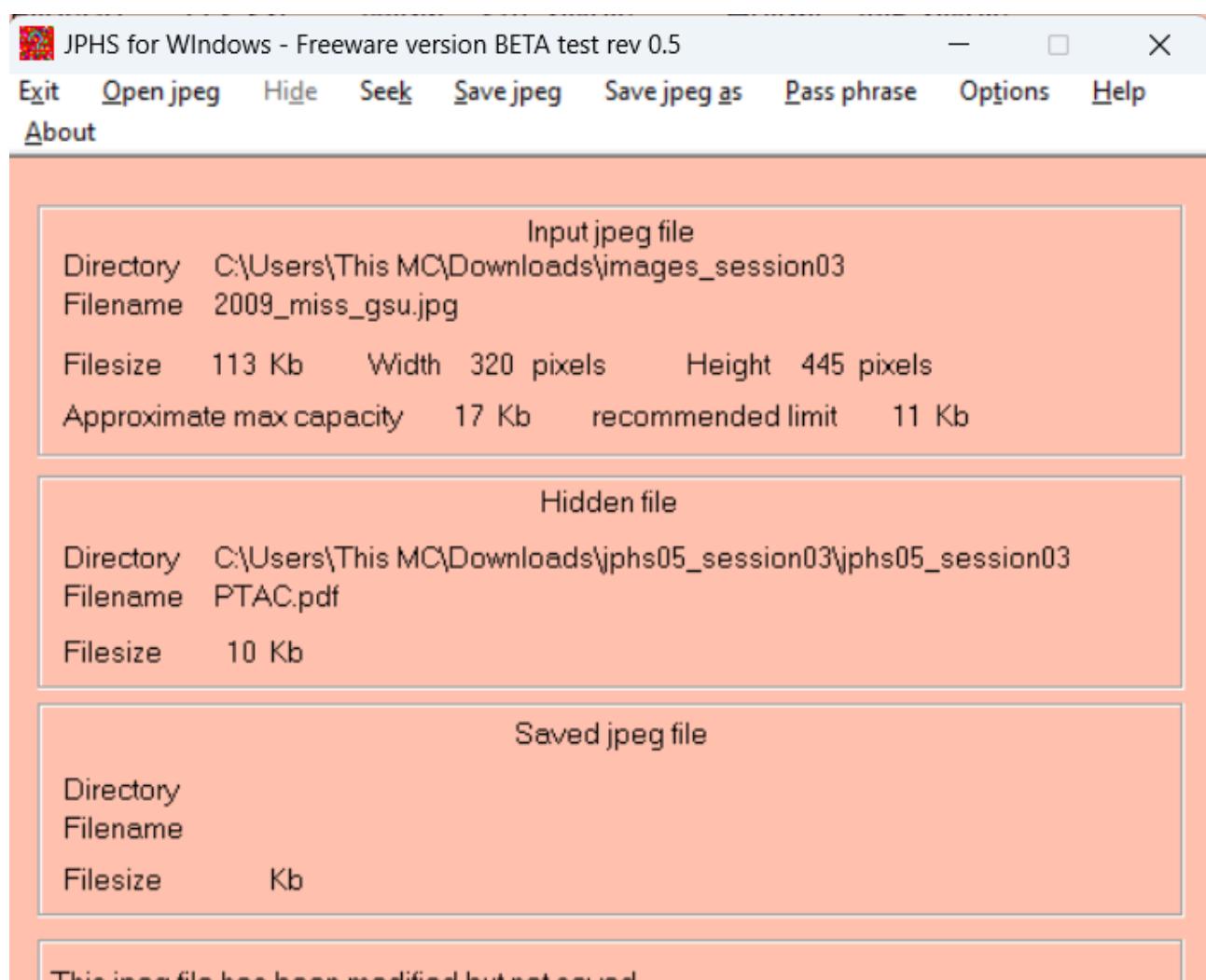
### Nội dung file PTAC.pdf

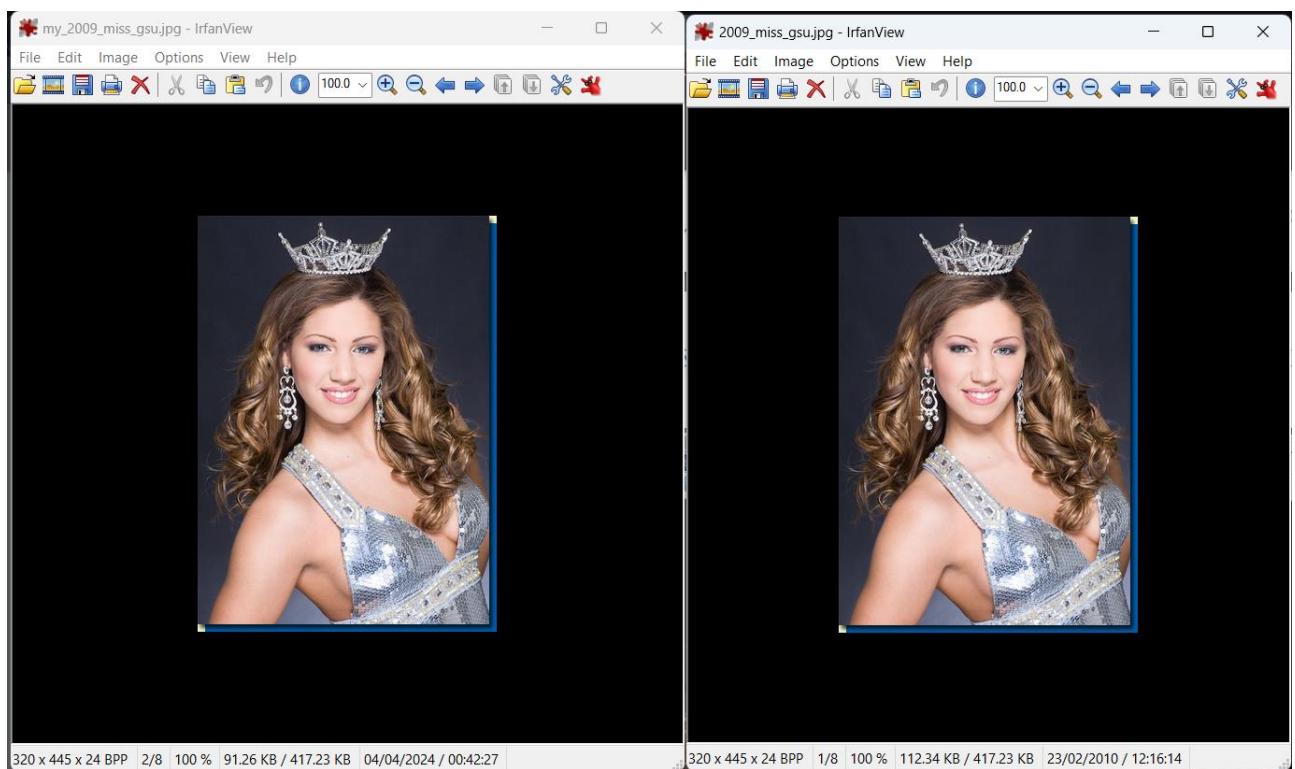
The screenshot shows the Foxit PDF Reader interface with a PDF titled "PTAC.pdf". The document contains a table with the following data:

Done	Name	User Name	E-mail	Password	External Login Info.
	Ann Rawlings	ARawlings	ARawlings@peoriaud.k12.az.us	your current password	pusd11user.name
	Chris Kuczka	CKuczka	CKuczka@peoriaud.k12.az.us	your current password	pusd11user.name
	Cindy Callaway	CCallaway	CCallaway@peoriaud.k12.az.us	your current password	pusd11user.name
	Douglas Pearson	DPearson	DPEarson@peoriaud.k12.az.us	your current password	pusd11user.name
	David Snyder	DSnyder	DSnyder@peoriaud.k12.az.us	your current password	pusd11user.name
	Jo Little	JLittle	JLittle@peoriaud.k12.az.us	your current password	pusd11user.name
	Julia Erickson	JErickson	JErickson@peoriaud.k12.az.us	your current password	pusd11user.name
	Larry Buchanan	LBuchanan	LBuchanan@peoriaud.k12.az.us	your current password	pusd11user.name
	Lissa Cuellar	LCuellar	LCuellar@peoriaud.k12.az.us	your current password	pusd11user.name
	Maggie Olnay	MOlnay	MOlnay@peoriaud.k12.az.us	your current password	pusd11user.name
	Nan Gillispie-DAC	NGillisp	NGillisp@peoriaud.k12.az.us	your current password	pusd11user.name
	Nathan Bowler	NBowler	NBowler@peoriaud.k12.az.us	your current password	pusd11user.name
	Patti Belltram	PBelltram	PBelltram@peoriaud.k12.az.us	your current password	pusd11user.name
	Phil Valentine	PValentine	PValentine@peoriaud.k12.az.us	your current password	pusd11user.name
	Robert Keagle	RKeagle	RKeagle@peoriaud.k12.az.us	your current password	pusd11user.name
	Rosemary Martin-Moore	RMMoore	RMMoore@peoriaud.k12.az.us	your current password	pusd11user.name
	Samantha Middagh	SMiddagh	SMiddagh@peoriaud.k12.az.us	your current password	pusd11user.name
	Sarah Balder	SBalder	SBalder@peoriaud.k12.az.us	your current password	pusd11user.name
	Shona Miranda	SMiranda	SMiranda@peoriaud.k12.az.us	your current password	pusd11user.name
	Stacy Swayoy	SSwayoy	SSwayoy@peoriaud.k12.az.us	your current password	pusd11user.name
	Toni Nevezrez	TNevarez	TNevarez@peoriaud.k12.az.us	your current password	pusd11user.name
	Terrie Rust	TRust	TRust@peoriaud.k12.az.us	your current password	pusd11user.name
	Valerie Nash	VNash	VNash@peoriaud.k12.az.us	your current password	pusd11user.name
	Bill Copeland	BilCopeland	BilCopeland@COX.NET	BilNeTA5	pusd11ext\Bill Copeland
	Tammarra Edgin	TammarraEdgin	tammarrae@microsoft.com	TeCom23	pusd11ext\Tammarra Edgin
	Diane Douglas	DianeDouglas	dmdouglas@cox.net	DdNet21	pusd11ext\Diane Douglas
	Mary Crespino	MaryCrespino	mcrespy@cox.net		



Thực hiện ẩn file PTAC.pdf vào file 2009\_miss\_gsu.jpg

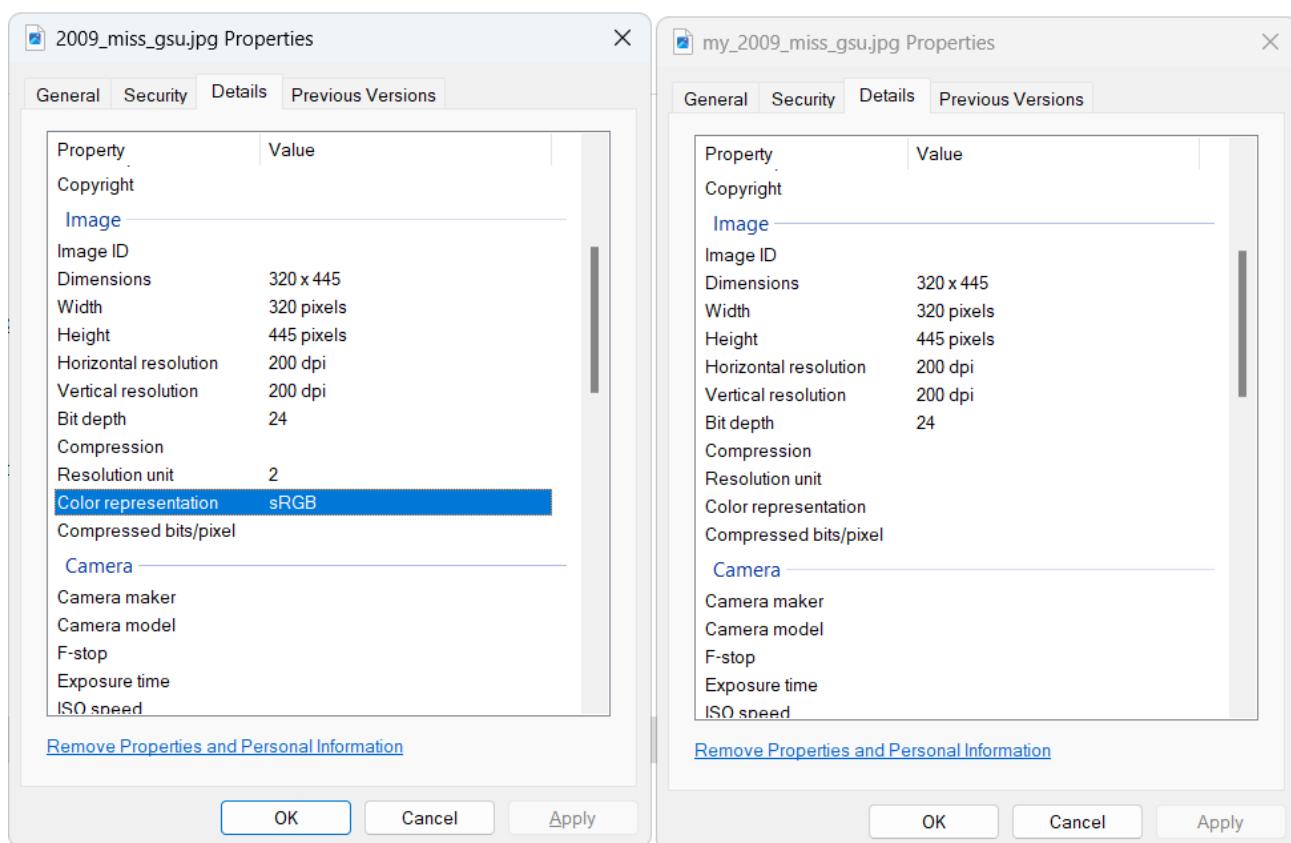




Kiểm tra nội dung file PTAC.pdf thì không thấy thay đổi.

Ta có thể thấy size của my\_2009\_miss\_gsu.jpg nhỏ hơn 2009\_miss\_gsu.jpg

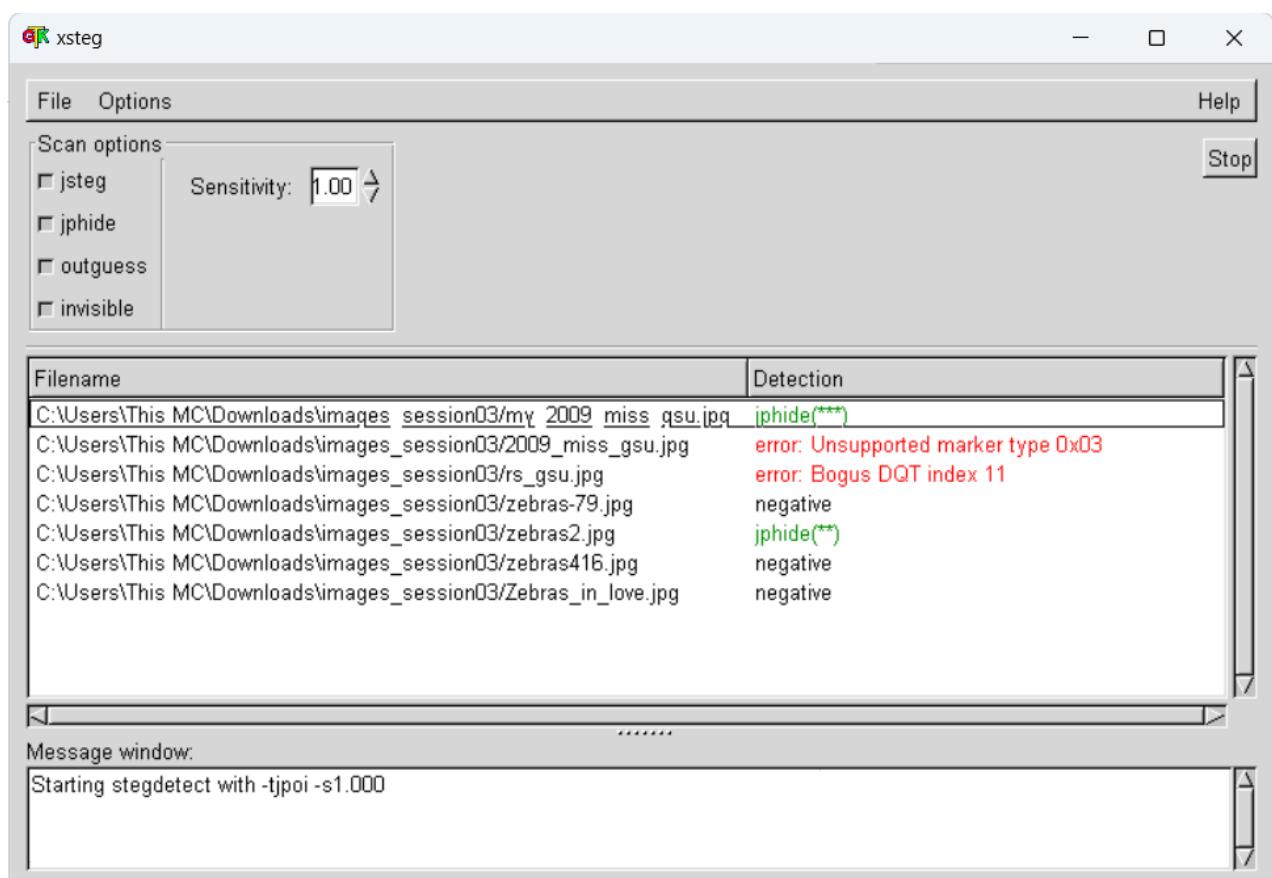
Chất lượng ảnh của my\_2009\_miss\_gsu.jpg cũng có một chút đậm màu hơn 2009\_miss\_gsu.jpg



### Kịch bản 01-c. Phát hiện dữ liệu được giấu trong ảnh JPEG sử dụng StegDetect.

- Tài nguyên: image\_session03.zip
- Công cụ: stegdetect04\_session03.zip. Thực hiện giải nén và chạy file "xsteg.exe"
- Chọn thư mục chứa ảnh cần phân tích. Thực hiện quét và đưa ra kết quả, nhận xét.
- Thực hiện bẻ khóa mật khẩu trong quá trình giấu tin. (Chuẩn bị: my\_2009\_miss\_gsu.jpg - ảnh đã giấu thông tin ở kịch bản 02 bên trên, Zebras2.jpg, Stegbreak.exe). Mật khẩu tìm thấy là gì? Nhận xét về khả năng tìm thấy của công cụ?
- Giải nén thông tin chứa trong file ảnh có phát hiện ẩn giấu thông tin bằng mật khẩu tìm được.

