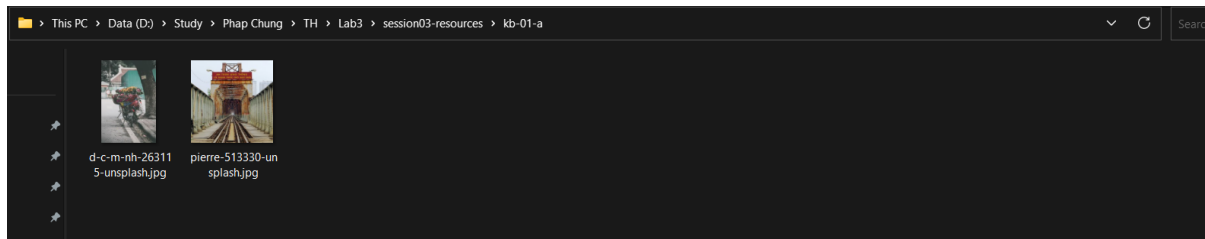
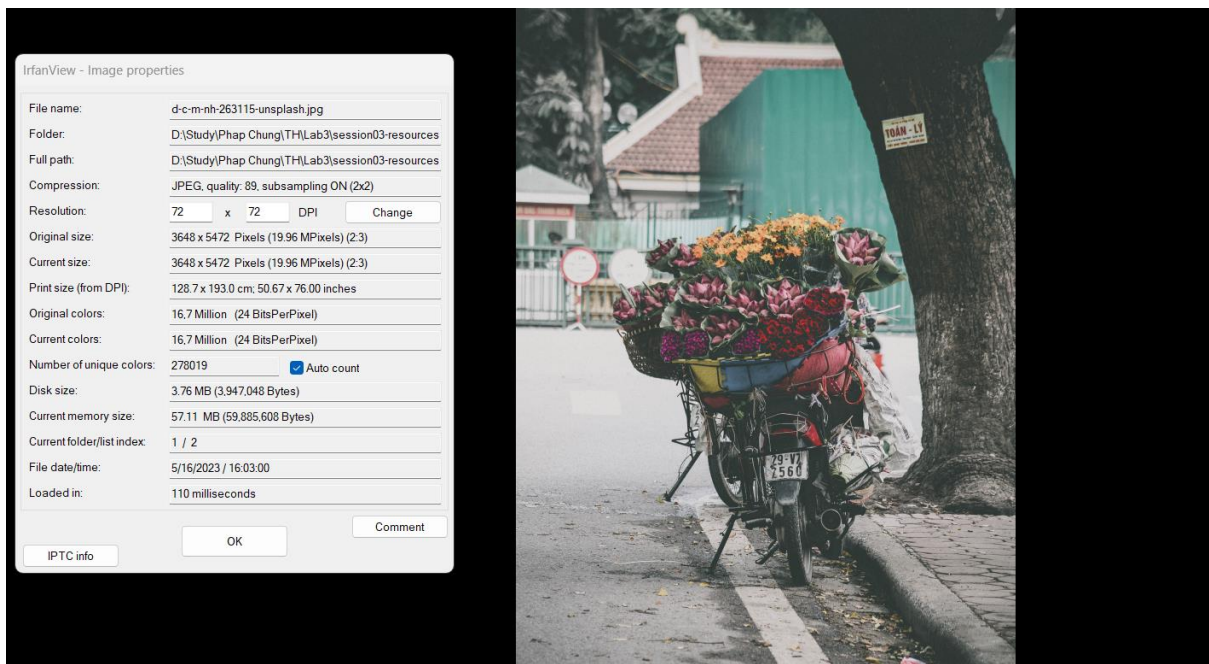


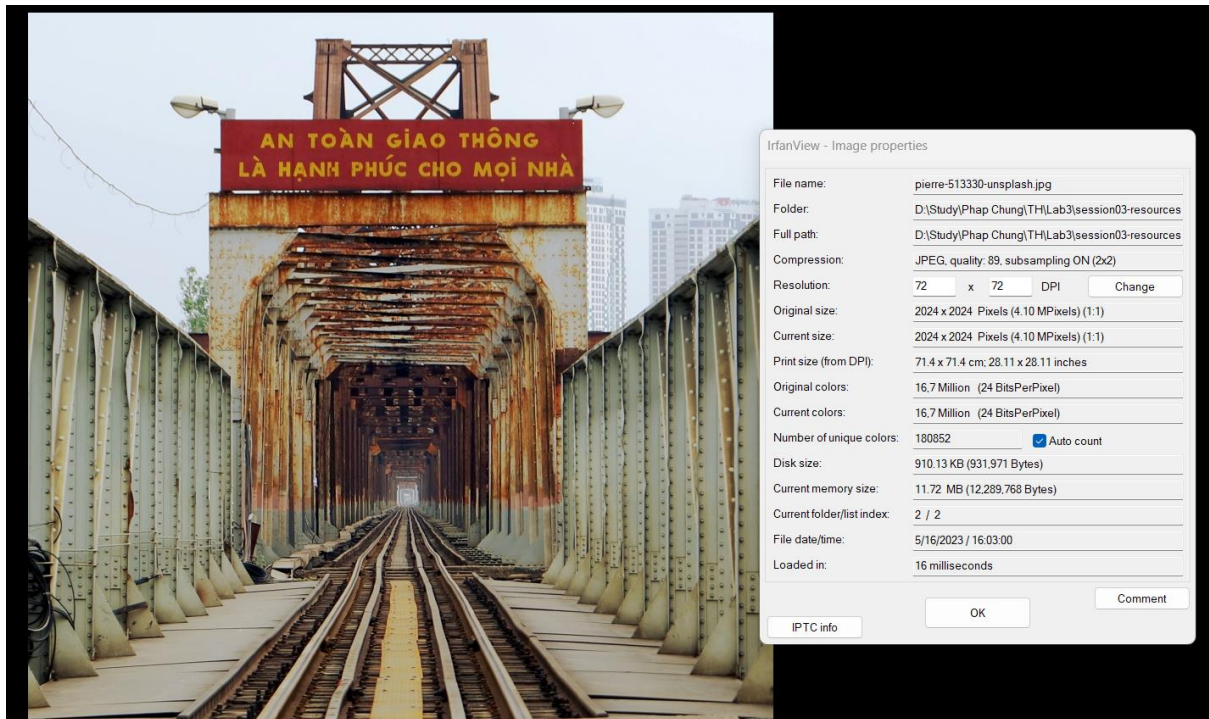
Kịch bản 01-a



- Ta tiến hành sử dụng công cụ infraview để phân tích 2 hình ảnh có trong thư mục kb-01-a

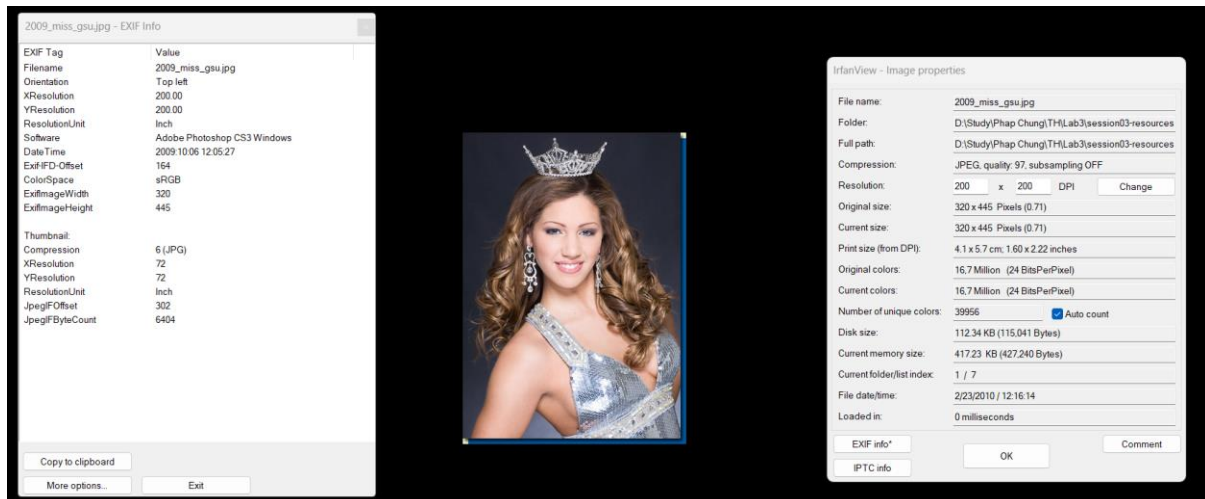


- Ảnh này cho ta các thông tin, ảnh này không có thông tin EXIF để trích xuất



- Tương tự với ảnh pierre-513330-unsplash.jpg cũng không có thông tin EXIF để có thể trích xuất

Kịch bản 01-b



- Đây là thông tin ảnh trước khi ta giấu thông tin

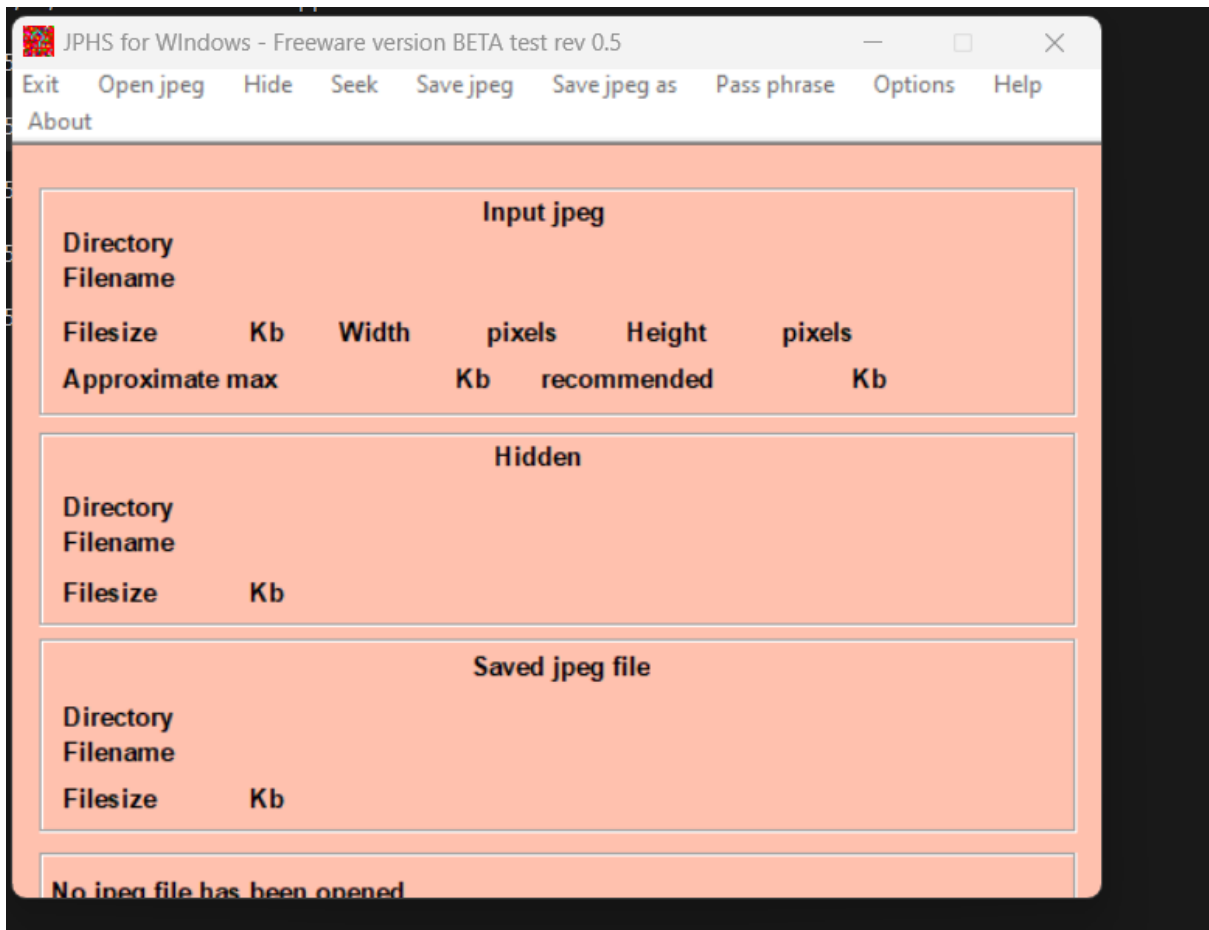
File Explorer path: This PC > Data (D:) > Study > Phap Chung > TH > Lab3 > session03-resources > jphs05_session03

