BÁO CÁO THỰC HÀNH

**Môn học: Pháp chứng kỹ thuật số**

**Lab 3:**

*GVHD: Đoàn Minh Trung*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT334.O21.ATTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Phạm Ngọc Thơ | 21522641 | 21522641@gm.uit.edu.vn |
| 2 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Kịch bản 1a, 1b, 1c (đã báo cáo ở lớp) | 100% |
| 2 | Kịch bản 2 |  |
| 3 | Kịch bản 3 (đã báo cáo ở lớp) | 100% |
| 4 | Kịch bản 4 (đã báo cáo tại lớp) | 100% |
| 5 | Kịch bản 5 |  |
| 6 | Kịch bản 6 |  |
| 7 | Kịch bản 7 |  |
| 8 | Kịch bản 8 |  |
| 9 | Kịch bản 9 |  |
| 10 | Kịch bản 10 |  |

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

BÁO CÁO CHI TIẾT

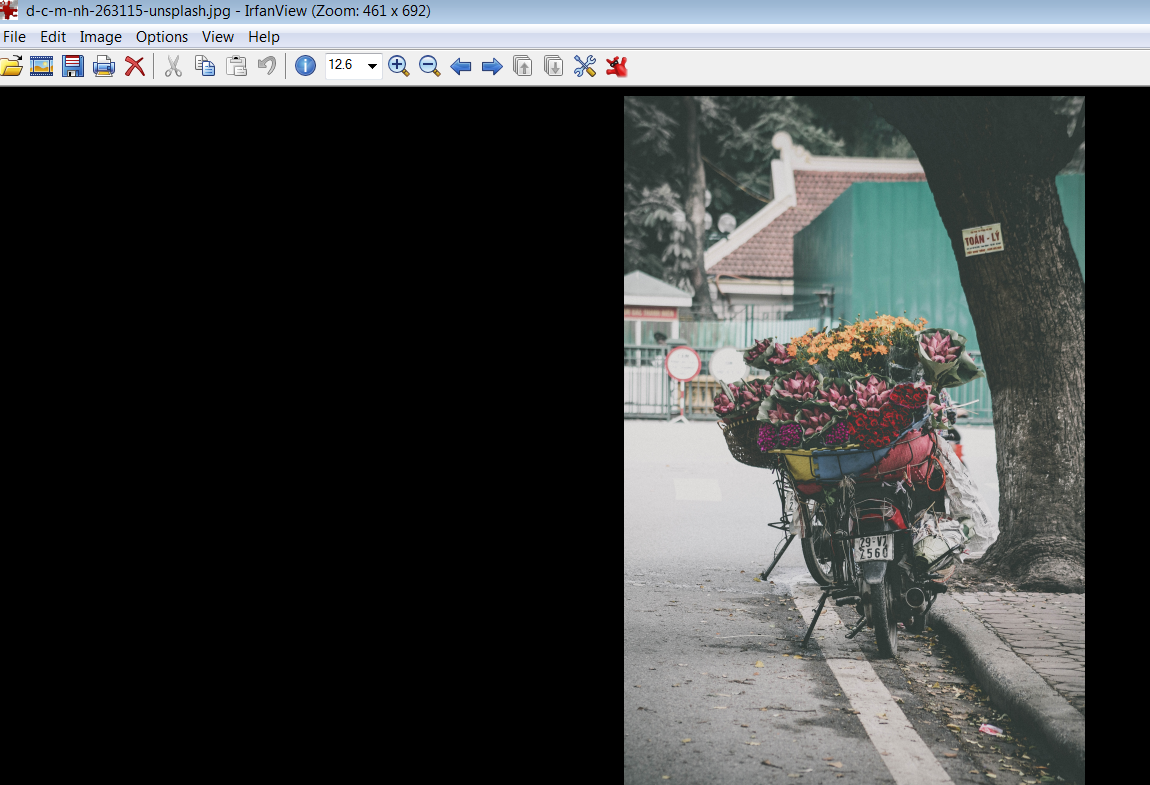
1. Kịch bản 1a: Thực hiện phân tích thông tin tập tin ảnh

- Tài nguyên thực hiện, nằm trong thư mục kb-01-a

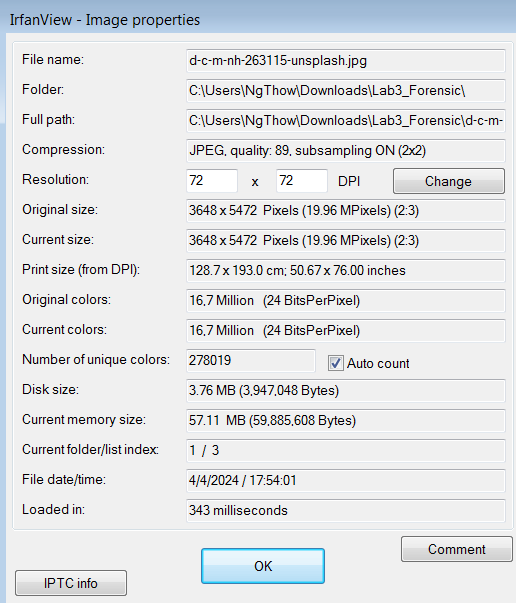
- Yêu cầu: Cung cấp các thông tin chi tiết liên quan tới các bức ảnh trên bằng phần mềm IrfanView.