Khi quét thử mục chứa các file ảnh my\_2009\_miss\_gsu.jpg và zebras2.jpg thì được kết quả.



Ở kịch bản 1-b ta đã cài đặt mật khẩu để ẩn file là UIT nên tool xsteg đã phát hiện ra file được che giấu trong file my\_2009\_miss\_gsu.jpg

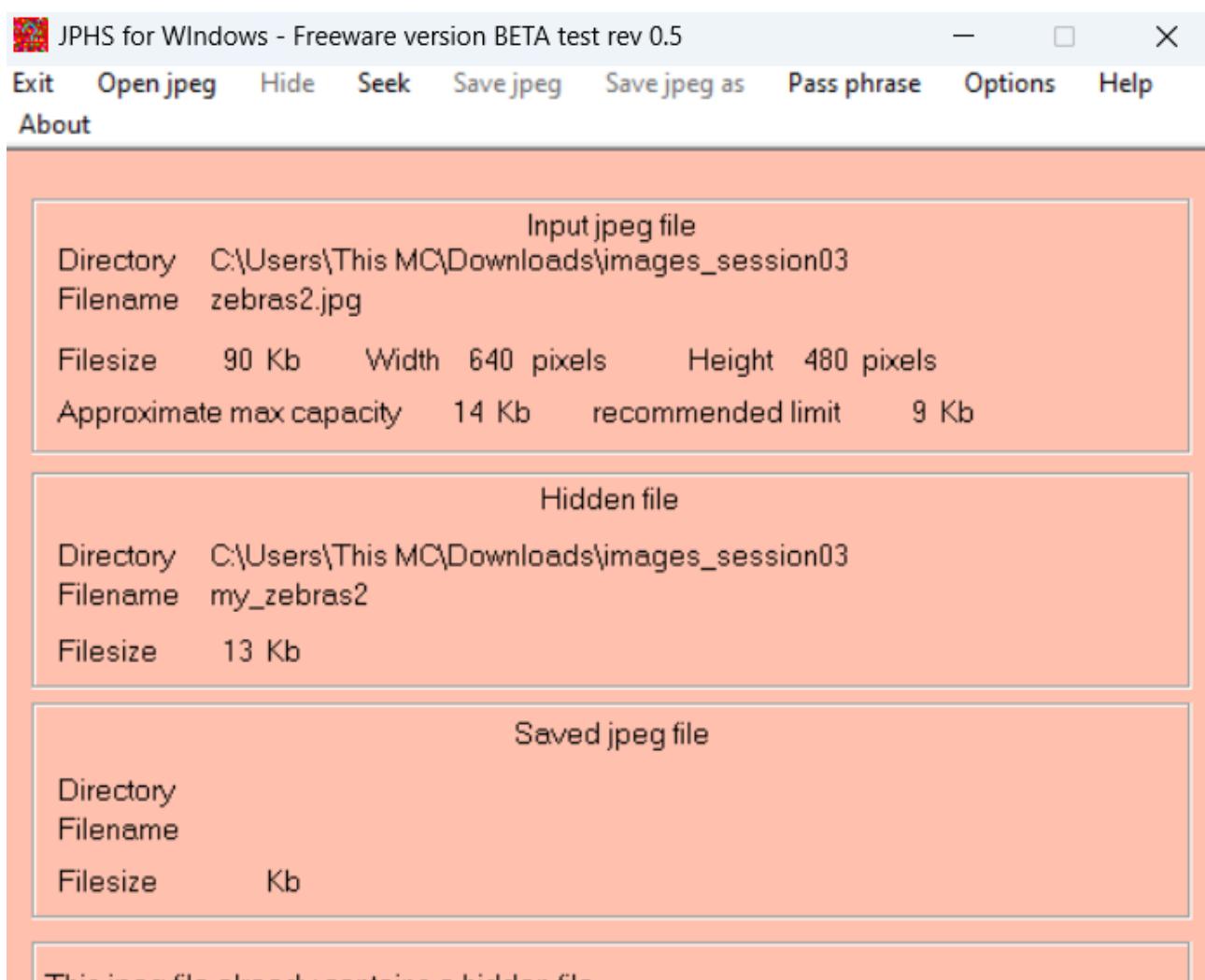
Tương tự xsteg cũng đoán ra file zebras2.jpg có file ẩn ở trong.

Sau đó ta dùng tool stegbreak.exe để bruteforce password của file zebras2.jpg

```
Windows PowerShell
PS C:\Users\This MC\Downloads\stegdetect04_session03> ./stegbreak.exe -r rules.ini -f MedDict.DIC zebras2.jpg
Loaded 1 files...
zebras2.jpg : jphide[v5](together)
Processed 1 files, found 1 embeddings.
Time: 4 seconds: Cracks: 68607, 17151.8 c/s
```

Tìm được password là together.

Dùng JPHS để xem file ẩn ở trong.



Trích xuất được ra nhưng chưa biết đây hiện tại là file gì.

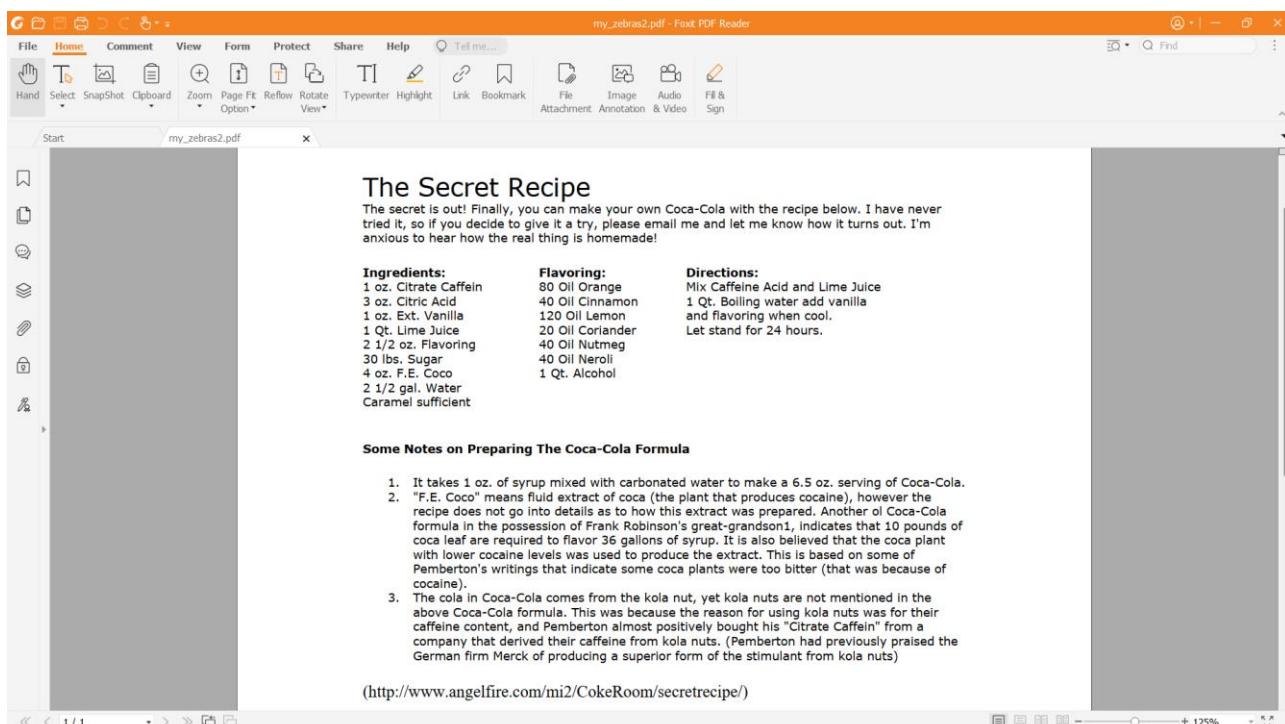
Name	Date modified	Type	Size
<b>▼ Today</b>			
my_zebras2	04/04/2024 12:56 AM	File	13 KB
my_PTAC.pdf	04/04/2024 12:46 AM	Foxit PDF Reader ...	10 KB
my_2009_miss_gsu.jpg	04/04/2024 12:42 AM	JPG File	92 KB
<b>▼ A long time ago</b>			
zebras2.jpg	23/02/2010 2:10 PM	JPG File	90 KB
New Text Document.txt	23/02/2010 2:04 PM	Text Document	2 KB
Zebras_in_love.jpg	23/02/2010 1:51 PM	JPG File	1,952 KB
zebras-79.jpg	23/02/2010 1:51 PM	JPG File	46 KB
zebras416.jpg	23/02/2010 1:50 PM	JPG File	38 KB
rs_gsu.jpg	23/02/2010 12:16 PM	JPG File	79 KB
2009_miss_gsu.jpg	23/02/2010 12:16 PM	JPG File	113 KB

Bỏ sang linux và dùng lệnh file để xem đó là file gì

```
longsix@MCComputer: ~      X + | ^ 
longsix@MCComputer:~$ file my_zebras2
my_zebras2: PDF document, version 1.4, 1 pages
longsix@MCComputer:~$ |
```

Ta có thể thấy file được trích xuất ra là file pdf.

Ta thực hiện rename và đọc kết quả.

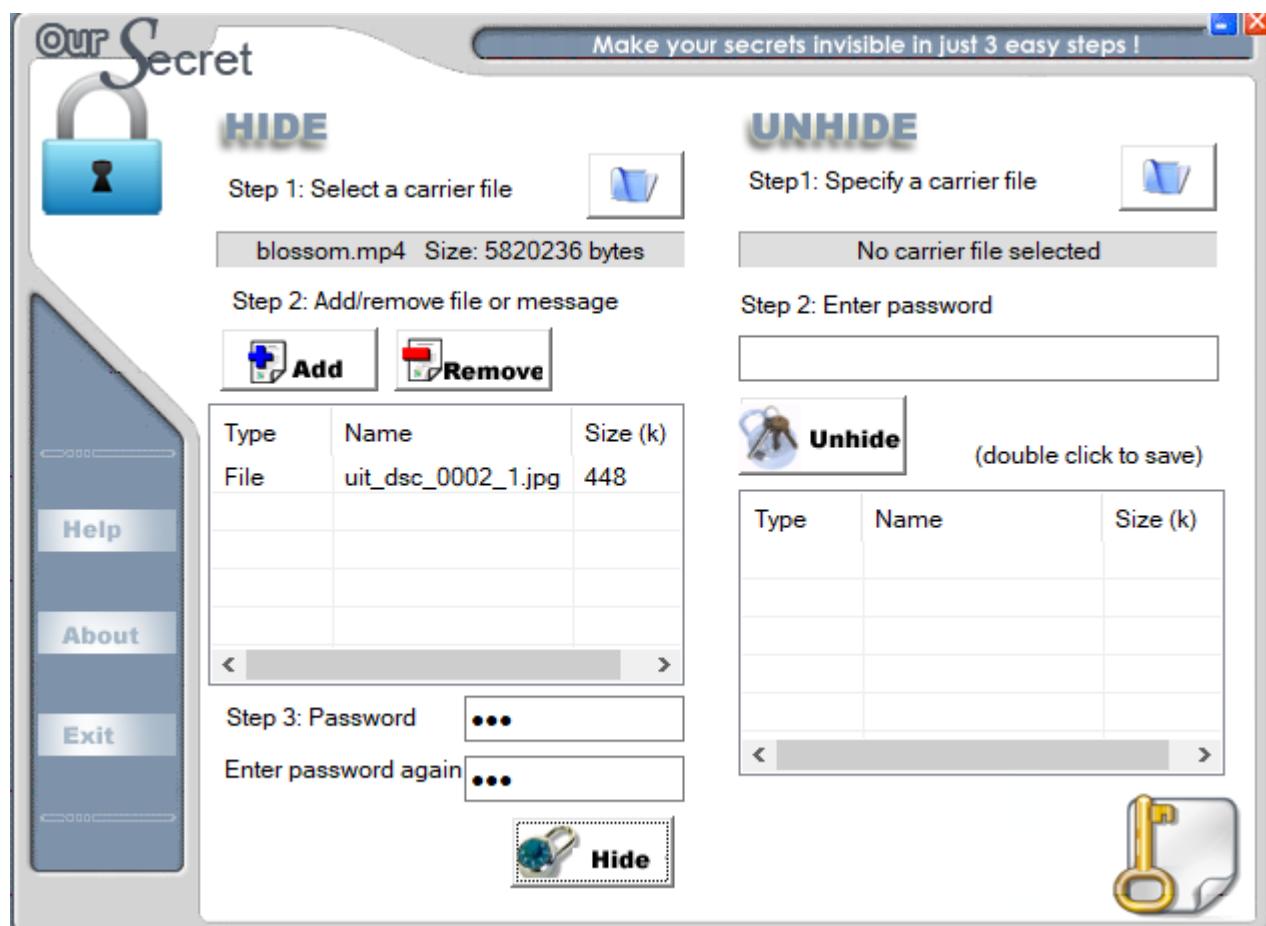


## Kịch bản 02. Ẩn giấu dữ liệu bằng công cụ Our Secret

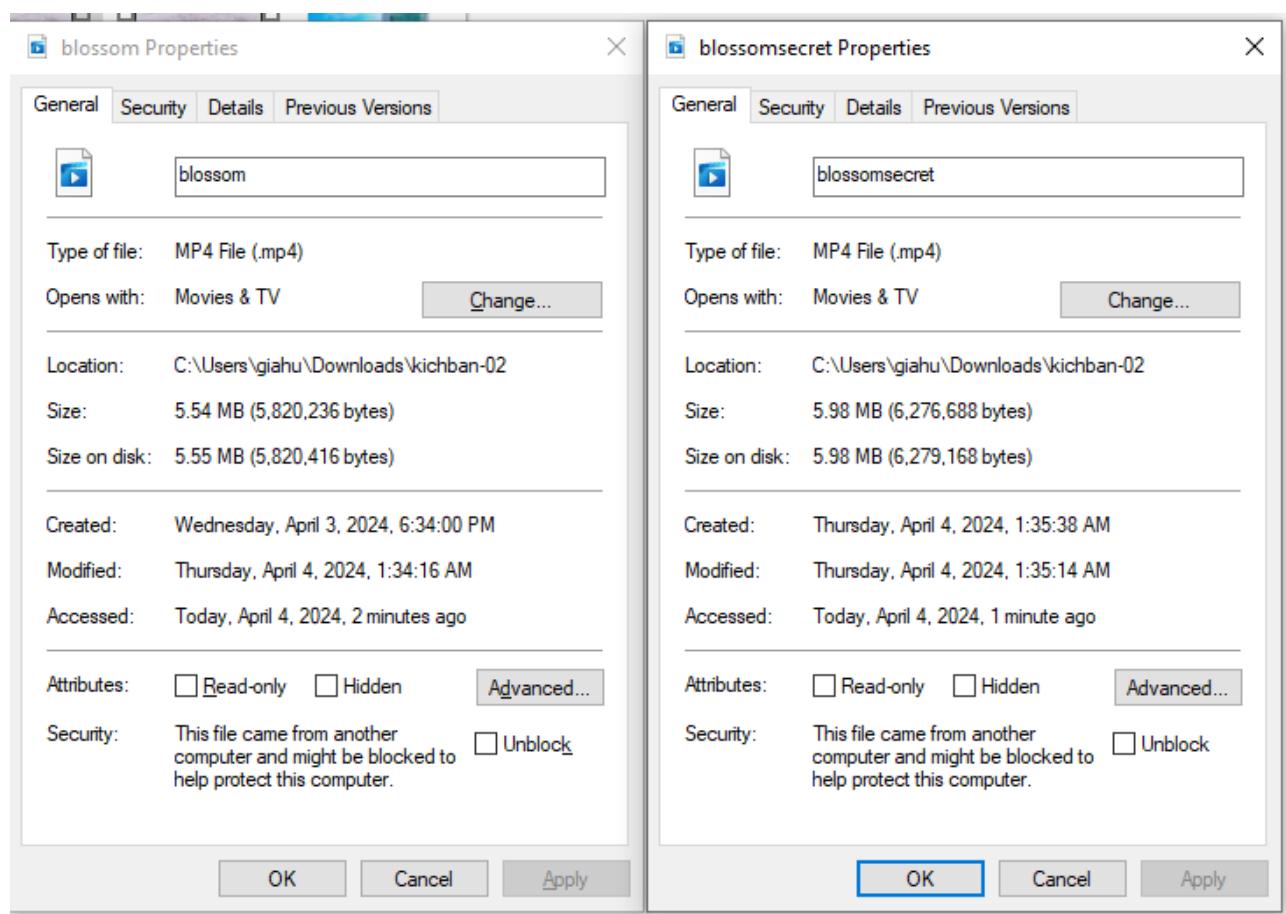
- Tài nguyên: uit\_dsc\_0002\_1.jpg, blossom.mp4
- Phần mềm Our Secret: có thể tải tại liên kết sau:  
<http://steganography.findmysoft.com/>
- Cài đặt phần mềm, sau đó giấu ảnh uit\_dsc\_0002\_1.jpg vào tập tin mp4. Đặt mật khẩu trong quá trình giấu tin là "E81". Nhận xét về sự thay đổi của video (thời gian, dung lượng, chất lượng) khi thêm ảnh vào đoạn phim blossom.mp4.
- Giải mã thông tin giấu trong đoạn phim blossom.mp4. Nhận xét về nội dung file giải mã được với file ban đầu (file/thông tin được chọn để giấu).

