BÁO CÁO THỰC HÀNH

**Môn học: Pháp chứng kỹ thuật số**

**Lab 3: Steganography & Steganaly**

*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 1-4 (đã báo cáo ở lớp) | 100% |
| 2 | Kịch bản 5 | 100% |
| 3 | Kịch bản 6 | 100% |
| 4 | Kịch bản 7 | 100% |
| 5 | Kịch bản 8 | 100% |
| 6 | Kịch bản 9 | 100% |
| 7 | Kịch bản 10 | 100% |

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

BÁO CÁO CHI TIẾT

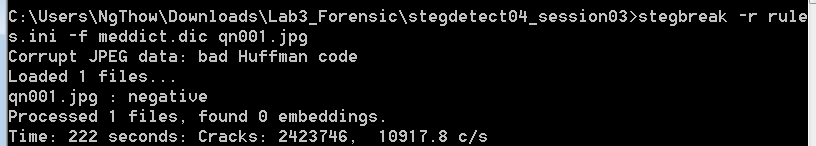
## **Kịch bản 5:**

- Tài nguyên thực hiện: qn001.jpg

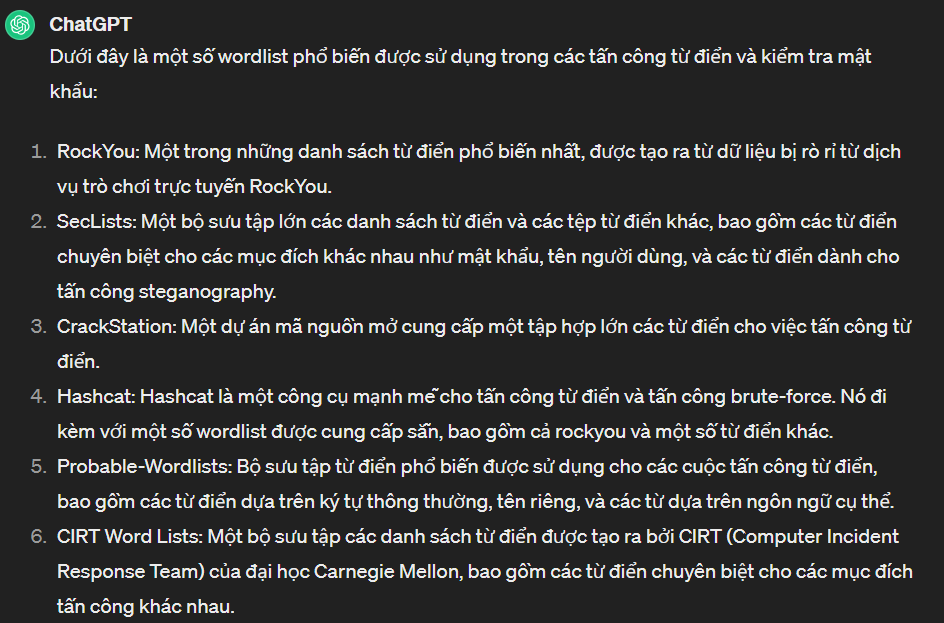
- Yêu cầu – Gợi ý: Tìm thông điệp (flag) được ẩn giấu. Thông tin flag liên quan đến Đội tuyển bóng đá nam Việt Nam.

Đáp án:

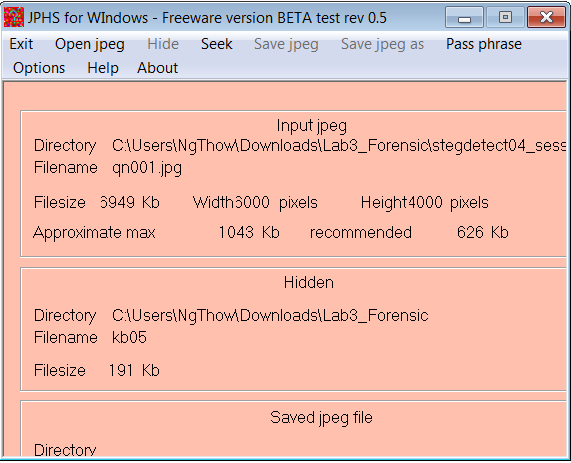
* Để tìm flag giấu trong file, có thể thực hiện bằng chức năng Seek của Jphswin, tuy nhiên cần password. Do đó em sẽ dùng tool stekbread để scan password trước:



