BÁO CÁO THỰC HÀNH

**Môn học: Pháp chứng kỹ thuật số**

**Lab 6: CTF challenges cuối kỳ**

*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 | 75% |
| 2 | Kịch bản 2 (còn câu g) | 100% |
| 3 | Kịch bản 3 (đã hoàn thành trên lớp) | 100% |
| 4 | Kịch bản 4 | 100% |

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

BÁO CÁO CHI TIẾT

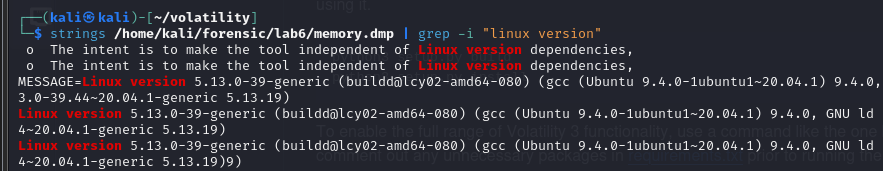
**1. Memory (Easy to Hard):**

* 1. *memory.dmp* - Có một command chứa thông báo lạ trong bash history, liệu bạn có thể khôi phục thông báo đó? Bạn phải xây dựng volatility và tìm profile.

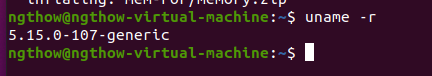
Tham khảo: <https://illuad.fr/2020/11/26/writeup-dga-ctf-bwing.html>

* Như thói quen thì em sẽ thực hiện *imageinfo* để kiểm tra thông tin của file. Tuy nhiên, quét rất lâu nhưng không hiện kết quả. Theo link tham khảo thầy cung cấp, em tìm được một số thông tin hữu ích về hệ điều hành và version của kernel như sau:

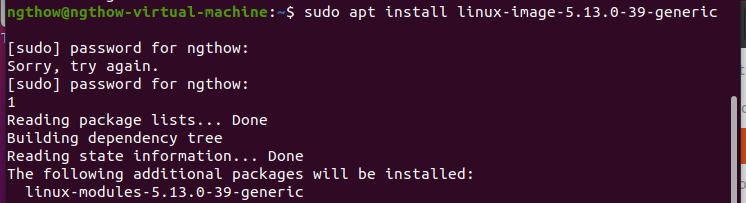


Một máy Ubuntu 20.04.2 LTS với kernel 5.13.0-39-generic

* Em chuyển sang máy Ubuntu 20.04.2 LTS để làm tiếp:



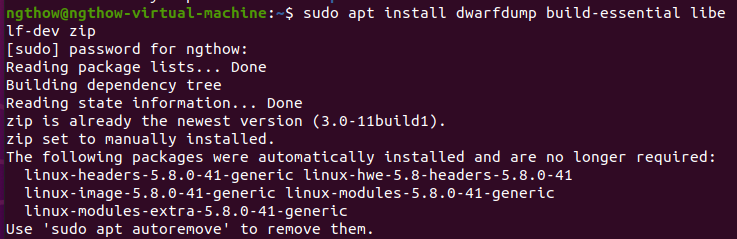
* Cài đặt kernel mới:



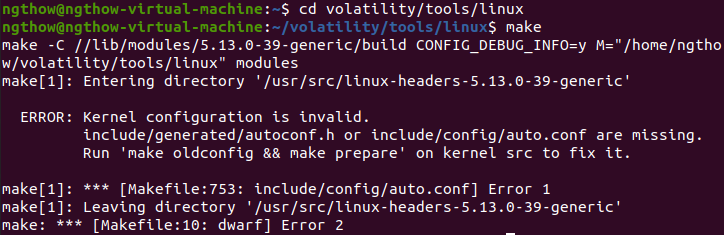
* Kiểm tra cài đặt thành công chưa:



* Cài đặt những tiện ích cần thiết:



* Tuy nhiên lỗi mà fix chưa được ạ!

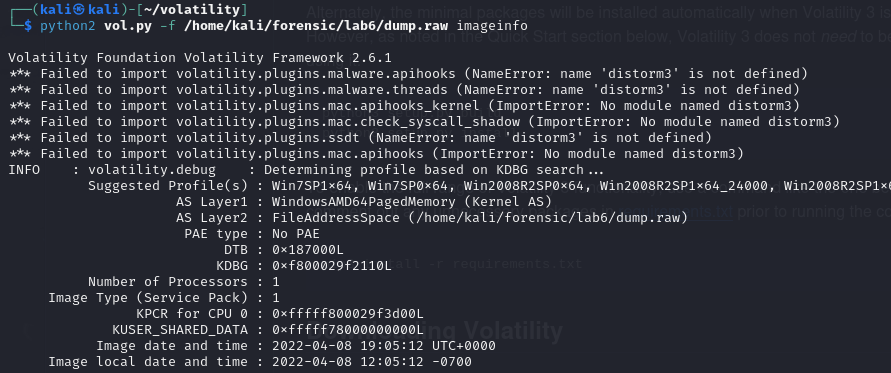


* 1. ***dump.raw* - Dường như đã có hành vi bất thường trên laptop của NHK, bạn có thể giúp chúng tôi điều tra:**

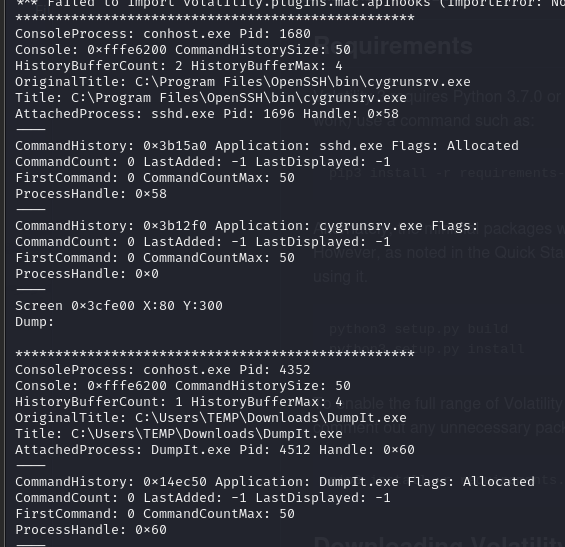
**+ Thu thập các file bất thường để ghép mảnh flag.**