*Đáp án:*

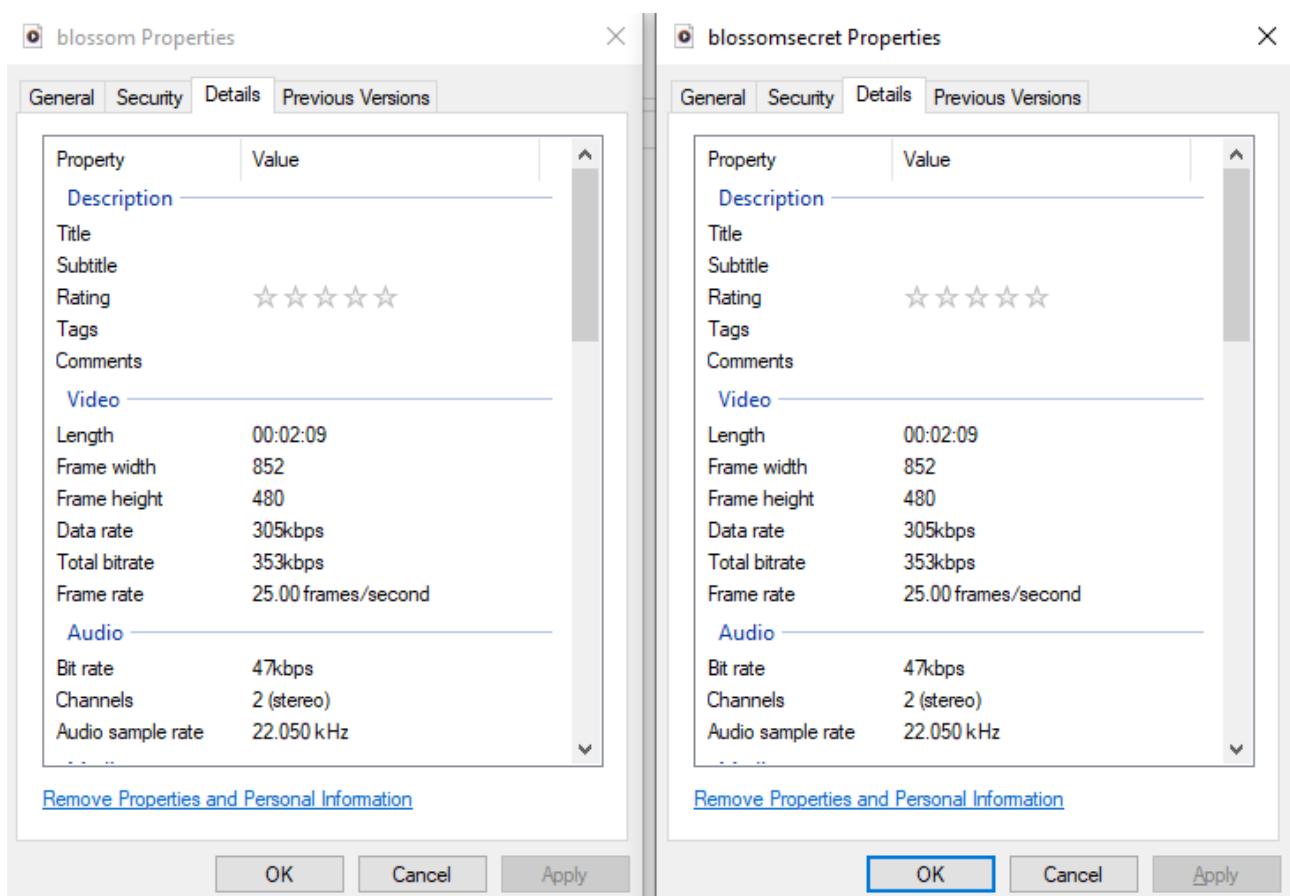
Sử dụng công cụ Our Secret để ẩn giấu ảnh uit\_dsc\_0002\_1.jpg vào tập tin mp4.  
Đặt mật khẩu là "E81".



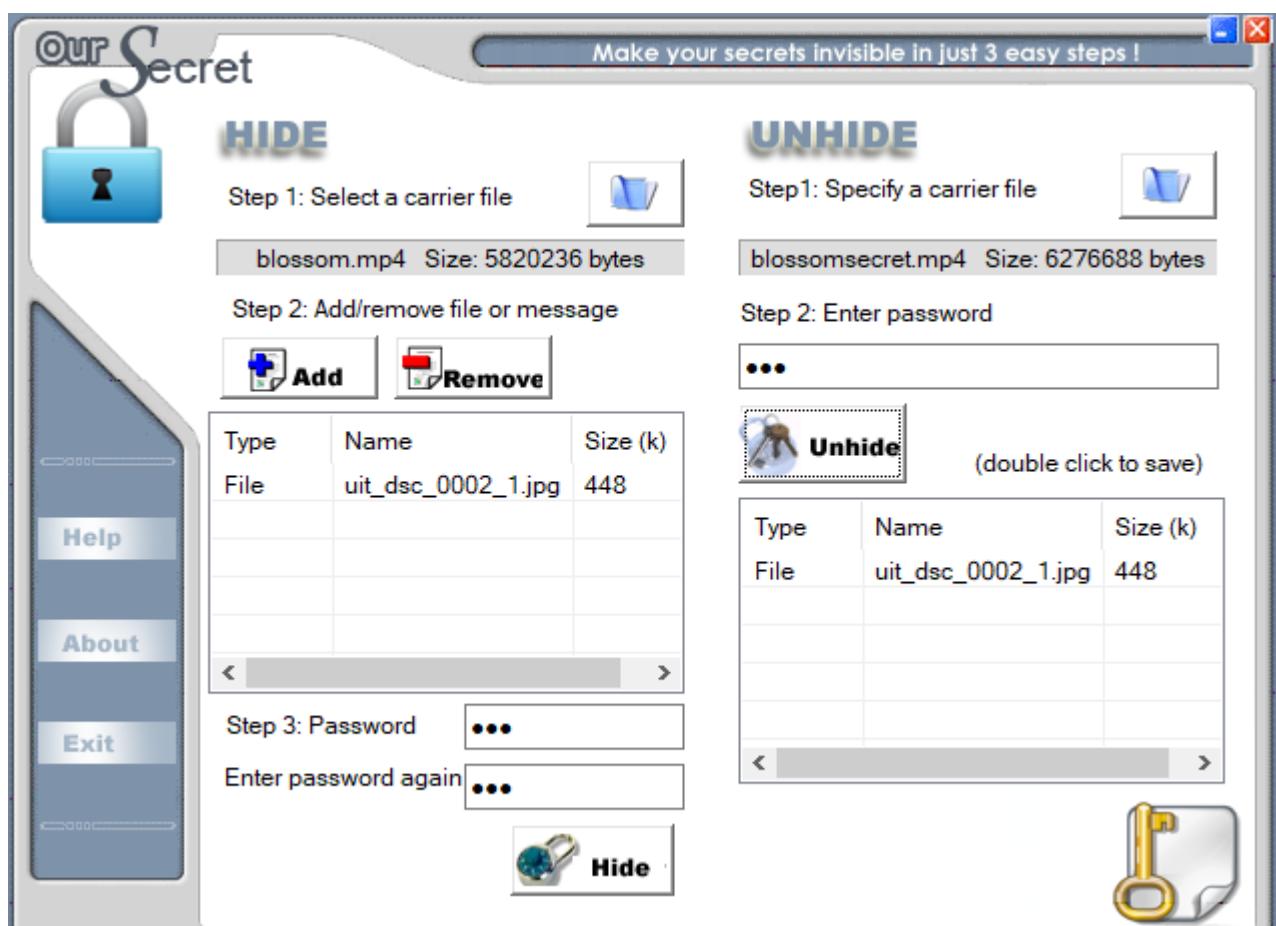
Ta thấy file mp4 sau khi chèn ảnh có dung lượng lớn hơn file gốc.



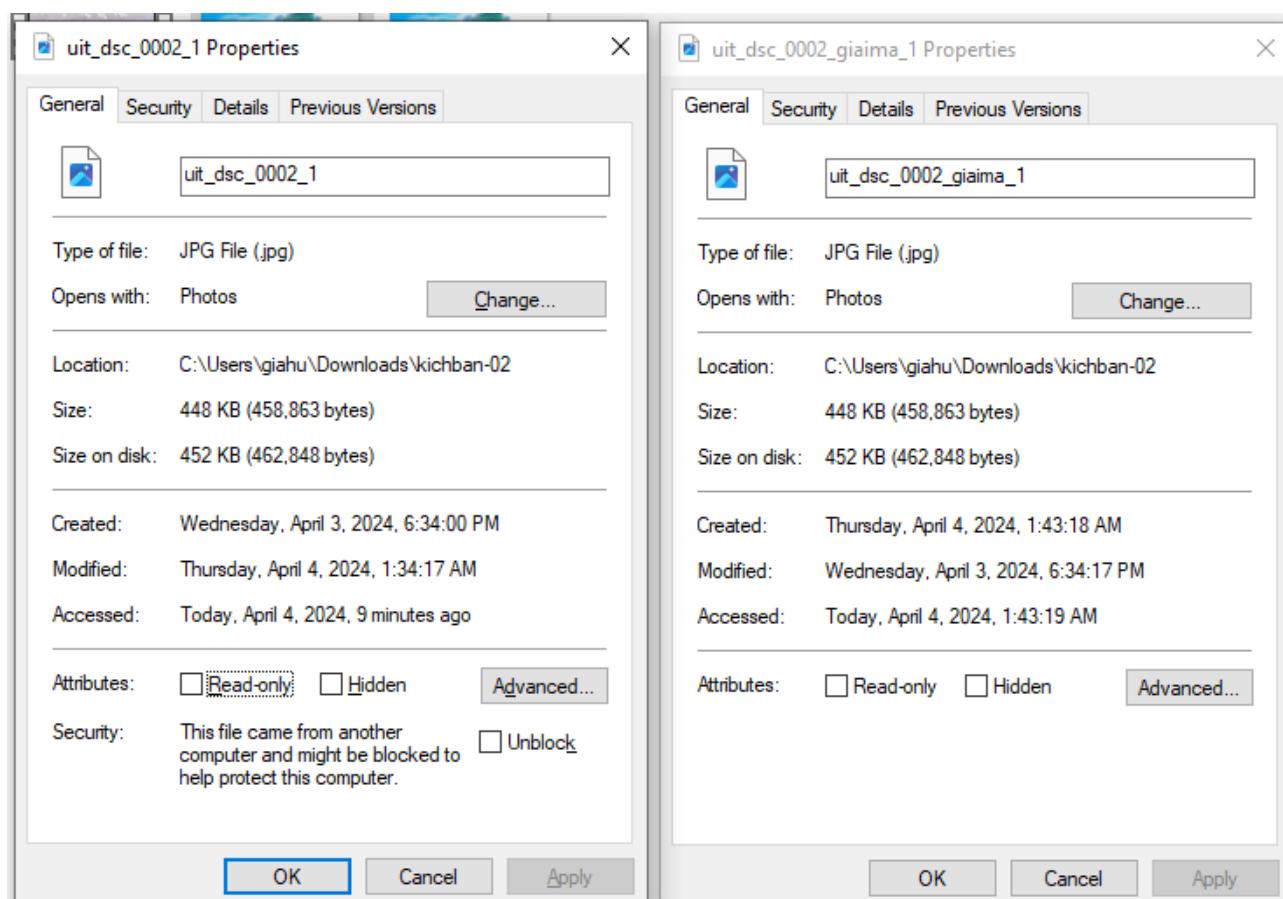
Còn về chất lượng và thời lượng thì không thấy sự khác biệt.



Thực hiện giải mã thông tin được ẩn giấu.



ảnh được giải mã và ảnh gốc cũng không khác biệt

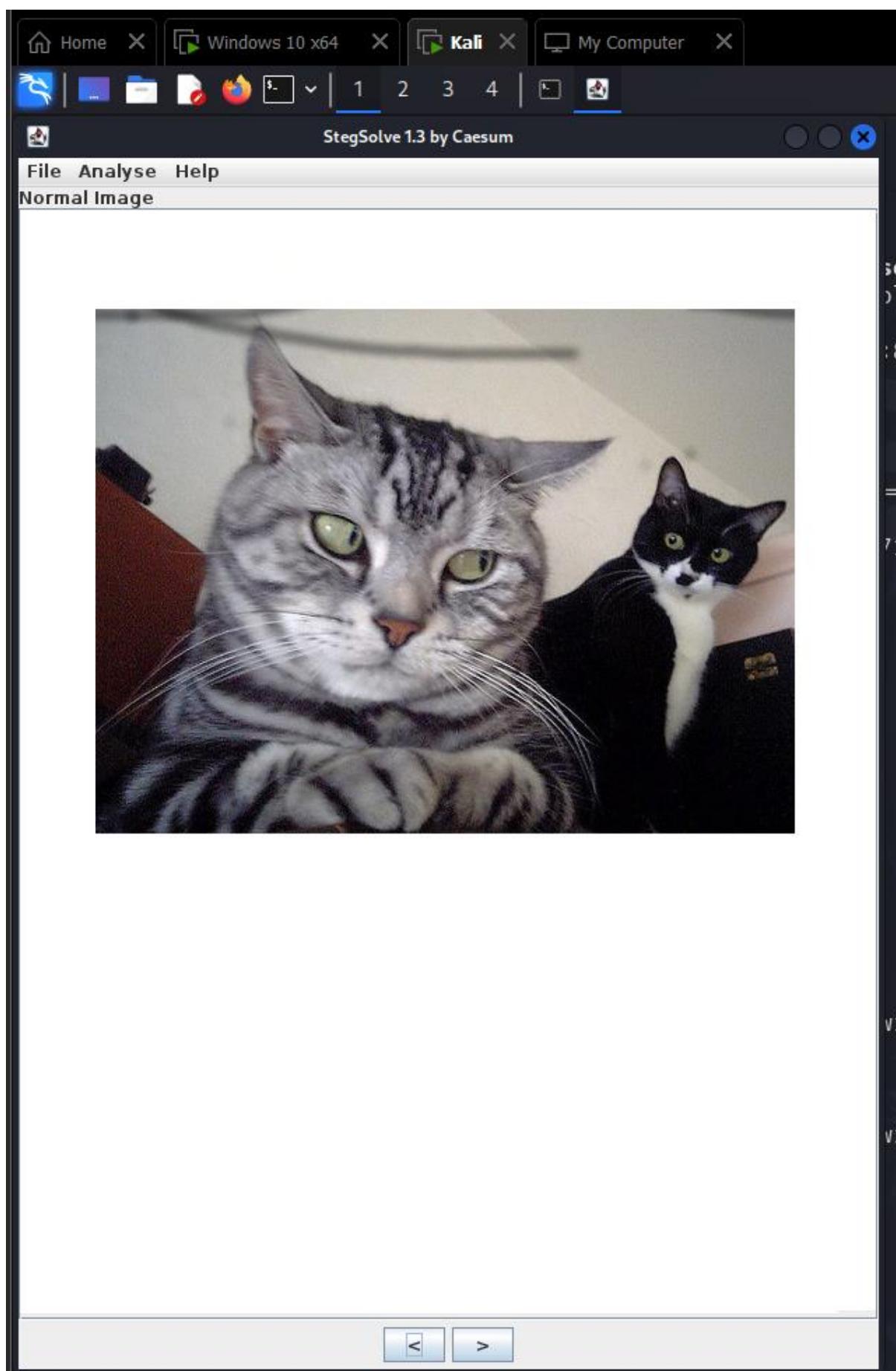


### Kịch bản 03. Điều tra thông tin được ẩn giấu

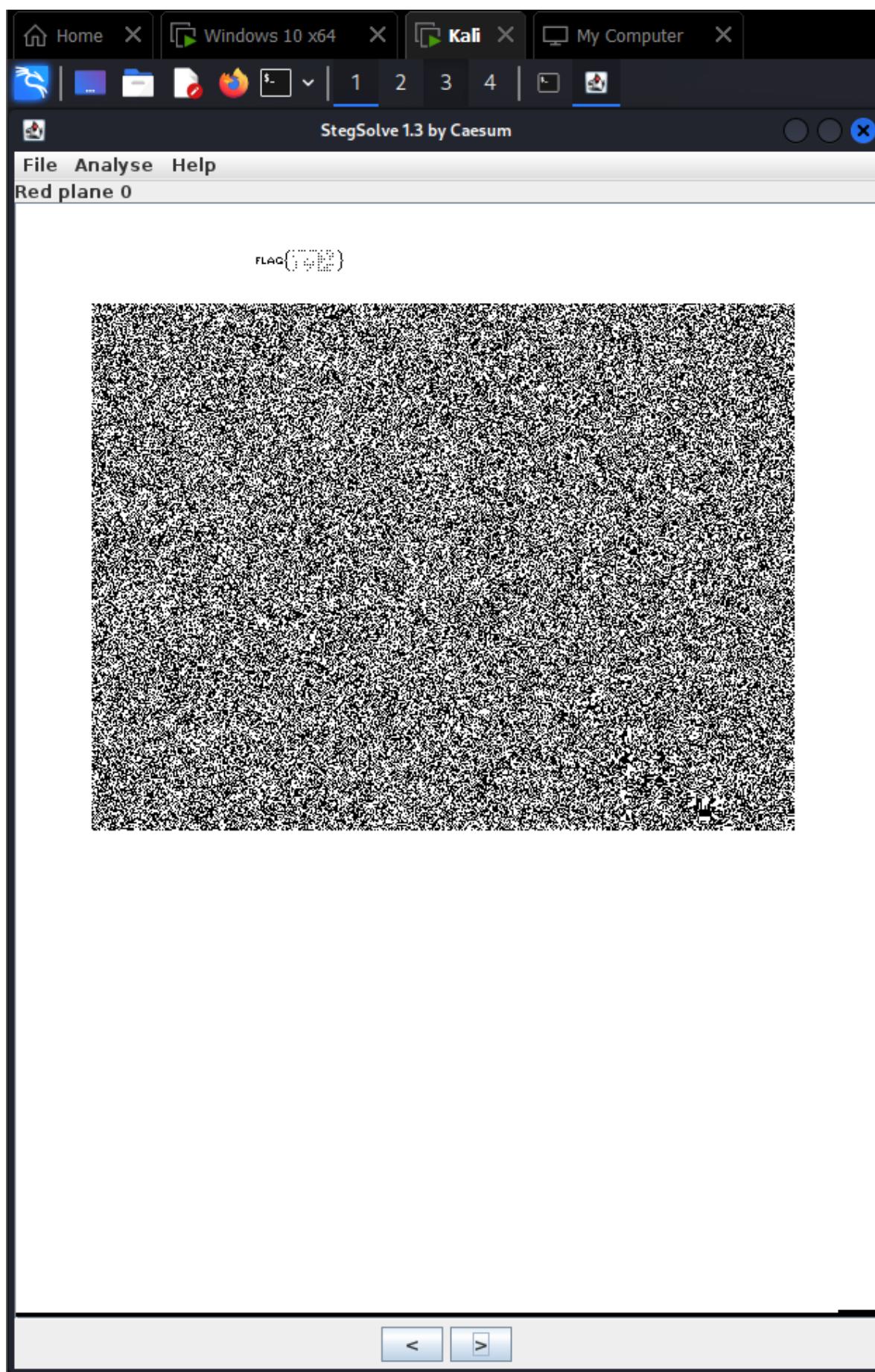
- Tài nguyên: kb03-suspicion.png
- Mô tả: Bức ảnh scan này đã được phục hồi từ các tập tin của một cựu nhân viên của Hiệp hội Ngờ ngẩn Miêu Quốc. Nhân viên điều tra cần phải tìm ra số sê-ri của máy in này để có thể xác định vị trí của thiết bị. Tìm số sê-ri của máy in.

