

BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số
Lab 3: Steganography & Steganalysis

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.P11.ANTT.1

Nhóm: N03

| STT | Họ và tên | MSSV | Email |
|-----|---------------------|----------|--|
| 1 | Lê Huy Hiệp | 21522067 | 21522067@gm.uit.edu.vn |
| 2 | Nguyễn Trần Duy Anh | 20520393 | 20520393@gm.uit.edu.vn |

2. NỘI DUNG THỰC HIỆN:¹

| STT | Công việc | Kết quả tự đánh giá |
|-----|--------------------------------------|---------------------|
| 1 | Kịch bản 6 | 100% |
| 2 | Kịch bản 7 | 100% |
| 3 | Kịch bản 8 | 100% |
| 4 | Kịch bản 10 | 100% |
| 5 | Kịch bản 1,3,4,5,9 (đã làm trên lớp) | 100% |

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

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

BÁO CÁO CHI TIẾT

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:

Sử dụng xsteg để quét



Không phát hiện gì trong file tiengiang003.jpg

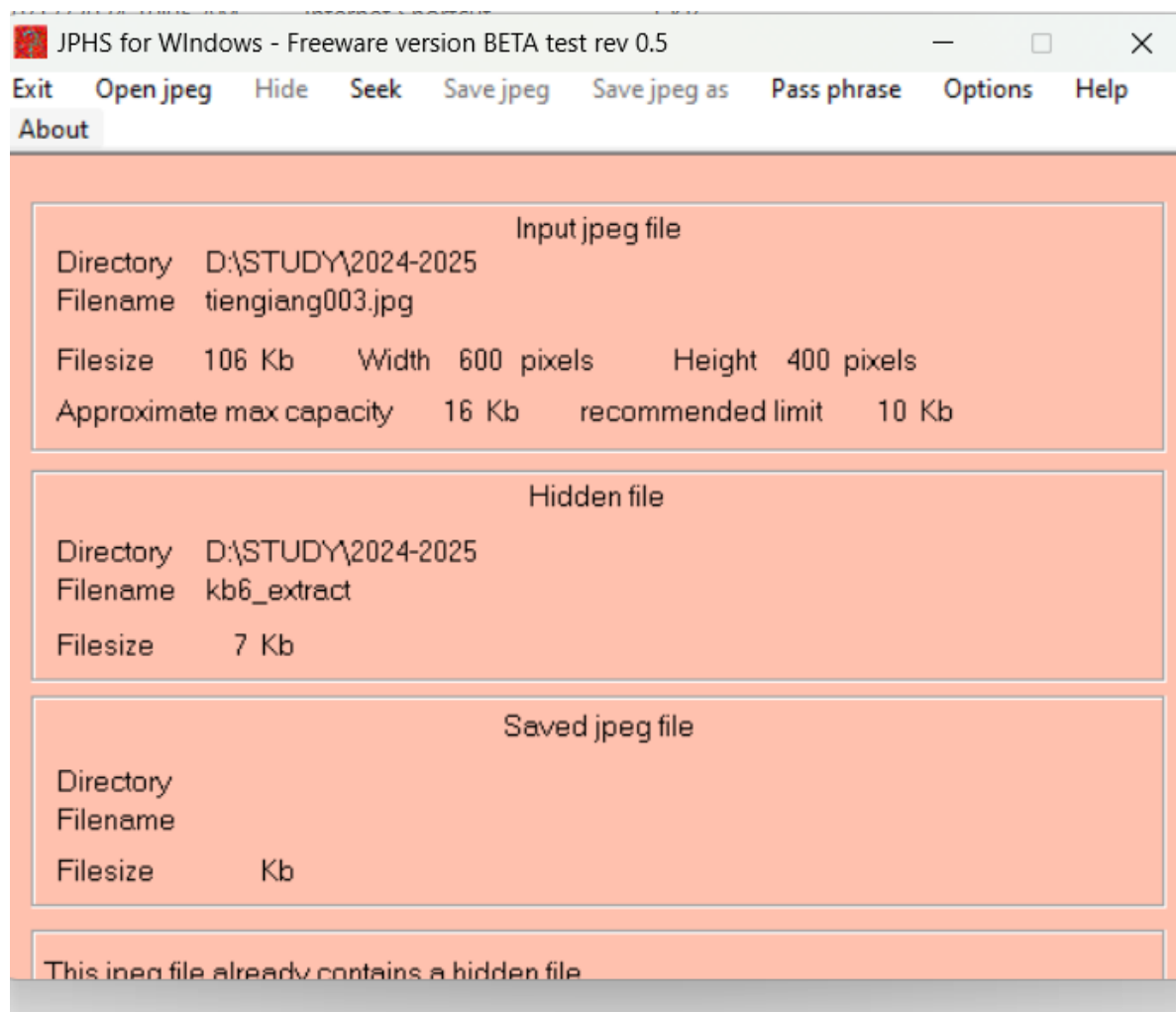
Sử dụng StegSolve và strings cũng không phát hiện gì bất thường