Đáp án:

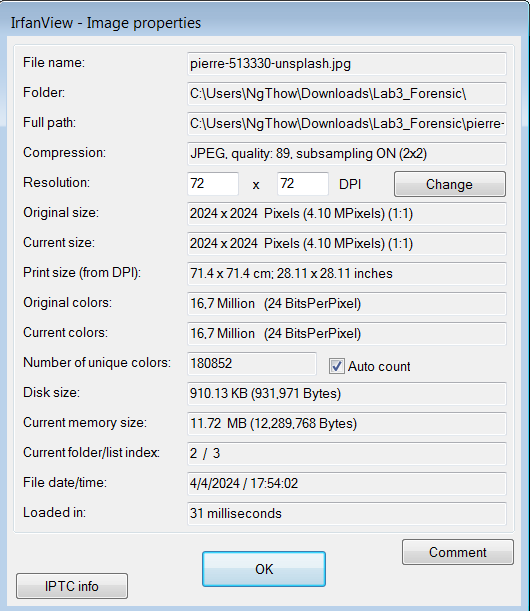
* File:
* Mở file bằng IrfanView: d-c-m-nh-263115-unsplash.jpg



* Xem thêm thông tin của ảnh. Ở menu, chọn Image -> Information:

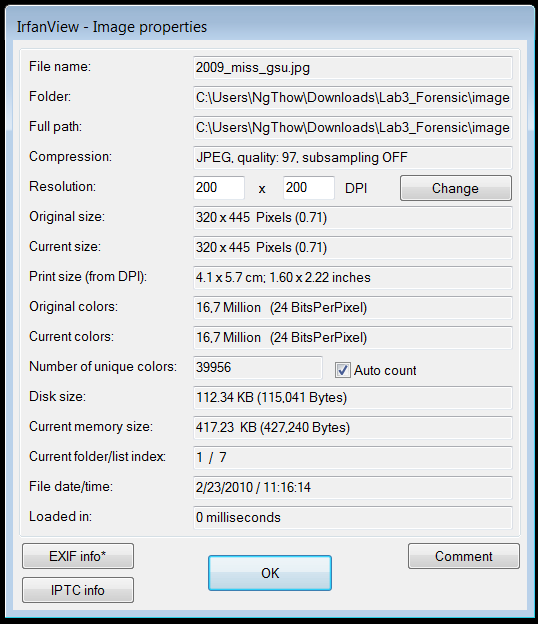


* File: pierre-513330-unsplash.jpg

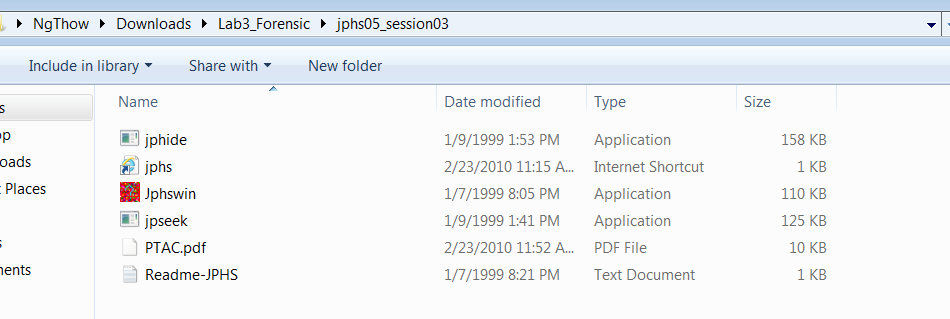


1. **Kịch bản 1b: Kịch bản 01-b: Giấu tin và giải mã thông tin trong ảnh:**

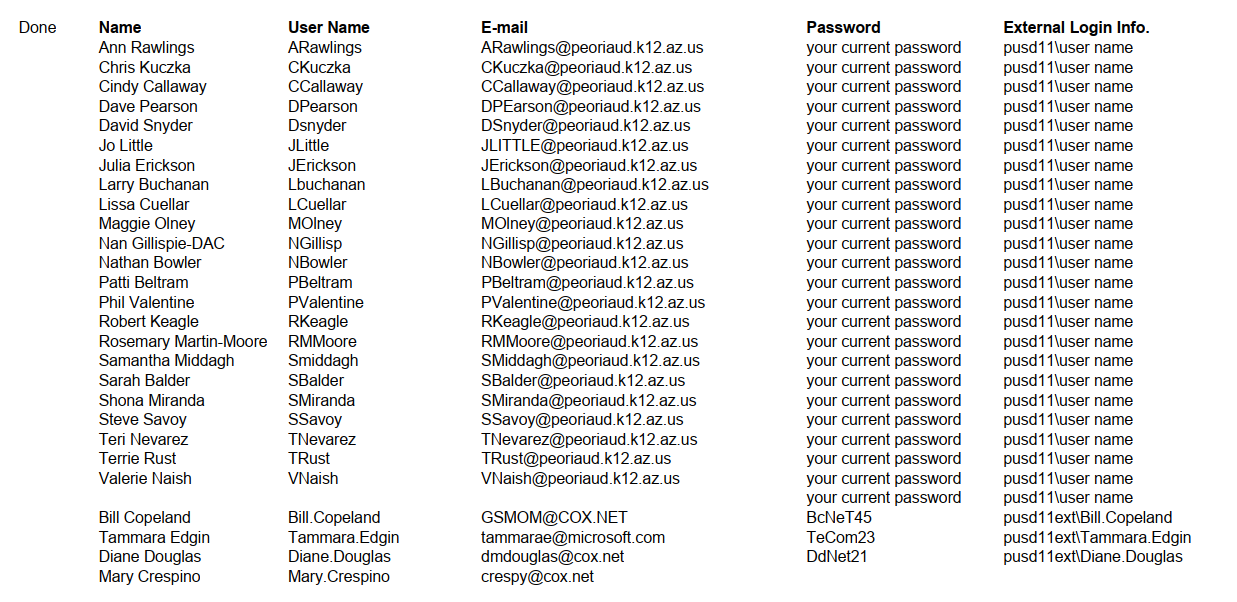
* Tài nguyên ảnh trong file nén images\_session03.zip (Ảnh: 2009\_miss\_gsu.jpg):



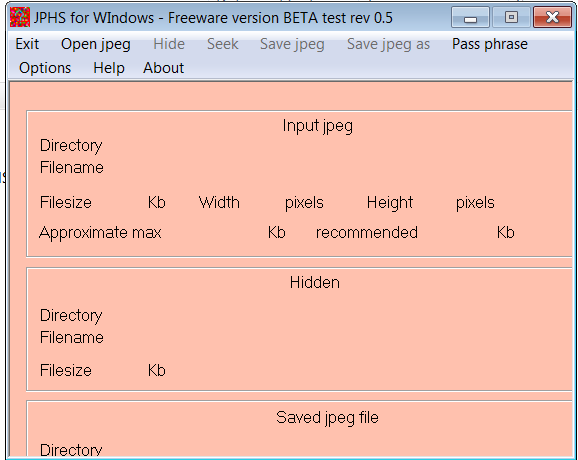
* Công cụ của kịch bản, dữ liệu cần giấu nằm trong file nén jphs05\_session03.zip. Giải nén ra:



* Nội dung file PTAC.pdf:



* Chạy file Jphswin.exe:

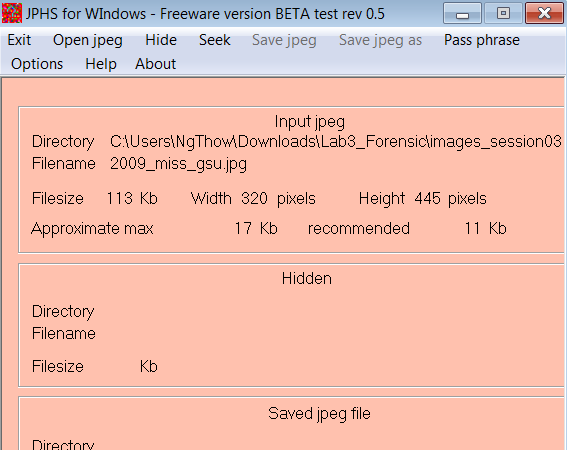


* Chọn “Open jpeg” để mở ảnh muốn giấu tin (2009\_miss\_gsu.jpg). Sau khi bấm chọn thêm ảnh vào, phần mềm sẽ hiển thị các thông tin gợi ý liên quan đến kích thước dữ liệu được hỗ trợ khi chèn vào ảnh:

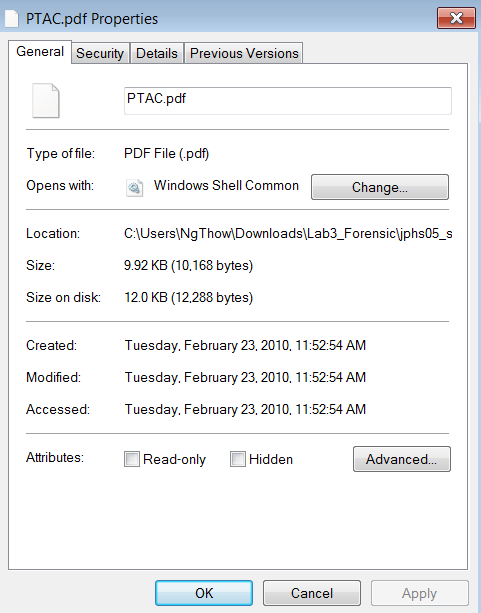
Dung lượng ảnh: 113Kb

Dung lượng dữ liệu tối đa có thể thêm vào: 17Kb

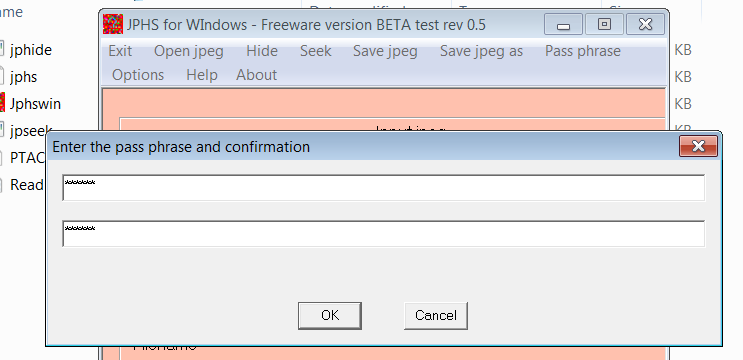
Dung lượng dữ liệu đề nghị thêm vào: 11Kb



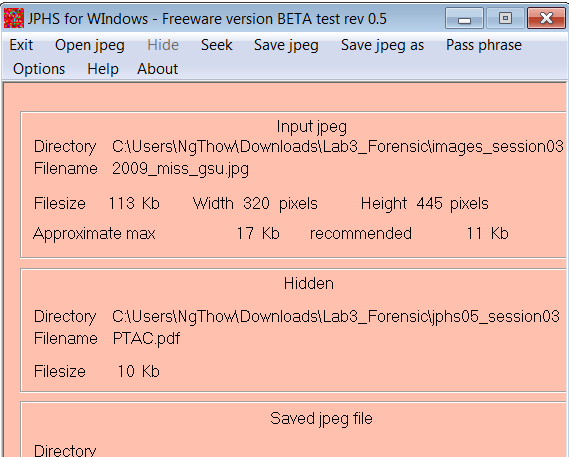
* Thông tin file PTAC.pdf muốn giấu có size là 9.92KB:

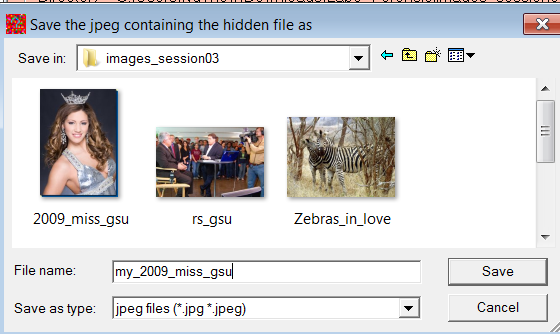


* Thêm dữ liệu muốn giấu. Chọn “hide”, đặt password là “ngthow” và nhấn OK:



* Sau khi chọn file cần giấu và đặt mật khẩu, chọn Save jpeg as, đặt tên là *my\_2009\_miss\_gsu.jpg* để lưu ảnh chứa thông tin. Cho biết sự khác biệt về 2 bức ảnh (dung lượng, chất lượng):

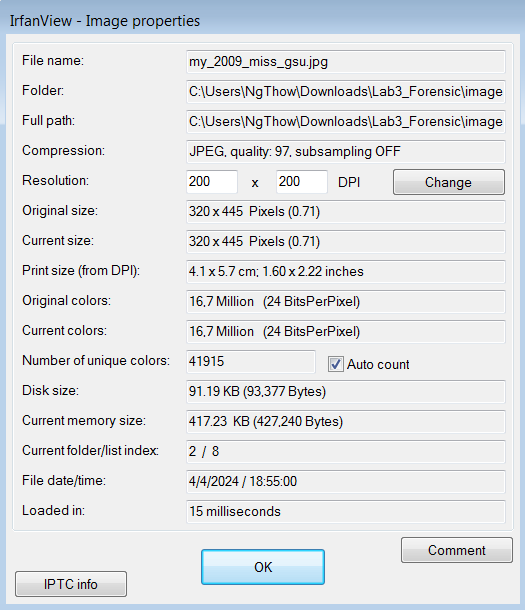
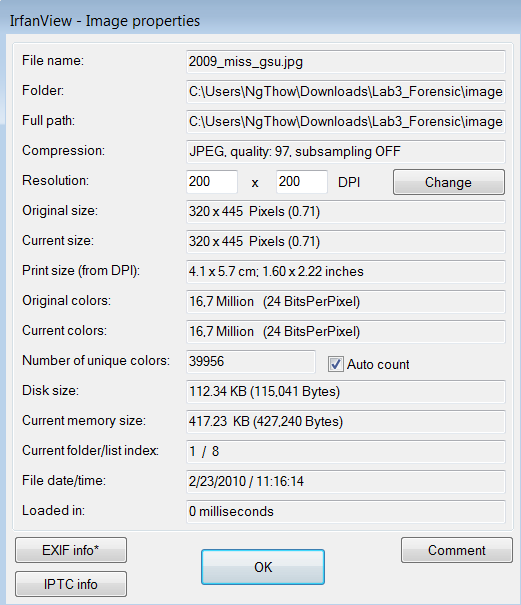




So sánh chất lượng 2 ảnh: bên trái màn hình là ảnh gốc, bên phải là ảnh có giấu thông tin. Nhìn chung 2 ảnh không có khác biệt nhiều, tuy nhiên có thể quan sát được ảnh chứa thông tin ẩn sáng màu hơn so với ảnh gốc:

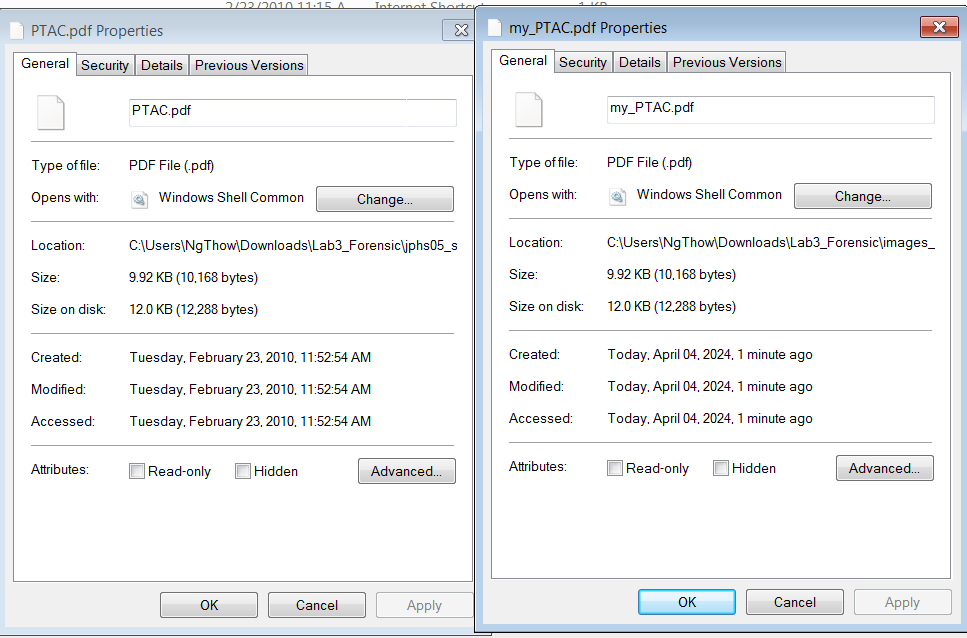


So sánh kích thước 2 ảnh: ảnh chứa thông tin ẩn có size nhỏ hơn ảnh gốc:



* Sau khi ẩn giấu thông tin, thực hiện khôi phục thông tin được giấu trong ảnh bằng chức năng Seek của phần mềm. Nhấn “Seek” trên menu để trích xuất thông tin trong ảnh. Nhập password “ngthow” (Password đặt khi thực hiện giấu tin). Lưu dữ liệu vừa trích xuất với tên “my\_PTAC.pdf”. Nhận xét về thông tin của file dữ liệu vừa trích xuất với dữ liệu ban đầu.

2 file có kích thước bằng nhau:



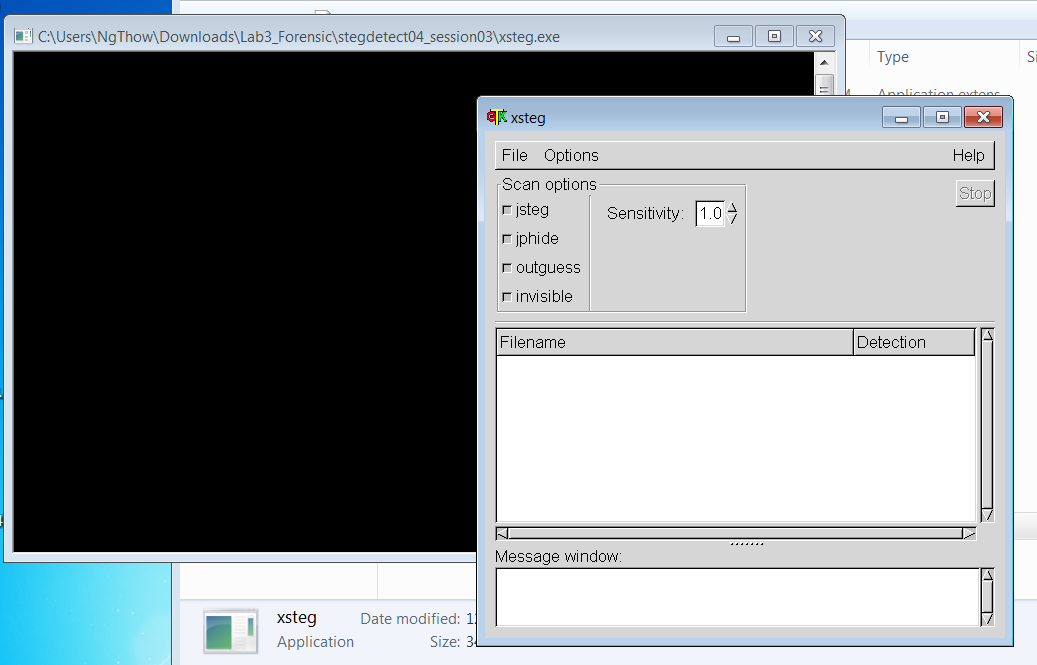
1. **Kịch bản 1c: Phát hiện dữ liệu được giấu trong ảnh JPEG sử dụng**

**StegDetect.**

- Tài nguyên: image\_session03.zip

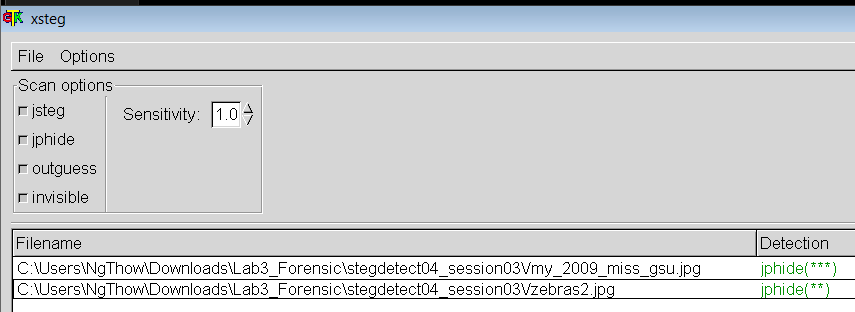
- Công cụ: stegdetect04\_session03.zip. Thực hiện giải nén và chạy file

“xsteg.exe”



- Chọn thư mục chứa ảnh cần phân tích. Thực hiện quét và đưa ra kết

quả, nhận xét.



Có 2 file được xác nhận là có giấu tin.

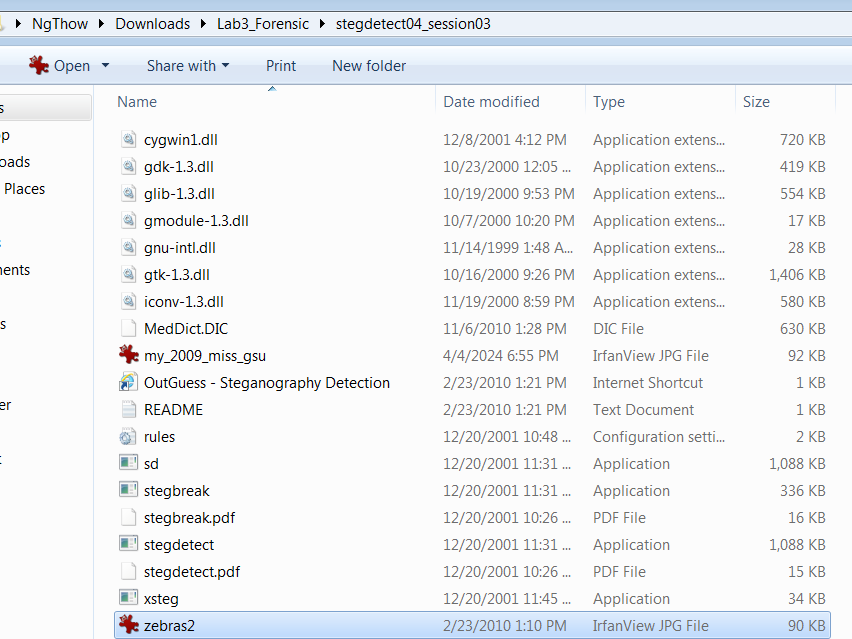
- Thực hiện bẻ khóa mật khẩu trong quá trình giấu tin. (Chuẩn bị:

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?

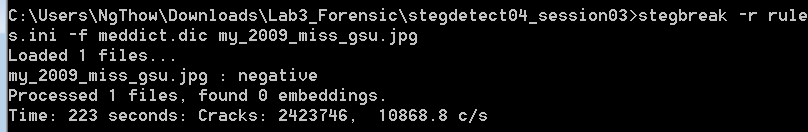
Chuyển 3 file về cùng 1 thư mục:



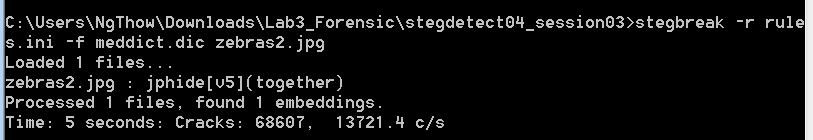
Thử mật khẩu với file ảnh để giải mã thông tin bằng cách sử dụng câu lệnh sau và scan từng file:

*stegbreak -r rules.ini -f meddict.dic my\_2009\_miss\_gsu.jpg*

File đầu tiên không có kết quả:



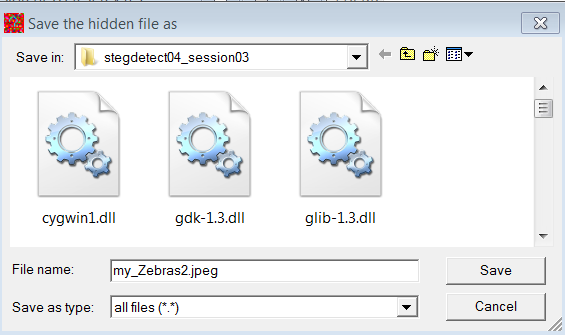
File thứ 2 tìm được password là “together”:



- Giải nén thông tin chứa trong file ảnh có phát hiện ẩn giấu thông tin

bằng mật khẩu tìm được:

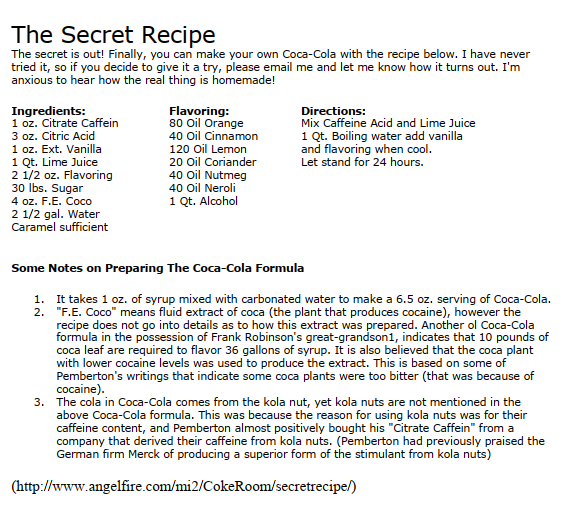
Sử dụng tool Jphswin và password vừa tìm được để seek:



- Mở file vừa giải mã được từ Zebras2.jpeg. Xác định đây có thể là định

dạng file gì? Xem nội dung của file này.

* Em lưu jpeg như trên mà đọc không được trên máy ảo win 7.
* Em chuyển sang pdf, thì lưu và đọc được. Nội dung file như sau:



1. **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).

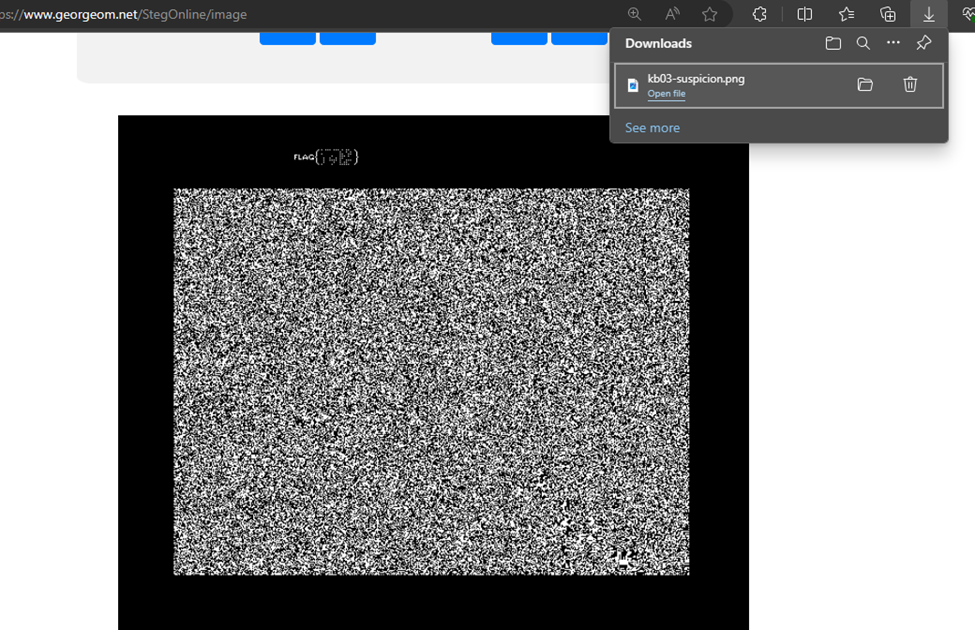
Đáp án:

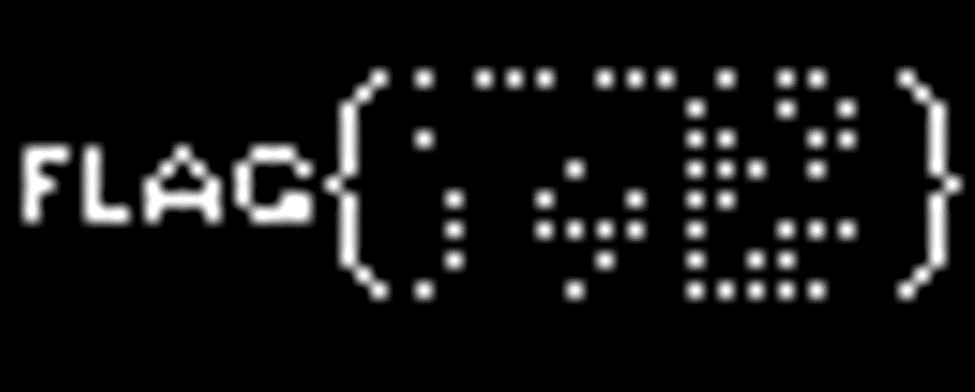
1. **Kịch bản 03. Điều tra thông tin được ẩn giấu**

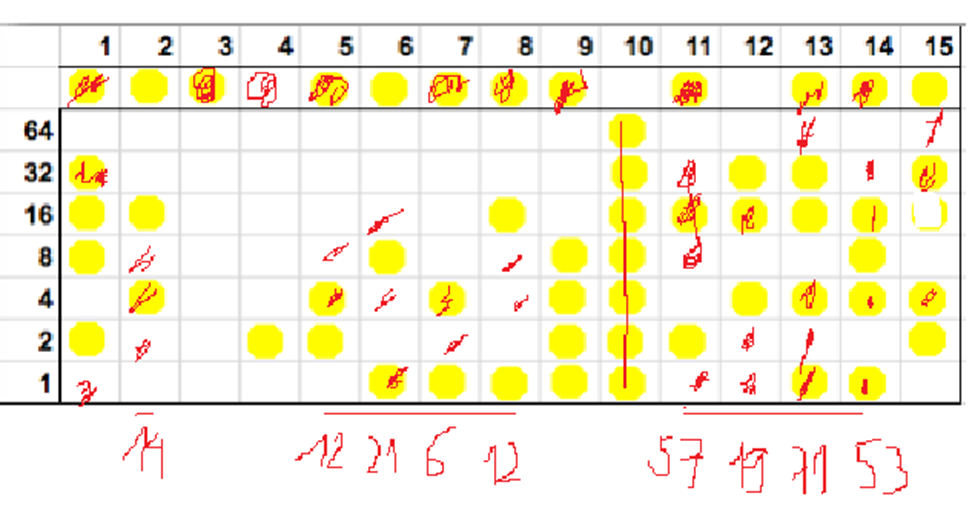
- Tài nguyên: kb03-suspicion.png

- Mô tả: Bức ảnh scan này đã được phục hồi từ các tập tin của một cựu nhân viên của Hiệp hội Ngớ 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:







− Printer Serial Number: 53711957

− Date: 6/21/12 (tức ngày 21 tháng 6 năm 2012)

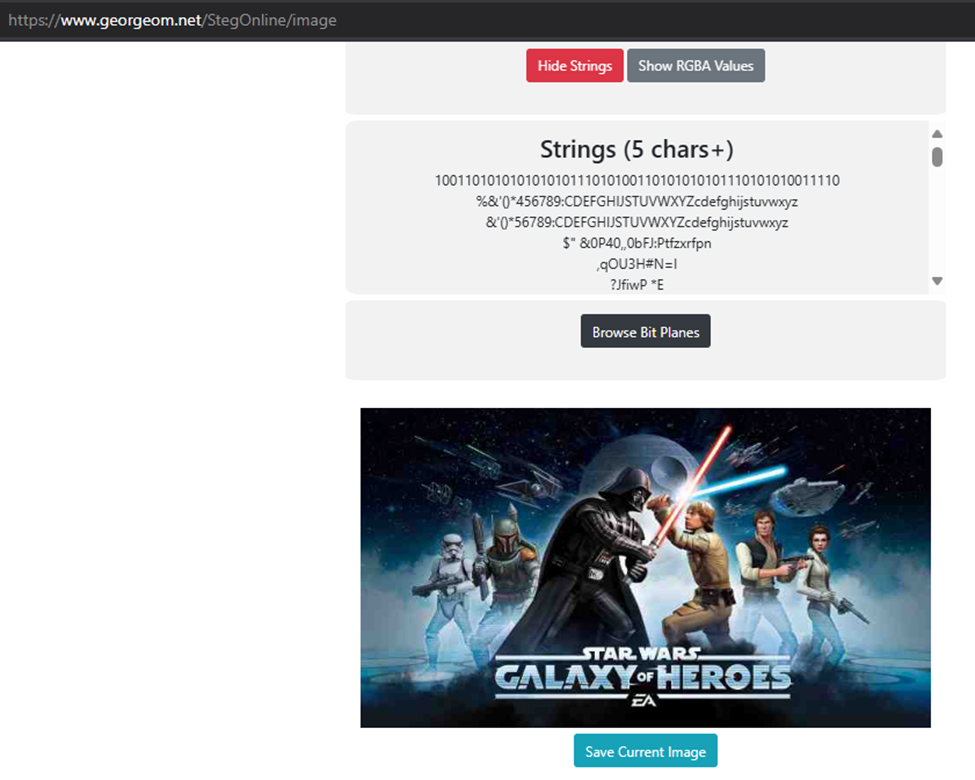
− Time: 12:14

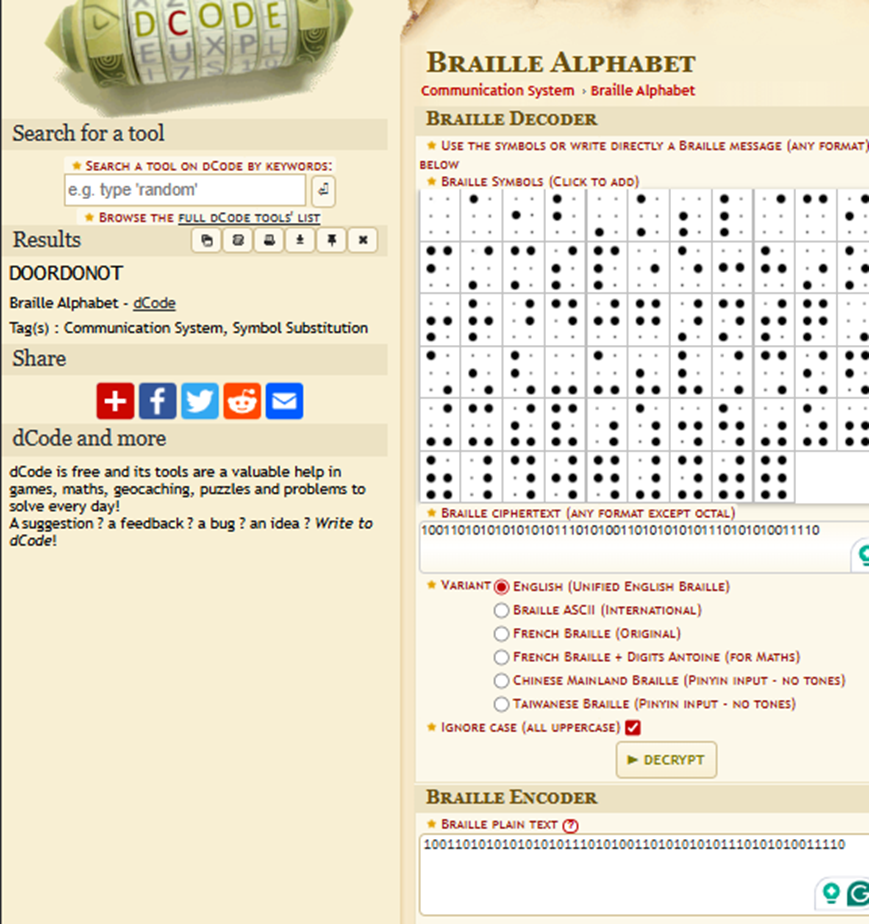
1. **Kịch bản 04. Điều tra thông tin được ẩn giấu**