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



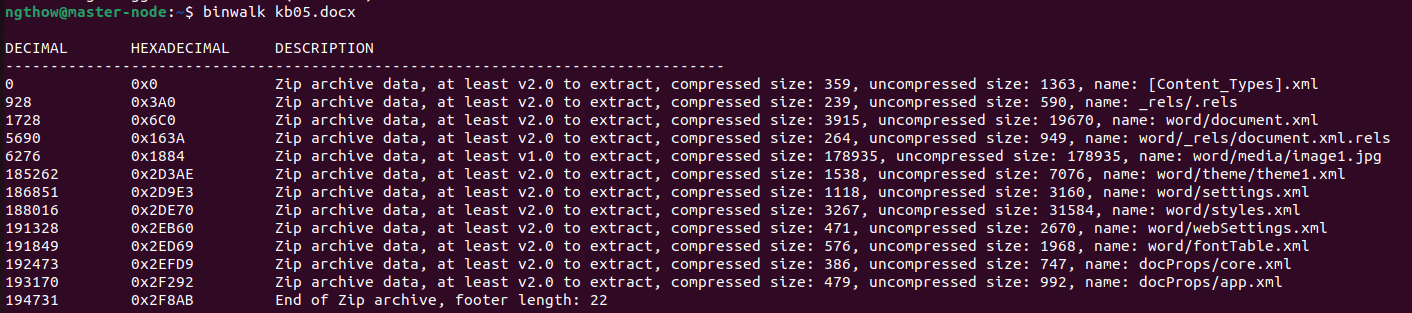
* Như đề xuất, em sẽ dùng rockyou, kết quả scan chỗ mục password bị trống, tức là Seek không cần pass, chuyển sang Jphswin:



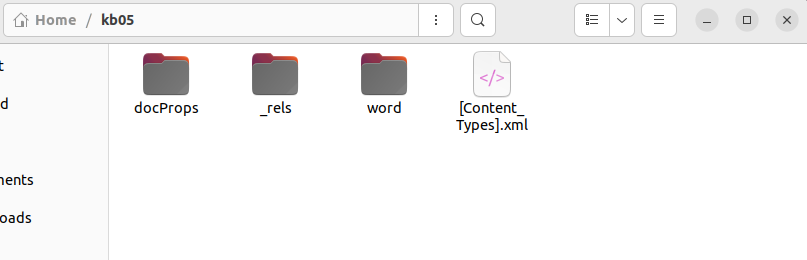
* Em seek và lưu kết quả vào file Kb05, mở trên word được đoạn văn bản phía dưới, tuy nhiên đọc thì flag ở đâu omg@@:



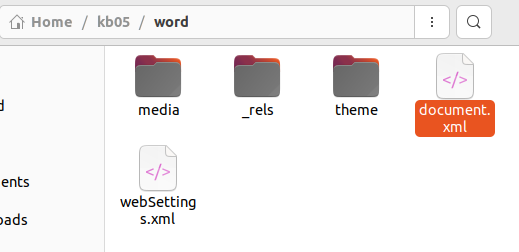
* Thử kiểm tra xem có file ẩn trong file doc này không bằng **binwalk**:



* File doc thực tế được nén theo định dạng zip. Do đó để mở được nội dung bên trong, em sẽ đổi đuôi file thành .zip và extract. Thu được:



* Sau khi mở lần lượt các file, tìm được file *document.xml* có nội dung được encode dưới dạng branfuck:





* Làm gọn đoạn văn bản trên để quy về brainfuck, nằm trong cặp <w> </w> với “&gt;” thay thế bằng “>” và “&lt” thay thế bằng “<”, được đoạn brainfuck như sau:

++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>.>+++++++++++.+++.-------------.+++++++++.+++++.----------.------.++++++++++++++++.<<++++++++++++++++++.+++++.>------.+++++++++++++++++++++.------------.+++++++++++.>++++++++.<++.>------------------.----.+++++++++++++++.------.<+++++++++++.>-.<

<--------

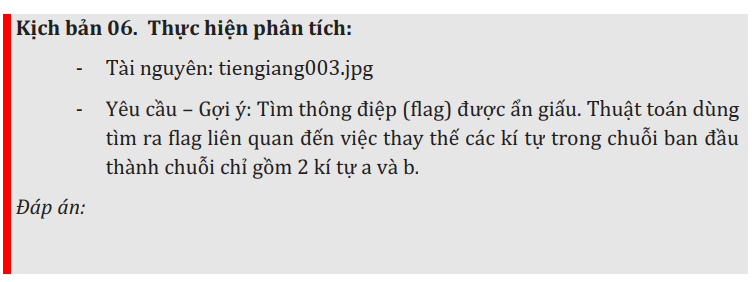
.>>++++++++++.<++++++++.+++++.<.++++++++++++++++++++++.>-------------.>----------.<+.>++.<++.+++++.--------.>++++++++++++++