Sử dụng stegbreak.exe


```
PS D:\STUDY\2024-2025 UIT\phapchung\Lab03-Steganography\RES-Steganography\OneDrive-2024-10-16\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: 0 seconds: Cracks: 4751, Inf c/s
PS D:\STUDY\2024-2025 UIT\phapchung\Lab03-Steganography\RES-Steganography\OneDrive-2024-10-16\session03-resources\stegdetect04_session03> |
```

Thấy được trong đây còn nhúng một tệp khác và không có mật khẩu

Sử dụng JPHS để trích xuất file



File đã trích xuất:

| | | | |
|---|--------------------|------|------|
|  kb6_extract | 10/21/2024 5:57 PM | File | 7 KB |
|---|--------------------|------|------|

Mở file này lên:



Sử dụng strings để đọc biểu diễn dưới dạng chuỗi, phát hiện dòng ***“wherE ShOUld onE ReaLly lOoK fOr tHis flag”***

```
jg3U
c)U>
IEND
wherE ShOUld onE ReaLly lOoK fOr tHis flag

(kali㉿kali)-[~/hiep/phapchung/Lab3]
$
```

Dựa vào gợi ý đề bài “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*.” Tìm được thuật toán mã hóa **Bacon Cypher** dựa trên hai kí tự A và B và sử dụng bảng thay thế.

| | | | |
|-----|-------|-----|-------|
| A | AAAAA | B | AAAAB |
| C | AAABA | D | AAABB |
| E | AABAA | F | AABAB |
| G | AABBA | H | AABBB |
| I=J | ABAAA | K | ABAAB |
| L | ABABA | M | ABABB |
| N | ABBAA | O | ABBAB |
| P | ABBBA | Q | ABBBB |
| R | BAAAA | S | BAAAB |
| T | BAABA | U=V | BAABB |
| W | BABAA | X | BABAB |
| Y | BABBA | Z | BABBB |

Thay thế chữ cái thường bằng 'A' và chữ cái hoa bằng 'B':

AAAAB BABBAA AAB BAABAA ABAA ABA ABAA AAAA

Dùng tool giải mã ta được:



Flag là: **BYDEITA**

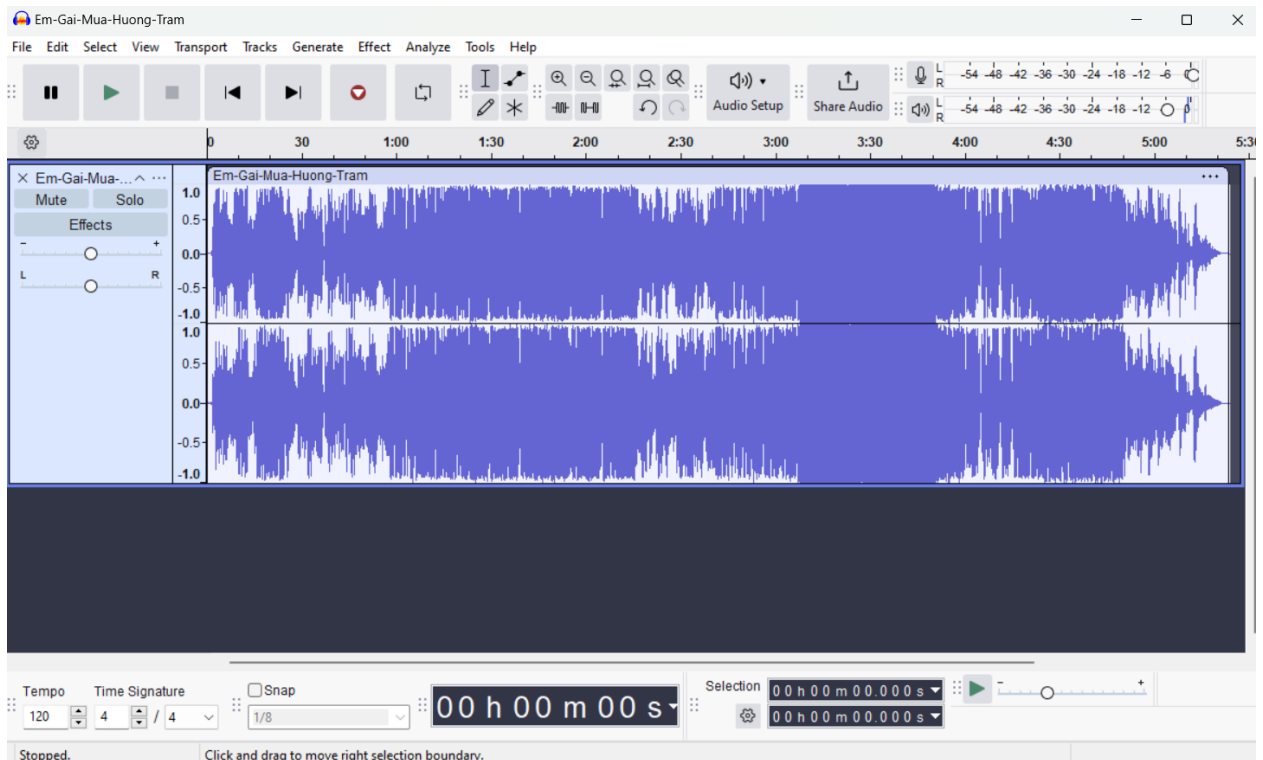
Kịch bản 7:

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

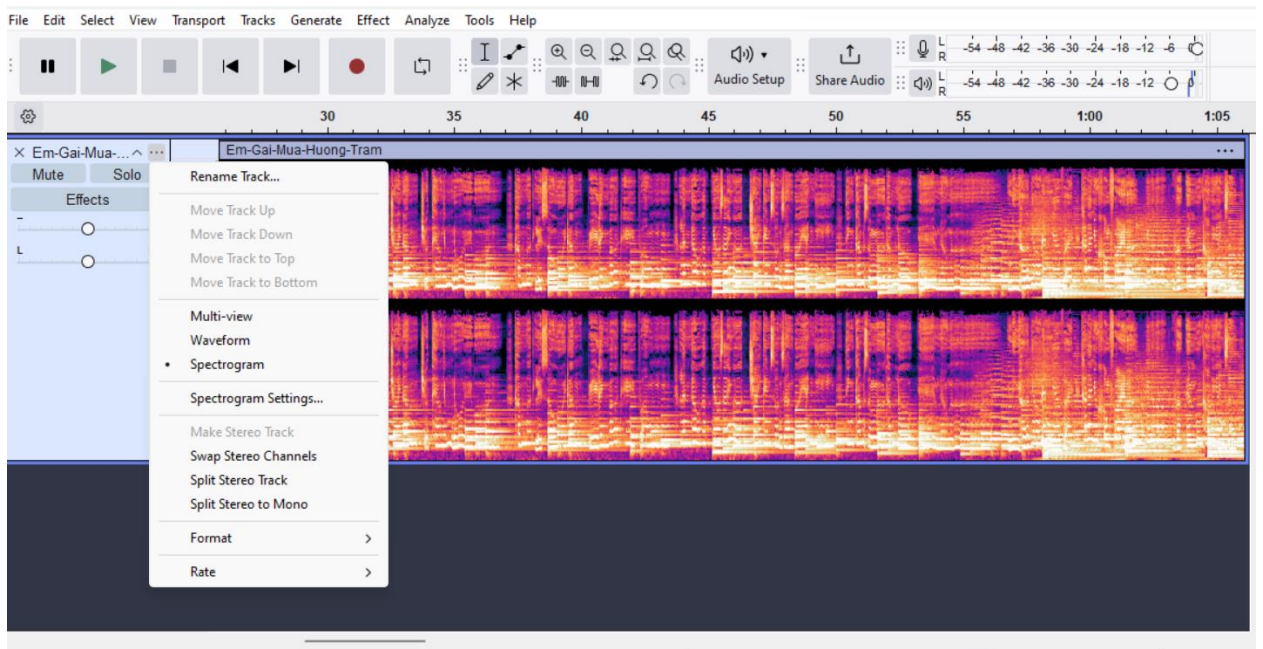
- Tài nguyên: kb07-res (Tìm thông tin ẩn giấu trong Em-Gai-Mua-Huong-Tram.mp3, capture-the-flag.png)