*Đáp án:*

Dùng tool stegsolve để mở file ảnh



Xem dưới gam màu red plane 0 thì thấy có flag



Ta thực hiện giải mã thông điệp FLAG.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
64	x							x	x		x		x		x
32	x						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
2		x				x				x		x	x		
1	x					x				x	x	x	x	x	
												57	19	71	53

Như vậy số seri là 53711957

#### Kịch bản 04. Điều tra thông tin được ẩn giấu

- Tài nguyên: star-wars.jpg
- Yêu cầu - Gợi ý: Bức ảnh được nhân viên điều tra tìm thấy trong một máy tính của một nghi phạm có sở thích xem ảnh của họa sĩ John Bramblitt. Tìm thông điệp được ẩn giấu, biết rằng thông điệp bắt đầu bằng "become".

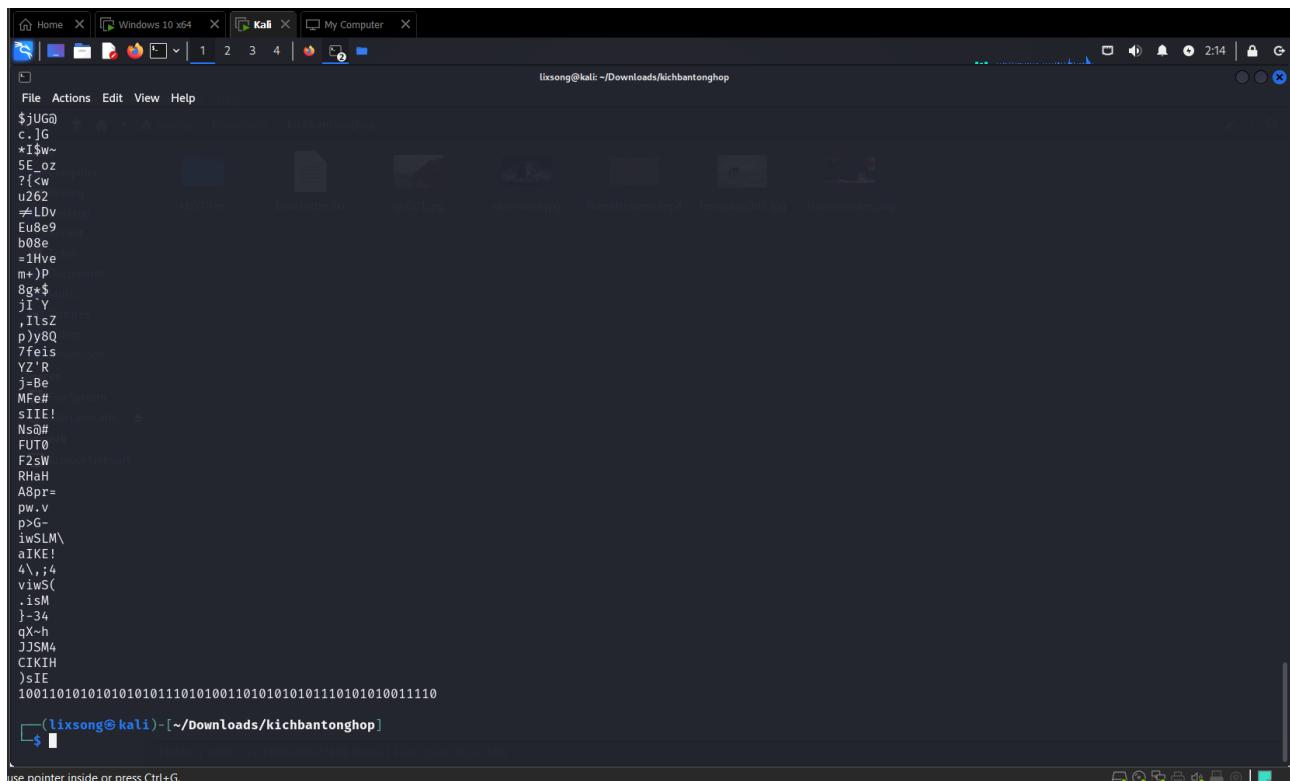
Đáp án:

Dùng strings để xem thử file này có gì không

```

(lixsong㉿kali)-[~/Downloads/kichbantonghop]
$ ls
LoveLetter.txt kb07-res qn001.jpg star-wars.jpg thecatreturns.mp4 tiengiang003.jpg transmission.png
(lixsong㉿kali)-[~/Downloads/kichbantonghop]
$ strings star-wars.jpg
JFIF
$"80P40,,0bFJ:Ptfxzrfpn
"$${0*x^44}^
$3br
%6'()x456789:CDEFIGHIJSTUVWXYZcdefghijstuvwxyz
#3R
6'()x456789:CDEFIGHIJSTUVWXYZcdefghijstuvwxyz
bQJ1)
$@;zw
zDj
L{R}iqA
@ Fx
rN*1GN
=00E
0f*(
?fswP *E
jqZ0Gn
SM'4P
M-Q!
-5F!
VrwF
3ePt'
E.1@ F8
$!d
!Nr(
}+V
Jwnp)
5$Wd
Vf9$
77oj
GSZ6c
7:b
s00T
h9nI

```



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.

Trong ngôn ngữ Braille thì mỗi chữ được thể hiện bởi 6 điểm → 6 bit

100110 101010 101010 111010 100110 101010 101110 101010 011110

Dùng công cụ decoder online để dịch các kí tự trên.

The screenshot shows a web browser with the URL [dcode.fr/braille-alphabet](https://dcode.fr/braille-alphabet). The page title is "Braille Alphabet". It features a search bar for tools, a "Braille Decoder" section with a large grid of Braille dots, and a "Summary" sidebar with links to various Braille-related topics.

**Braille Alphabet**  
Communication System - Braille Alphabet

**Braille Decoder**

Use the symbols or write directly a Braille message (any format) below

BRILLE SYMBOLS (CLICK TO ADD)

BRILLE CIPHERTEXT (ANY FORMAT EXCEPT OCTAL)  
1001101010101010101110101001101010101011101010100  
11110

VARIANT  ENGLISH (UNIFIED ENGLISH BRAILLE)  BRAILLE ASCII (INTERNATIONAL)  FRENCH BRAILLE (ORIGINAL)  FRENCH BRAILLE + DIGITS ANTOINE (FOR MATHS)  CHINESE MAINLAND BRAILLE (PINYIN INPUT - NO TONES)

**Summary**

- Braille Decoder
- Braille Encoder
- What is Braille? (Definition)
- How to encrypt using Braille cipher?
- How to decrypt Braille cipher?
- How to recognize Braille ciphertext?
- What are the variants of the Braille cipher?
- How to print Braille?
- When was Braille alphabet invented?

**Similar pages**

- Symbols Cipher List
- French Sign Language
- Morse Code
- Dotless Font
- G8 Braille Code
- Chappe Code
- Navy Signals Code
- DCODE'S TOOLS LIST

Ta được kết quả là doordonot. Chuỗi này khả năng là 1 key nào đó.

Thực hiện dùng steghide và password doordonot để extract file ẩn trong file stars-war.jpg.

Cat file flag.txt thấy nó ở dạng base64 ta thực hiện decode lại thì được kết quả:  
becomeajedimasteryouwill

```

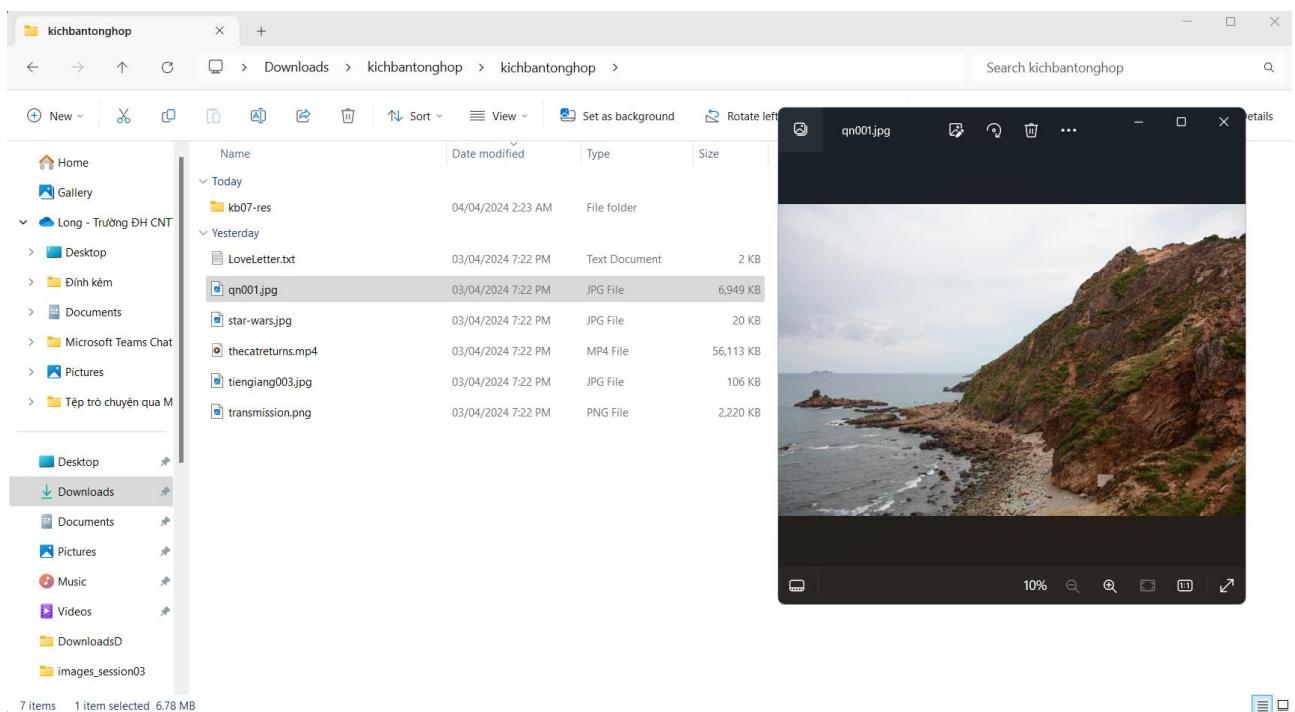
Home X Windows 10 x64 X Kali X My Computer X
File Actions Edit View Help
ls LoveLetter.txt kb07-res qn001.jpg star-wars.jpg thecatreturns.mp4 tiengiang003.jpg transmission.png
steghide extract -sf star-wars.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
ls LoveLetter.txt flag.txt kb07-res qn001.jpg star-wars.jpg thecatreturns.mp4 tiengiang003.jpg transmission.png
cat flag.txt
YmVjb21lYWplZGltYXN0ZXJ5b3V3aWxs
echo "YmVjb21lYWplZGltYXN0ZXJ5b3V3aWxs" | base64 --decode
becomeajedimasteryouwill

```

### Kịch bản 05. Thực hiện phân tích, tìm thông tin ẩn giấu trong ảnh

- Tài nguyên thực hiện: qn001.jpg
- Yêu cầu – Gợi ý: Tìm thông điệp (flag) được ẩn giấu. Thông tin flag liên quan đến Đội tuyển bóng đá nam Việt Nam.

Gợi ý:



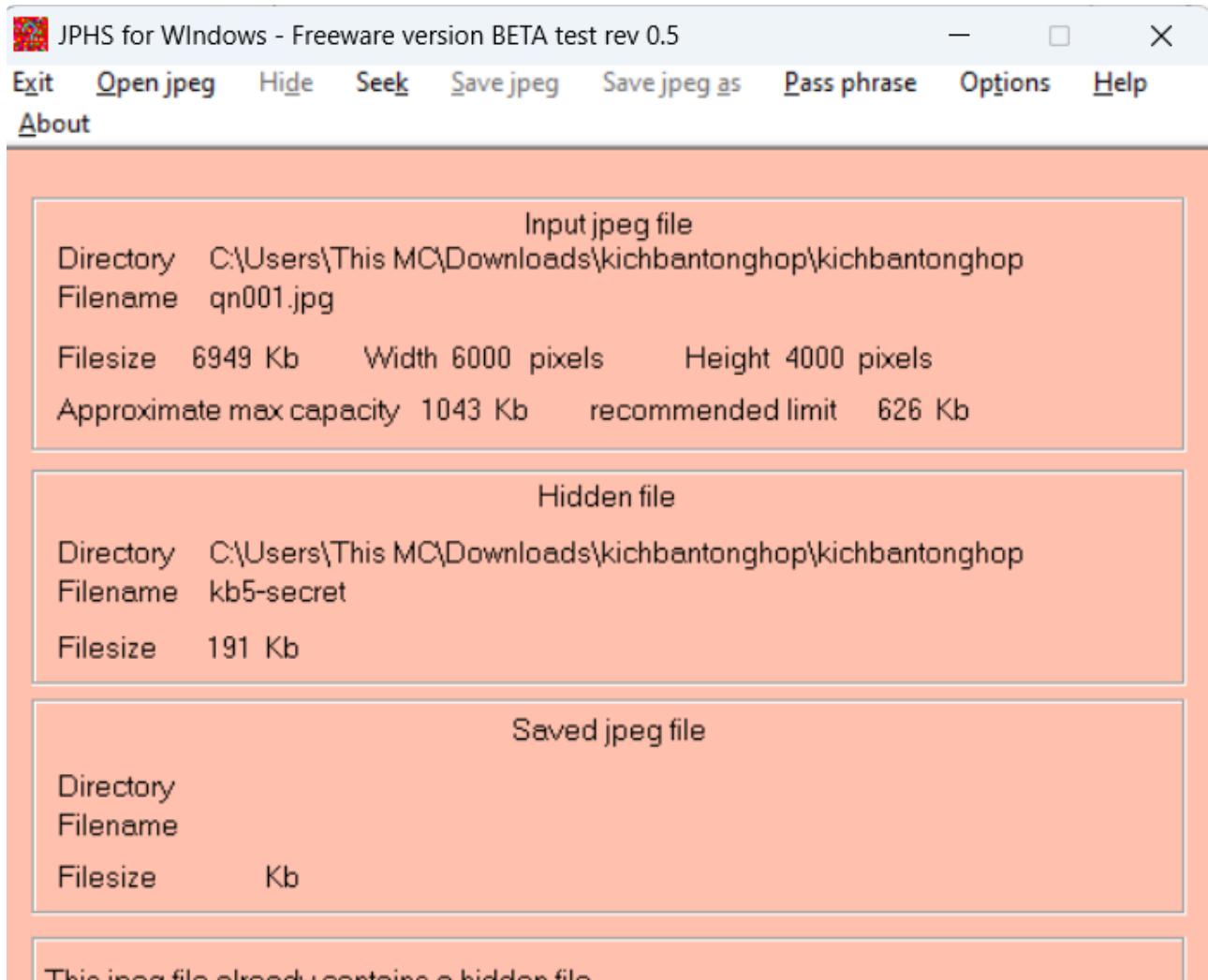
Ta thấy đây chỉ là 1 file ảnh mà lên đến 6,949 KB nên ta đoán sẽ có chứa file ẩn ở trong.

Dùng tool stegbreak để tìm file ẩn theo wordlists rockyou.txt

```
PS C:\Users\This MC\Downloads\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]()
Processed 1 files, found 1 embeddings.
Time: 1 seconds: Cracks: 4751, 4751.0 c/s
PS C:\Users\This MC\Downloads\stegdetect04_session03>
```

Ta thấy có một file ẩn được nhúng trong ảnh.