	Name	Date modified	Type	Size
	jphide.exe	5/16/2023 4:03 PM	Application	158 KB
✦	jphs	5/16/2023 4:03 PM	Internet Shortcut	1 KB
✦	Jphswin.exe	5/16/2023 4:03 PM	Application	110 KB
✦	jpseek.exe	5/16/2023 4:03 PM	Application	125 KB
✦	PTAC.pdf	5/16/2023 4:03 PM	Microsoft Edge PD...	10 KB
✦	Readme-JPHS.txt	5/16/2023 4:03 PM	Tài liệu văn bản	1 KB

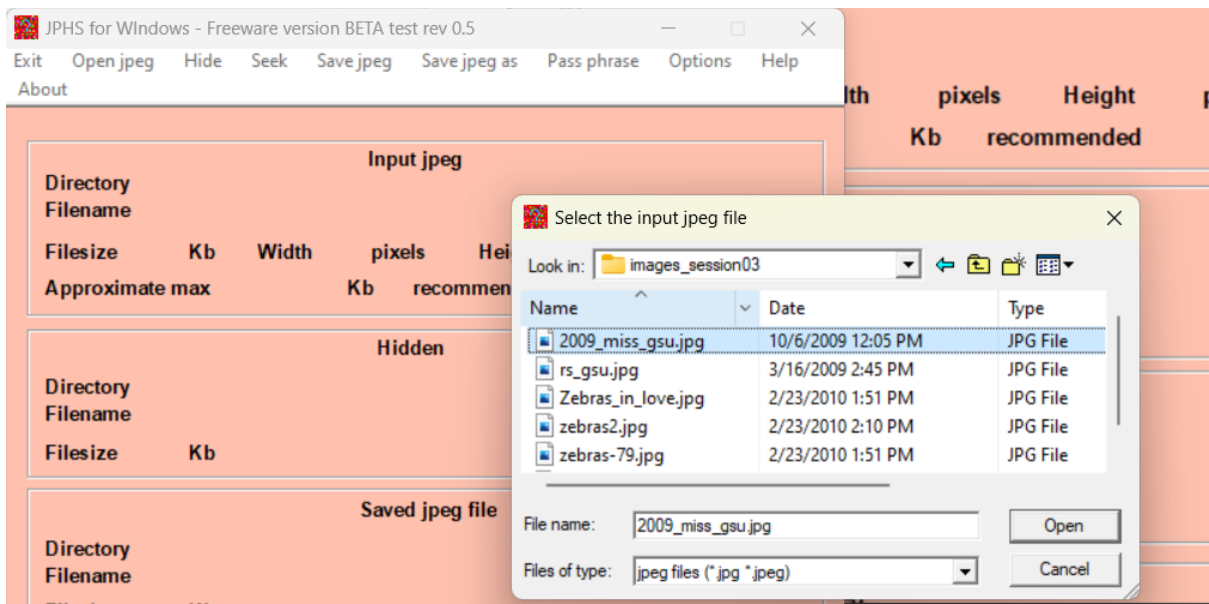
- Dữ liệu cần giấu nằm trong file nén jphs05_session03.zip

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
	Dave 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 Olney	MOlney	MOlney@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
	Pati Beltram	PBeltram	PBeltram@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
	Steve Savoy	SSavoy	SSavoy@peoriaud.k12.az.us	your current password	pusd11user name
	Teri Nevarez	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 Naish	VNaish	VNaish@peoriaud.k12.az.us	your current password	pusd11user name
	Bill Copeland	Bill.Copeland	GSMOM@COX.NET	your current password	pusd11user name
	Tammara Edgin	Tammara.Edgin	tammarae@microsoft.com	BoNeT45	pusd11extBill.Copeland
	Diane Douglas	Diane.Douglas	dmdouglas@cox.net	TeCom23	pusd11extTammara.Edgin
	Mary Crespino	Mary.Crespino	crespy@cox.net	DoNet21	pusd11extDiane.Douglas

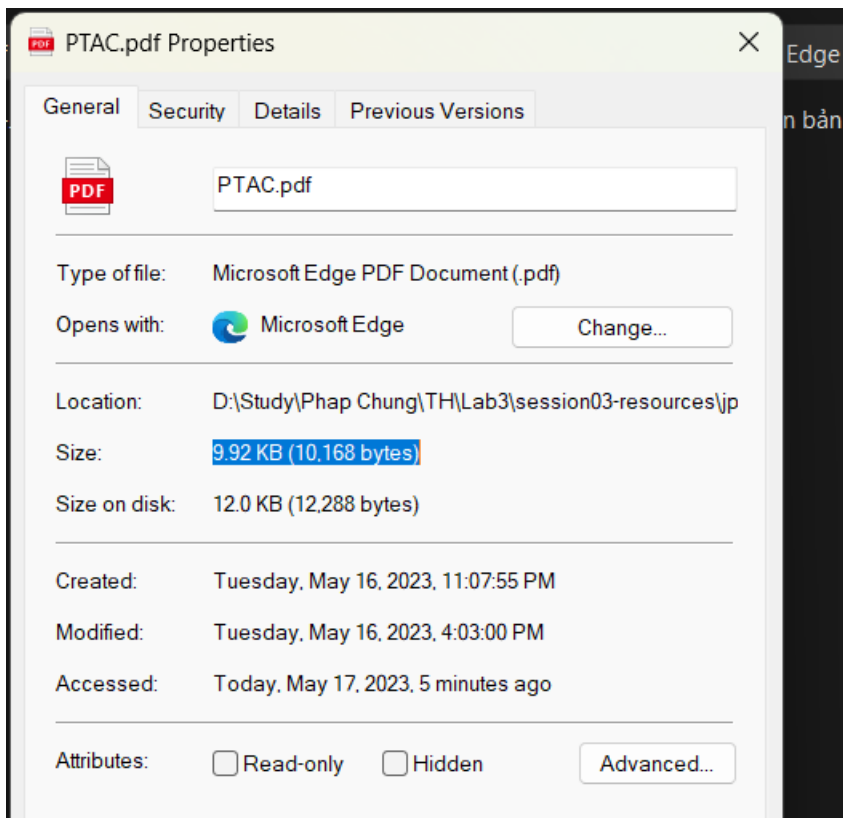
- Đây là thông tin trong file pdf ta cần giấu



- Chạy file Jphswin.exe



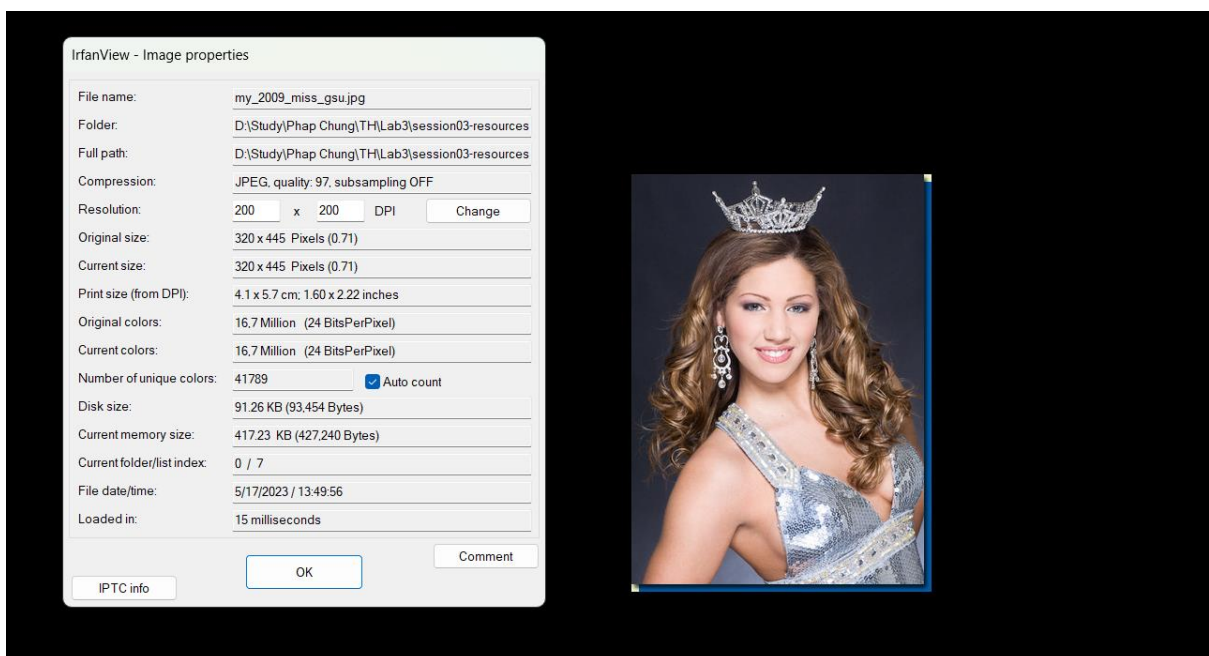
- Chọn open jpeg để chọn ảnh ta muốn giấu