Đáp án:

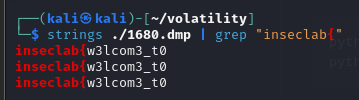
* Xác định hệ điều hành, là *Win7SP1x64*:



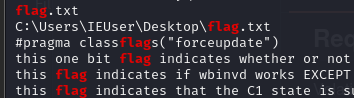
* Dùng plugin *consoles* thì em xem được có 2 tiến trình đáng ngờ, em xem PID 1680 trước:



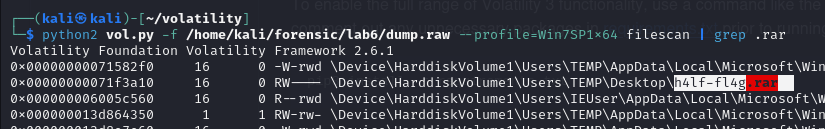
* Tìm chuỗi trong file *1680.dmp* với từ khóa ***inseclab{***, em tìm được mảnh flag đầu tiên:



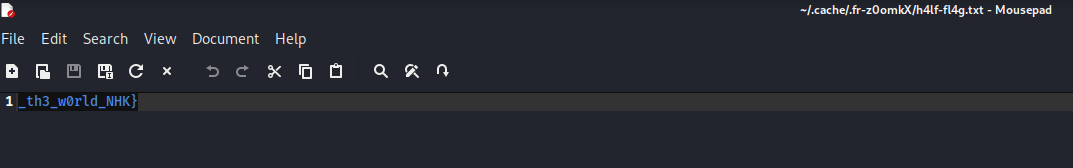
* Hơn nữa, trong quá trình tìm kiếm với từ khóa *flag*, em tìm được đường dẫn đến tệp *flag.txt:*



* Tìm file theo định dạng .rar, em thu được kết quả, đây có lẽ là file chứa phần còn lại của flag:



* Sau khi dump file, file yêu cầu mật khẩu để giải nén. Em dùng **JohnTheRipper** với *rockyou* để tìm pass.
* Tìm được password là **r0cky0u,** flag:



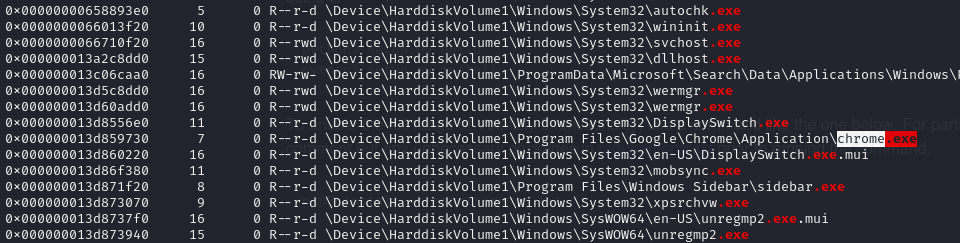
=> flag: **inseclab{w3lcom3\_t0\_th3\_w0rld\_NHK}**

* 1. *Tiktoor-Erawlam.raw* - A critical document has been encrypted for some reason. Know that he always uses the same password. As an incident investigator, can you investigate and recover the file?

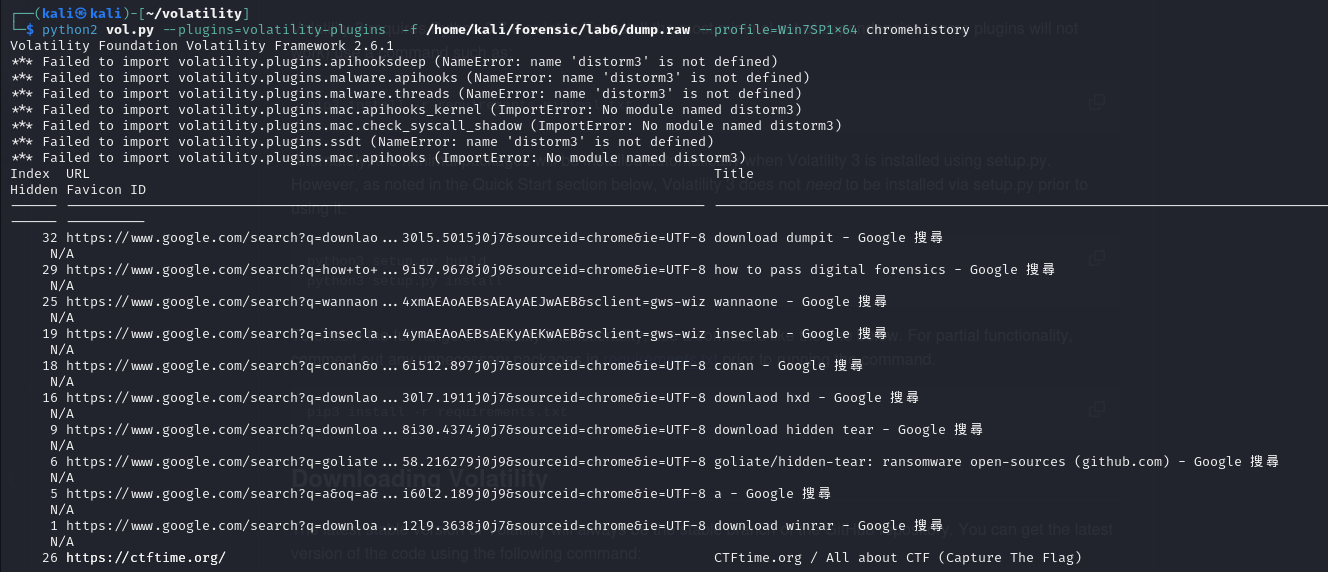
Format flag: flag{flag1-flag2-flag3)