Đáp án:

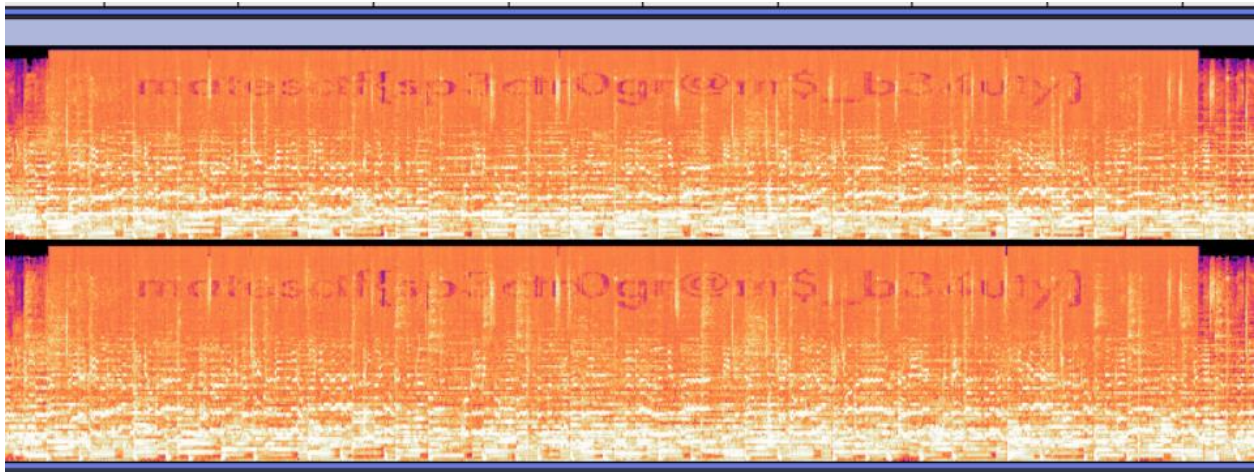
Sử dụng **Audacity**: Phần mềm chỉnh sửa âm thanh miễn phí và mã nguồn mở, cho phép bạn tạo và phân tích biểu đồ tần số âm thanh dễ dàng. Audacity cung cấp các công cụ mạnh mẽ để xử lý và hiển thị các tín hiệu âm thanh.