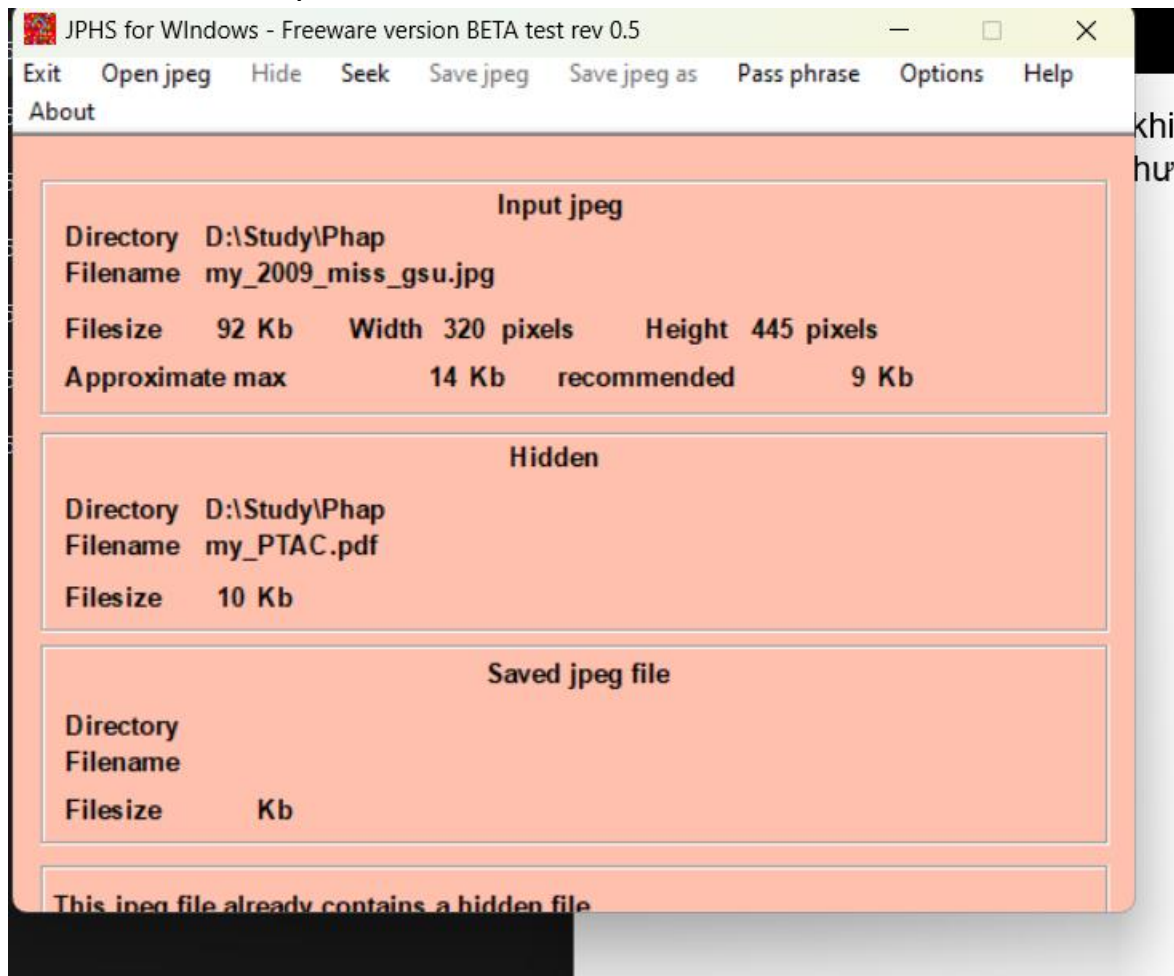
- Ta thấy thông tin ta muốn giấu nhỏ hơn kích thước recommend thì có thể giấu được



- Chọn thêm dữ liệu muốn giấu “hide” và đặt password là “UIT”



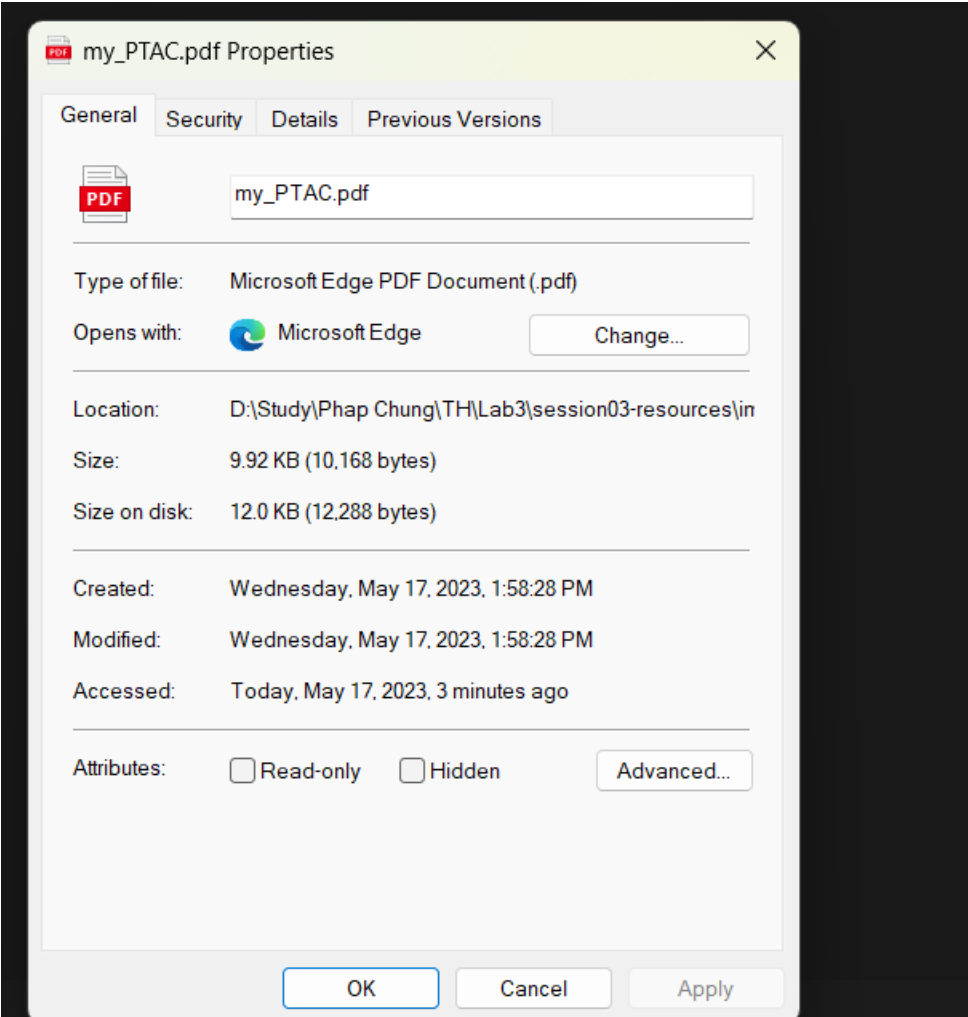
- Đây là thông tin ảnh sau khi ta đã giấu
- Chất lượng ảnh thì vẫn như cũ còn kích thước disk size thì đã giảm dù ta chèn 1 file pdf thêm vào



- Sử dụng chức năng seek để lấy lại file và đặt tên là my_PTAC.pdf

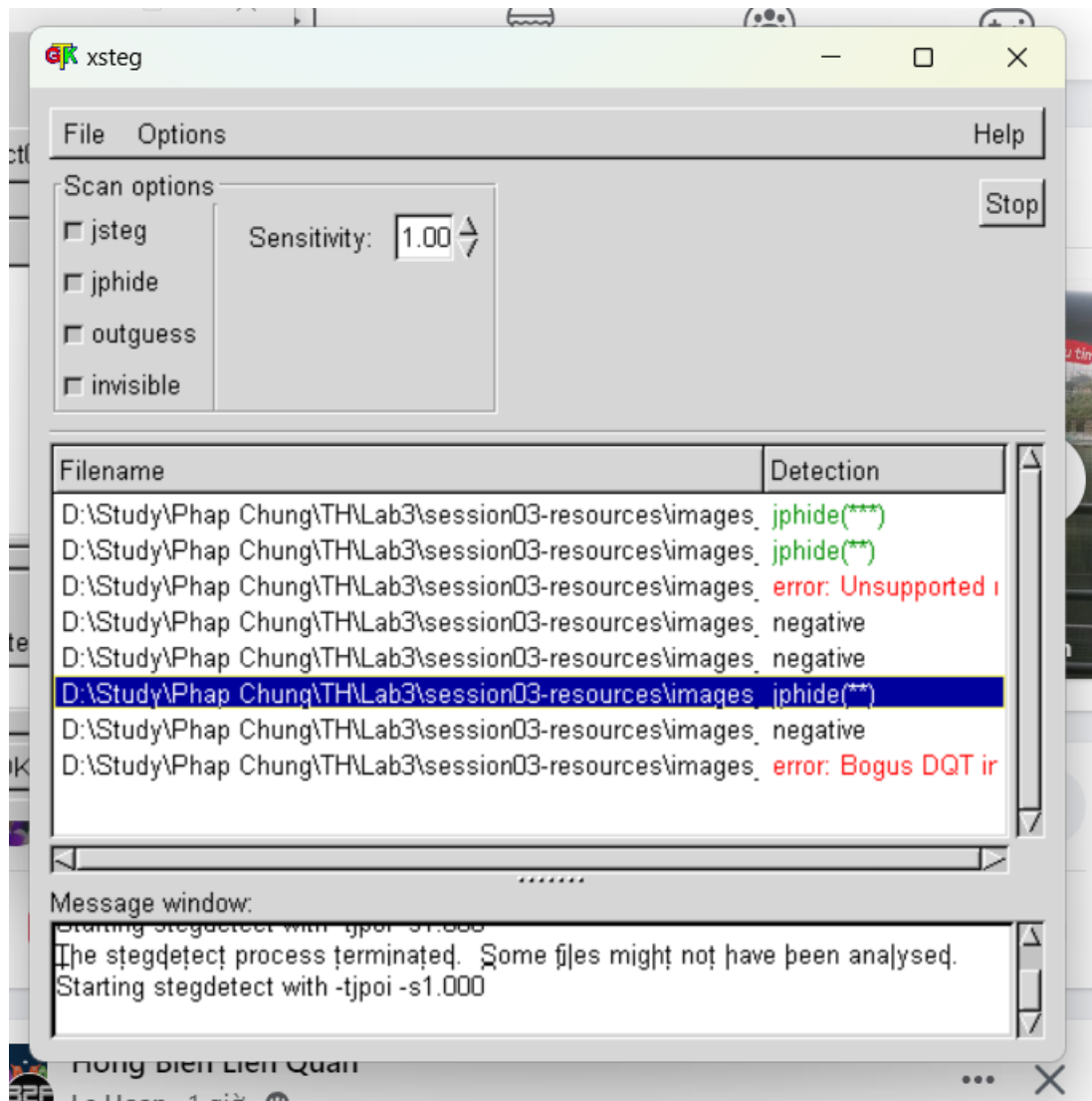
Done	Name	User Name	E-mail	Password	External Login Info.
	Ann Rawlings	ARawlings	ARawlings@peoriaud.k12.az.us	your current password	pusd11\user name
	Chris Kuczka	CKuczka	CKuczka@peoriaud.k12.az.us	your current password	pusd11\user name
	Cindy Callaway	CCallaway	CCallaway@peoriaud.k12.az.us	your current password	pusd11\user name
	Dave Pearson	DPearson	DPearson@peoriaud.k12.az.us	your current password	pusd11\user name
	David Snyder	DSnyder	DSnyder@peoriaud.k12.az.us	your current password	pusd11\user name
	Jo Little	JLittle	JLittle@peoriaud.k12.az.us	your current password	pusd11\user name
	Julia Erickson	JErickson	JErickson@peoriaud.k12.az.us	your current password	pusd11\user name
	Larry Buchanan	LBuchanan	LBuchanan@peoriaud.k12.az.us	your current password	pusd11\user name
	Lissa Cuellar	LCuellar	LCuellar@peoriaud.k12.az.us	your current password	pusd11\user name
	Maggie Olney	MOlney	MOlney@peoriaud.k12.az.us	your current password	pusd11\user name
	Nan Gillispie-DAC	NGillisp	NGillisp@peoriaud.k12.az.us	your current password	pusd11\user name
	Nathan Bowler	NBowler	NBowler@peoriaud.k12.az.us	your current password	pusd11\user name
	Patti Beltram	PBeltram	PBeltram@peoriaud.k12.az.us	your current password	pusd11\user name
	Phil Valentine	PValentine	PValentine@peoriaud.k12.az.us	your current password	pusd11\user name
	Robert Keagle	RKeagle	RKeagle@peoriaud.k12.az.us	your current password	pusd11\user name
	Rosemary Martin-Moore	RM Moore	RM Moore@peoriaud.k12.az.us	your current password	pusd11\user name
	Samantha Middagh	SMiddagh	SMiddagh@peoriaud.k12.az.us	your current password	pusd11\user name
	Sarah Balder	SBalder	SBalder@peoriaud.k12.az.us	your current password	pusd11\user name
	Shona Miranda	SMiranda	SMiranda@peoriaud.k12.az.us	your current password	pusd11\user name
	Steve Savoy	SSavoy	SSavoy@peoriaud.k12.az.us	your current password	pusd11\user name
	Teri Nevarez	TNevarez	TNevarez@peoriaud.k12.az.us	your current password	pusd11\user name
	Terrie Rust	TRust	TRust@peoriaud.k12.az.us	your current password	pusd11\user name
	Valerie Naish	VNaish	VNaish@peoriaud.k12.az.us	your current password	pusd11\user name
	Bill Copeland	Bill.Copeland	GSMOM@COX.NET	BcNeT45	pusd11\text\Bill.Copeland
	Tammara Edgin	tammarae@microsoft.com	tammarae@microsoft.com	TeCom23	pusd11\text\Tammara.Edgin
	Diane Douglas	dmndouglas@cox.net	dmndouglas@cox.net	DdNeI21	pusd11\text\Diane.Douglas
	Mary Crespino	Mary.Crespino	crespny@cox.net		