Dùng JPHS để lấy file đó ra. Chọn Seek -> Phần passphrase ta để trống



Name	Date modified	Type	Size
<b>Today</b>			
kb5-secret	04/04/2024 2:33 AM	File	191 KB
kb07-res	04/04/2024 2:23 AM	File folder	
<b>Yesterday</b>			
LoveLetter.txt	03/04/2024 7:22 PM	Text Document	2 KB
qn001.jpg	03/04/2024 7:22 PM	JPG File	6,949 KB
star-wars.jpg	03/04/2024 7:22 PM	JPG File	20 KB
thecatreturns.mp4	03/04/2024 7:22 PM	MP4 File	56,113 KB
tiengiang003.jpg	03/04/2024 7:22 PM	JPG File	106 KB
transmission.png	03/04/2024 7:22 PM	PNG File	2,220 KB

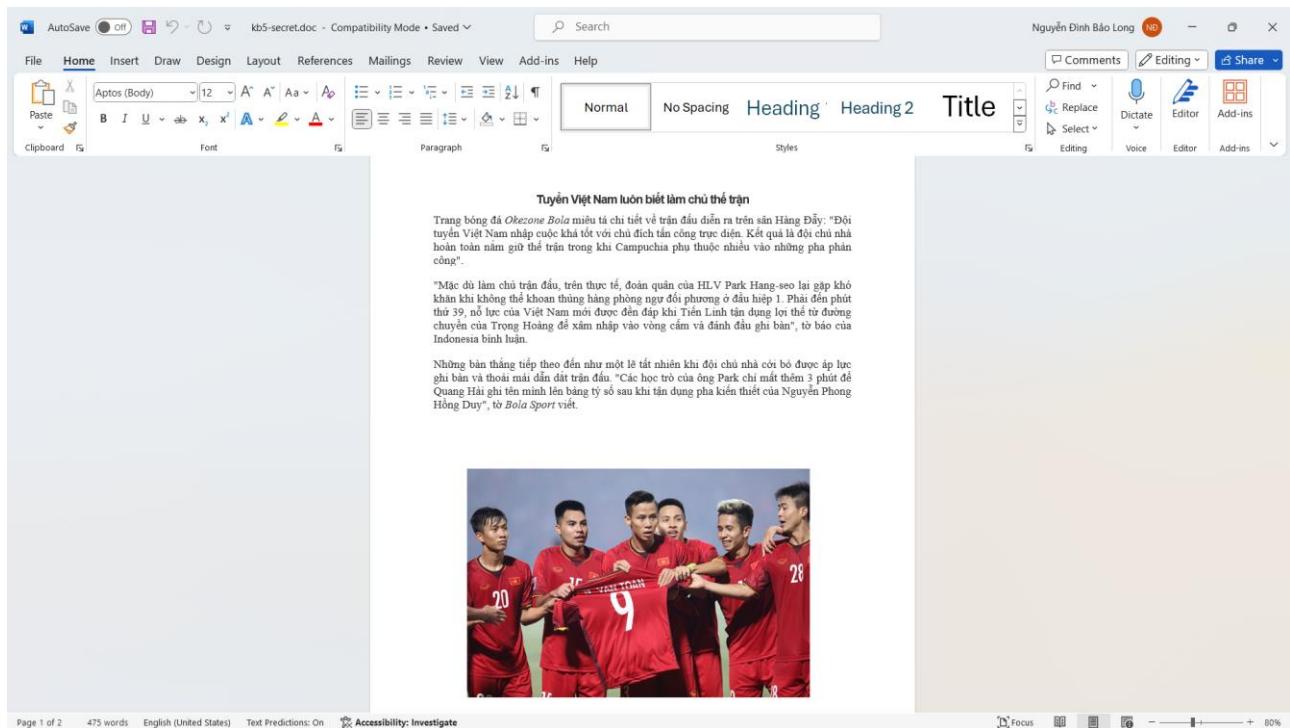
Chuyển sang linux và xem đó là file gì thì thấy là file doc.

```

longsix@MCComputer:~$ ls
DigiCertGlobalRootCA.crt.pem  NT521  kb5-secret  payload  pwndbg  shellcode.c  volatility
NT230                         bin    my_zebras2  peda     shellcode  shellcode.txt
longsix@MCComputer:~$ file kb5-secret
kb5-secret: Microsoft Word 2007+
longsix@MCComputer:~$ |

```

Mở file doc ra thì thấy nội dung liên quan đến bóng đá Việt Nam như đề bài nhưng không thấy flag.



Thực hiện chuyển file này sang kali để phân tích tiếp

```
C:\Users\This MC\Downloads\kichbantonghop\kichbantonghop>scp "C:\Users\This MC\Downloads\kichbantonghop\kichbantonghop\kb5-secret.doc" lixsong@192.168.110.130:/home/Lixsong/Downloads/kichbantonghop
kb5-secret.doc
100% 198KB 27.3MB/s 00:00
C:\Users\This MC\Downloads\kichbantonghop\kichbantonghop>
```

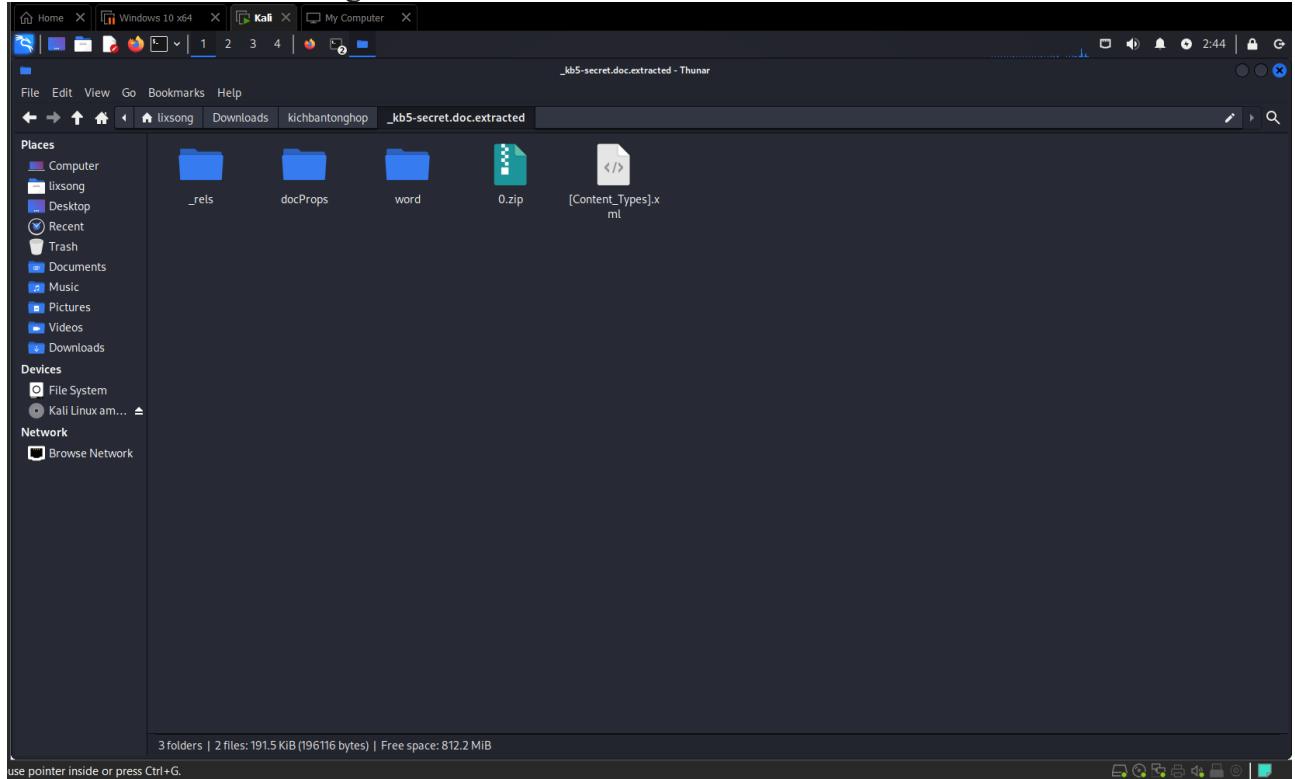
Dùng binwalk để xem có file ẩn và trích xuất ra

```
[lixsong@kali]-[~/Downloads/kichbantonghop]
└─$ binwalk -e kb5-secret.doc

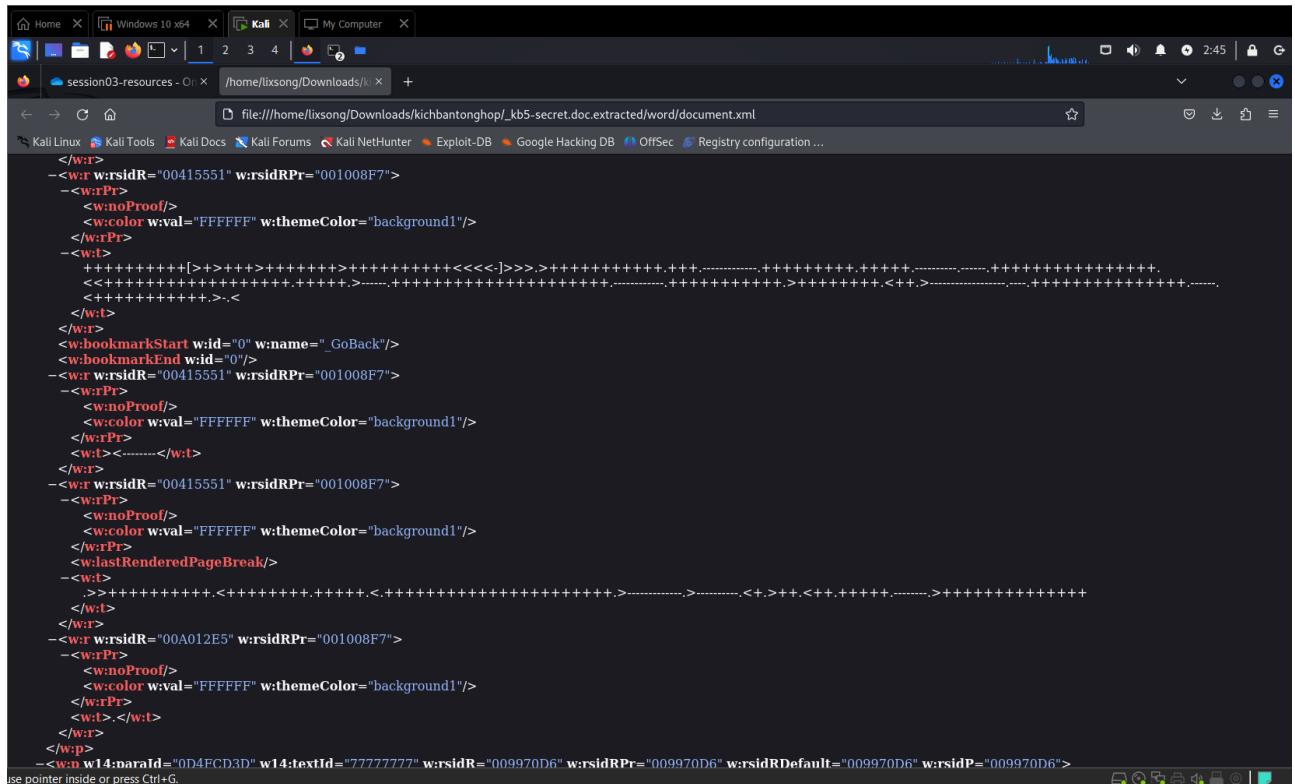
DECIMAL      HEXADECIMAL   DESCRIPTION
_____
0            0x0          Zip archive data, at least v2.0 to extract, compressed size: 359, uncompressed size: 1363, name: [Content_Types].xml
928          0x3A0        Zip archive data, at least v2.0 to extract, compressed size: 239, uncompressed size: 590, name: _rels/.rels
1728          0x6C0        Zip archive data, at least v2.0 to extract, compressed size: 3915, uncompressed size: 19670, name: word/document.xml
5690          0x163A       Zip archive data, at least v2.0 to extract, compressed size: 264, uncompressed size: 949, name: word/_rels/document.xml.rels
6276          0x1884       Zip archive data, at least v1.0 to extract, compressed size: 178935, uncompressed size: 178935, name: word/media/image1.jpg
185262         0x2D3AE     Zip archive data, at least v2.0 to extract, compressed size: 1538, uncompressed size: 7076, name: word/theme/theme1.xml
188051         0x2D9E3     Zip archive data, at least v2.0 to extract, compressed size: 1118, uncompressed size: 3160, name: word/settings.xml
188016         0x2DE70     Zip archive data, at least v2.0 to extract, compressed size: 471, uncompressed size: 2670, name: word/webSettings.xml
191328         0x2EB60     Zip archive data, at least v2.0 to extract, compressed size: 576, uncompressed size: 1968, name: word/fontTable.xml
191849         0x2ED69     Zip archive data, at least v2.0 to extract, compressed size: 3267, uncompressed size: 31584, name: word/styles.xml
192473         0x2EFD9     Zip archive data, at least v2.0 to extract, compressed size: 386, uncompressed size: 747, name: docProps/core.xml
193170         0x2F292     Zip archive data, at least v2.0 to extract, compressed size: 479, uncompressed size: 992, name: docProps/app.xml
194731         0x2F8AB     End of Zip archive, footer length: 22

[lixsong@kali]-[~/Downloads/kichbantonghop]
└─$
```

Thực hiện tìm kiếm trong các file được trích xuất



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



Dùng tool decrypt online để giải mã thì thu được kết quả

The screenshot shows the dCode Brainfuck Language - Online Decoder interface. On the left, there's a search bar for tools and a results section for Brainfuck. The main area contains a Brainfuck Interpreter with code input, execution results, and memory dump. To the right, there's a summary of Brainfuck-related topics and similar pages.

Forensics05@UIT{Vietnam-win-Cambodia}

### Kịch bản 06. Thực hiện phân tích:

- Tài nguyên: tiengiang003.jpg
- Yêu cầu – Gợi ý: Tìm thông điệp (flag) được ẩn giấu. Thuật toán dùng tìm ra flag liên quan đến việc thay thế các kí tự trong chuỗi ban đầu thành chuỗi chỉ gồm 2 kí tự a và b.

*Đáp án:*

Tiếp tục thực hiện dùng stegbreak để tìm file ẩn

```
PS C:\Users\This MC\Downloads\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\This MC\Downloads\stegdetect04_session03> |
```

Tiếp theo dùng JPHS để trích xuất file ẩn ra.

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\This MC\Downloads\kichbantonghop\kichbantonghop  
Filename tiengiang003.jpg

Filesize 106 Kb Width 600 pixels Height 400 pixels

Approximate max capacity 16 Kb recommended limit 10 Kb

Hidden file

Directory C:\Users\This MC\Downloads\kichbantonghop\kichbantonghop  
Filename kb06-secret

Filesize 7 Kb

Saved jpeg file

Directory  
Filename  
Filesize Kb

This inner file already contains a hidden file

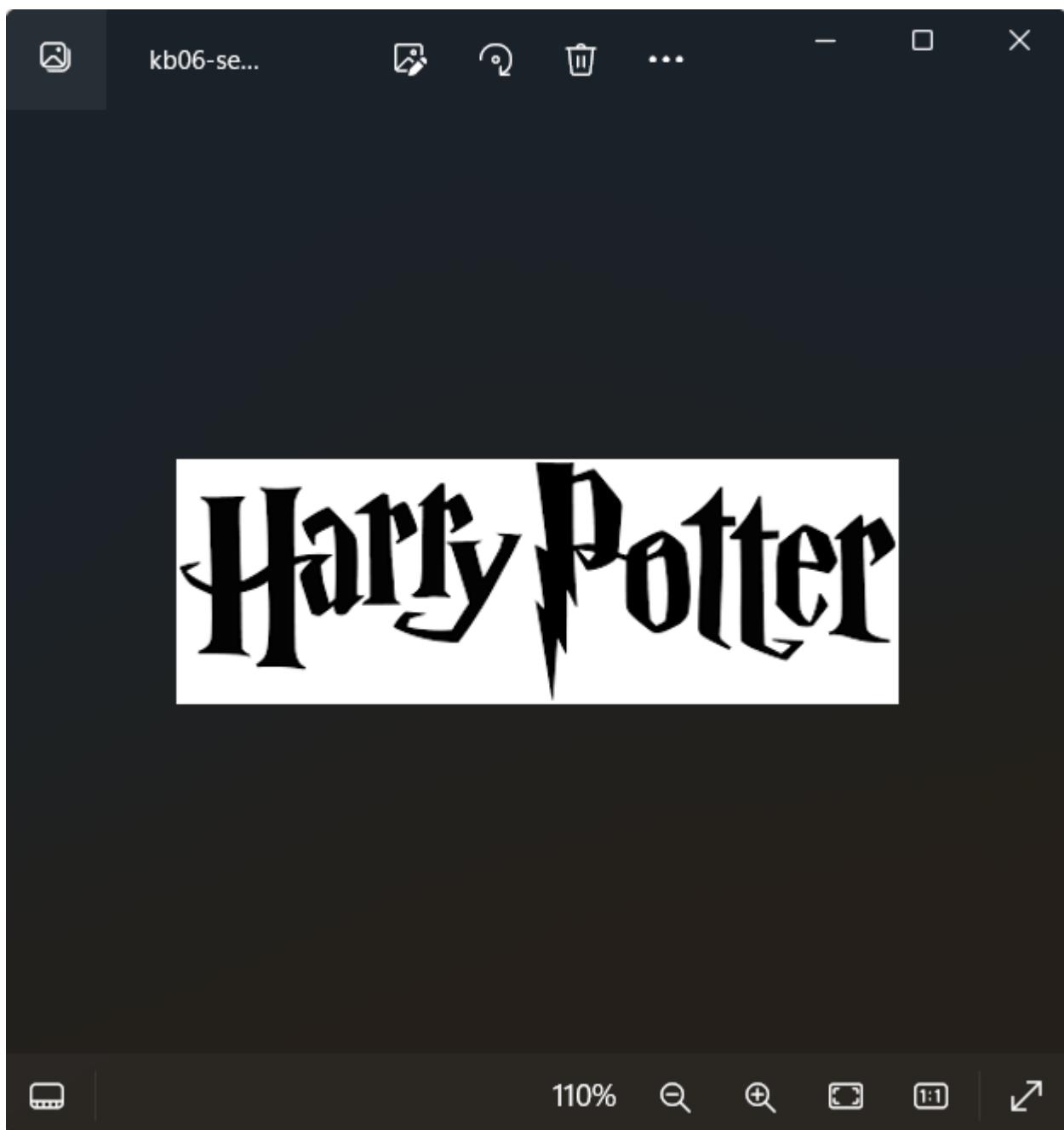
Chuyển file kb06-secret sang linux để tiếp tục phân tích

```
C:\Users\This MC\Downloads\kichbantonghop\kichbantonghop>scp "C:\Users\This MC\Downloads\kichbantonghop\kichbantonghop\kb06-secret.png" lixsong@192.168.110.130:/home/lixsong/Downloads/kichbantonghop
lixsong@192.168.110.130's password:
kb06-secret.png
C:\Users\This MC\Downloads\kichbantonghop\kichbantonghop>
```

Check thử xem file output là file gì thì thấy là file ảnh png.

```
[(lixsong㉿kali)-[~/Downloads/kichbantonghop]]$ file kb06-secret
kb06-secret: PNG image data, 385 x 131, 8-bit colormap, non-interlaced
<w:bookmark w:id="0" />
[(lixsong㉿kali)-[~/Downloads/kichbantonghop]]$ [REDACTED]
<w:color w:val="FFFFFF" w:themeColor="background1"/>
```

Rename và view thử ảnh.