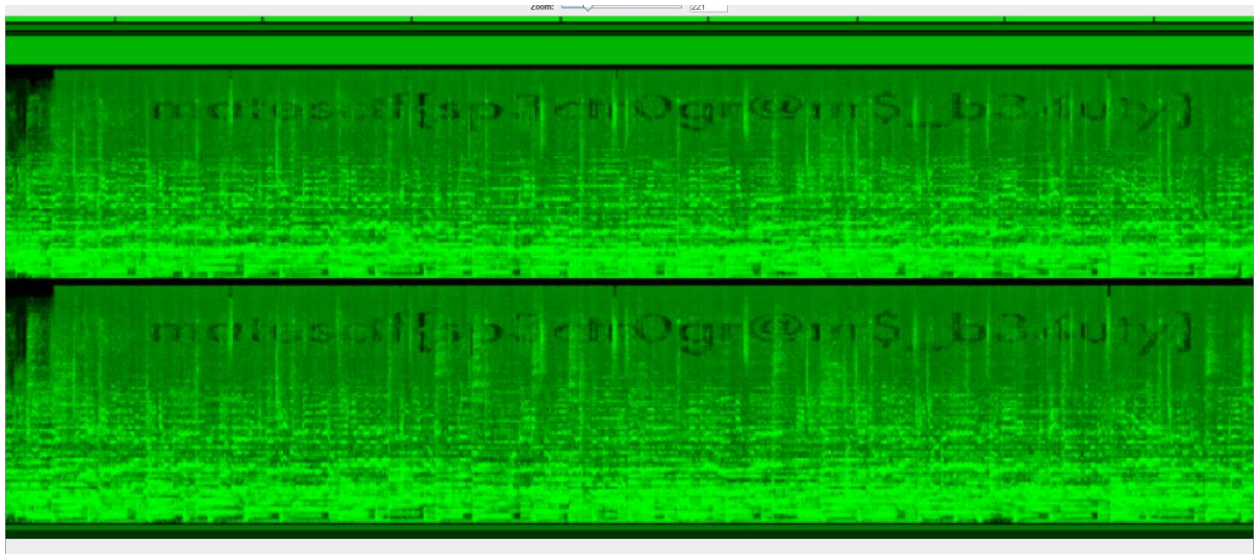
Xem ở chế độ spectrogram:



Phát hiện



Đổi màu cho dễ nhìn



Flag: `matesctf{sp3ctrOgr@m$_b34uty}`

Kịch bản 8:

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>

Mở file LoveLetter.txt lên thì ta thấy có những ký tự đáng chú ý

```
(kali@kali) ~/Desktop
$ 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-Tongued 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 anyway. Did you know that a monkey is either going to be a Cereopithecoid or a Platyrrhine? It's true! and there are 264 species of monkey that are known. Sure is a lot of them! But skinks are also cool, there are over 1200 different 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.
```

Sử dụng lệnh xxd để xem file dưới dạng hex, ta thấy khoảng cách có kí tự 0x20, nhưng có kí tự khác thay dấu cách là 0xa0

```
$ 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.
```

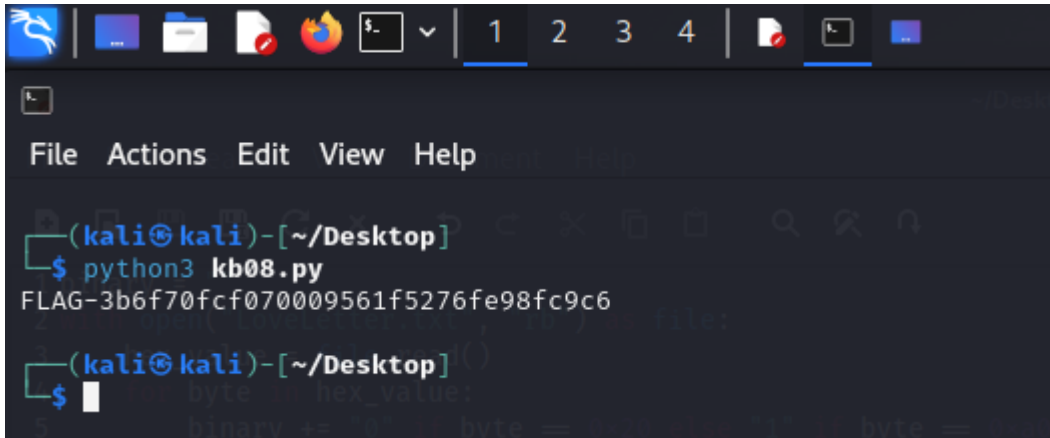
Ta thử gán giá trị 0x20 là 0 còn 0xa0 là 1 thì ta lấy được 1 chuỗi 24 bit như sau:
01000110 01001100 01000001 01000111

Dịch chuỗi này bằng cách tra cứu các ký tự ASCII ta có được từ FLAG.