+ **Liệu họ có để lại những dấu vết trên trình duyệt web?**

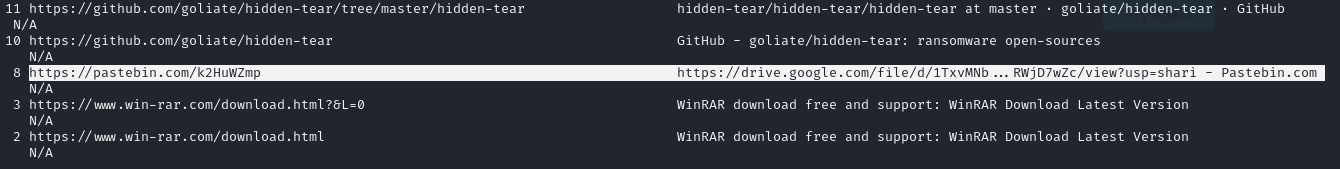
* Kiểm tra để xem họ dùng trình duyệt web nào:



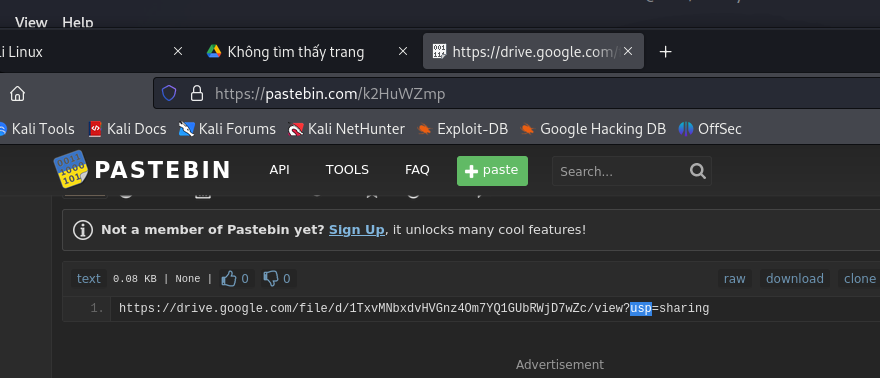
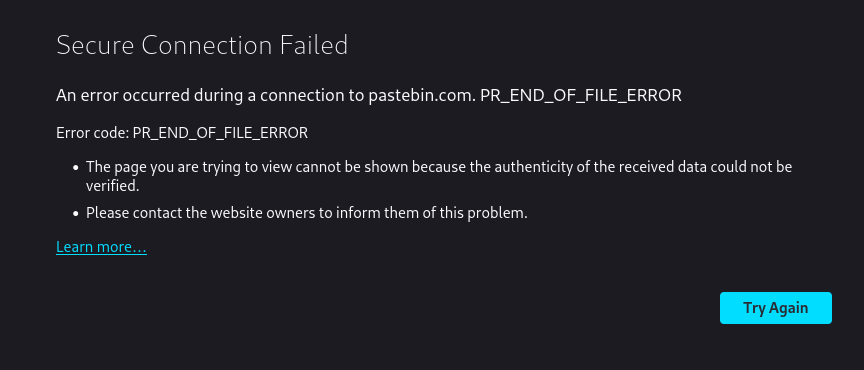
* Xác định được là Chrome nên dùng *chromehistory* xem lịch sử duyệt web:

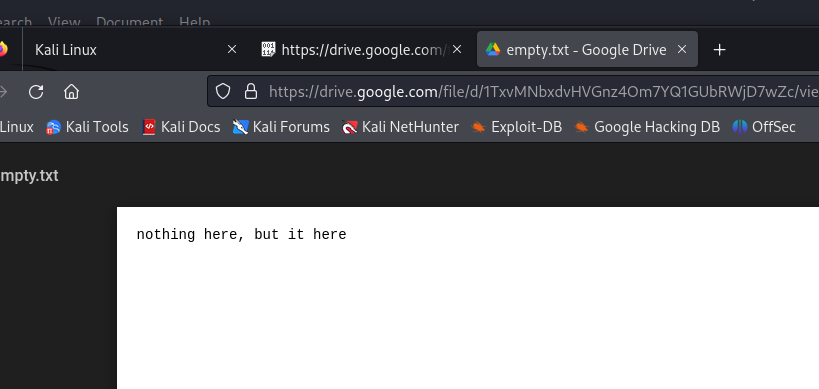


* Có link gg drive, tuy nhiên mở trên Firefox thì không được:

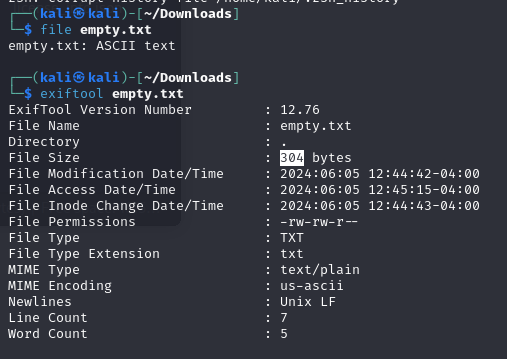


* Có liên quan đến link pasebin bên cạnh, nhưng mở bình thường không truy cập được, nên dùng VPN:

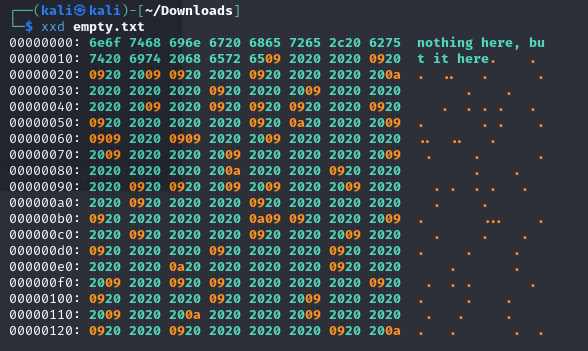
Có link được hiển thị, mở ra thì chuyển hướng đến file:



* Kiểm tra file bằng **binwalk, file** nhưng không có kết quả, nên em dùng exiftool, quan sát thấy size file lớn hơn so với dòng ký tự được hiển thị, nên có thể có thông tin ẩn trong file:



* Dùng **xxd** kiểm tra - đây là một dạng bài thuộc whitespace steganography program:



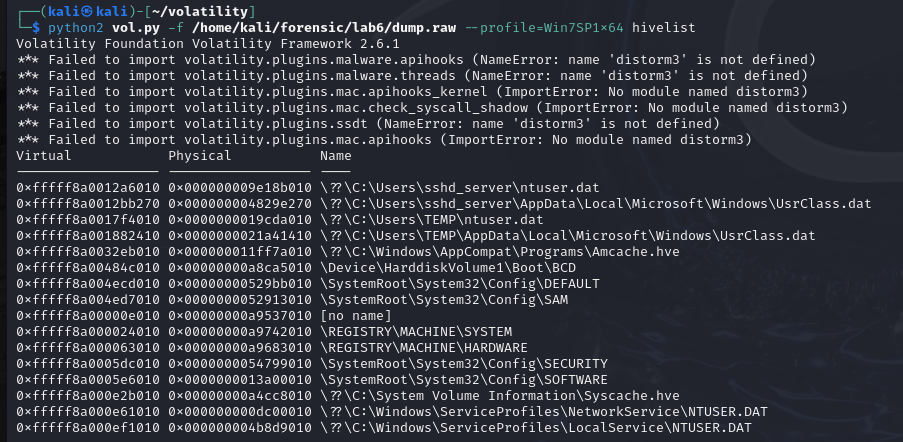
* Sử dụng *stegsnow* giải mã, được flag:



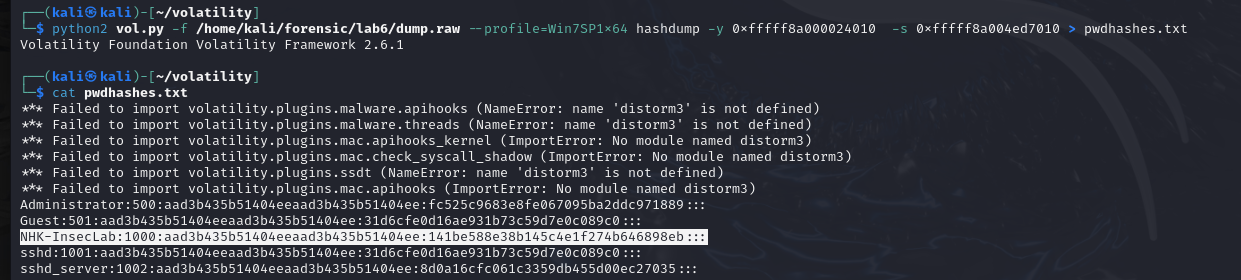
=> flag: inseclab{y0u\_c4n\_s33\_fl4g}

**+ Và hình như kẻ xâm nhập bằng một cách nào đó đã lấy được password laptop của NHK. Hãy tìm password đó.**

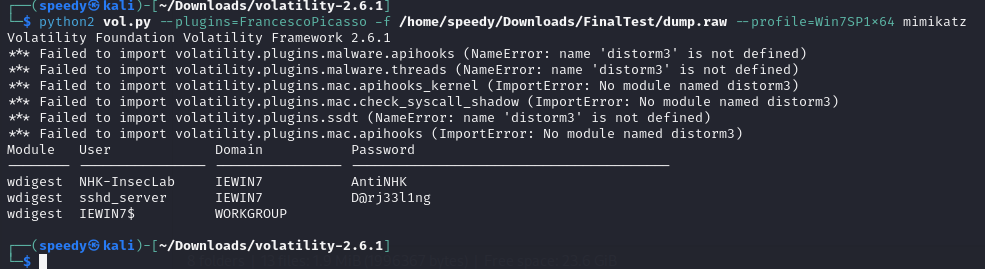
* Dùng *hivelist* lấy ra trường địa chỉ bắt đầu trọng bộ nhớ của nơi lưu trữ thông tin đăng ký và quản lý về tài khọản người dùng Windọws:



* Tương tự lab 1, ta sẽ quan tâm đến SAM, hashdump:



* Lsass.exe là một quy trình thiết yếu chịu trách nhiệm về chính sách bảo mật trên Windows. Nó xác minh tên đăng nhập và mật khẩu, do đó cần sử dụng Mimikatz để decode tìm password. Plugin có thể xem thêm tại https://github.com/volatilityfoundation/community/blob/master/FrancescoPicasso/mimikatz.py . Thực hiện như sau:



=> flag: inseclab{AntiNHK}.