* Dùng tool để decode, được kết quả:

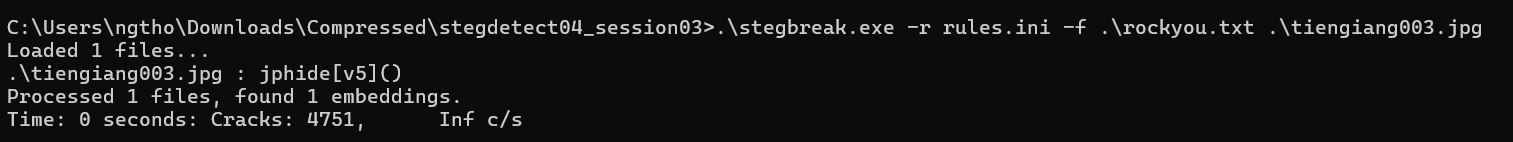


Vậy flag là: **Forensics05@UIT{Vietnam-win-Cambodia}**

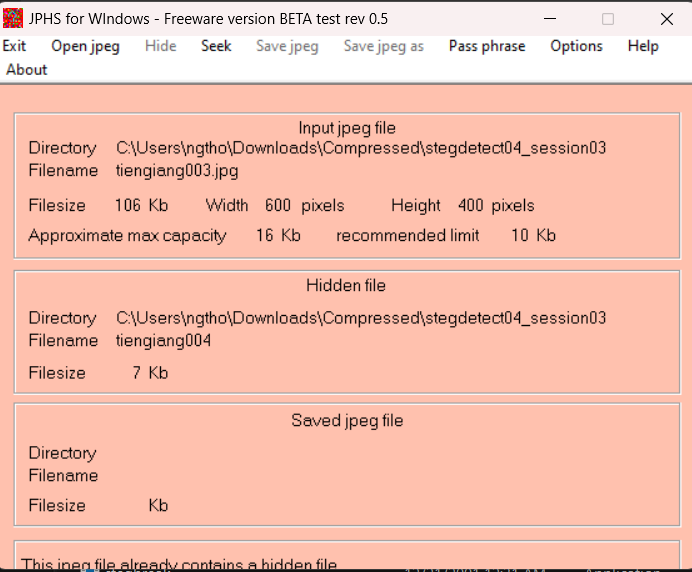
## **Kịch bản 6:**



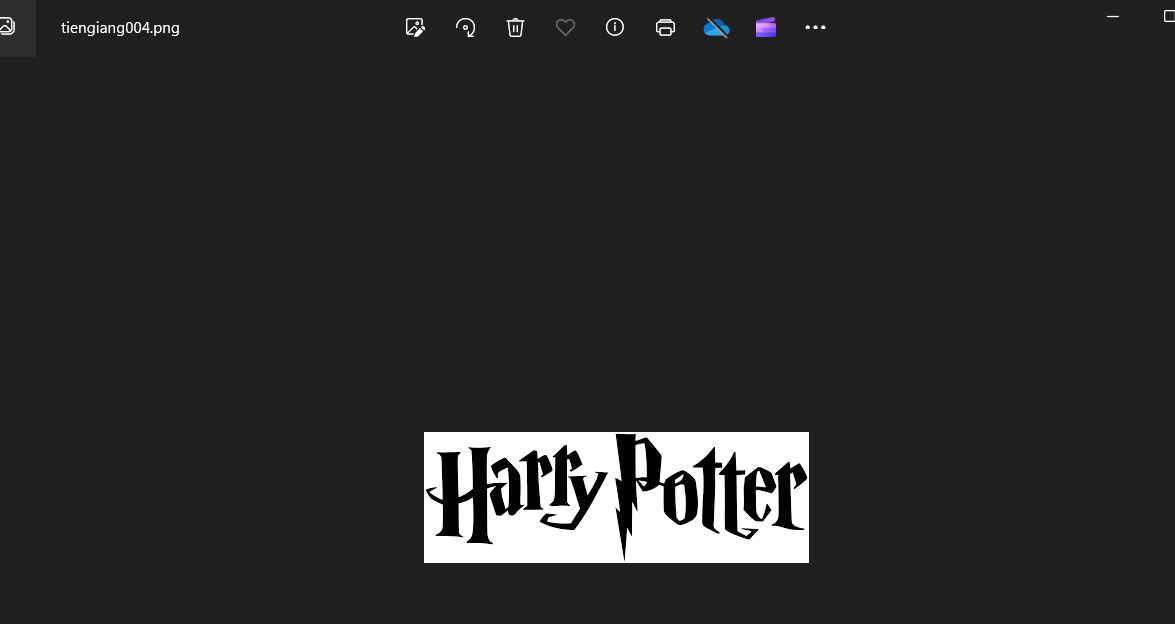
* Kiểm tra file bằng stegbreak, biết được trong file ảnh tiengiang003.jpg có nhúng một file khác:



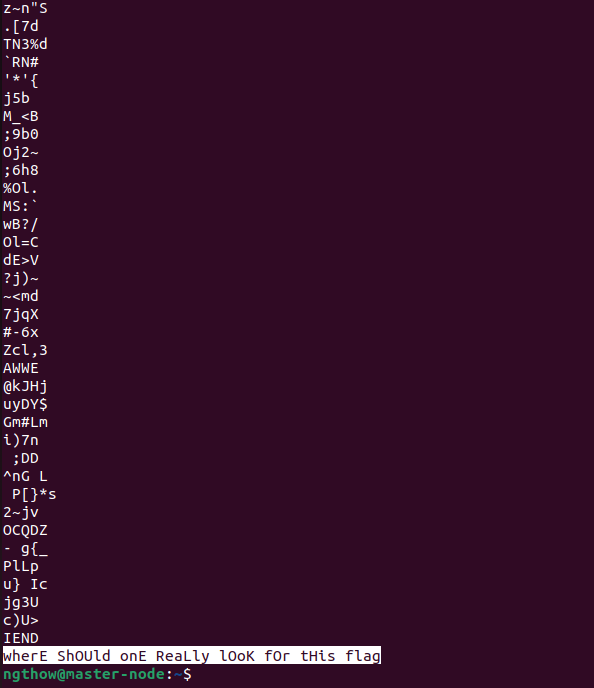
* Dùng JPHS để trích xuất file ảnh, do không có password nên Seek sẽ để trống phần password:



* File trích xuất được em lưu là *tiengiang004*, sau khi thử thay đổi file với các đuôi khác nhau, thì đến png sẽ mở được file:



* Dùng *strings* để tìm chuỗi trong file, tìm được chuỗi sau:



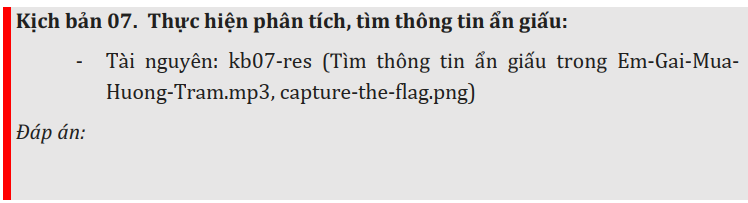
* Đề bài có gợi ý “Thuật toán dùng tìm ra flag liên quan đến việc thay thế các kí tự trong chuỗi ban đầu thành chuỗi chỉ gồm 2 kí tự a và b.”, nên đây có thể là kỹ thuật Bacon Cipher chỉ biểu diễn dưới dạng A và B. Nếu “A” là chữ in thường, “B” là chữ in hoa thì được:

AAAAB BABBAA AAB BAABAA ABAB ABA ABAA AAAA

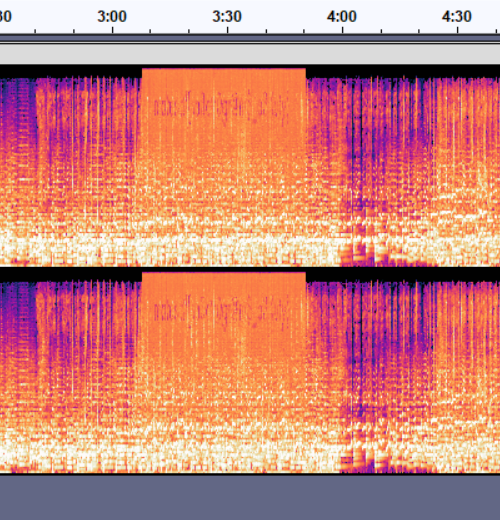
* Dùng tool để giải mã, được flag là: BYDELTA