Dùng strings để phân tích.

```

└─(lixsong㉿kali)-[~/Downloads/kichbantonghop]
$ strings kb06-secret.png
IHDR <++++++[>+>++++>++++++>++++++<<<-]>>,>+++++++
PLTE <+++++++.+++++,>-----,+++++++
AAA;;,</w:t>
ZZZnnn ``222"""))
$$$ ... 666 <w:bookmarkStart w:id="0" w:name="_GoBack"/>
IDATx <w:bookmarkEnd w:id="0"/>
<^sb <w:r w:rsidR="00415551" w:rsidRPr="001008F7">
Y~yxP <w:rPr>
&Dlu <w:color w:val="FFFFFF" w:themeColor="background1"/>
*Z c </w:rPr>
(*@` <w:t><-----</w:t>
M*JB </w:r>
E6)h <w:r w:rsidR="00415551" w:rsidRPr="001008F7">
P;/ed <w:rPr>
crft <w:color w:val="FFFFFF" w:themeColor="background1"/>
6>1h </w:rPr>
(kt0 <w:color w:val="FFFFFF" w:themeColor="background1"/>
FP>Q </w:rPr>
E@e ) <w:lastRenderedPageBreak/>
@&N <w:t>
[%EG .>+++++++.<+++++++.+++++.<.+++++++.+++++++.>-
7A?AX </w:t>
AL1Rh <w:r>
R)r4! <w:rPr>
%cra <w:color w:val="FFFFFF" w:themeColor="background1"/>
F"#Fw$ </w:rPr>
,q;vJ <w:color w:val="FFFFFF" w:themeColor="background1"/>
H`up </w:rPr>
JP#]@* <w:t>.</w:t>
QvRu </w:r>
kMWz <w:p w14:paraId="0D4FCD3D" w14:textId="77777777" w:rsidR="009970D6" w:rsidRP="009970D6" w:rsidRPr="009970D6" w:rsidRPr="009970D6">
Wp)EzM </w:p>

```

```

Home X Windows 10 x64 X Kali X My Computer X
File Actions Edit View Help
g>TgOf z~n"S .[7d TN3%d -<w:rPr>
`RN# <w:noProof/>
'*' { <w:color w:val="FFFFFF" w:themeColor="background1"/>
j5b </w:rPr>
M_<B ;9b0 ++++++[>+>++++>++++++>++++++><<<-]>>.>+++++++
0j2~ <<+++++++.+++++.>-----,+++++++.+++++++.-----
;6h8 <+++++++.>.-<
%ol. </w:t>
MS: </w:r>
wB?/ <w:bookmarkStart w:id="0" w:name="_GoBack"/>
Ol=C <w:bookmarkEnd w:id="0"/>
dE>V <w:r w:rsidR="00415551" w:rsidRPr="001008F7">
?j )~ <w:rPr>
~<md <w:color w:val="FFFFFF" w:themeColor="background1"/>
7jqX </w:rPr>
#-6x <w:t><-----</w:t>
Zcl,3 </w:r>
AWWE <w:r w:rsidR="00415551" w:rsidRPr="001008F7">
@kJHj <w:rPr>
uyDY$ <w:noProof/>
Gm#Lm <w:color w:val="FFFFFF" w:themeColor="background1"/>
i)7n </w:rPr>
;DD <w:lastRenderedPageBreak/>
^nG L <w:t>
P[ }*s <----->+++++++.<+++++++.+++++.<+++++++.+++++++.>-----
2~jv </w:t>
OCQDZ <----->+
- g{_- <w:r w:rsidR="00A012E5" w:rsidRPr="001008F7">
PlLp <w:rPr>
u} Ic <w:noProof/>
jg3U <w:color w:val="FFFFFF" w:themeColor="background1"/>
c)U> </w:rPr>
IEND <----->+
wherE ShOUld onE ReaLLy lOoK fOr tHis flag
</w:r>
( lixsong@kali )-[ ~/Downloads/kichbantonghop ]
$ <w:pPr>
use pointer inside or press Ctrl+G.

```

Thấy có dòng là wherE ShOUld onE ReaLLy lOoK fOr tHis flag.

Ta có hint của đề bài là thuật toán dùng tìm ra flag liên quan đến việc thay thế các kí tự trong chuỗi ban đầu thành chuỗi chỉ gồm 2 kí tự a và b.

Thử search trên mạng xem đó là thuật toán gì thì thấy có vẻ đó là baconian cipher

Khoảng 3.530.000 kết quả (0,32 giây)

The Baconian cipher is a substitution cipher in which each letter is replaced by a sequence of 5 characters. In the original cipher, these were sequences of 'A's and 'B's e.g. the letter 'D' was replaced by 'aaabb', the letter 'O' was replaced by 'abbaa' etc. Each letter is assigned to a string of five binary digits. 3 tháng 5, 2023

**GeeksforGeeks** https://www.geeksforgeeks.org/baconian-cipher/

**Baconian Cipher - GeeksforGeeks**

Ở đây ta dễ nhận ra thuộc tính hoa thường trong đoạn “wherE ShOUld onE ReaLly lOoK fOr tHis flag” nay ta tìm được.

Ta thử set chữ thường là A và chữ hoa là B thì thông điệp của ta sẽ trở thành.

AAAAB BABBA AAB BAABA ABAB ABA ABAA AAAA

Ta đã có đoạn bacon cipher và giờ dùng tool decrypt online để giải mã

Kết quả thu được: BYDELTA.

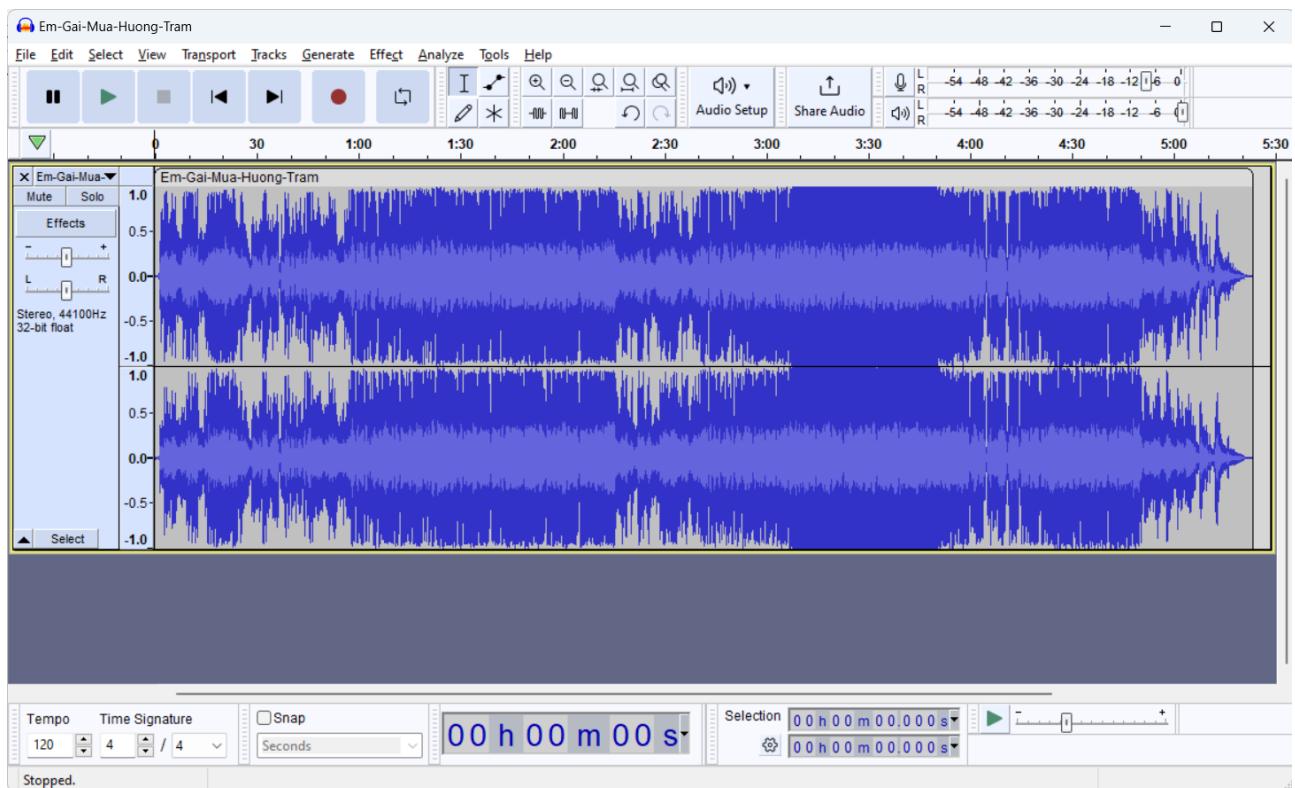
### Kịch bản 07. Thực hiện phân tích, tìm thông tin ẩn giấu:

- Tài nguyên: kb07-res (Tìm thông tin ẩn giấu trong Em-Gai-Mua-Huong-Tram.mp3, capture-the-flag.png)

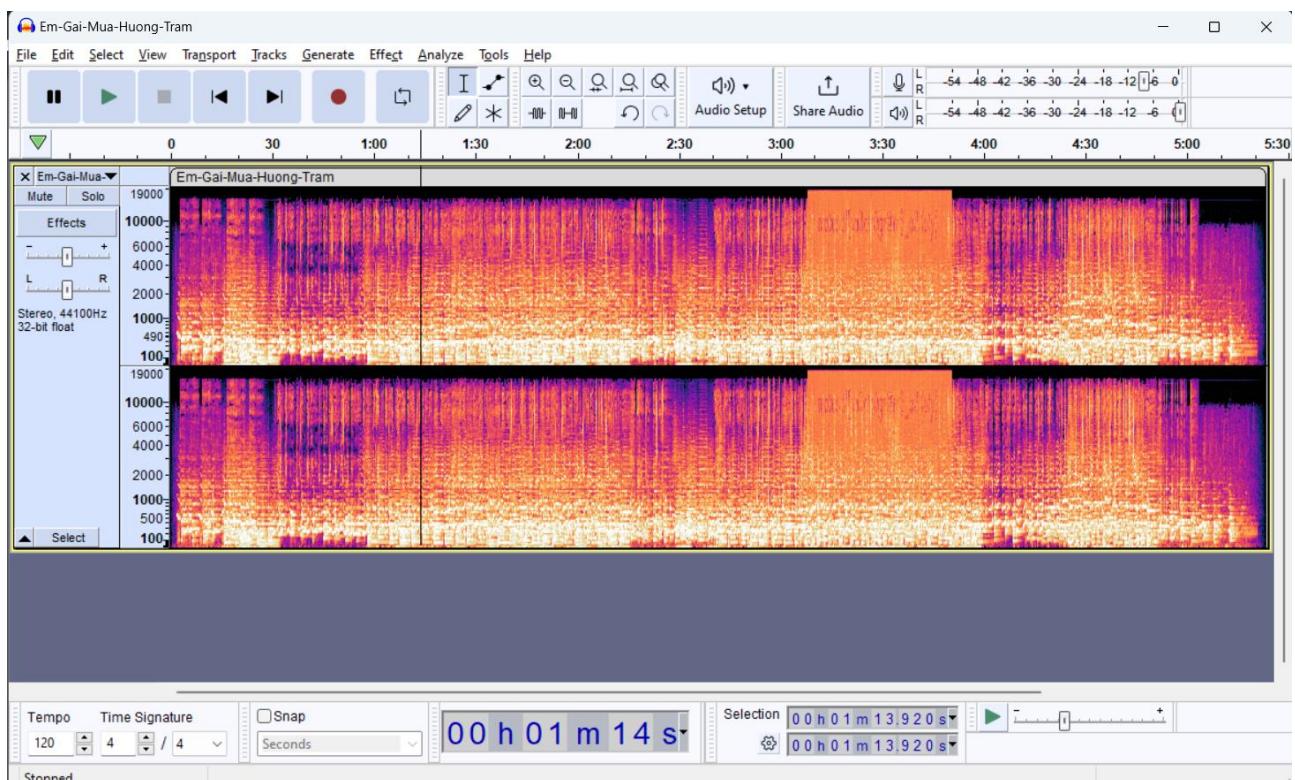
Dáp án:

Ta thấy đây là challenge về 1 file âm thanh, thử search tìm kiếm trên mạng thì thấy gợi ý là sử dụng Audacity để phân tích file audio trong lĩnh vực Forensics.

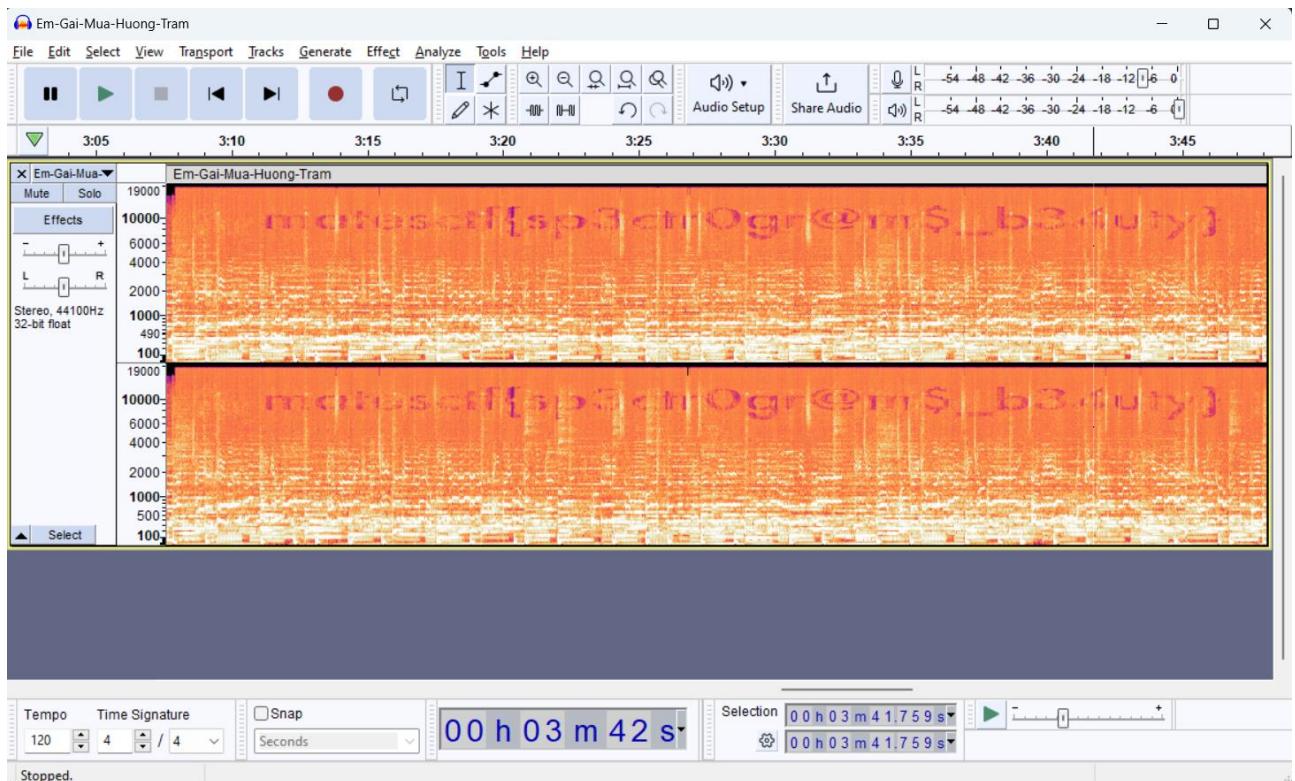
Mở file mp4 với audacity.



Chuyển sang dạng view ở spectrum thì thấy có dòng chữ



Thủ phòng to ra thì ta được flag là



matesctf{sp3ctr0gr@m\$.\_b34uty}

### Kịch bản 08. Thực hiện phân tích, tìm thông tin ẩn giấu:

- Tài nguyên: LoveLetter.txt
- Yêu cầu - Gợi ý: Có gì đó đáng ngờ trong bức thư tình mà bạn đang đọc. Nhân viên điều tra cũng nghĩ rằng bức thư tình này chứa một thông điệp bí mật nào đó. Hãy tìm thông điệp được ẩn giấu (flag). Flag có dạng “FLAG-\*”
- Link CTF: <https://ringzer0ctf.com/challenges/215>

Thử đọc file LoveLetter.txt thì thấy có vài ký tự lạ

```
(lixsong㉿kali) [~/Downloads/kichbantonghop]
└─$ cat LoveLetter.txt
I went to the park today, saw a lot of fish. Fish are cool, but they aren't my favorite animal!! The monkey is a good animal, so is the Blue-Tounged Skink, but I rarely get to see those at the park! All of this makes me sad, but just encourages me to travel more. I'll start researching where in the world I can see these animals in their natural habitat and start visiting them! Sounds like a good time, I'll update here with my plans. It might be a long while though, because I get so busy with work and never have time to do the actual things I want to do! Oh to be me, and to never go out for working. Well, at least the people at my company are nice! Working there is fun, and I do get to do some things with friends through work, but I still wish I could make friends with those monkeys and skinks! Well, I guess it's official: I shall travel! Not just the rant from this blog post, but an actual thing I will do. Well, I'll show you guys all the pictures anyways. Did you know that a monkey is either going to be a Cercopithecoid or a Platyrhyn? It's true! and there are over 1200 different species of monkey that are known. Sure is a lot of them! But skinks are also cool, there are over 264 species of skink! Skins are lizards, but they look more like snakes with legs to me! But I guess since skinks have a tail and snakes don't ... Oh I don't know! I love animals of all kinds, can't even pick favorites. I'm sorry fish, you guys are good animals too. ha ha, alright, I'll stop my ranting.

--End journal entry
└─$
```

Thử xxd xem thử hex

```
(lixsong㉿kali)-[~/Downloads/kichbantonghop]
$ xxd LoveLetter.txt | head
00000000: 4920 7765 6e74 a074 6f20 7468 6520 7061 I went.to the pa
00000010: 726b 2074 6f64 6179 2ca0 7361 77a0 6120 rk today,.saw.a
00000020: 6c6f 7420 6f66 a066 6973 682e 2046 6973 lot.of.fish. Fis
00000030: 6820 6172 65a0 636f 6f6c 2ca0 6275 7420 h are.cool,.but
00000040: 7468 6579 2061 7265 6e27 7420 6d79 a066 they aren't my.f
00000050: 6176 6f72 6974 6520 616e 696d 616c 2121 avorite animal!!
00000060: 2054 6865 206d 6f6e 6b65 7920 6973 2061 The monkey is a
00000070: a067 6f6f 6420 616e 696d 616c 2ca0 736f .good animal,.so
00000080: 2069 7320 7468 6520 426c 7565 2d54 6f75 is the Blue-Tou
00000090: 6e67 6564 a053 6b69 6e6b 2ca0 6275 74a0 nged.Skink,.but.

(lixsong㉿kali)-[~/Downloads/kichbantonghop]
$
```

Ở đây ta thấy theo ascii thì khoảng trắng có kí tự là 0x20 nhưng mà ở đây cũng có một vài kí tự 0xA0.