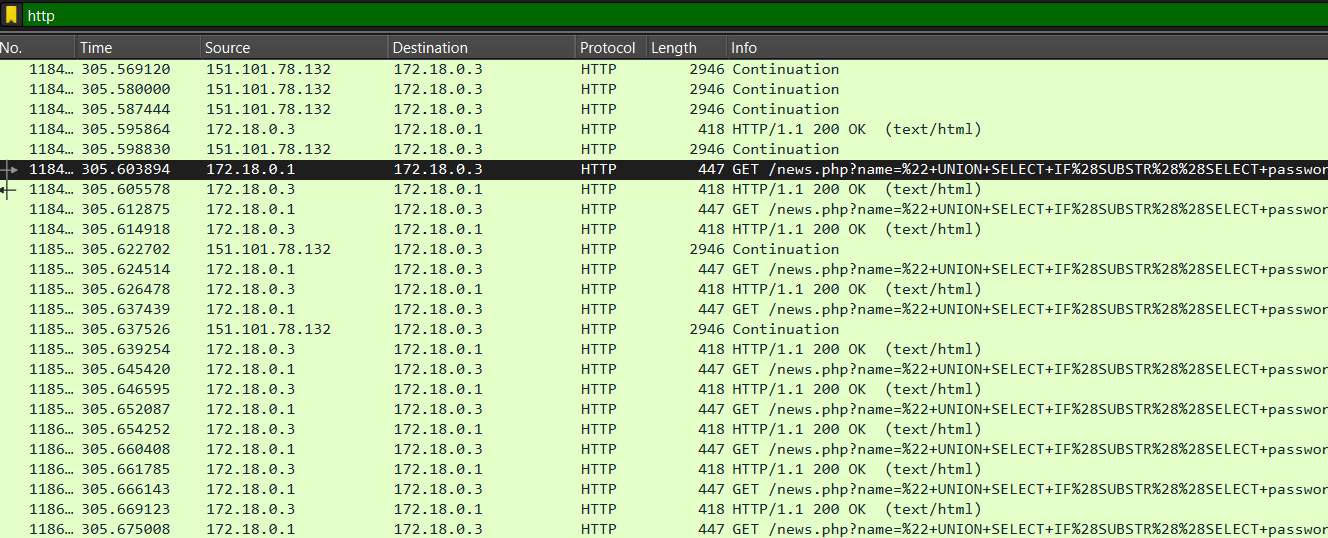
**2. Network (Medium):**

**g. Có vẻ là hacker đã lấy được mật khẩu của admin. Nhưng có người lại bảo là chưa. Vậy hacker đã lấy được mật khẩu của admin chưa? Mật khẩu của admin là gì? Hacker đã lấy được gì?**

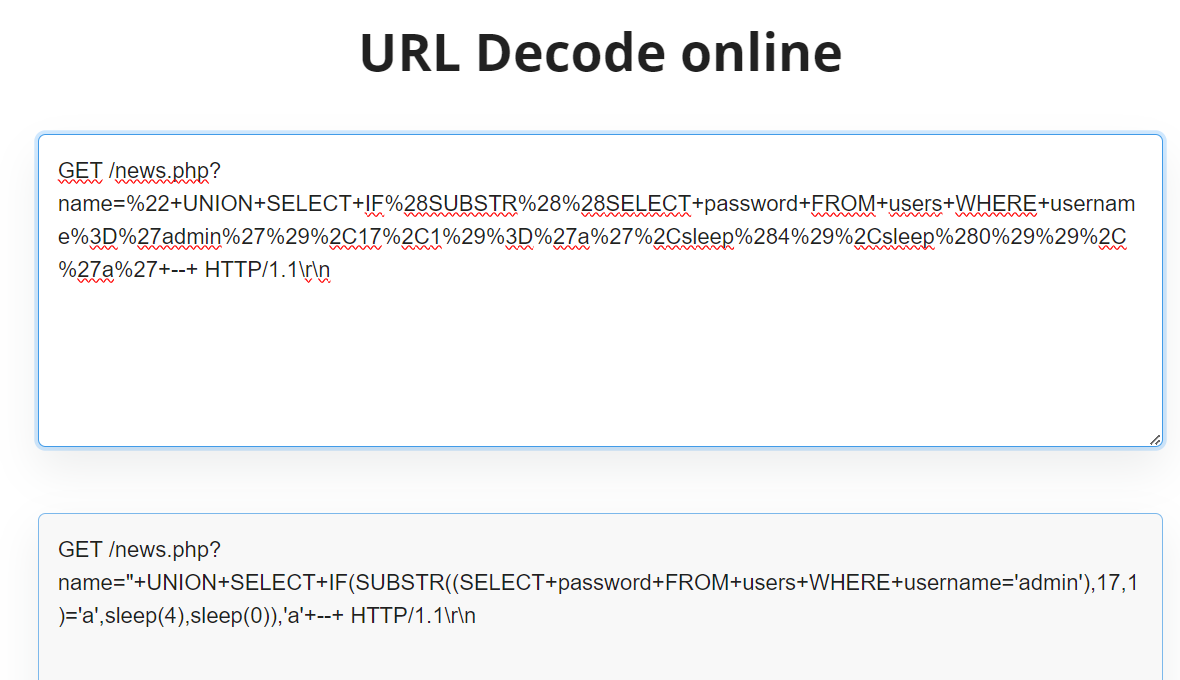
**Đáp án:**

- Hacker chưa lấy được mật khẩu của admin. Có cố gắng dò password nhưng chưa đúng. Cụ thể quá trình này diễn ra như sau:

* Sử dụng filter để lọc những gói tin html được gửi từ IP attacker đến Database, attacker liên tục request để truy xuất dữ liệu từ db:



* Sử dụng <https://www.urldecoder.io/> để decode nội dung. Tông quan, attacker sẽ so sánh lần lượt từng ký tự trong password với các ký tự trong bảng chữ cái, bảng số và các ký tự đặc biệt. Chọn tùy ý một gói tin để decode:



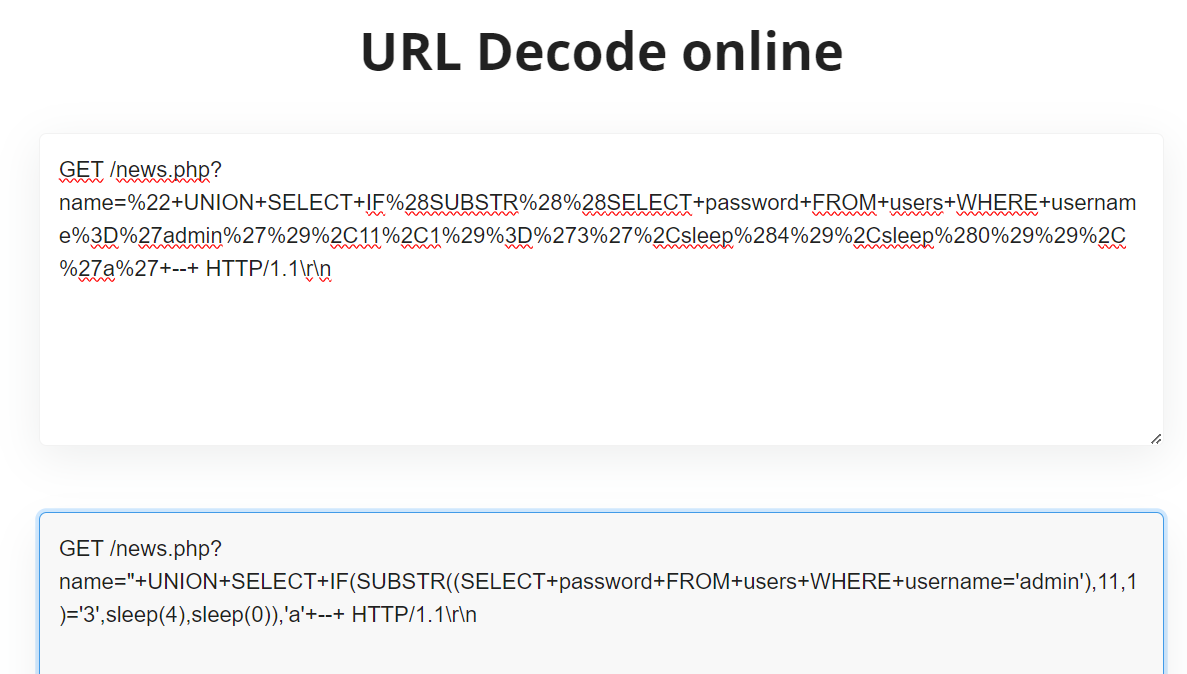
Giải thích sơ lược về nội dung decode được: Đoạn mã này là một ví dụ về một cuộc tấn công SQL injection. Trong ngữ cảnh này, nó cố gắng truy vấn cơ sở dữ liệu thông qua một trang web. Đoạn mã cố gắng lấy mật khẩu của người dùng có tên là 'admin' từ bảng 'users'.

UNION SELECT: Đây là một phần của cuộc tấn công SQL injection.

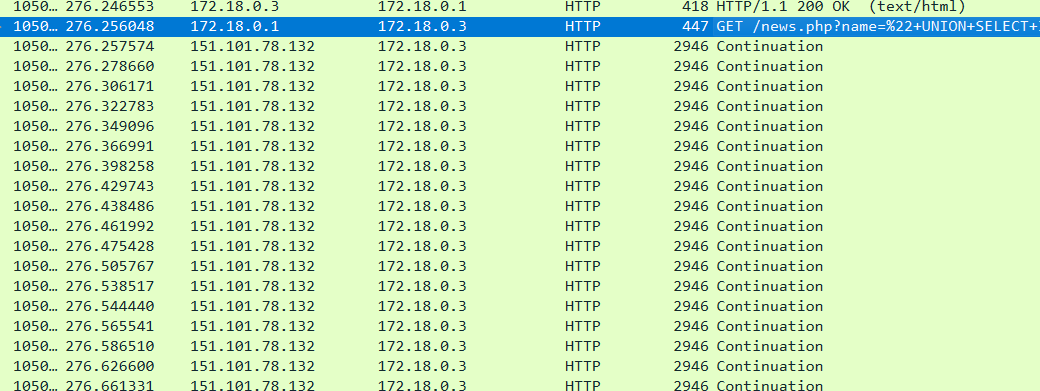
IF(SUBSTR((SELECT password FROM users WHERE username='admin'),17,1)='b',sleep(4),sleep(0)): Đây là một điều kiện IF trong SQL, kiểm tra xem ký tự thứ 17 của mật khẩu của người dùng 'admin' có phải là 'b' không. Nếu là 'b', hàm sleep(4) sẽ được gọi, ngủ trong 4 giây. Nếu không, sleep(0) sẽ được gọi, thực thi bình thường.

‘a’ + --: Kết thúc câu lệnh SQL với dấu "--" để bỏ qua mọi thứ còn lại

* Khi đã tìm được đúng ký tự, sẽ ngủ 4s. Ví dụ dò đến ký tự thứ 11, kí tự đúng là **3**, nội dung gói tin như sau:

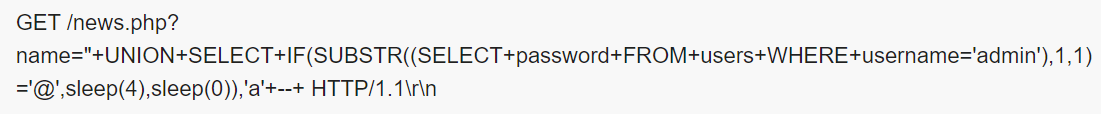


Thì chương trình sẽ không gửi truy vấn liên tục trong 4s, nghỉ 4s sau đó mới dò tiếp ký tự thứ 12:

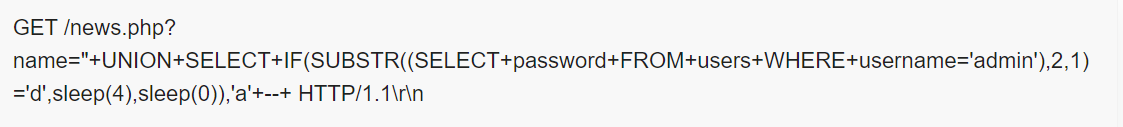


* Dựa vào flow này, chúng ta sẽ lần lượt xem các kí tự mà attacker dò được là gì và sai ở đâu mà không tìm ra được password:

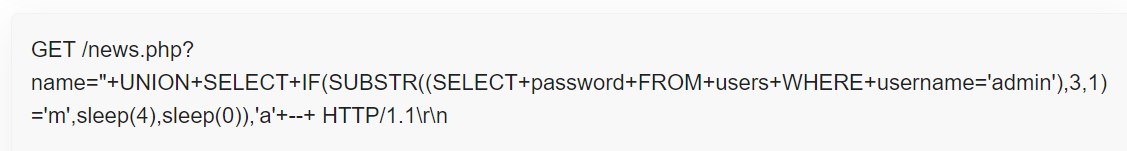
@:



d:



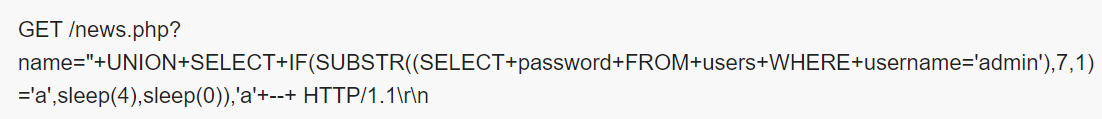
m:



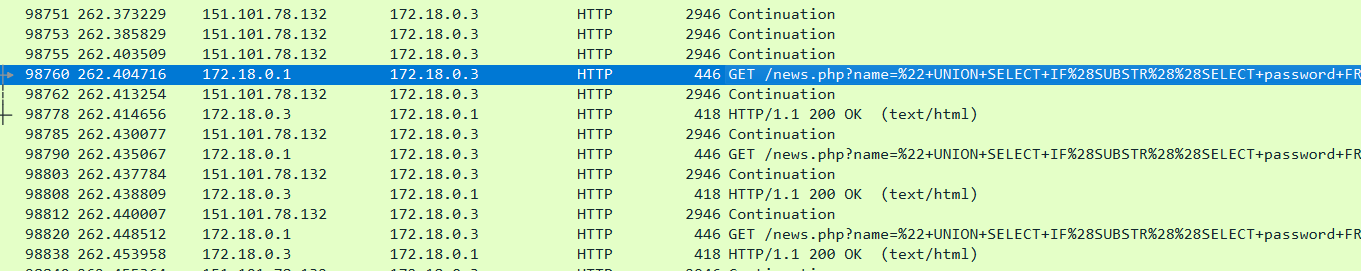
Lặp lại các bước nên em không chụp màn hình nữa, chỉ liệt kê các ký tự:

**1n\_a3...**

Thấy ký tự sai rồi nên em dừng decode ở đây. Attacker chọn ký tự thứ 7 là “a”, trong khi password đúng phải là “s”:

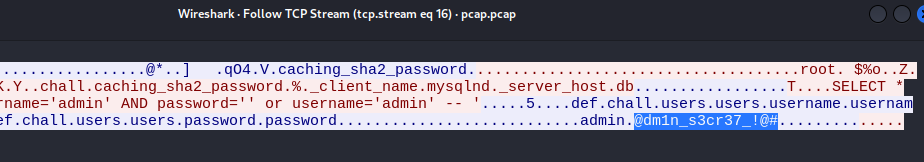


Và đây là gói tin đã gây ra sai lầm:



- Password của admin: **@dm1n\_s3cr37\_!@#**

Tuy nhiên đây là gói tin do web server truy vấn đến database nên cuối cùng, attacker vẫn không dò được password:



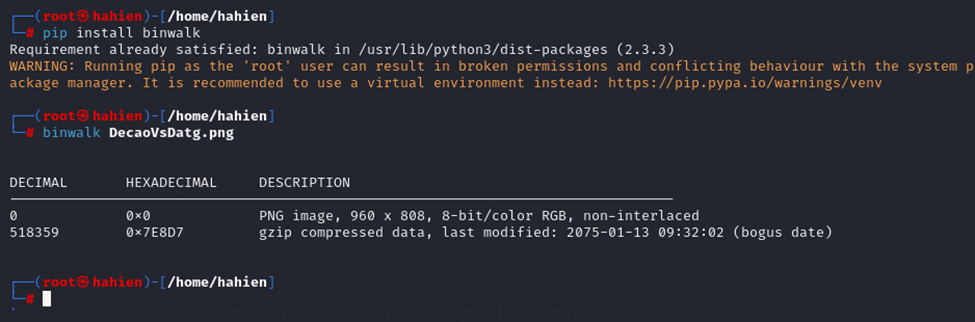
**4. Steganography (Maybe easy):**

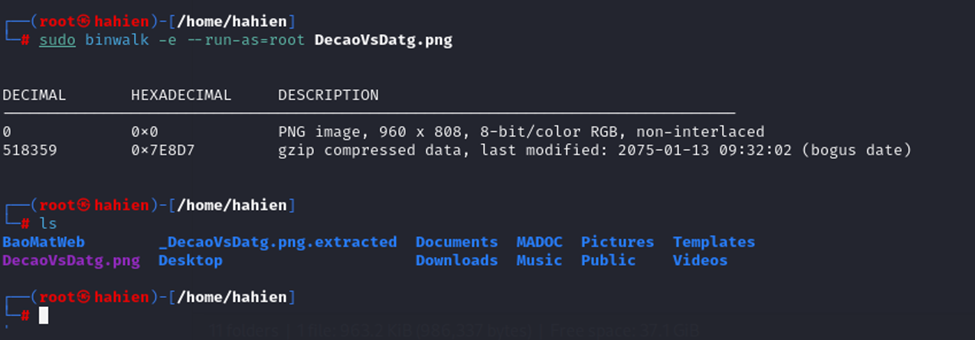
*DecaoVsDatg.enc.png* - Hiện tại cộng đồng mạng chưa xác định được ai là võ sĩ mạnh nhất thời đại. Hãy tìm flag được giấu trong bức ảnh để xác định được ai là võ sĩ đấm đau nhất nhé :)) . Flag sẽ là một câu danh ngôn mà ai cũng biết…