- Đây là thông tin sau khi lấy lại được



- Đây là properties của file sau khi trích xuất

Kịch bản 01-c



- Khi ta quét ảnh my_2009_miss_gsu.jpg và zebras2.jpg thì được kết quả jphide còn các file còn lại là error hoặc là negative

```

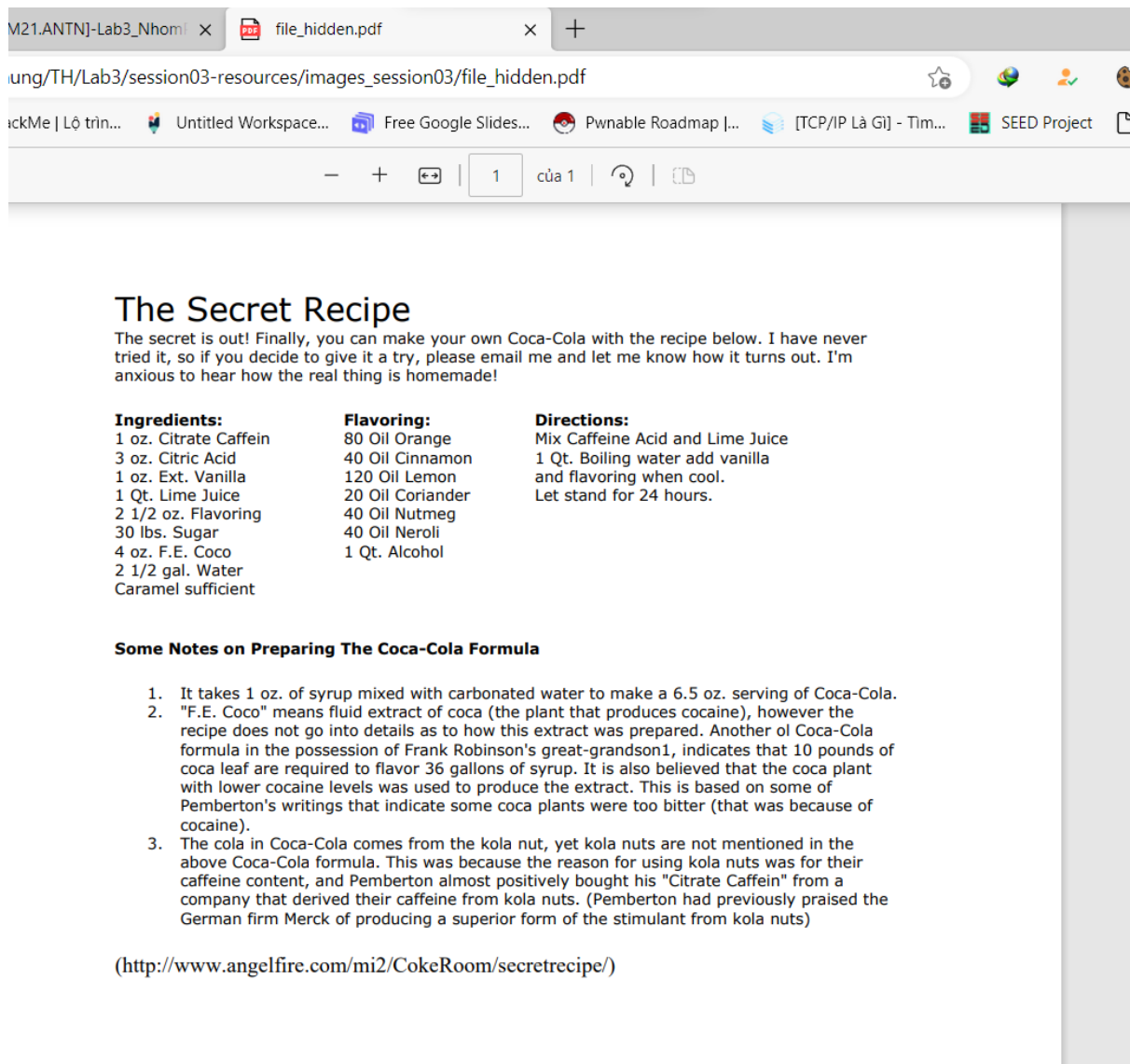
Time: 126 seconds: Cracks: 2423746, 18958.6 c/s
PS D:\Study\Phap Chung\TH\Lab3\session03-resources\stegdetect04_session03> .\stegbreak.exe -r rules.ini -f meddict.dic "
D:\Study\Phap Chung\TH\Lab3\session03-resources\images_session03\zebras2.jpg"
Loaded 1 files...
D:\Study\Phap Chung\TH\Lab3\session03-resources\images_session03\zebras2.jpg : jphide[v5](together)
Processed 1 files, found 1 embeddings.
Time: 3 seconds: Cracks: 68607, 22869.0 c/s
PS D:\Study\Phap Chung\TH\Lab3\session03-resources\stegdetect04_session03> .\stegbreak.exe -r rules.ini -f meddict.dic "
D:\Study\Phap Chung\TH\Lab3\session03-resources\images_session03\my_2009_miss_gsu.jpg"
Loaded 1 files...
D:\Study\Phap Chung\TH\Lab3\session03-resources\images_session03\my_2009_miss_gsu.jpg : negative
Processed 1 files, found 0 embeddings.
Time: 127 seconds: Cracks: 2423746, 19084.6 c/s
PS D:\Study\Phap Chung\TH\Lab3\session03-resources\stegdetect04_session03>

```

- Ta dùng phần mềm stegbreak để bẻ khóa mật khẩu trong ảnh
- Nhưng ở đây nó chỉ bẻ khóa được file zebras2 có thể mật khẩu UIT không phổ biến hoặc cách thức giấu thông tin sử dụng cách thức khác nên có thể nó không bẻ khóa được
- Mật khẩu của zebras2 là **“together”**



- Vào tool sử dụng chức năng seek sau đó nhập mật khẩu là together sau đó lưu lại dưới tên là file_hidden.pdf



- Đây là file sau khi ta có thể đọc được

Kịch bản 04

```
(kali@kali)-[~/Desktop]
$ xxd -g 1 star-wars.jpg
00000000: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 .....JFIF.....
00000010: 00 60 00 00 ff db 00 43 00 20 16 18 1c 18 14 20 ..^.....C. ....
00000020: 1c 1a 1c 24 22 20 26 30 50 34 30 2c 2c 30 62 46 ... $" 60P40,,0bF
00000030: 4a 3a 50 74 66 7a 78 72 66 70 6e 80 90 b8 9c 80 J:Ptfzxrpn....
00000040: 88 ae 8a 6e 70 a0 da a2 ae be c4 ce d0 ce 7c 9a ... np.....|.
00000050: e2 f2 e0 c8 f0 b8 ca ce c6 ff db 00 43 01 22 24 .....C."$
00000060: 24 30 2a 30 5e 34 34 5e c6 84 70 84 c6 c6 c6 c6 $0*0^44^..p....
00000070: c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 .....
00000080: c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 .....
```

- Sử dụng công cụ xxd để xem dạng hex của file start-wars.jpg

```
00004e80: 4b49 4500 2d28 a4a5 a005 a70a 6d2d 003a KIE.-(. . . . .m~.:
00004e90: 8a4c d14c 9168 a28a 0614 5145 0014 5145 .L.L.h....QE..QE
00004ea0: 0014 5145 0014 5145 0014 5145 0014 5145 ..QE..QE..QE..QE
00004eb0: 0014 5145 300a 5cd2 5140 1fff d931 3030 ..QE0.\.Q@...100
00004ec0: 3131 3031 3031 3031 3031 3031 3031 3031 11010101010101
00004ed0: 3131 3031 3031 3030 3131 3031 3031 3031 1101010011010101
00004ee0: 3031 3031 3131 3031 3031 3030 3131 3131 0101110101010011
00004ef0: 3131 300a                                     110.
```

- Ở dưới ta thấy có 1 loạt mã nhị phân

```
(kali@kali)-[~/Desktop]
$ python3
Python 3.11.2 (main, Mar 13 2023, 12:18:29) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> len("100110101010101010111010100110101010101110101001110")
54
>>>
```

- Trích xuất ra và phân tích
- Length của chuỗi nhị phân này là 54. Ban đầu mình định decode theo ASCII nhưng mà ký tự ASCII là 8 bits ứng với 1 bytes/1 ký tự. Theo gợi ý, đề bài có cung cấp thông tin về một họa sĩ khuyết tật mắt (mù lòa) tên là John Bramblitt . Điều này cho hint rằng ông cũng tổng thông điệp vào bằng mã cho người khiếm thị. Độ dài 54 này chia hết cho 6 nên mình cũng nghĩ đến mã Braille dành cho người khiếm thị là hợp lý

The braille alphabet

a	b	c	d	e	f	g	h	i
•	•	••	••	•	••	••	••	•
j	k	l	m	n	o	p	q	r
••	•	•	••	••	•	••	••	••
s	t	u	v	x	y	z		w
•	••	•	•	••	••	••		••


- Phân cách thành chuỗi 6 bits
100110 101010 101010 111010 100110 101010 101110 101010
011110
- Ta có thể xem cách giải mã từ binary thành dạng ASCII từ link này
https://en.wikipedia.org/wiki/Braille_ASCII
- Vậy theo link đó ta sẽ decode được là : “doordonot”

```
steghide: did not write to file "output.txt".
(kali@kali)-[~/Desktop]
$ steghide extract -sf star-wars.jpg -p doordonot -xf output2.txt
wrote extracted data to "output2.txt".
```

- Có được password thì ta dùng steghide sau đó output được lưu vào file output2.txt

```
(kali@kali)-[~/Desktop]
$ cat output2.txt
YmVjb21lYWplZGltYXN0ZXJ5b3V3aWxs
(kali@kali)-[~/Desktop]
$
```

- Output được mã hóa base64



YmVjb21lYWplZGltYXN0ZXJ5b3V3aWxs

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

▼

Source character set.