Thử app dụng theo câu bacon cipher.

Thử gán giá trị cho 0x20 là 0 còn 0xA0 là 1 thì ta có chuỗi sau:

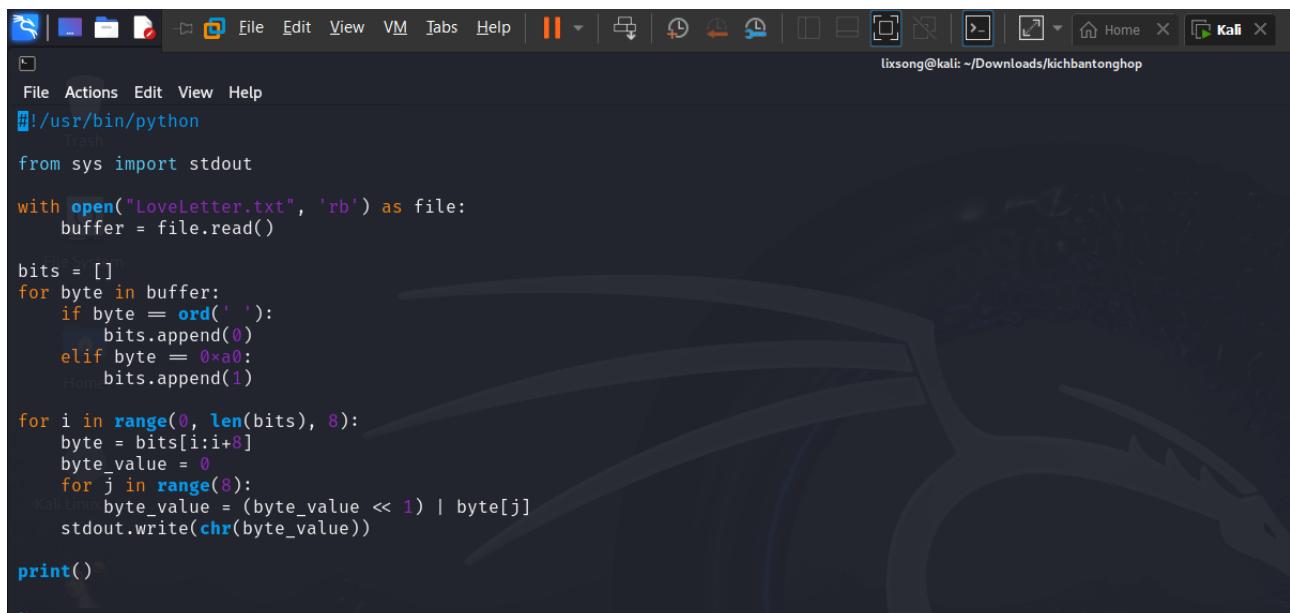
```
010001100100110001000001010001110010110100110011011001100110011000
11011100110000011001100110001101100110001100000011011100110000001100000011
000000111001001101001101100011000101100110001101010011001000110111001101
10011001100110010100111001001110000110011001100111001011000110011001100110110
```

Ta thấy có 296 bit không chia hết cho 5 mà chia hết cho 8 và có đủ bit cho "FLAG-" cộng với 32 ký tự. Vì vậy chúng ta có thể chia bit thành nhóm 8 bit và tra cứu các ký tự ASCII của chúng.

01000110	01001100	01000001	01000111	00101101	00110011	01100010	00110110
F	L	A	G	-	3	b	6
01100010	00110111	00110000	01100110	01100011	01100110	00110000	00110111
f	7	0	f	c	f	0	7
00110000	00110000	00110000	00111001	00110101	00110110	00110001	01100110
0	0	0	9	5	6	1	f
00110101	00110010	00110111	00110110	01100110	01100101	00111001	00111000
5	2	7	6	f	e	9	8
01100010	01100011	00111001	01100011	00110110			
f	c	9	c	6			

Vậy ta có flag là FLAG-3b6f70fcf070009561f5276fe98fc9c6

Ta viết 1 đoạn script để tìm FLAG



```

File Actions Edit View Help
#!/usr/bin/python
from sys import stdout

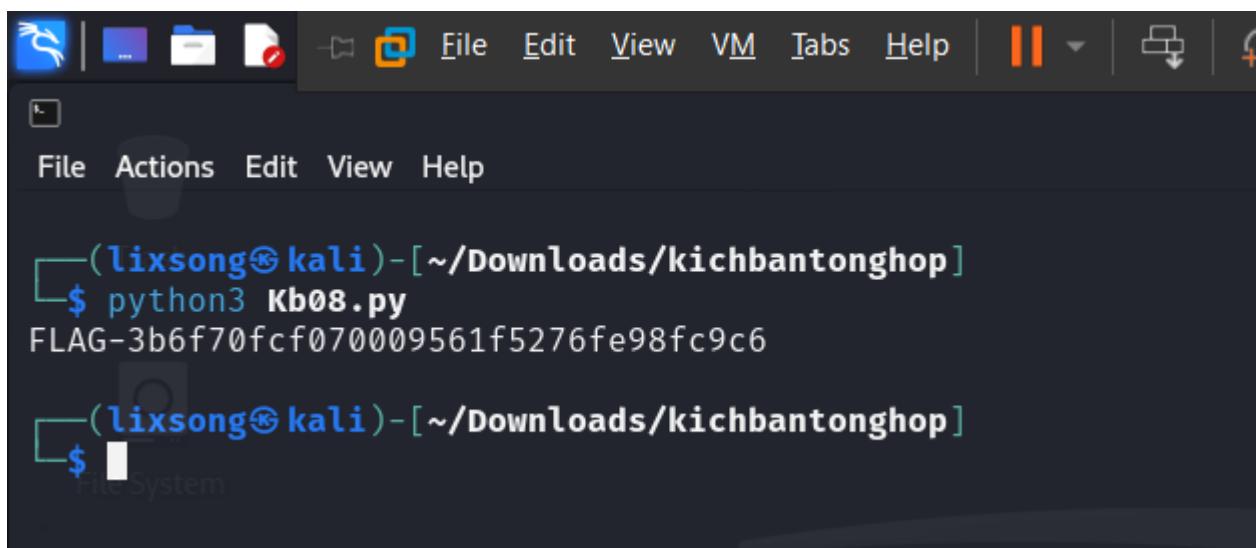
with open("LoveLetter.txt", 'rb') as file:
    buffer = file.read()

bits = []
for byte in buffer:
    if byte == ord(' '):
        bits.append(0)
    elif byte == 0xa0:
        bits.append(1)

for i in range(0, len(bits), 8):
    byte = bits[i:i+8]
    byte_value = 0
    for j in range(8):
        Kali Linux byte_value = (byte_value << 1) | byte[j]
        stdout.write(chr(byte_value))

print()
~
```

Kết quả thu được



```

File Actions Edit View Help

└─(lixsong㉿kali)-[~/Downloads/kichbantonghop]
└─$ python3 Kb08.py
FLAG-3b6f70fcf070009561f5276fe98fc9c6

└─(lixsong㉿kali)-[~/Downloads/kichbantonghop]
└─$ ┌── [File System]
```

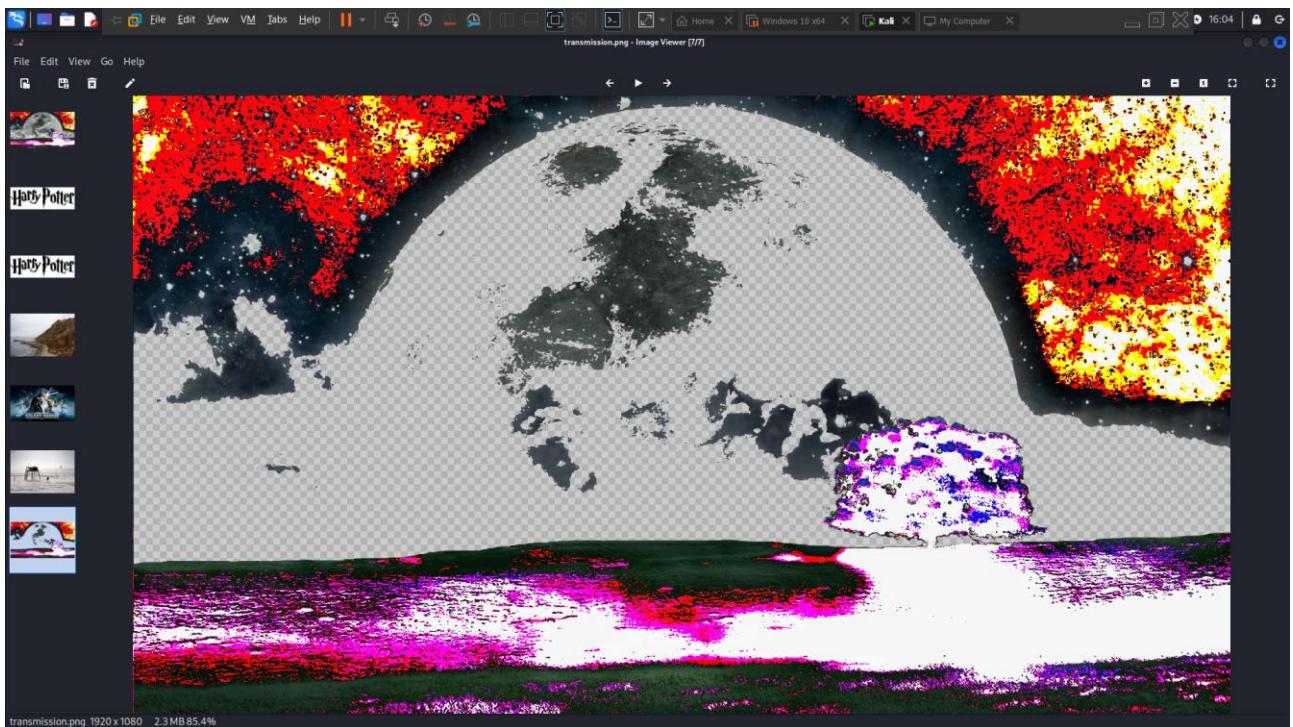
FLAG-3b6f70fcf070009561f5276fe98fc9c6

### Kịch bản 09. Thực hiện phân tích, tìm thông tin ẩn giấu:

- Tài nguyên: transmission.png
- Yêu cầu - Gợi ý: Tìm thông điệp được ẩn giấu bằng các công cụ đã học trong buổi này.

*Đáp án:*

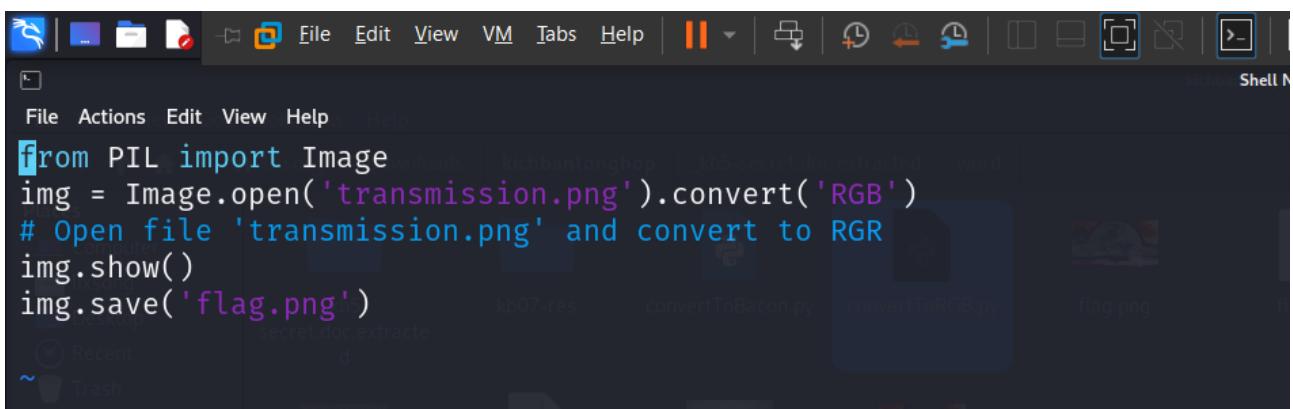
Mở file ảnh bằng và quan sát.



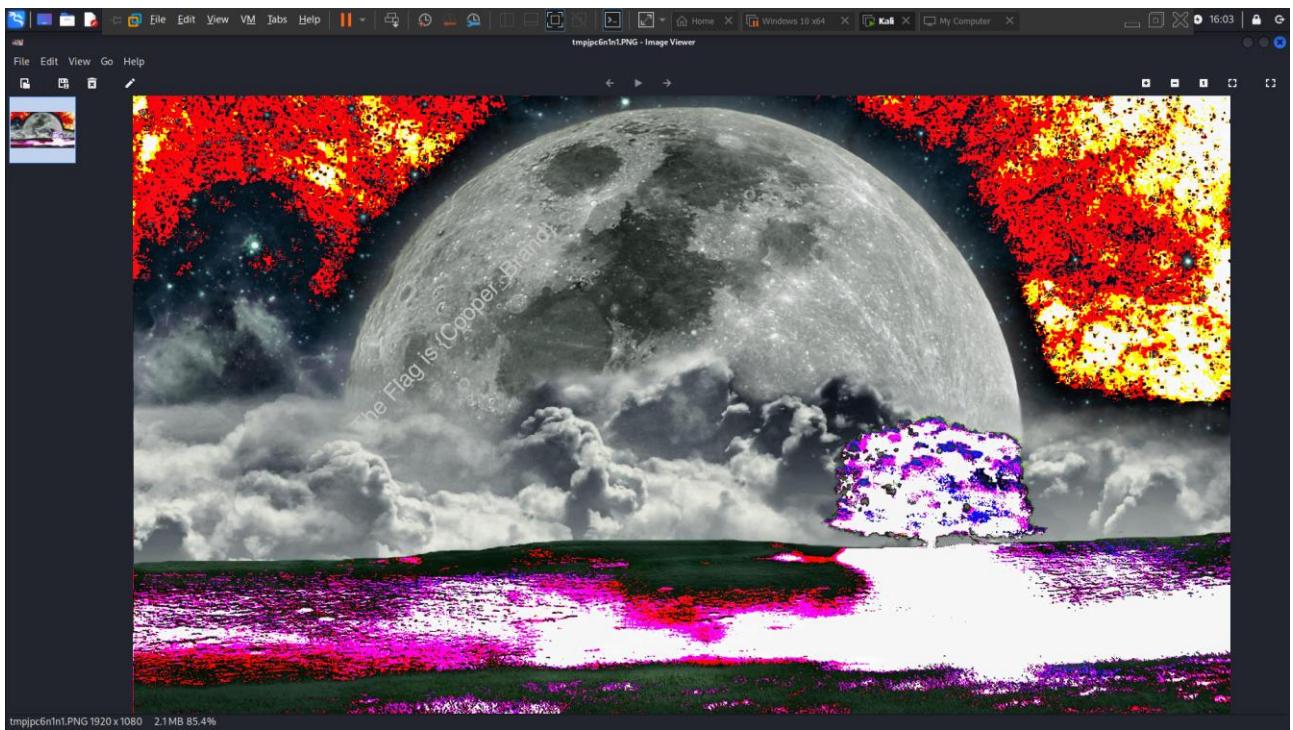
Ta thấy một phần của image bị transparent.

Ta dùng thư viện pillow xử lý ảnh và convert các điểm màu transparency thành RGB.