Đây có thể là thông điệp chúng ta cần tìm nên viết thử đoạn code python tìm FLAG

```
1 binary = ""
2 with open("LoveLetter.txt", "rb") as file:
3     hex_value = file.read()
4     for byte in hex_value:
5         binary += "0" if byte == 0x20 else "1" if byte == 0xa0 else ""
6
7 char=[]
8 for i in range(0, len(binary), 8):
9     byte = binary[i:i + 8]
10    char_code = int(byte, 2)
11    character = chr(char_code)
12    char.append(character)
13
14
15 output = ''.join(char)
16
17 print(output)
18
```

Ta ra được kết quả: FLAG-3b6f70fcf070009561f5276fe98fc9c6



```
(kali㉿kali)-[~/Desktop]
$ python3 kb08.py
FLAG-3b6f70fcf070009561f5276fe98fc9c6

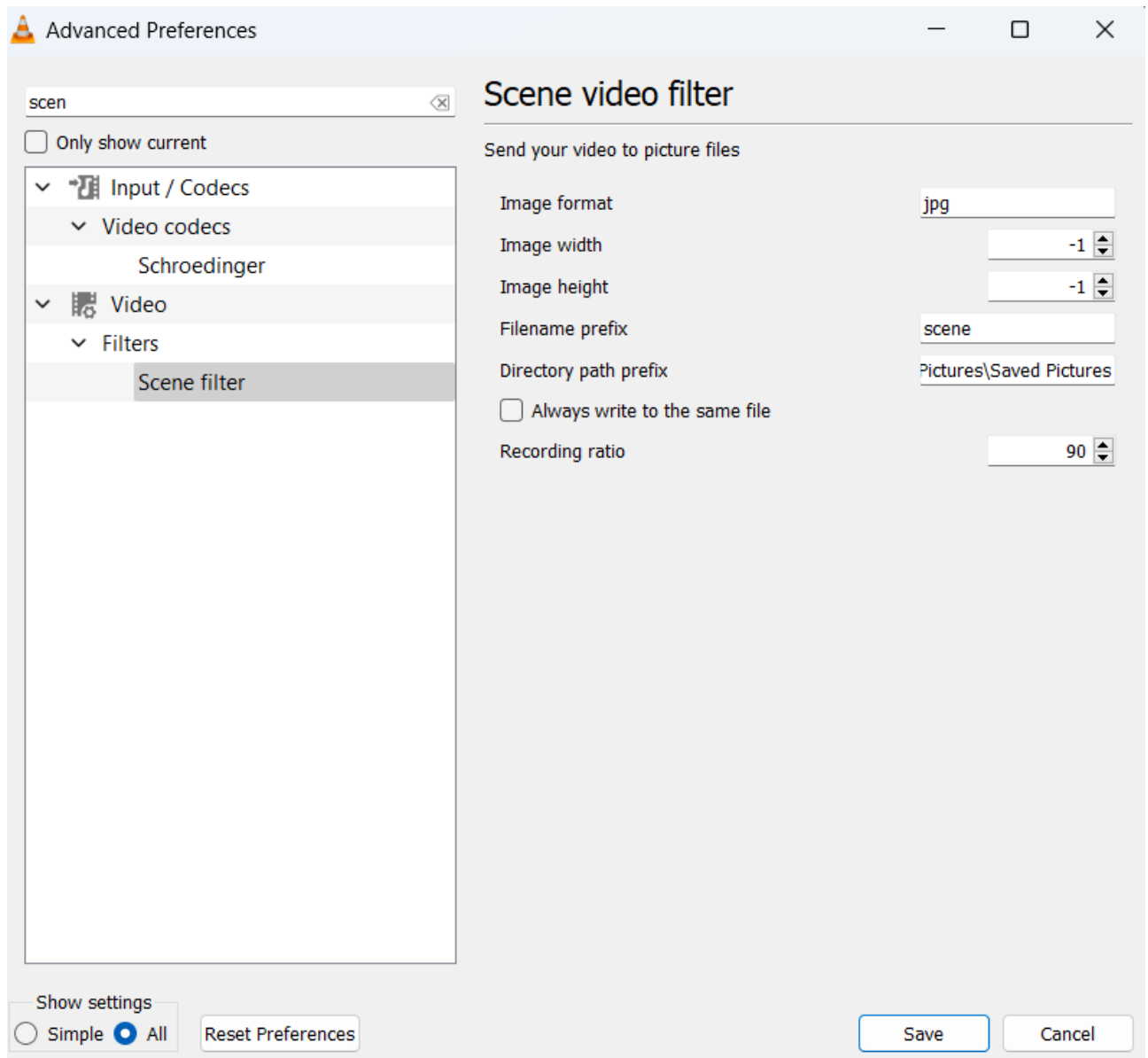
(kali㉿kali)-[~/Desktop]
$
```