☐

Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< **DECODE** >

Decodes your data into the area below.

becomeajedimasteryouwill

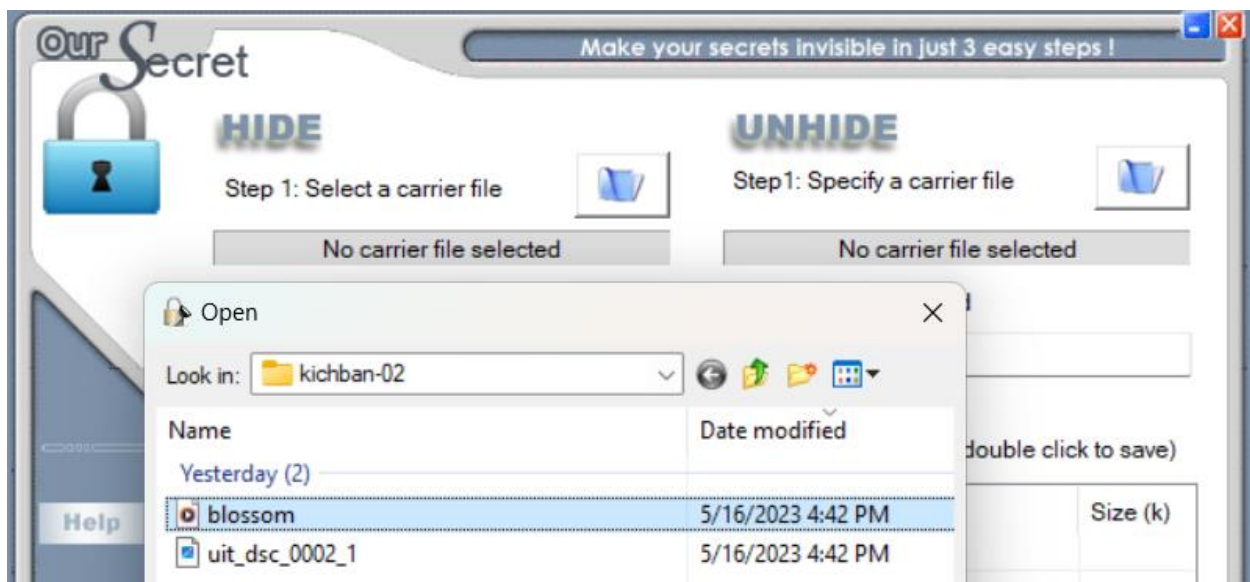
- Ta giải mã có được thông điệp ẩn “**becomeajedimasteryouwill**”

2. Kịch bản 2

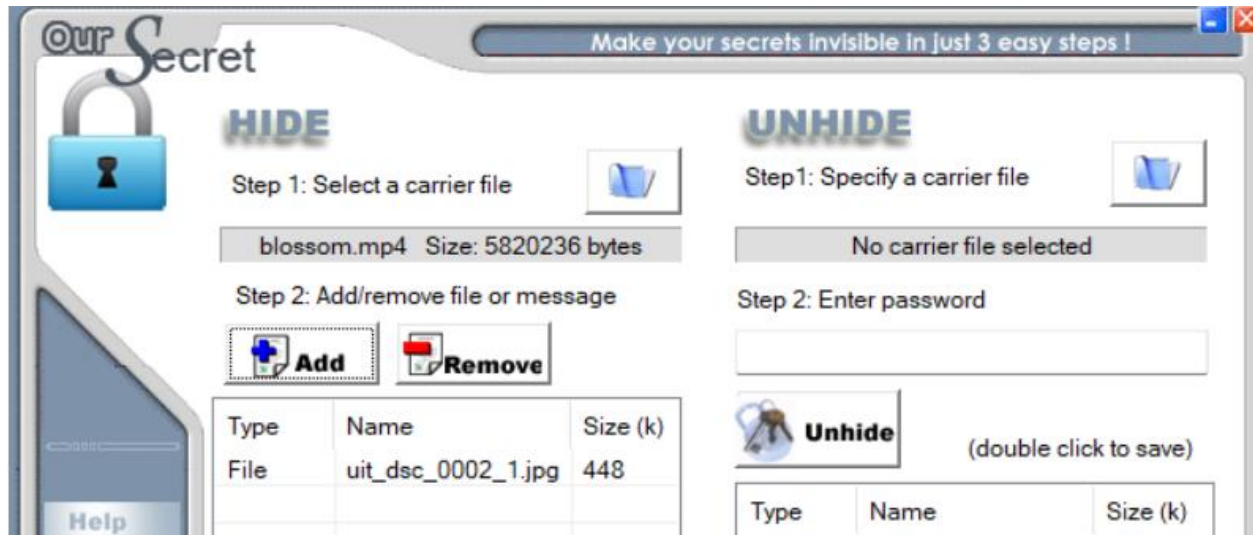
Kịch bản 02. Ẩn giấu dữ liệu bằng công cụ Our Secret

- 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).

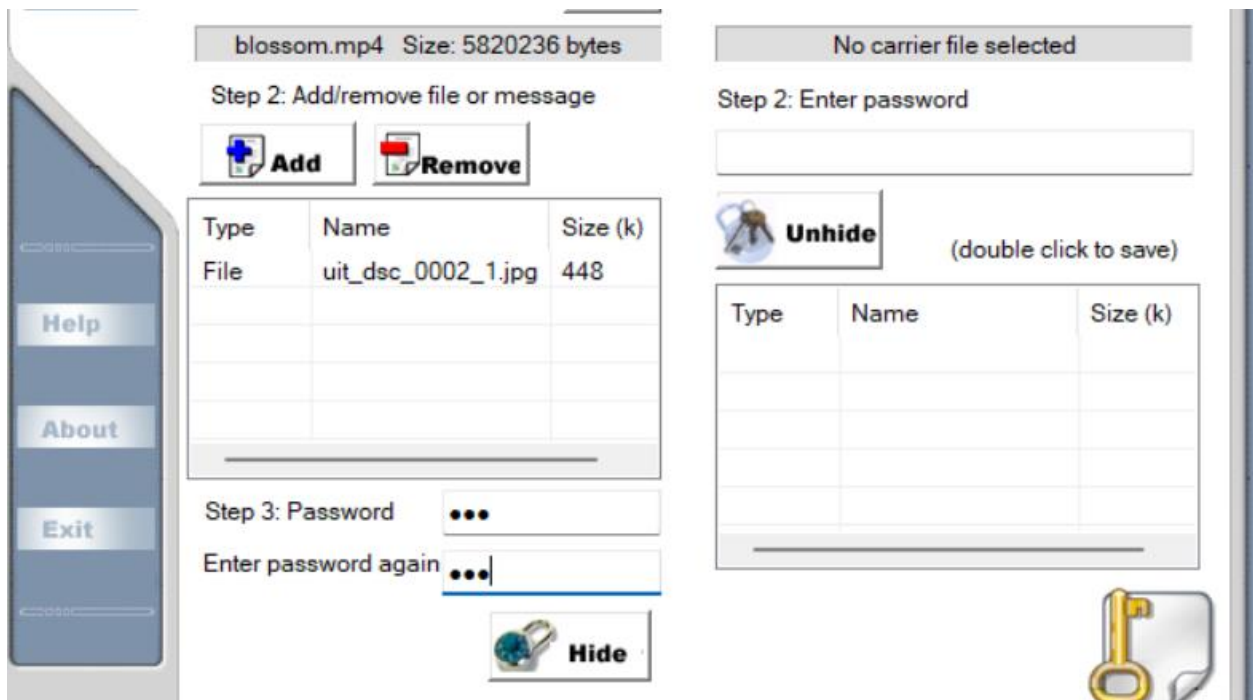
- Giấu ảnh uit_dsc_0002_1.jpg vào tập tin mp4
 - o Thêm file mp4 ở mục Select a carrier file (Step 1)



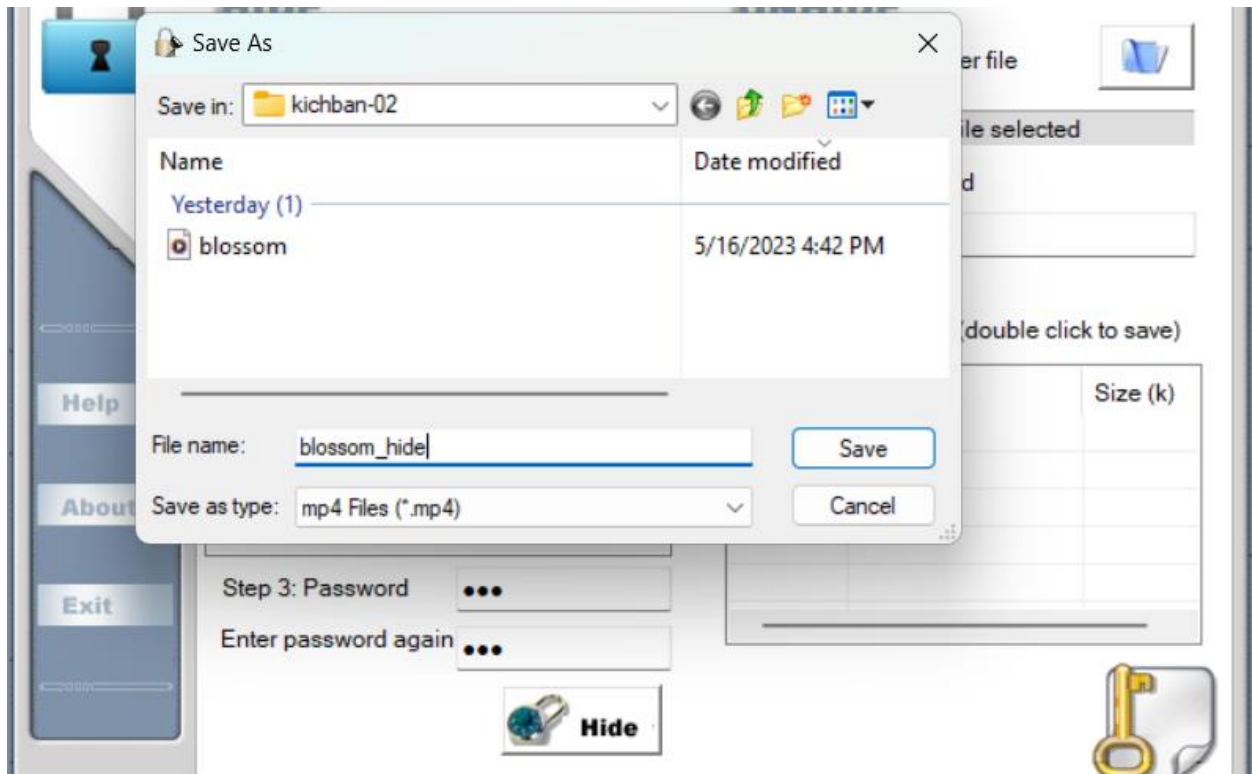
- Thêm file hình ảnh (Step 2)