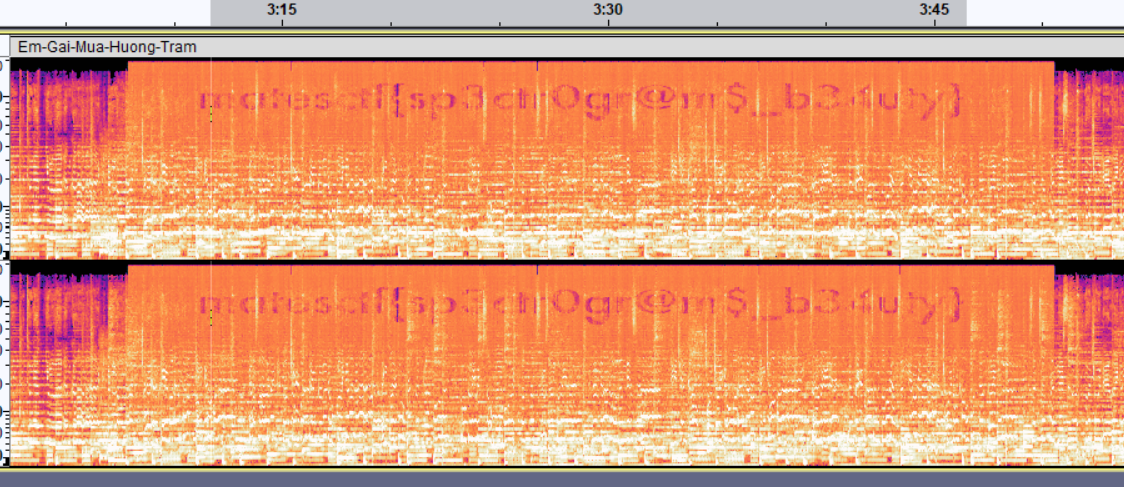
1. **Kịch bản 7:**



* Để kiểm tra file âm thanh, em dùng tool Audacity. Mở file sau đó chọn chế độ Spectrogram, ta sẽ thấy beat hiện lên dưới dạng biểu đồ màu sắc. Có một đoạn của biểu đồ dường như là chữ xuất hiện:



* Flag: **matesctf{sp3ctrOgr@m$\_b34uty}**



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

A screenshot of a computer

Description automatically generated

* Bây giờ, ta có tài nguyên là LoveLetter.txt thì chúng ta sẽ xem trong đó có gì trước:

A close up of a text

Description automatically generated

* Ta nhận thấy thông tin về dấu cách không bình thường. Có thể có thứ chúng ta cần khai thác ở những dấu cách bình thường và những dấu cách đặc biệt trên.
* Dưới đây là một chương trình Python để giải mã một chuỗi ký tự được đánh dấu, trong đó dấu cách các ký tự đặc biệt được đánh dấu là 1 và các dấu cách thông thường được đánh dấu là 0. Sau đó, chương trình thực hiện chuyển đổi chuỗi nhị phân thành dạng decimal và sử dụng hàm unhexlify từ thư viện binascii để chuyển đổi lại thành chuỗi ban đầu.

A screen shot of a computer

Description automatically generated

* Chạy code và xem kết quả:

A screenshot of a computer program

Description automatically generated

* FLAG: b'FLAG-3b6f70fcf070009561f5276fe98fc9c6'

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

A screenshot of a computer

Description automatically generated

* Đầu tiên, mở xem tài nguyên ảnh transmission xem sao:

A screenshot of a computer screen

Description automatically generated

* Ta nhận thấy rằng, màu sắc của ảnh này chưa chính xác là màu ảnh bình thường được biểu diễn theo 3 màu RGB (Red, Green, Blue).
* Bây giờ ta sẽ thực hiện chuyển đổi ảnh sang định dạng màu RGB bằng code python sau đây:

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated

* Bây giờ, hãy cùng xem ảnh mới được convert xem có gì khác biệt:

A screenshot of a computer screen

Description automatically generated

* FLAG: {Cooper\_Brand}

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

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

* Bật lại video và xem, sau đó kiểm tra đường dẫn xem đã có ảnh chưa

A screenshot of a computer

Description automatically generated

* Dùng took <https://www.diffchecker.com/> để thực hiện kiểm tra
* Giữa ảnh 1 và 91

A screenshot of a computer

Description automatically generated

* Giữa ảnh 1 và 81

A screenshot of a computer

Description automatically generated

* 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 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)