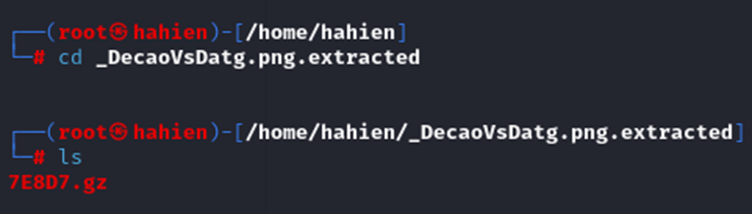
Format flag: inseclab{...}

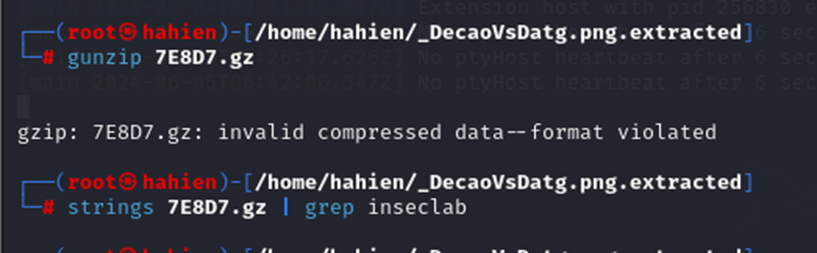
*Đáp án:*

* Đầu tiên, em thử dùng stegOnline, nhưng không thu được kết quả gì.
* Tiếp đến em dùng binwark để xem thông tin ảnh có chứa tệp ẩn không.





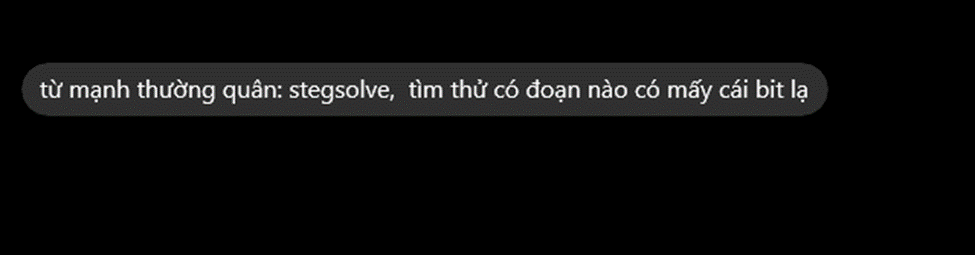




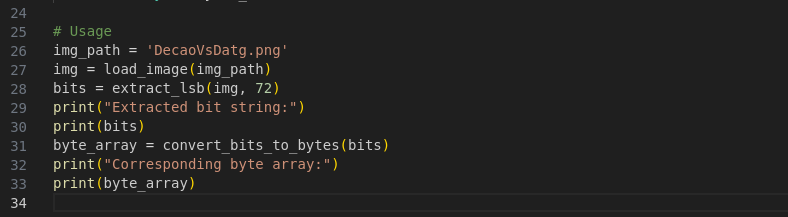
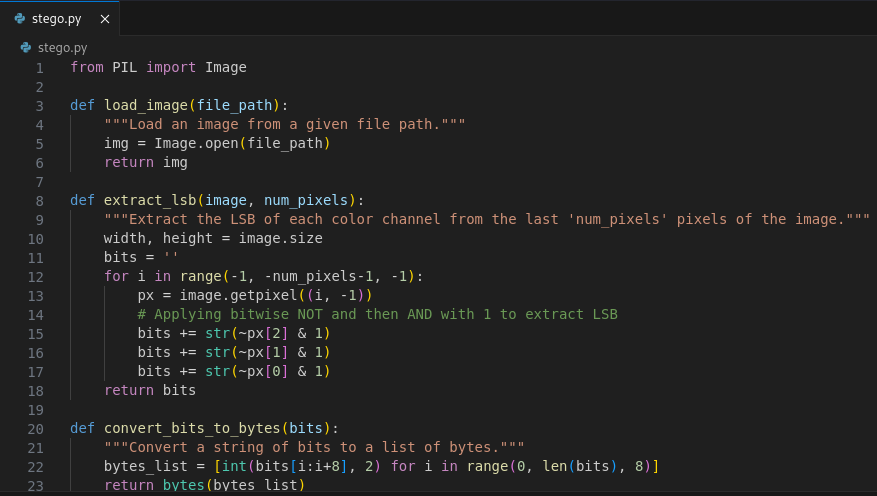
* Không giải nén được, nên em tìm cách khác thui.
* Hết cách, em hi vọng vào cái ảnh ban đầu xem kỹ nó có gì không.



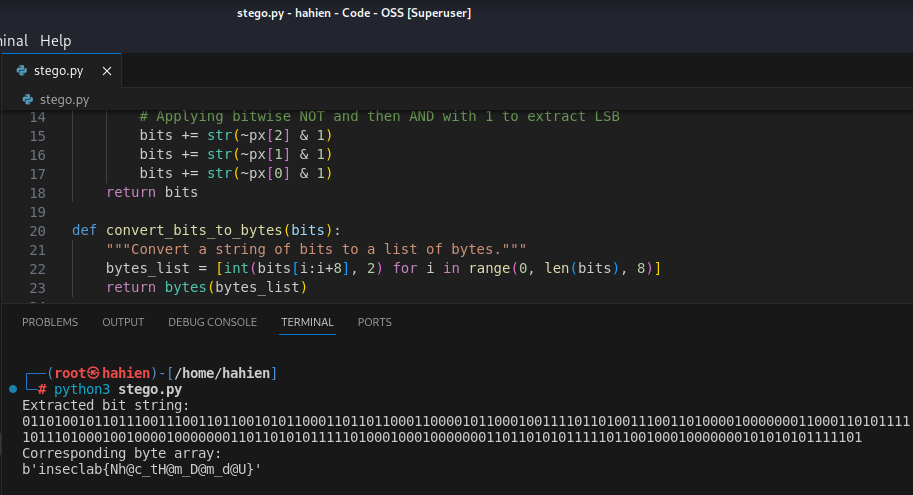
* TROLL Cả SHOWBIZ -> em nghĩ nó liên quan đến các bits cùng với hint đã tìm kiếm được.



* Từ đó, có đoạn code sau:



* Và kết quả là:



* FLAG: inseclab{Nh@c\_tH@m\_D@m\_d@U}

---

***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)