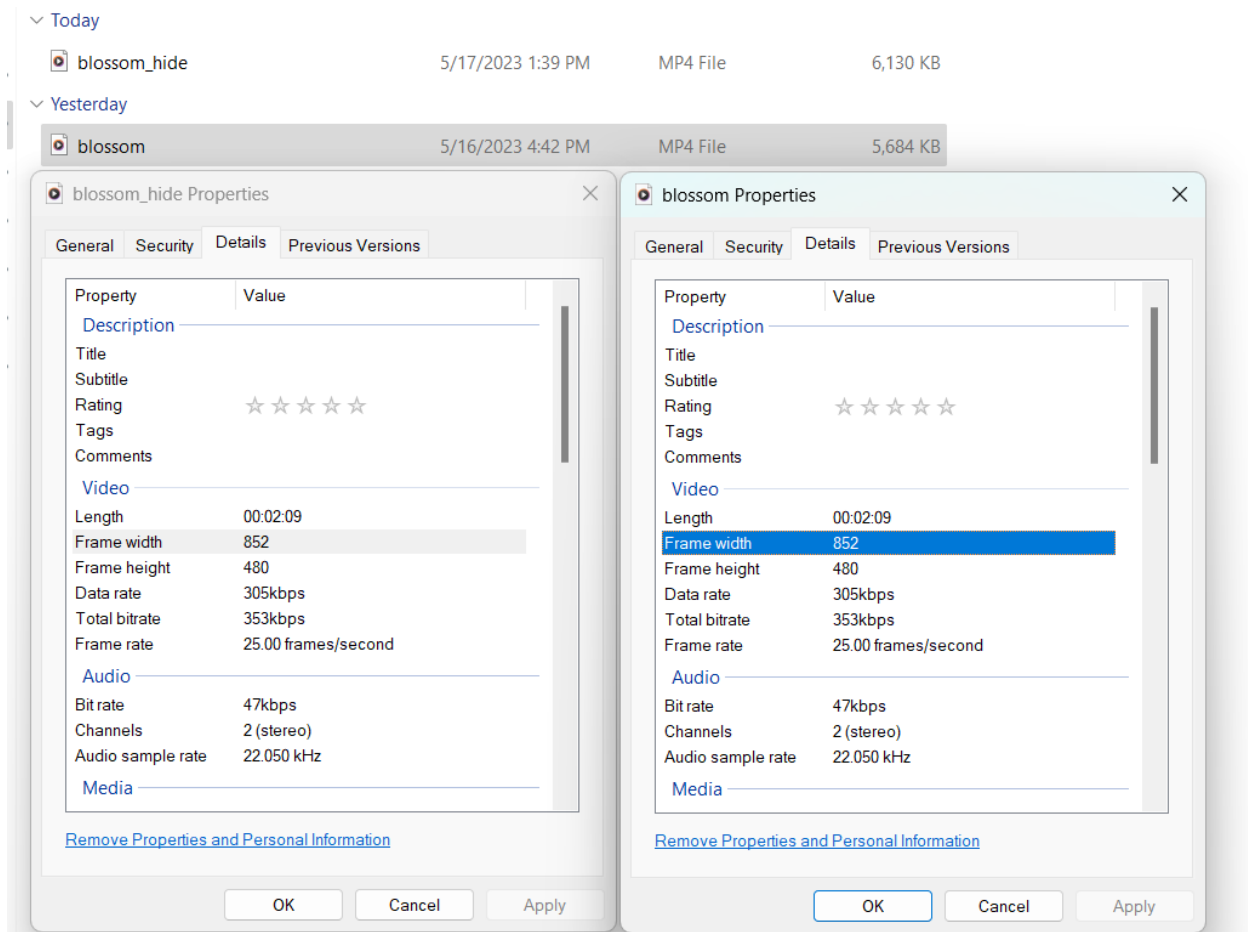
- Đặt mật khẩu là “E81” (Step 3)



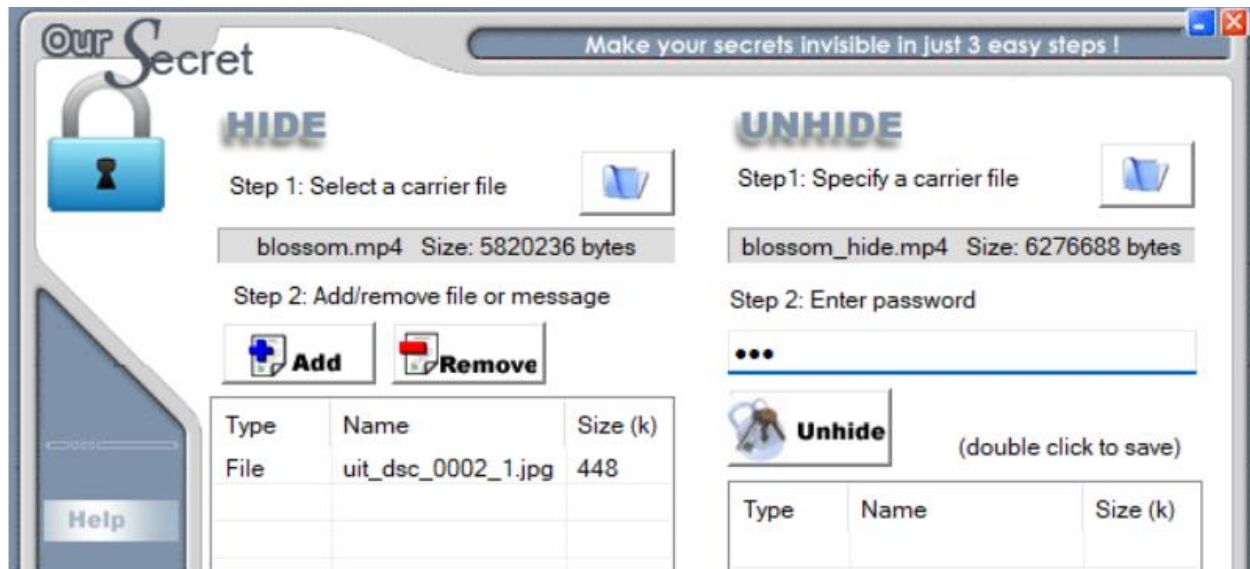
- Click vào ô “Hide” để tiến hành giấu ảnh vào file mp4 đồng thời đặt tên cho file mới là blossom_hide



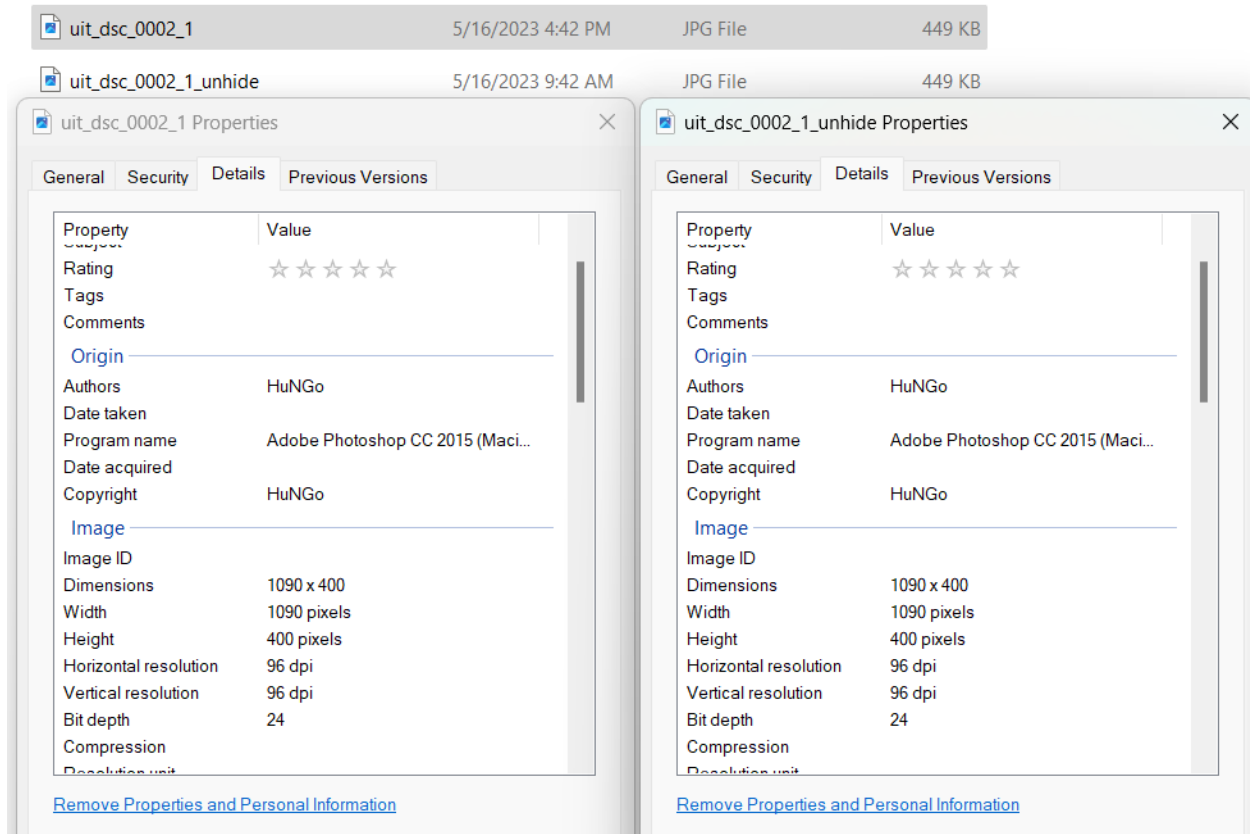
- Nhận xét về sự thay đổi của file video: có sự khác biệt về dung lượng (file mới nặng hơn so với file gốc), còn về chất lượng và độ dài video thì không có khác biệt.