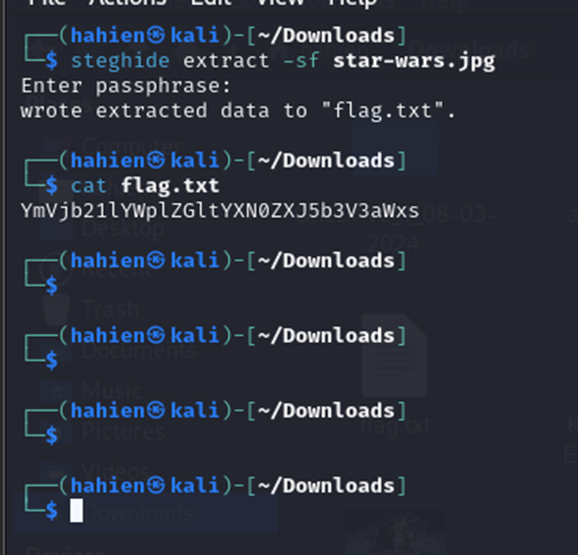
- Tài nguyên: star-wars.jpg

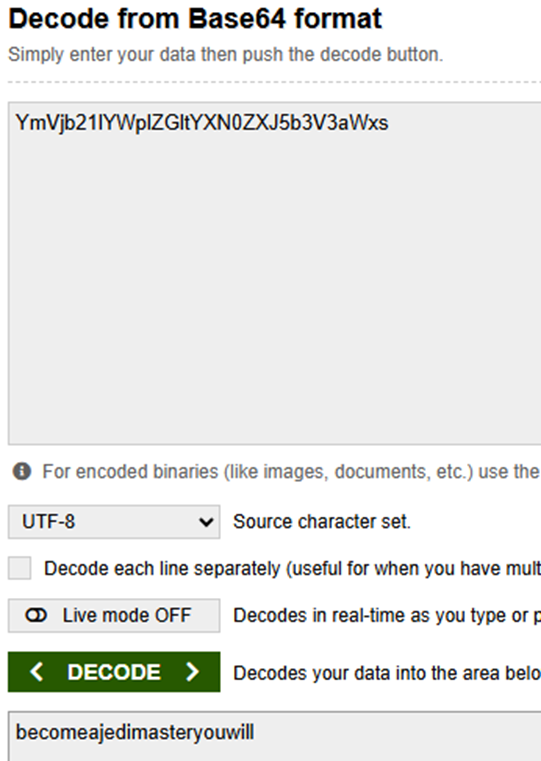
- Yêu cầu – Gợi ý: Bức ảnh được nhân viên điều tra tìm thấy trong một máy tính của một nghi phạm có sở thích xem ảnh của họa sĩ John Bramblitt. Tìm thông điệp được ẩn giấu, biết rằng thông điệp bắt đầu bằng “become”.

Đáp án:









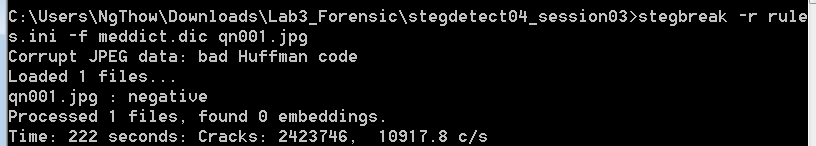
1. **Kịch bản 05. Thực hiện phân tích, tìm thông tin ẩn giấu trong ảnh**

- Tài nguyên thực hiện: qn001.jpg

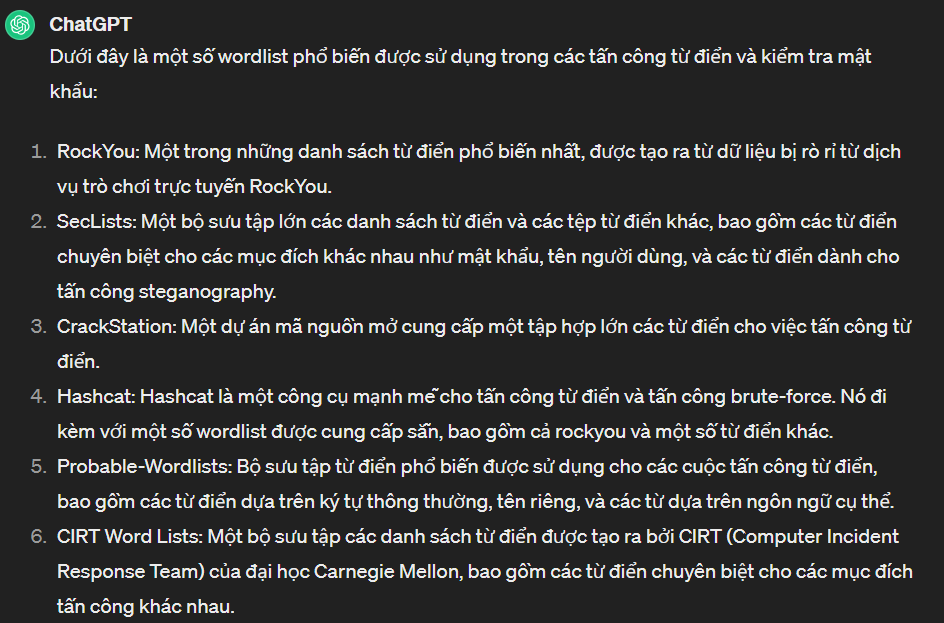
- Yêu cầu – Gợi ý: Tìm thông điệp (flag) được ẩn giấu. Thông tin flag liên quan đến Đội tuyển bóng đá nam Việt Nam.

Đáp án:

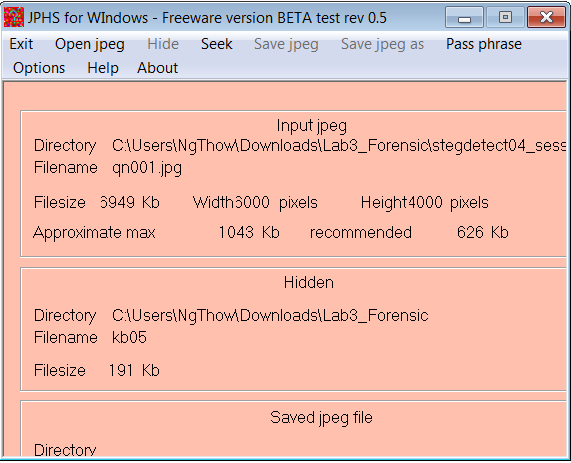
* Để tìm flag giấu trong file, có thể thực hiện bằng chức năng Seek của Jphswin, tuy nhiên cần password. Do đó em sẽ dùng tool stekbread để scan password trước:



Wordlist meddict.dic không in ra được thông tin gì cả. Em tra ChatGPT để tìm wordlist khác:



* Như đề xuất, em sẽ dùng rockyou, kết quả scan chỗ mục password bị trống, tức là Seek không cần pass, chuyển sang Jphswin:



* Em seek và lưu kết quả vào file Kb05, mở trên word được đoạn văn bản phía dưới, tuy nhiên đọc thì flag ở đâu omg@@:



1. 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:

---

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

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, 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]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Exe01\_Group03.*

* 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 nộp.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)