Ta code một đoạn code ngắn để xử lý việc này



## Kết quả thu được

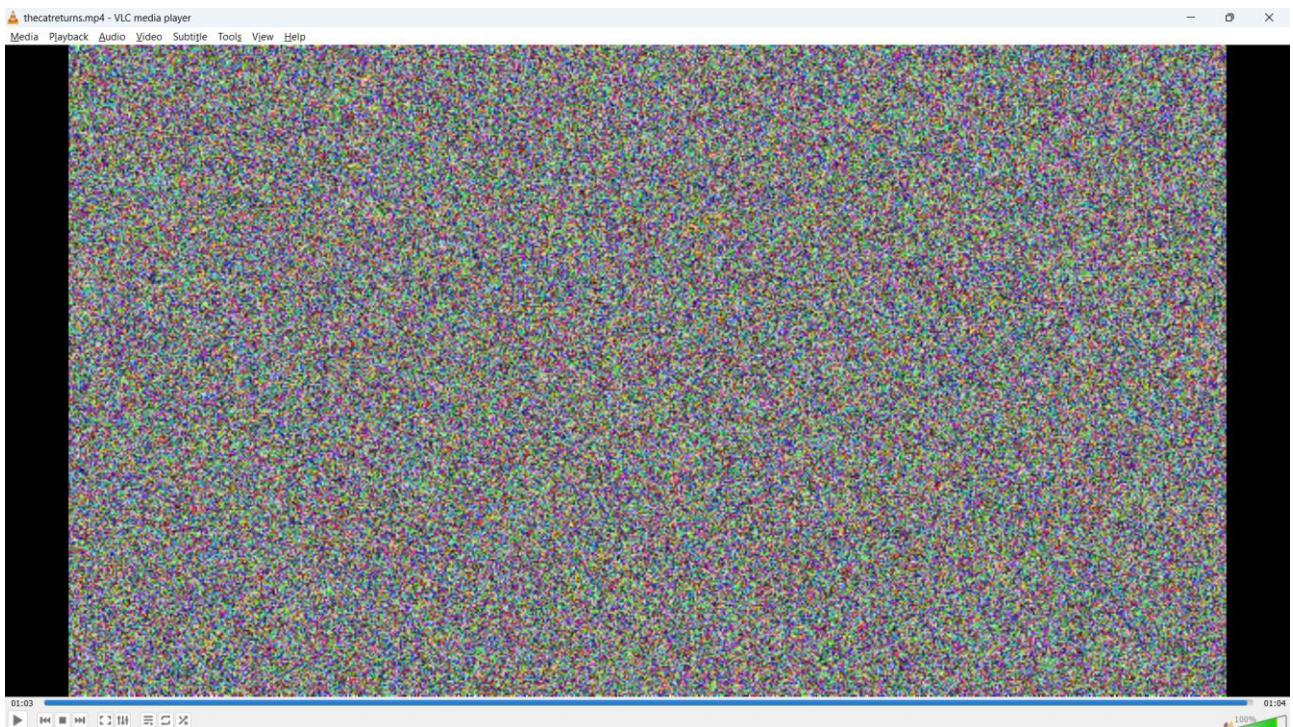


Flag: {Cooper\_Brand}

#### Kịch bản 10. Thực hiện phân tích, tìm thông tin ẩn giấu:

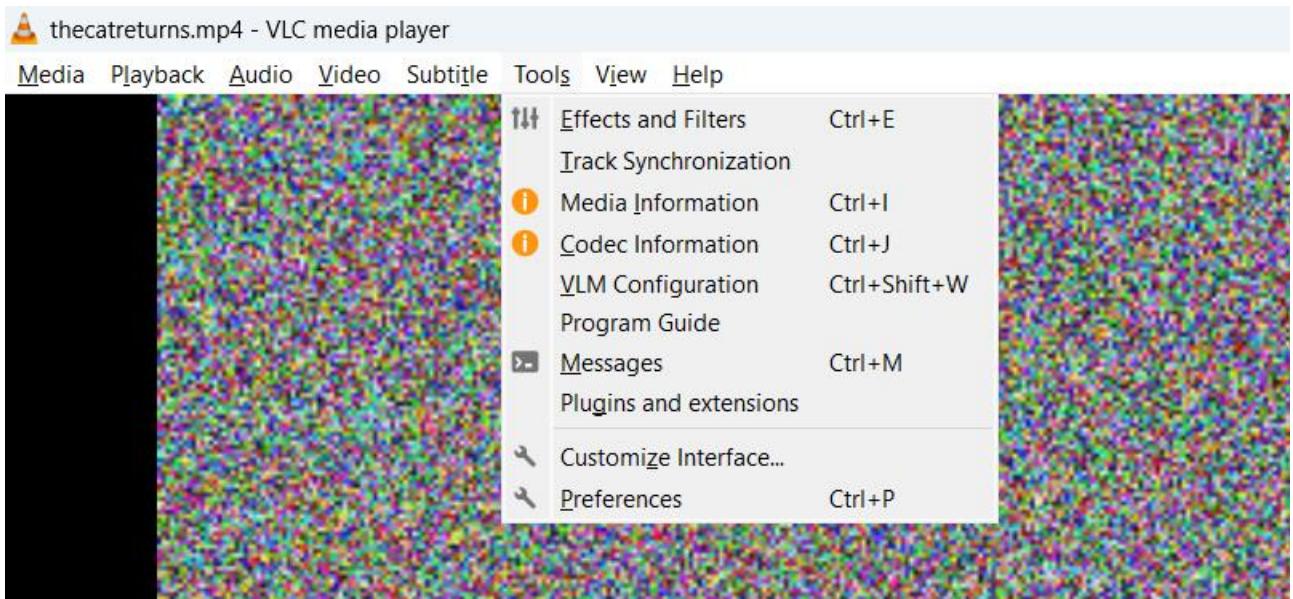
- Tài nguyên: thecatreturns.mp4
- Yêu cầu – Gợi ý: Tìm sự khác biệt giữa các khung hình (frame) trong đoạn phim đã cho. Chuyển nội dung đoạn phim thành các khung hình để phân tích. Công cụ ffmpeg, ImageJ.

Đáp án:



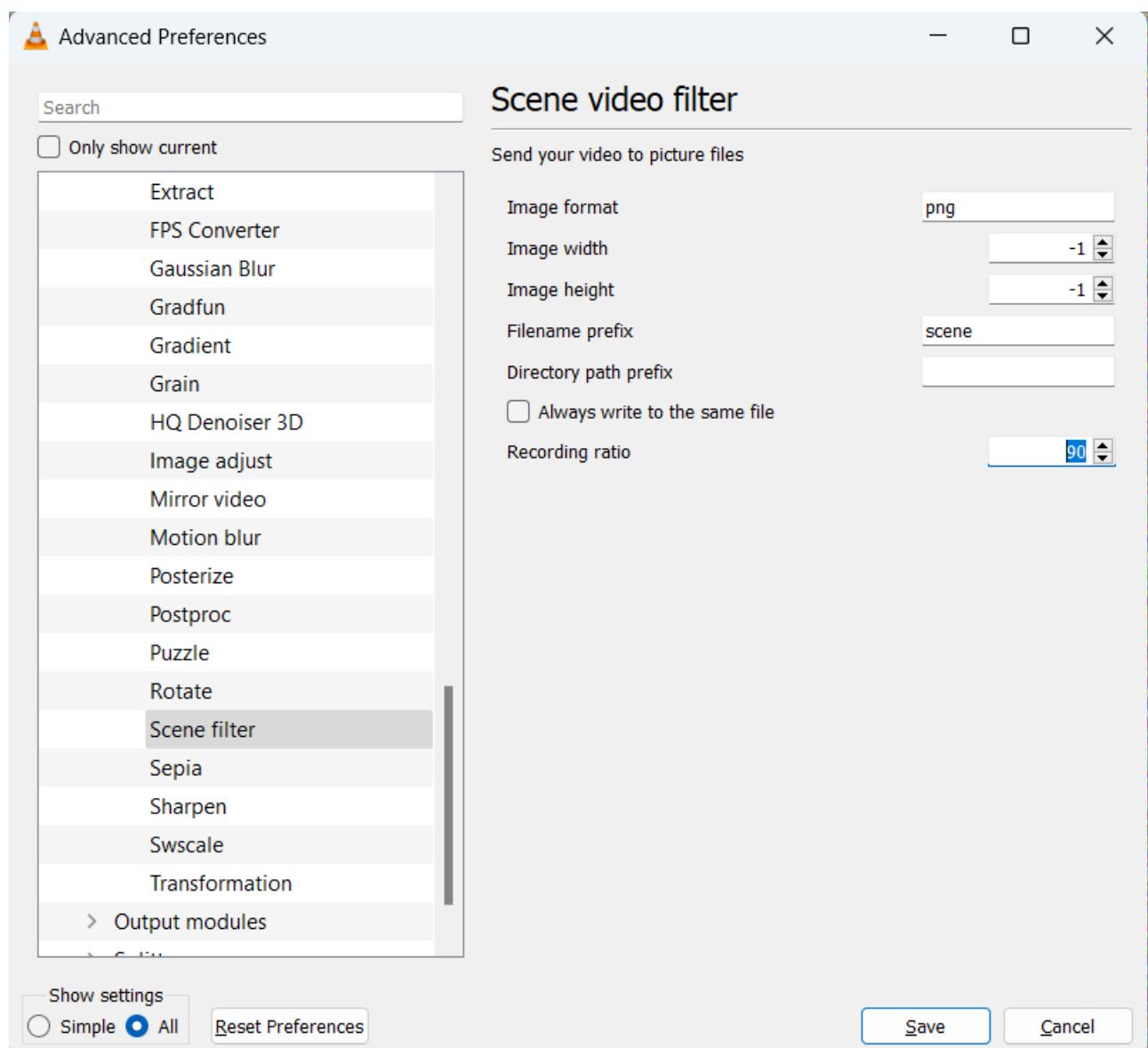
Ta có thể dễ dàng nhận ra rằng video này bị làm nhiễu và cũng có thể nhận thấy một vài chuyển động nào đó trong video nên ý tưởng ở đây là chia video thành các frame dưới dạng hình ảnh.

Công cụ VLC có thể giúp ta thực hiện công việc trên. Đầu tiên ta mở Preference lên như trong hình.

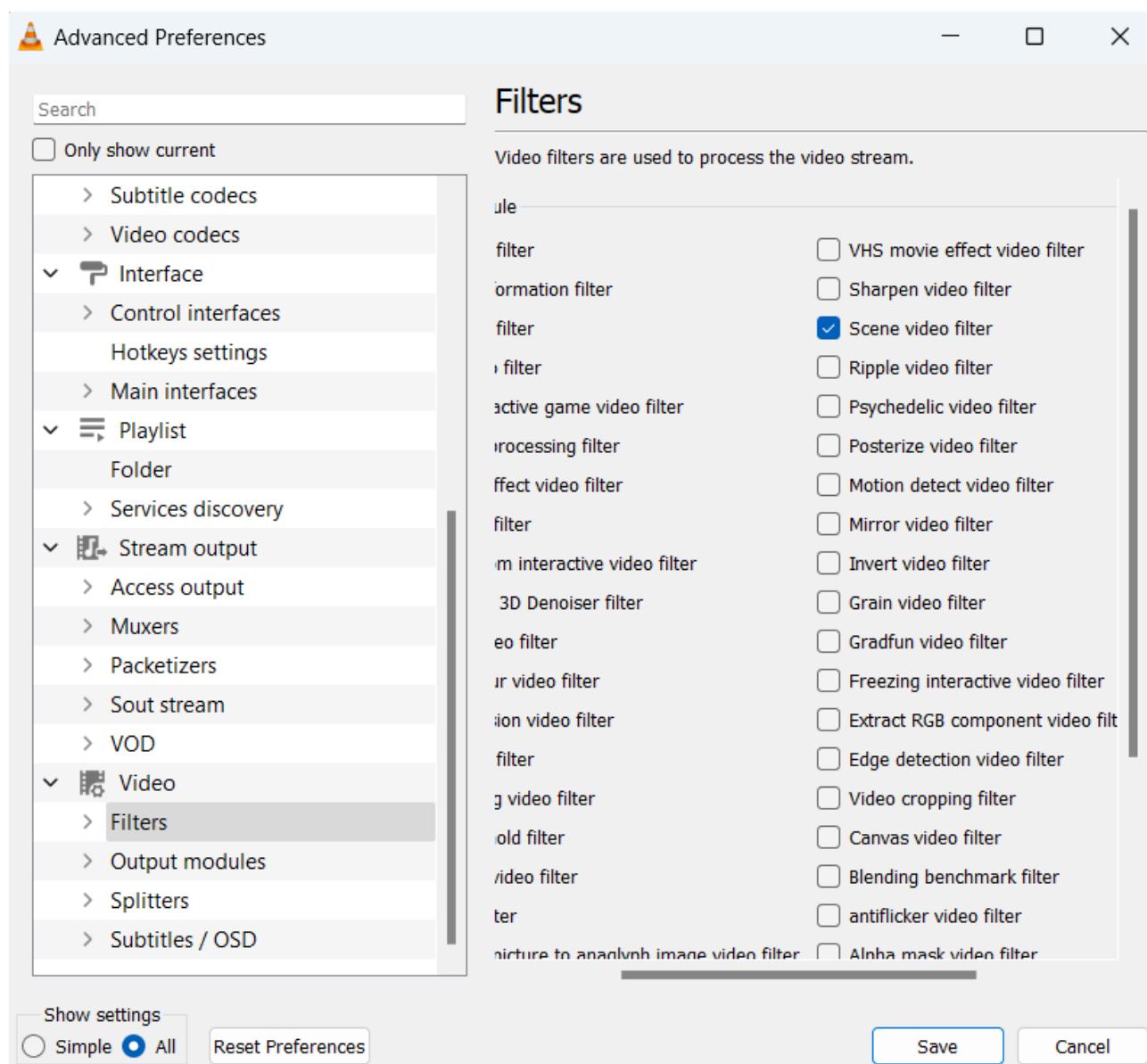


Tiếp theo chọn All ở Show Setting -> Video -> Filters -> Scene Filter

Tại tab Scene video filter ta điền các thông tin như hình, ở chỗ Recording ratio ta để là 90 -> cứ 3s ta lưu 1 ảnh (do tốc độ khung hình của video là 30fps)



Nhấn save và tắt VLC đi và mở lại video.



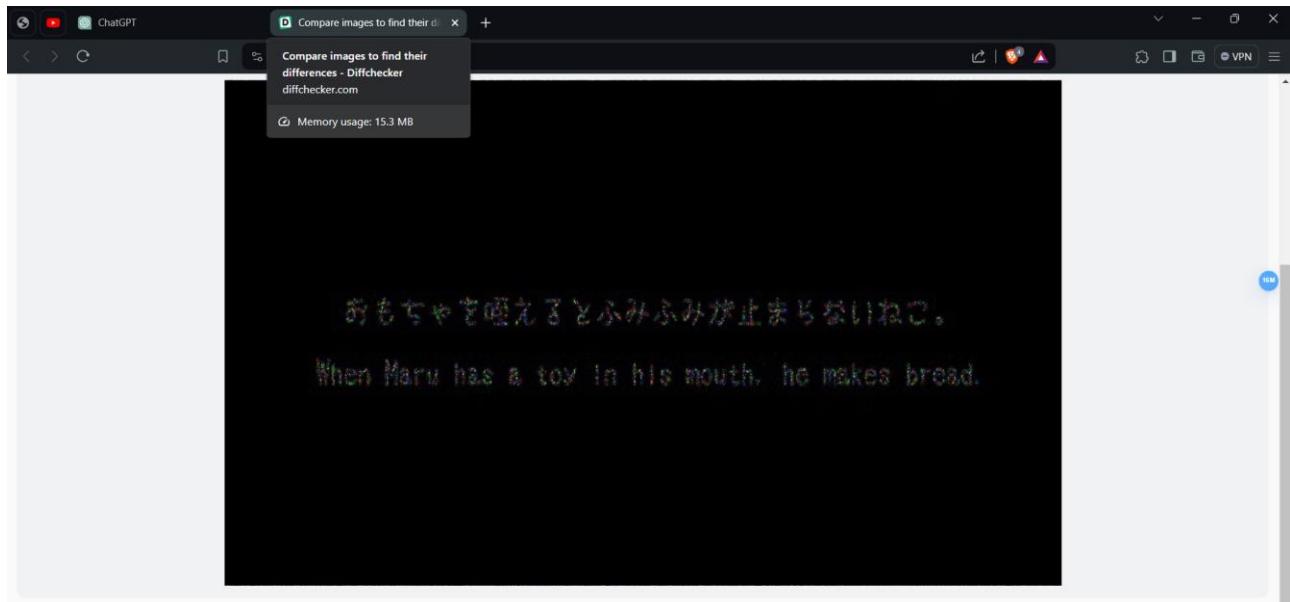
Ta vào tiếp preferences và vào filter để bật scene video filter lên.

Sau mỗi 3s video sẽ generate ra một ảnh theo như ta cấu hình, để video (1:04 -> 64s) chạy hết ta sẽ có  $64/3 = 21.(3) = 22$  ảnh, như bên dưới:

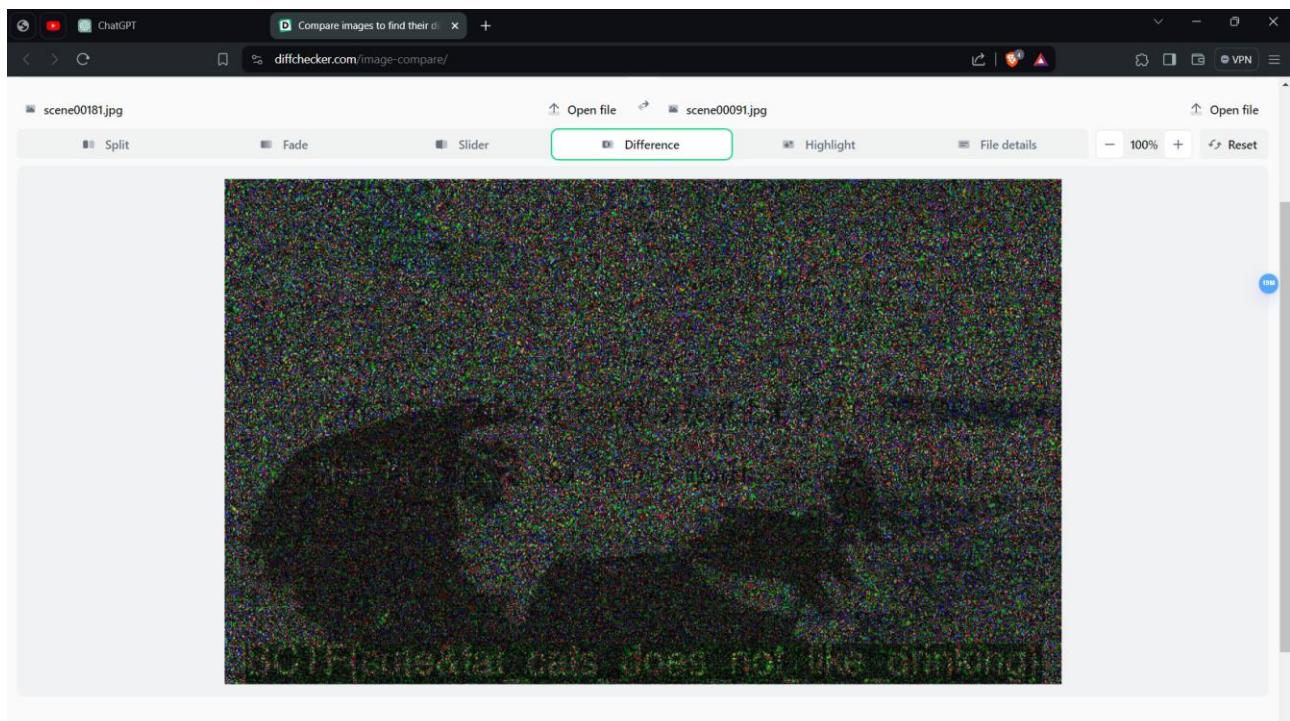


Vậy là ta đã có các frame ảnh. Theo đề gợi ý thì ta cần so sánh sự khác nhau giữa chúng. Nên là ta sẽ dùng tool <https://www.diffchecker.com/image-compare/> để show nội dung khác nhau giữa 2 ảnh và làm rõ nó lên

Ta so sánh từng ảnh với nhau để thấy sự khác biệt  
ảnh scene00001.jpg với scene00091.jpg



Tiếp tục so sánh scene00091.jpg với scene00181.jpg .



Ta thấy có flag: BCTF{cute&fat\_cats\_does\_not\_like\_drinking}