- Giải mã thông tin giấu trong đoạn phim
 - o Chọn file cần giải mã là blossom_hide và nhập password là E81 -> Unhide -> Save với tên file là uit_dsc_0002_1_unhide

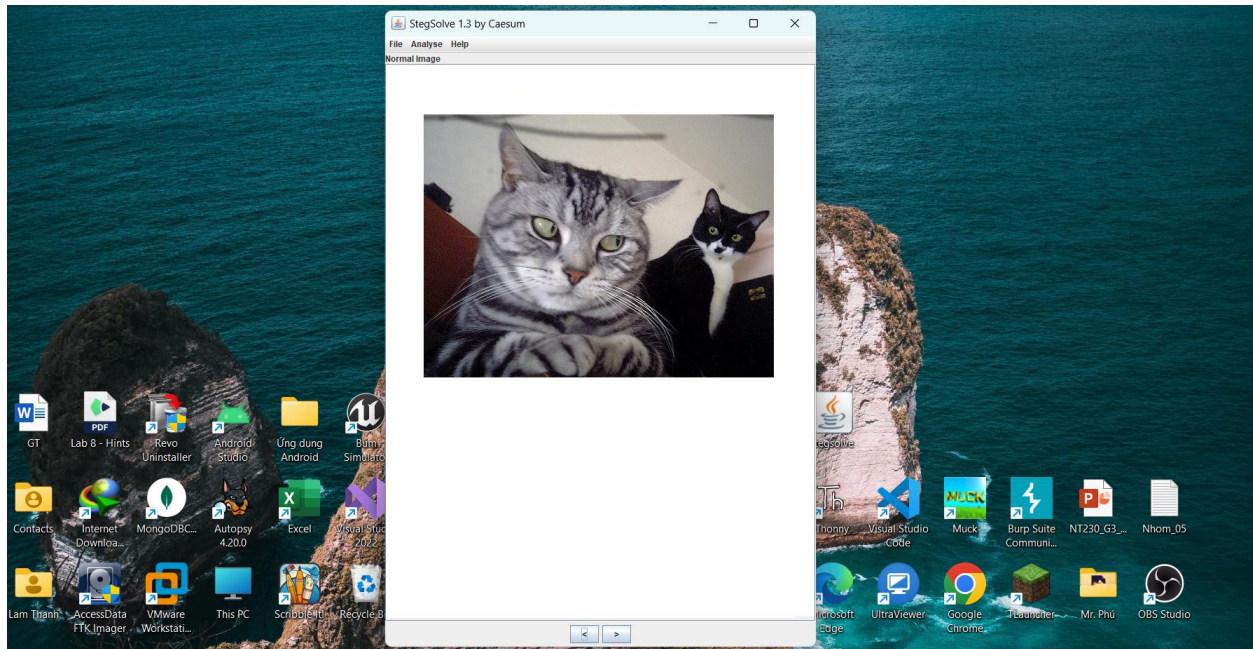


- Nhận xét về nội dung file giải mã được với file ban đầu (file/thông tin được chọn để giấu): file gốc và file có được sau khi unhide hoàn toàn giống nhau.

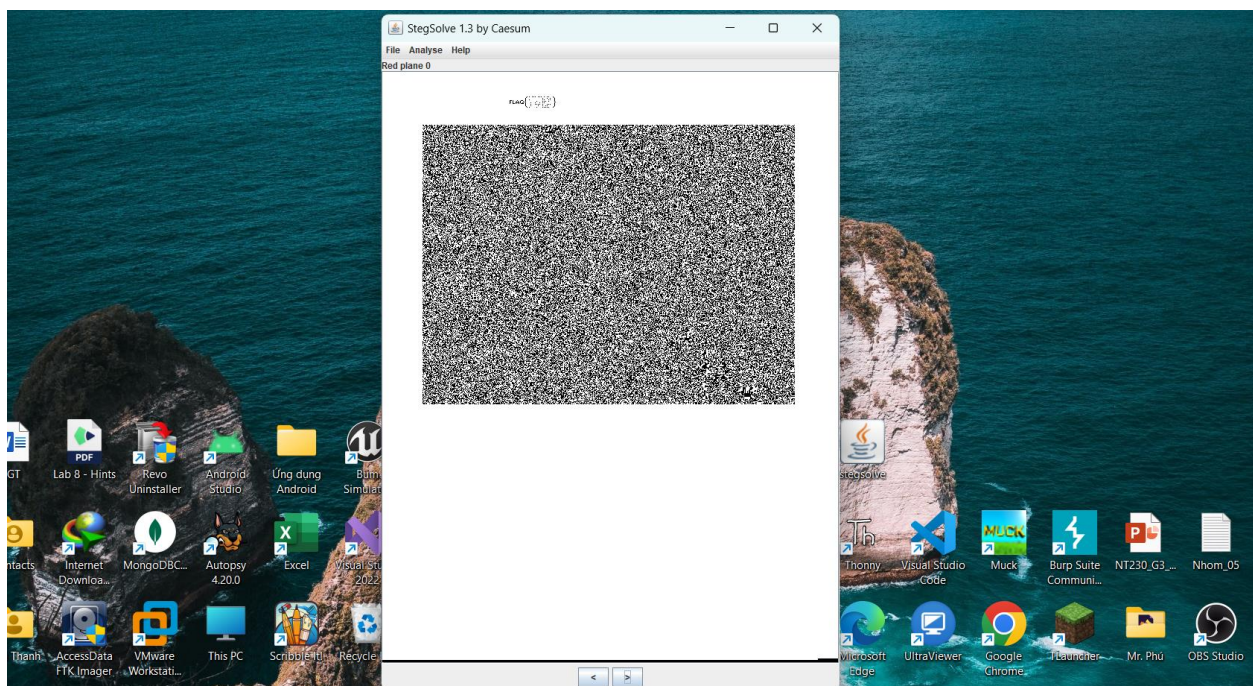


3. Kịch bản 3

- Sử dụng công cụ StegSolve để điều chỉnh bản màu của ảnh để tìm Flag

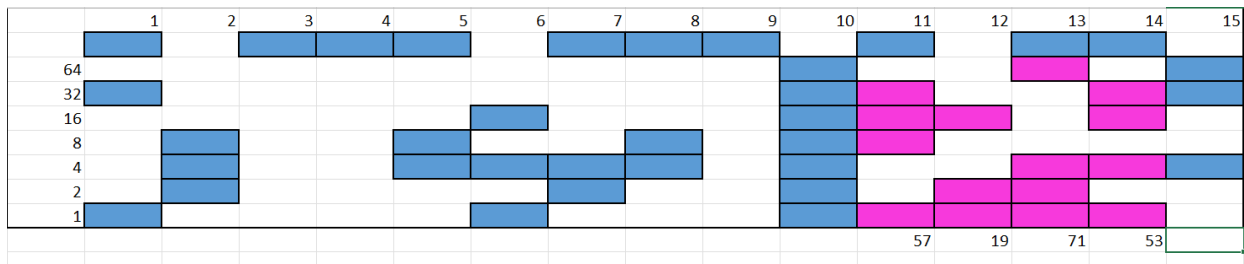


- Sau khi điều chỉnh và xem xét các bản màu ta tìm được flag ở bản màu Red Plane 0



100

- Sử dụng kỹ thuật Printer Steganography theo như gợi ý của lab



➔ Số seri của máy in là 53 71 19 57

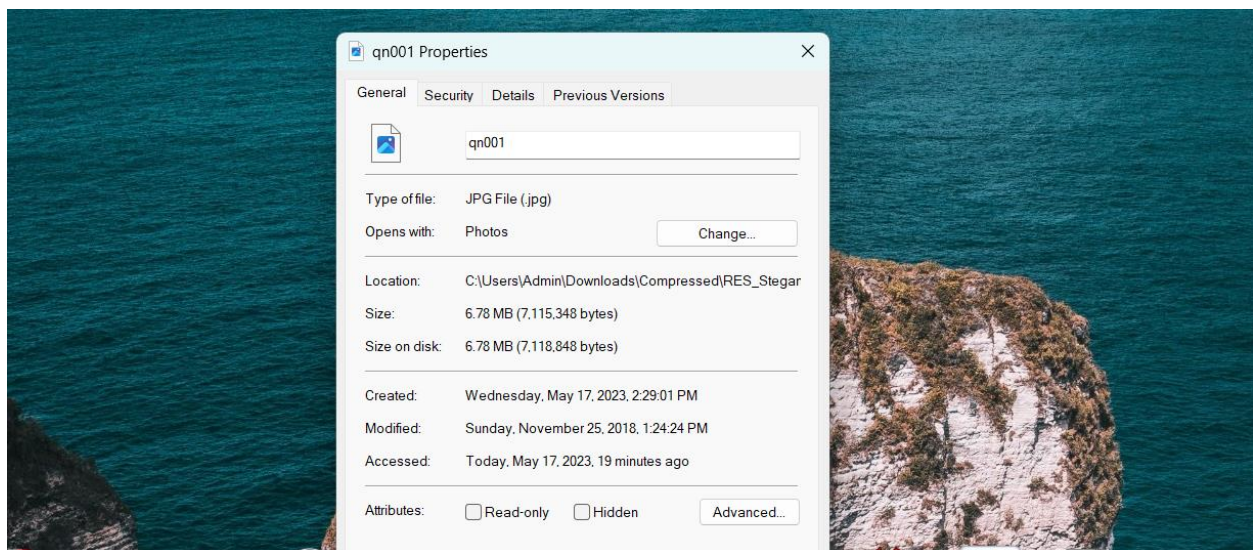
5. Kịch bản 5

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

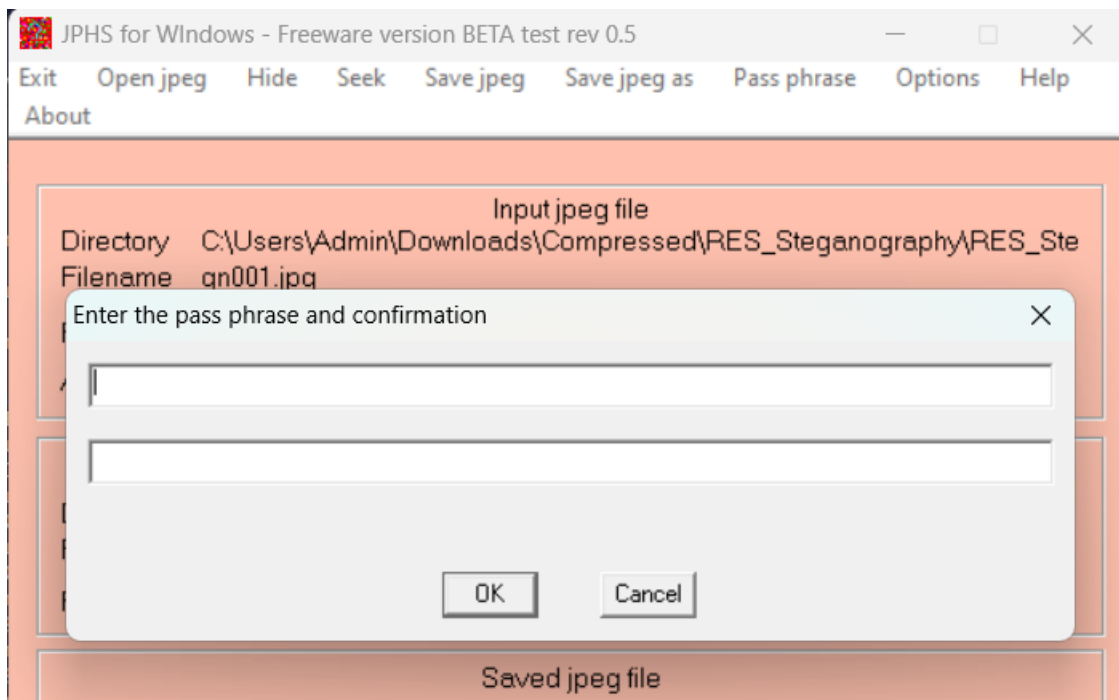
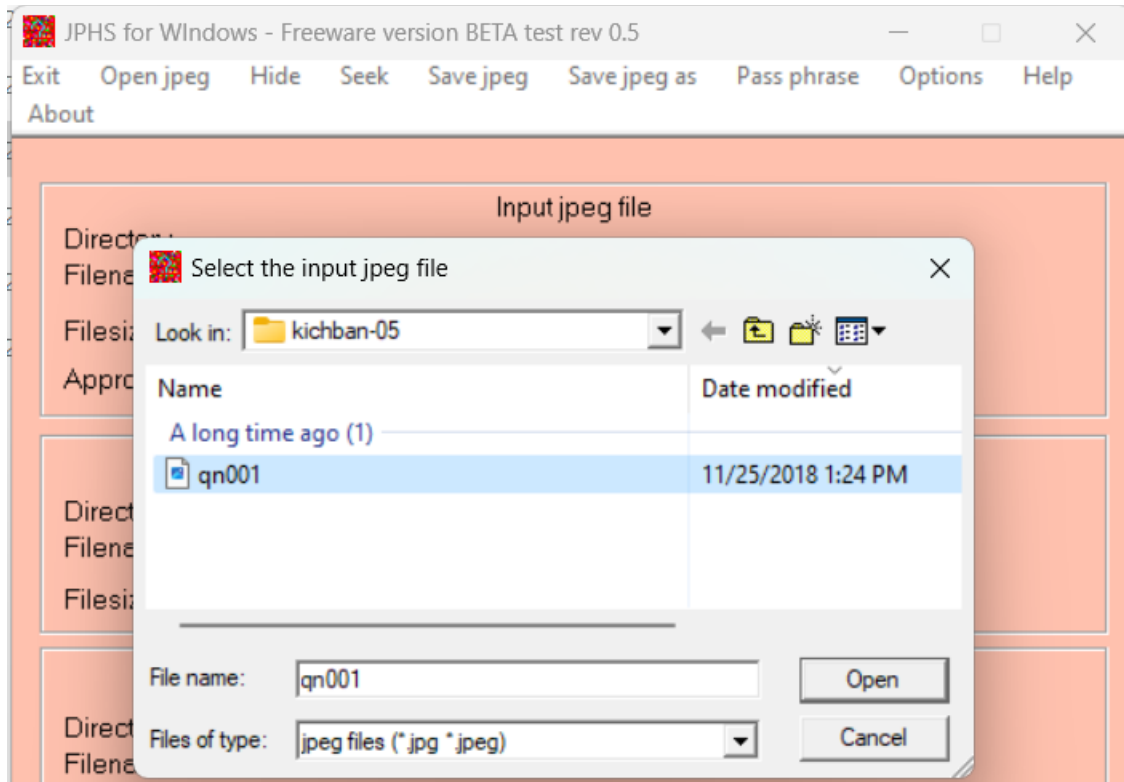
- Tài nguyên thực hiện: qn001.jpg
- Yêu cầu – Gợi ý: Tìm thông điệp (flag) được ẩn giấu. Thông tin flag liên quan đến Đội tuyển bóng đá nam Việt Nam.

Gợi ý:



- Ta xem thông tin hình ảnh thì thấy dung lượng của file ảnh là tầm 6 MB, hơi lớn so với 1 file hình ảnh. Vì vậy có thể có file khác được nhúng vào trong hình ảnh này.



- Trong bài lab có đề cập tới công cụ JPHS dùng để ẩn giấu thông tin trong các ảnh JPEG ở các bit thấp. Sau khi tìm hiểu cách sử dụng thì ta sẽ dùng nó để trích xuất tệp được nhúng vào file ảnh



- Kết quả: có 1 file được trích xuất

Name	Date modified	Type	Size
▼ Today			
 cau5	5/17/2023 3:07 PM	File	191 KB
▼ A long time ago			
 qn001	11/25/2018 1:24 PM	JPG File	6,949 KB

- Đưa vào linux ta kiểm tra thì biết được đây là file word -> đổi đuôi thành .doc

```
(kali@kali)-[~/Downloads]
$ file cau5
cau5: Microsoft Word 2007+
```

Nội dung file .doc

Tuyển Việt Nam luôn biết làm chủ thế trận

Trang bóng đá *Okezone Bola* miêu tả chi tiết về trận đấu diễn ra trên sân Hàng Đẫy: "Đội tuyển Việt Nam nhập cuộc khá tốt với chủ đích tấn công trực diện. Kết quả là đội chủ nhà hoàn toàn nằm giữ thế trận trong khi Campuchia phải thuộc nhiều vào những pha phản công".

"Mặc dù làm chủ trận đấu, trận thực tế, đoàn quân của HLV Park Hang-seo lại gặp khó khăn khi không thể khoan thủng hàng phòng ngự đối phương ở đầu hiệp 1. Phải đến phút thứ 39, nỗ lực của Việt Nam mới được đền đáp khi Tiến Linh tận dụng lợi thế từ đường chuyền của Trọng Hoàng để xâm nhập vào vòng cấm và đánh đầu ghi bàn", từ báo của Indonesia *Bình luận*.

Những bàn thắng tiếp theo đến như một lá tất nhiên khi đội chủ nhà cội họ được áp lực ghi bàn và thoải mái dẫn dắt trận đấu. Các học trò của ông Park chỉ mất thêm 3 phút để Quang Hải ghi tên mình lên bảng tỷ số sau khi tận dụng pha kiến thiết của Nguyễn Phong Hồng Duy", từ *Bola Sport* viết.



Trang *Straits Times* của Singapore đặc biệt ấn tượng với pha làm bàn của Văn Đức khi miêu tả đây là "cú sút đầy lạnh lùng quyết đoán từ một pha xoay người rất nhanh, nâng tỷ số lên 3-0 để ấn định một chiến thắng không có gì phải bàn cãi cho Việt Nam".

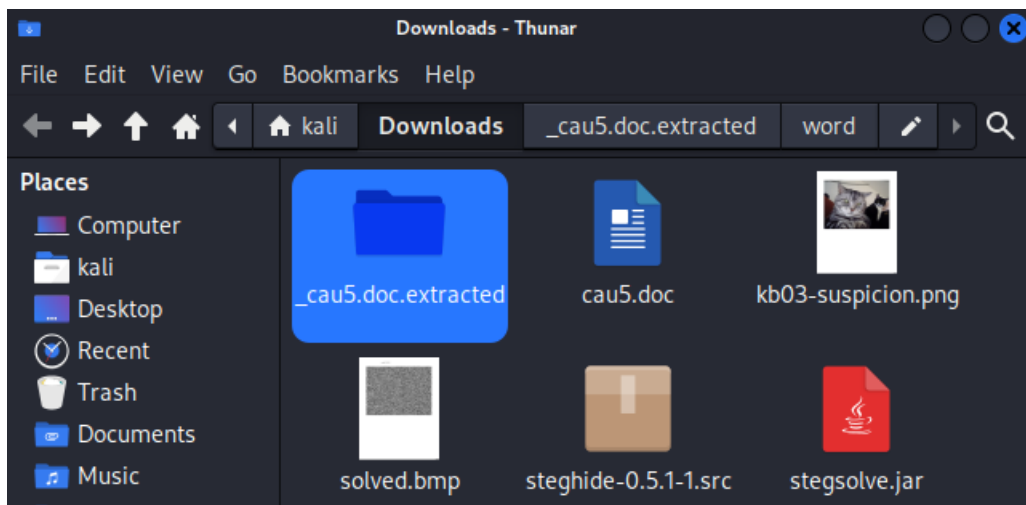
Coi đây là màn trình diễn tốt nhất của tuyển Việt Nam từ đầu chiến dịch AFF Cup 2018 đến nay, *Fox Sports Asia* nhận định: "Thầy trò Park Hang-seo đã chạm đến vòng knock-out bằng chiến thắng hủy diệt 3-0 trước Campuchia. Thắng lợi này không chỉ đảm bảo cho họ một vé vào bán kết, mà với thất bại của Myanmar trước Malaysia, nhà vô địch Đông Nam Á năm 2008 đã kết thúc vòng bảng với tư cách là đội đứng đầu bảng A".

Trang *FourFourTwo* lại đánh giá cao khả năng xoay tua nhân sự của thuyền trưởng người Hàn Quốc: "Đội tuyển Việt Nam dễ dàng vượt qua Campuchia để dẫn đầu bảng A. Trong bối cảnh Campuchia đã bị loại, HLV Park cất những trụ cột như Xuân Trường, Anh Đức và Công Phượng để tạo điều kiện cho nhiều cầu thủ khác có cơ hội ra sân gây ấn tượng". *Reuters* gọi đây là "thắng lợi như thường lệ của đội tuyển Việt Nam trước Campuchia. Malaysia cũng đã đánh bại Myanmar để cùng Việt Nam - ứng cử viên sáng giá cho chức vô địch - tiến vào bán kết ASEAN".

- Trong file này không có nội dung nào liên quan tới flag. Sau khi tìm hiểu và tham khảo thì ta sẽ tiếp tục trích xuất một file ẩn nữa trong file .doc này bằng công cụ binwalk

```
(kali@kali)-[~/Downloads]
$ binwalk -e cau5.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
186851	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: 3267, uncompressed size: 31584, name: word/styles.xml
191328	0x2EB60	Zip archive data, at least v2.0 to extract, compressed size: 471, uncompressed size: 2670, name: word/webSettings.xml
191849	0x2ED69	Zip archive data, at least v2.0 to extract, compressed size: 576, uncompressed size: 1968, name: word/fontTable.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



- Lần lượt đọc nội dung trong các file trong thư mục vừa trích xuất được, sau một thời gian thì ta tìm được một đoạn mã có vẻ như liên quan tới mã hóa “BrainF*ck” trong file document.xml trong thư mục Word

- Ta thử từng đoạn hoặc copy cả 2 đoạn và sử dụng tool online là <https://www.dcode.fr/brainfuck-language> để tiến hành decode



- Kết quả: tìm được Flag là **Forensics05@UIT{Vietnam-win-Cambodia}**