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

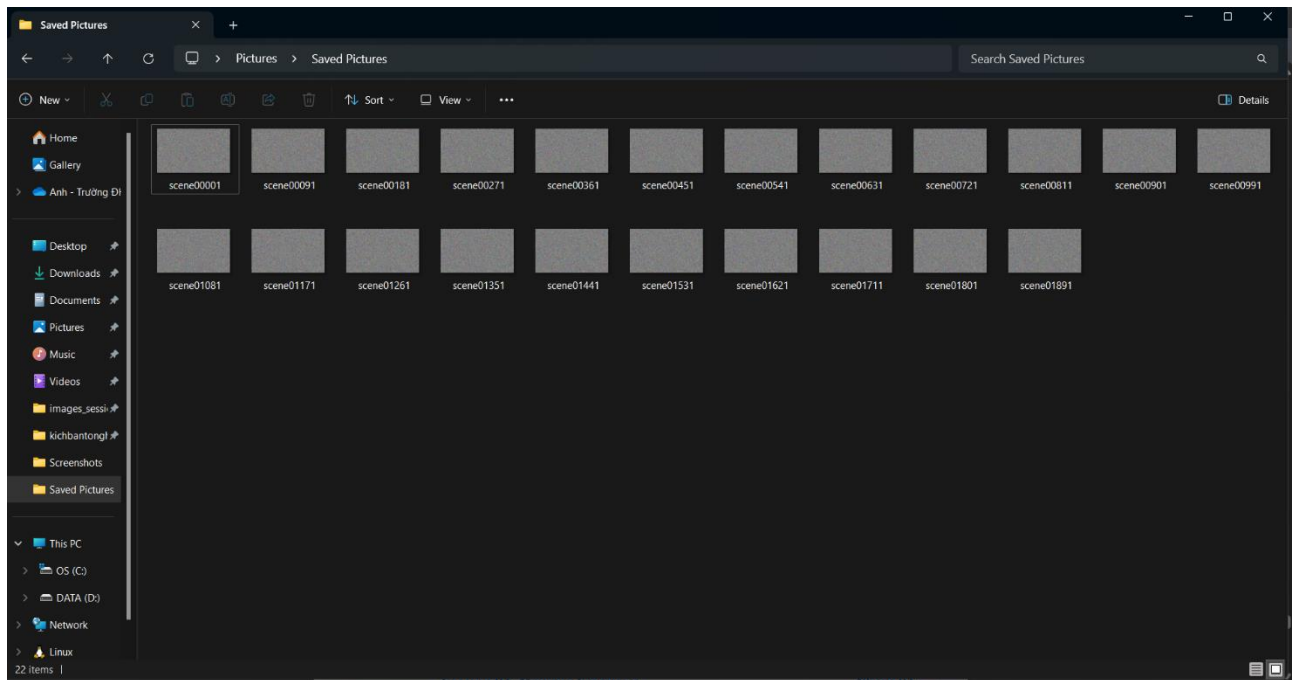
- Tài nguyên: thecatreturns.mp4
- Yêu cầu – Gợi ý: Tìm sự khác biệt giữa các khung hình (frame) trong đoạn phim đã cho. Chuyển nội dung đoạn phim thành các khung hình để phân tích. Công cụ ffmpeg, ImageJ.

Đáp án:

Để tìm ra sự khác biệt giữa các khung hình, ta sử dụng công cụ VLC media player. Sau đó mở Tools\ Preferences, chọn All ở góc dưới trái của tab để mở Advanced Preferences, tìm Scene Filter như trong hình, setting như trong ảnh.



Chạy video, công cụ sẽ tự động cắt frame lưu vào thư mục đã chọn



Sử dụng trang web [Compare images to find their differences - Diffchecker](#) để so sánh từng ảnh tìm sự khác biệt



Khi so sánh đến ảnh scene00001.jpg và scene00181.jpg ta thấy được thông tin cần tìm: SCTF{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 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, trộm, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT