BÁO CÁO BÀI TẬP LÝ THUYẾT

**Môn học: Pháp chứng kỹ thuật số**

**Bài tập: Mem Labs**

*GVHD: Nghi Hoàng Khoa*

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 |
| 3 | Nguyễn Ngọc Nhung | 21521248 | 21521248@gm.uit.edu.vn |

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

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Lab 1 | 100% |
| 2 | Lab 2 | 100% |
| 3 | Lab 3 | 100% |
| 4 | Lab 4 | 100% |
| 5 | Lab 5 | 100% |
| 6 | Lab 6 |  |

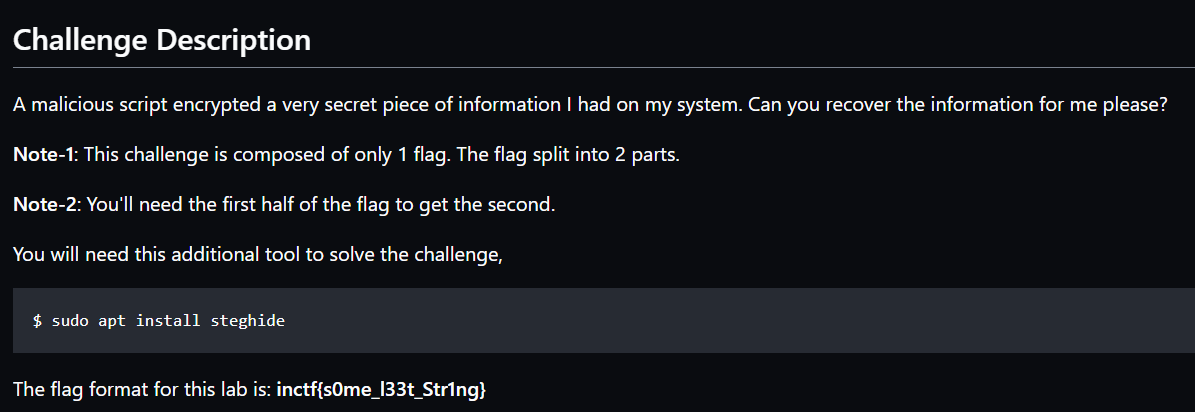
**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

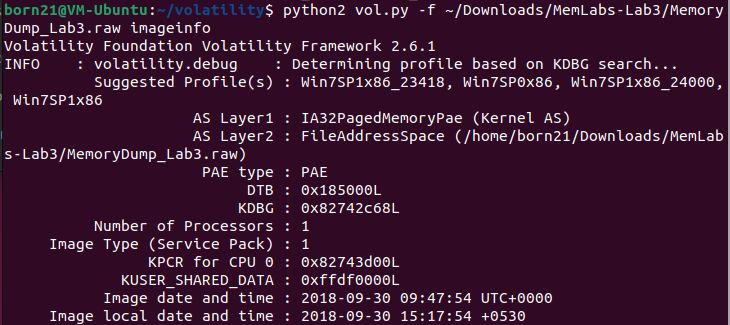
## Lab 1: Beginner's Luck

## Lab 2: A New World

## Lab 3: The Evil's Den



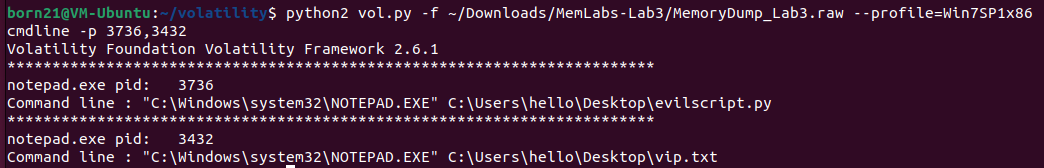
* Xem thông tin file dump.



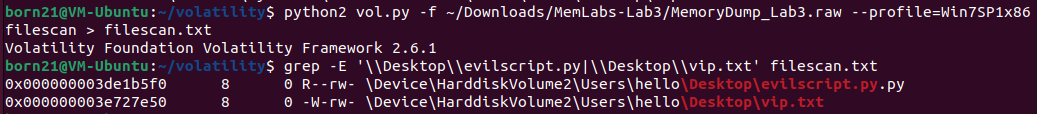
* Đầu tiên, kiểm tra các tiến trình đang chạy bằng plugin pstree.



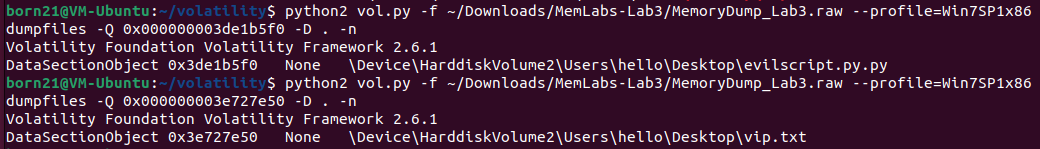
* Hiện có hai quy trình của chương trình notepad.exe đang chạy trên máy tính với các ID quy trình (Pid) là 3736 và 3432. Bằng cách sử dụng plugin cmdline, có thể xem được các tập tin cụ thể đã được mở bằng các phiên bản của chương trình notepad.exe này.



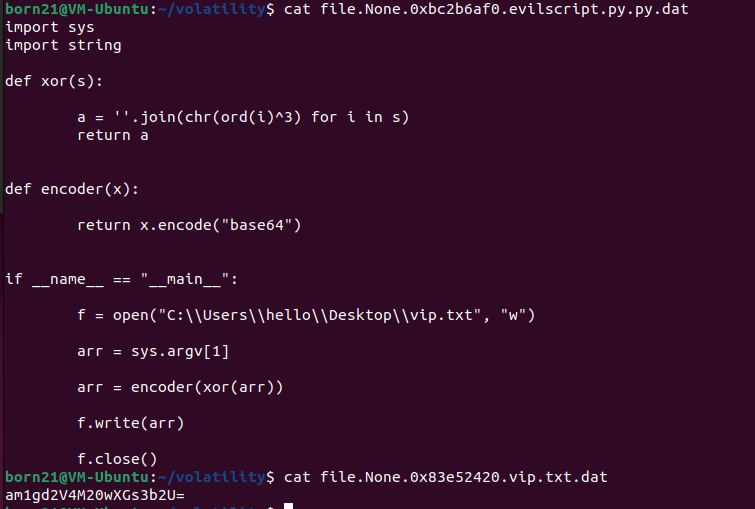
* Notepad đang mở 2 tệp evilscript.py và vip.txt. Để xem nội dung của 2 file, trước tiên, sử dụng plugin filescan để quét thông tin 2 file này.



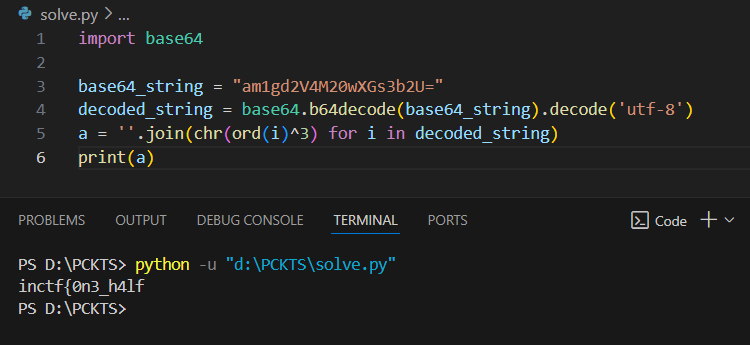
* Biết được offset của 2 file, ta tiến hành dumpfiles.



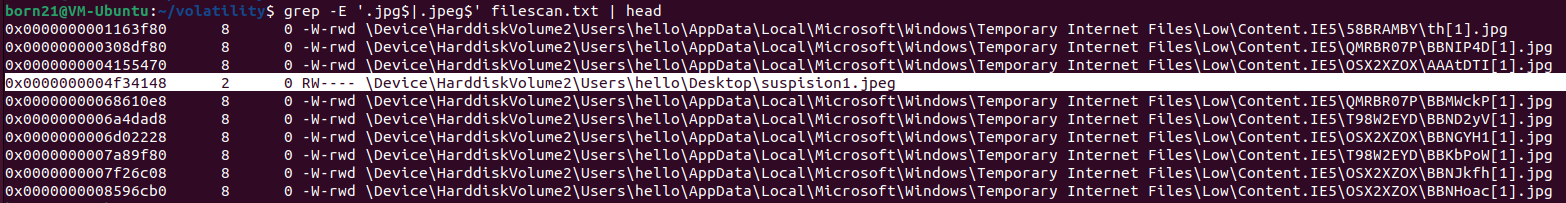
* Đọc nội dung 2 file vừa dump.



* Đoạn code trong file evilscript.py thực hiện mã hoá một chuỗi input bằng cách xor mỗi kí tự trong chuỗi với 3, sau đó mã hoá base64 và ghi vào tệp vip.txt
* Để biết được chuỗi input ban đầu, ta tiến hành đảo ngược quá trình trên.



* Ta có được 1 phần của flag: inctf{0n3\_h4lf
* Từ gợi ý steghide của đề bài, chúng ta sẽ scan những định dạng tệp hình ảnh phổ biến.



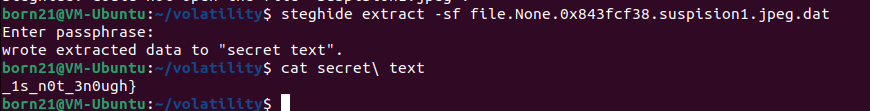
* Trong kết quả trả về có 1 tệp khá đặc biệt nên chúng ta sẽ dump file này để xem nội dung.



* File thu được:

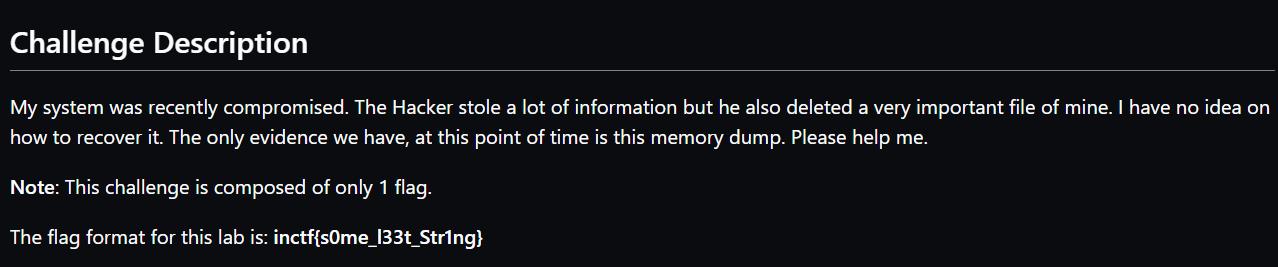


* Không có thông tin gì ở đây, chúng ta có thể dùng steghide để kiểm tra xem có nội dung nào được ẩn hay không.

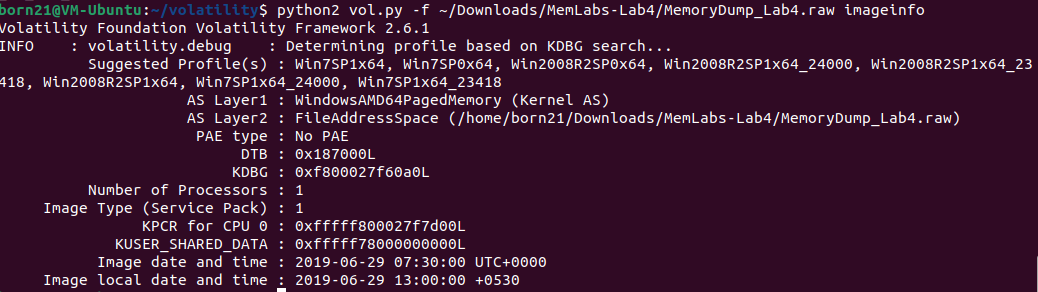


* Password là 1 phần của flag đã giải trước đó. Ta biết được phần còn lại của flag.
* Flag: inctf{0n3\_h4lf \_1s\_n0t\_3n0ugh}

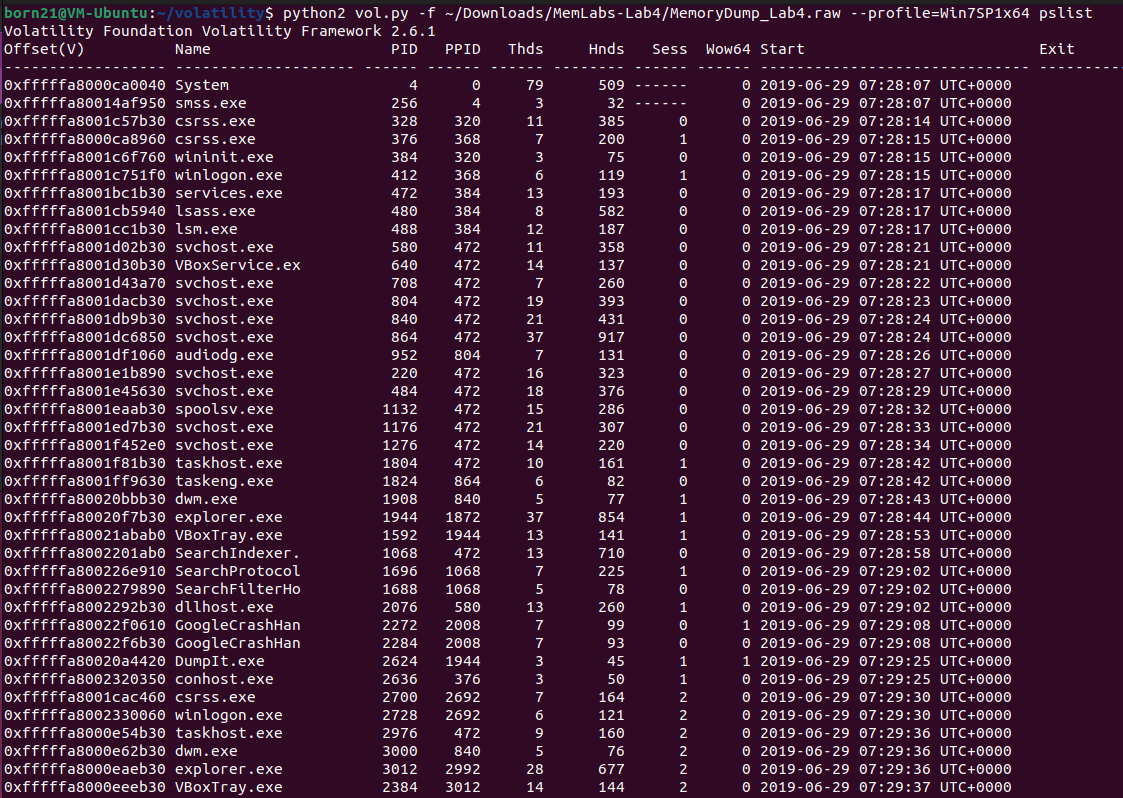
## Lab 4: Obsession



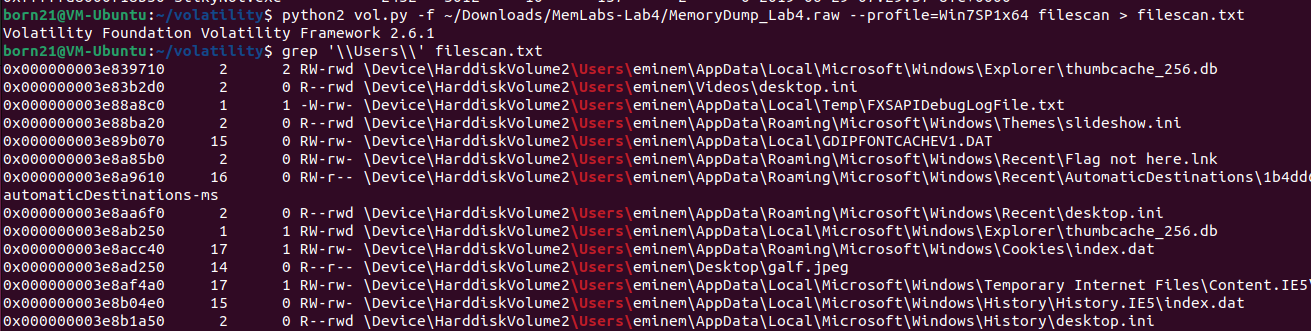
* Xem thông tin file dump.



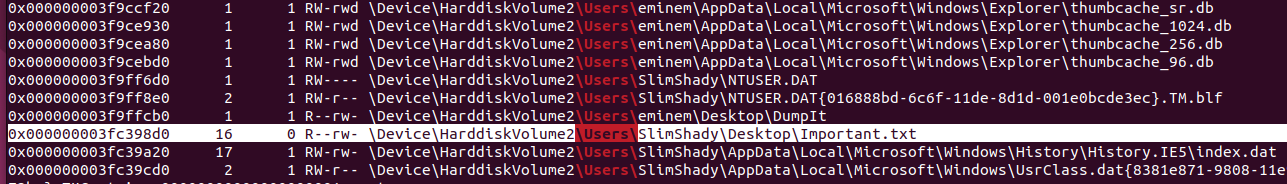
* Kiểm tra các tiến trình đang chạy.



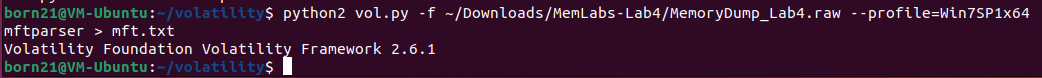
* Không khai thác được thông tin gì từ các tiến trình. Từ gợi ý đề bài là file đã bị xoá, chúng ta hãy thử filescan. File rất quan trọng đối với người dùng có thể sẽ được lưu trong thư mục User nên sẽ lọc ra các tệp ở trong thư mục này.



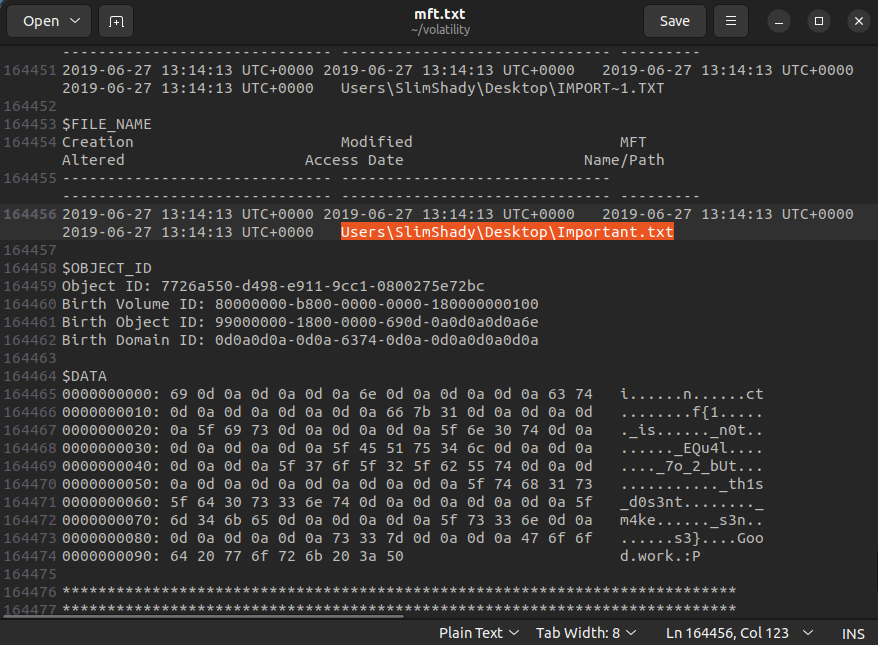
* Chú ý vào file sau, đây có thể sẽ là file quan trọng mà đề bài nhắc tới:



* Thử dumpfile để xem nội dung nhưng không có output nào được tạo ra. Có thể dữ liệu đã bị xoá sẽ còn lưu lại ở một nơi khác. Trên phân vùng NTFS, các tệp nhỏ (tối đa vài trăm byte) có thể được lưu trữ dưới dạng thường trú trong thuộc tính $DATA trong Master File Table (MFT) . Chúng ta có thể sử dụng plugin mftparser để phân tích MFT và sử dụng lại grep để lọc mục nhập có liên quan.



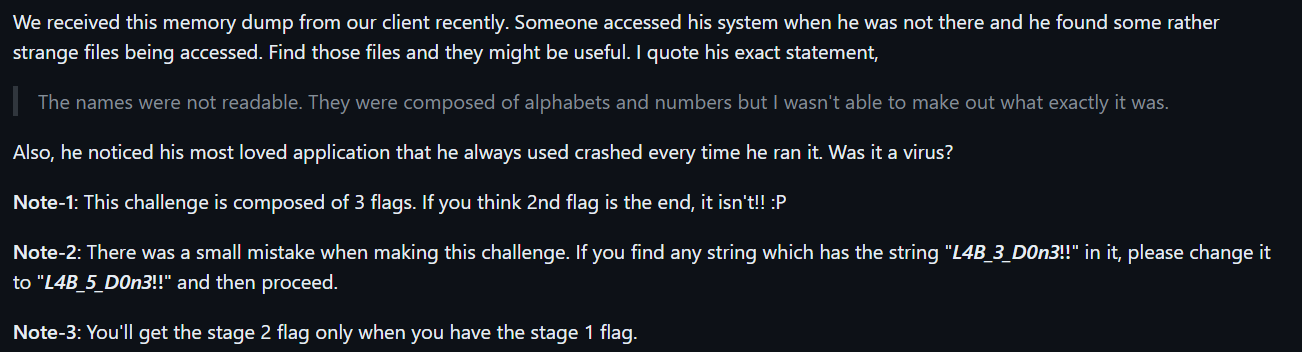
* Mở file output và tìm kiếm chuỗi Users\SlimShady\Desktop\Important.txt, chúng ta tìm được nội dung file đã xoá.



* Có nhiều khoảng trắng được chèn vào flag, xoá những khoảng trắng này chúng ta thu được kết quả:
* Flag: inctf{1\_is\_n0t\_EQu4l\_7o\_2\_bUt\_th1s\_d0s3nt\_m4ke\_s3ns3}

## Lab 5: Black Tuesday

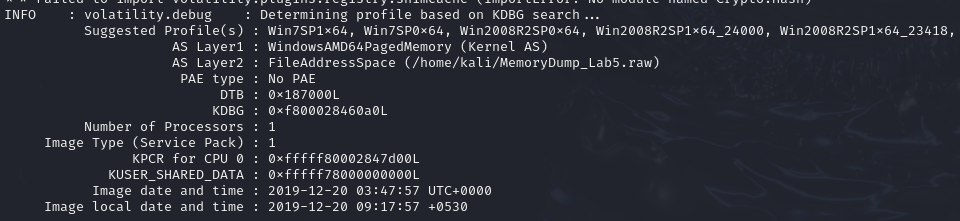
* Mô tả challenge:



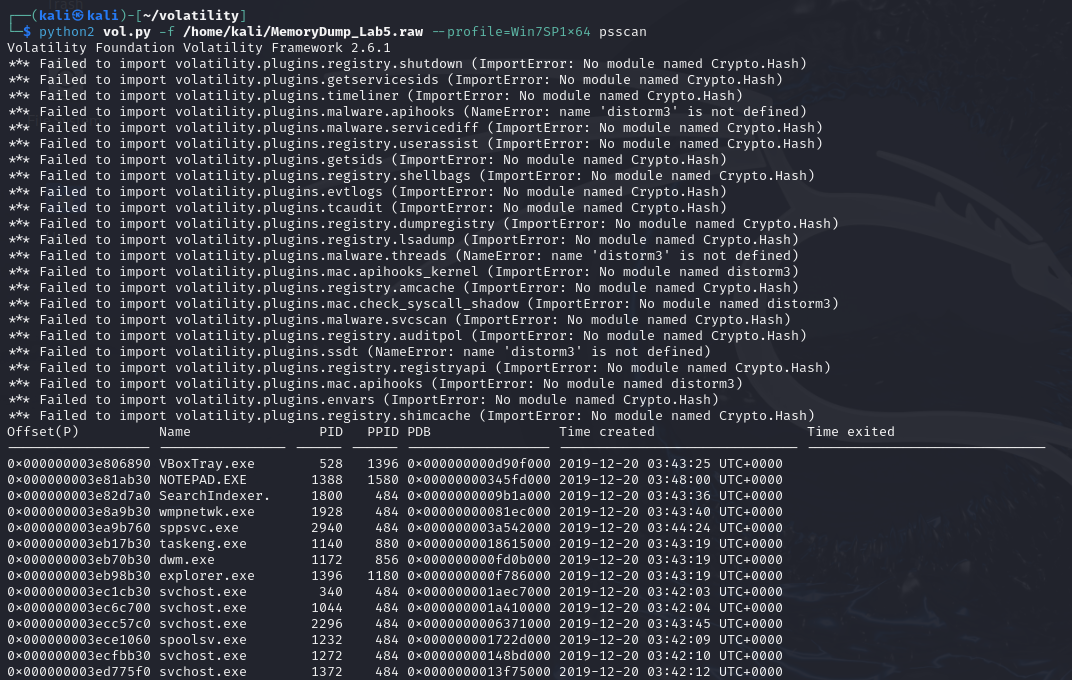
Gần đây chúng tôi đã nhận được kết xuất bộ nhớ này từ khách hàng của mình. Ai đó đã truy cập vào hệ thống của anh ấy khi anh ấy không có ở đó và anh ấy phát hiện thấy một số tệp khá lạ đang được truy cập. Tìm những tập tin đó và chúng có thể hữu ích. Tôi trích dẫn chính xác tuyên bố của anh ấy, Những cái tên không thể đọc được. Chúng bao gồm các bảng chữ cái và số nhưng tôi không thể biết chính xác nó là gì. Ngoài ra, anh ấy còn nhận thấy ứng dụng yêu thích nhất mà anh ấy luôn sử dụng bị lỗi mỗi khi chạy nó. Đó có phải là virus không?

Lab 5 có 3 flags.

* Sau khi tải và giải nén, được 1 tập tin raw. Em sử dụng plugin imageinfo để kiểm tra thông tin của file dump:

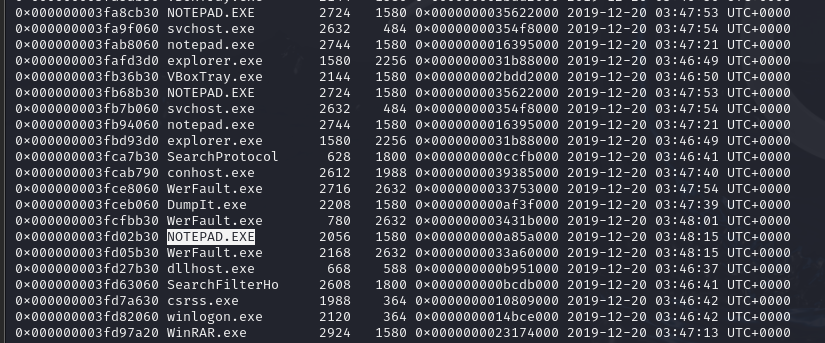


* Dùng *psscan* để kiểm tra các process đang chạy:

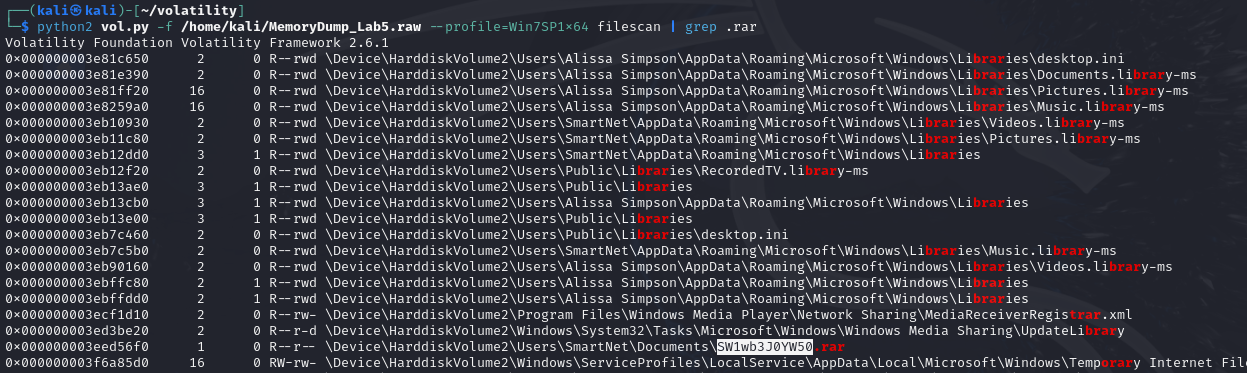


Do em cài lại máy ảo nên lỗi Crypto.Hash em chưa kịp fix, để dễ quan sát thì em sẽ chỉ chụp kết quả sau khi chạy plugin chứ không chụp lại câu lệnh ạ.

Lướt xuống phía dưới, em tìm thấy 2 ứng dụng quen thuộc là NOTEPAD và WinRAR:

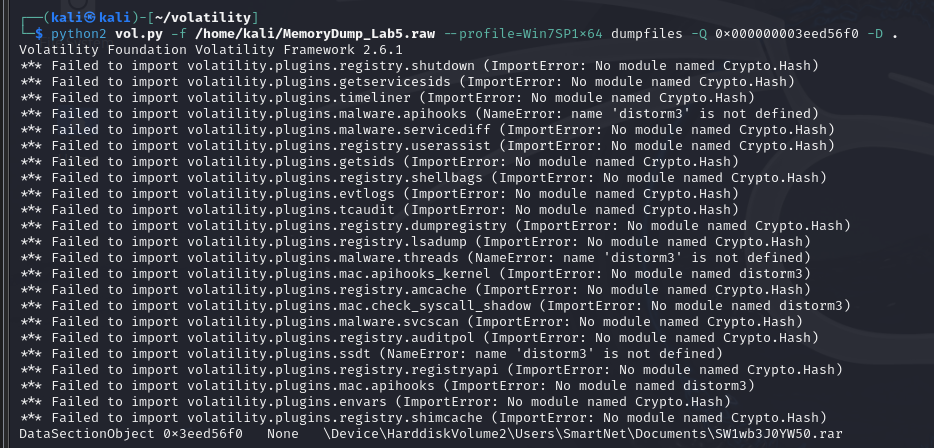


* Do đó, em sẽ tìm file .rar bằng *filescan | grep .rar*:

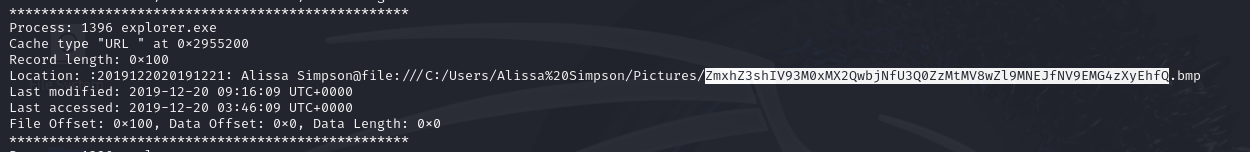


Có một file với tên kỳ lạ, đọc vào không hiểu rõ đó là file gì.

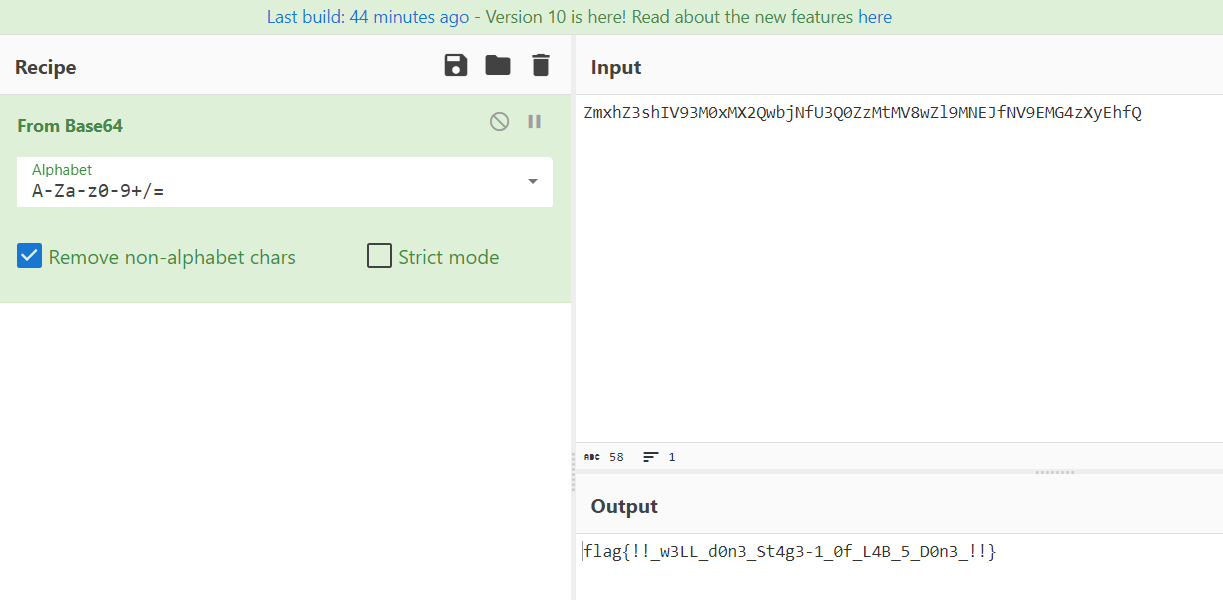
* Để xem rõ về file .rar trên, em sẽ dùng *dumpfile:*



* Sau khi dump thì được 1 file nén. Tuy nhiên nó cần password để mở. Em thực hiện tiếp để tìm password đầu tiên.
* Kiểm tra lịch sử duyệt web bằng *iehistory*, em tìm được đoạn mã đang ngờ:

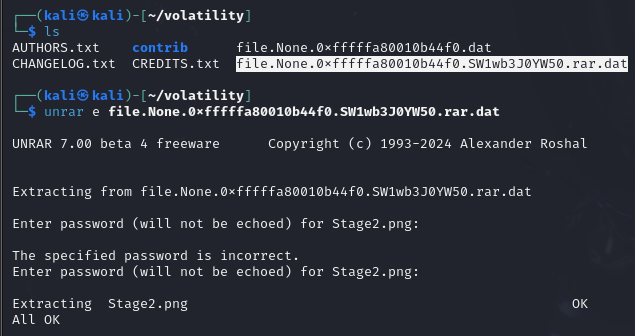


* Em decode đoạn mã trên bằng CyberChef, thành công tìm được cờ đầu tiên:

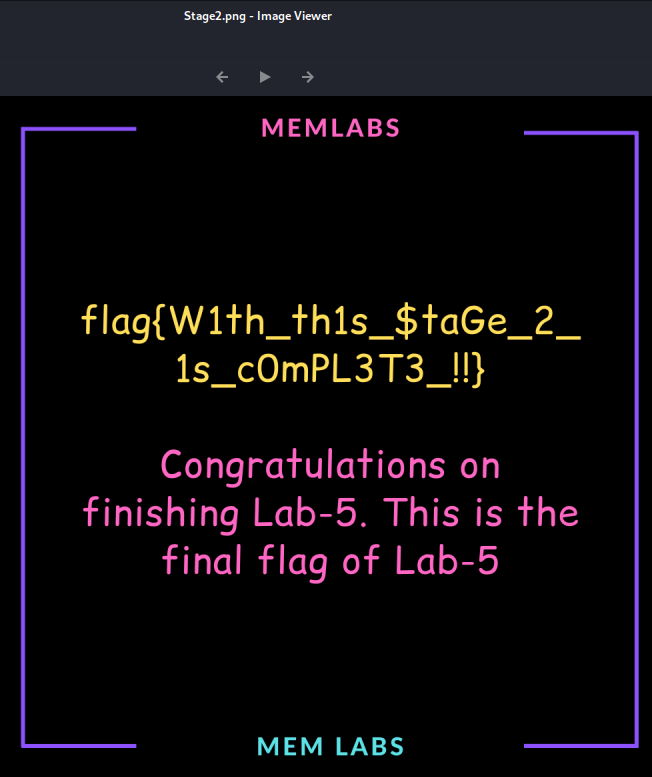


## flag{!!\_w3LL\_d0n3\_St4g3-1\_0f\_L4B\_5\_D0n3\_!!}

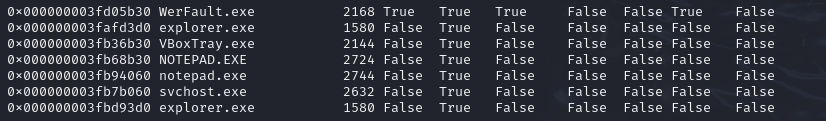
* Flag trên chính là password cần tìm, nhập vào thì đã extract được 1 file ảnh png:



Và flag thứ 2 là

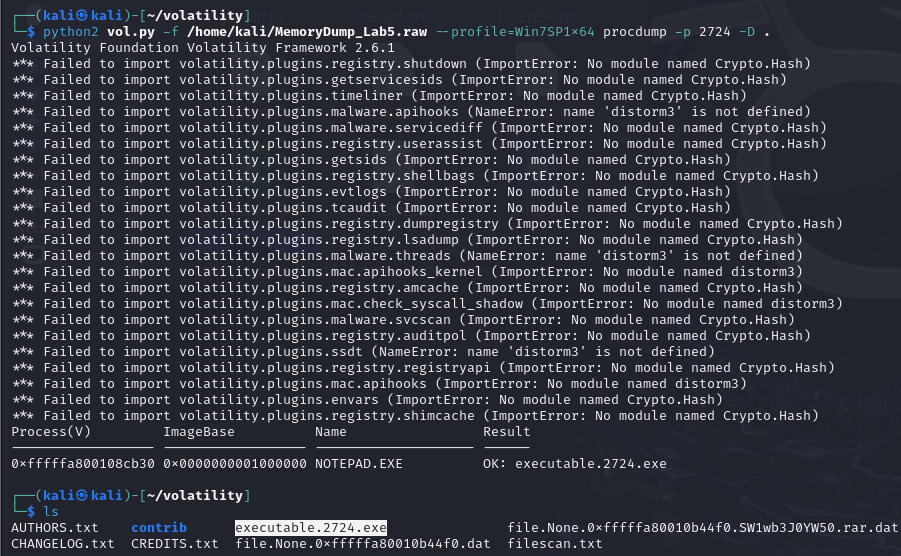


* Tuy nhiên, đề yêu cầu 3 flag, nên tìm tiếp flag cuối cùng, em sẽ xử lý tiếp NODEPAD.exe. Dùng *psxview* để xem các quá trình ẩn trên hệ thống:



NODEPAD có nhiều tiến trình, tuy nhiên do đề có nói truy cập nhưng không sử dụng được, nên em sẽ chọn tiến trình bị false nhiều nhất có PID là 2724.

* Sử dụng procdump:

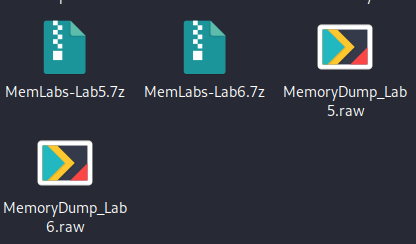


## Lab 6: The Reckoning

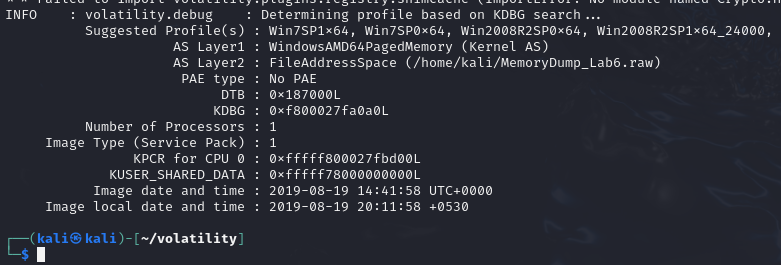
* Đề bài: Chúng tôi đã nhận được kết xuất bộ nhớ này từ Cục Tình báo. Họ cho rằng bằng chứng này có thể nắm giữ một số bí mật của trùm xã hội đen David Benjamin. Kho ký ức này được lấy từ một trong những nhân viên của anh ta, người đã bị FBI bắt giữ hồi đầu tuần. Công việc của bạn là xem qua vùng kết xuất bộ nhớ và xem liệu bạn có thể tìm ra điều gì không. FBI cũng nói rằng David đã liên lạc với các nhân viên của mình qua internet nên đây có thể là nơi tốt để bắt đầu. Lưu ý: Thử thách này gồm 1 lá cờ chia làm 2 phần.

Định dạng cờ cho phòng thí nghiệm này là: inctf{s0me\_l33t\_Str1ng}

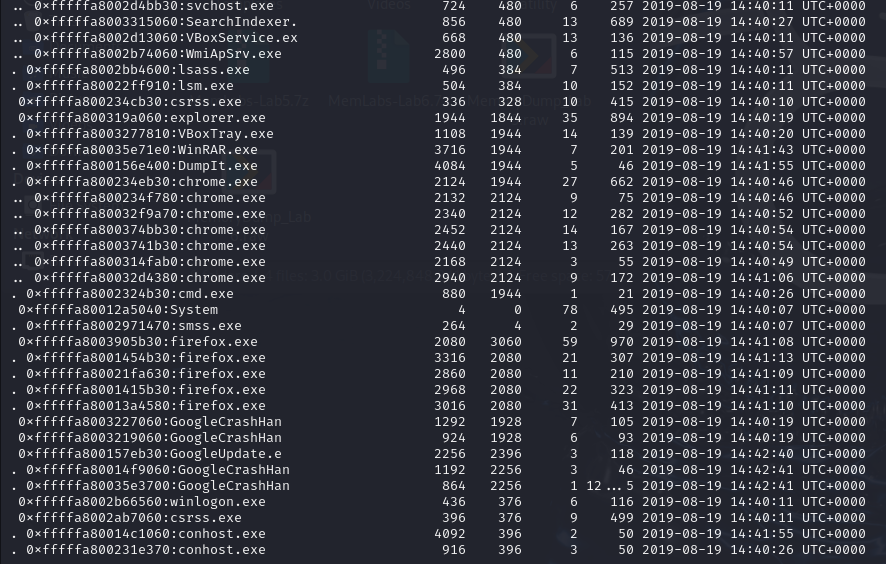
* Tải file về và giải nén:



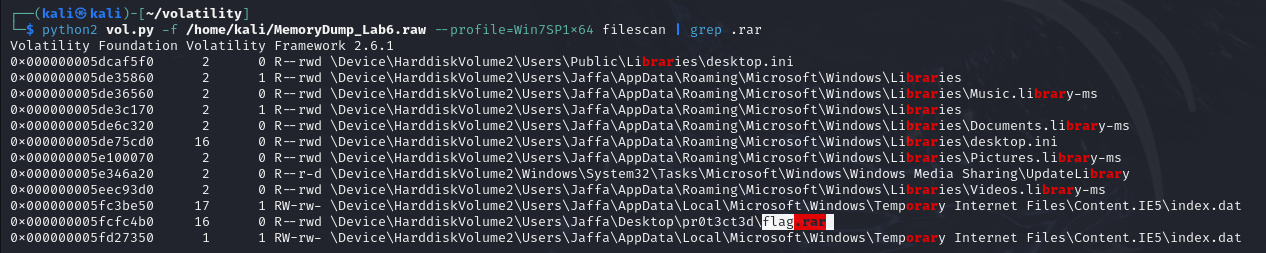
* Tương tự như lab 5, dùng *imageinfo* để xem thông tin:



* Kiểm tra các tiến trình đang chạy bằng *pstree*:

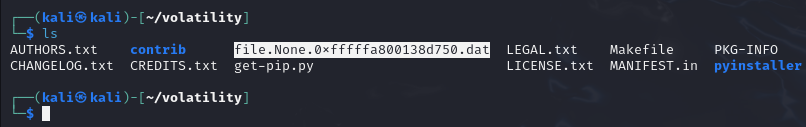


* Một vài cái tiêu biểu là WinRAR, firefox, chrome. Em sẽ bắt đầu trước với WinRAR, plugin *filescan*:



Tìm được file flag.rar.

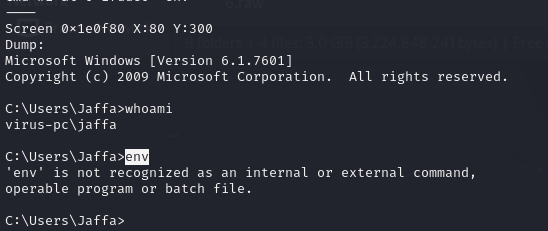
* Tương tự lab 5, em sẽ dump file này:



* Giải nén file. Tuy nhiên cần password:



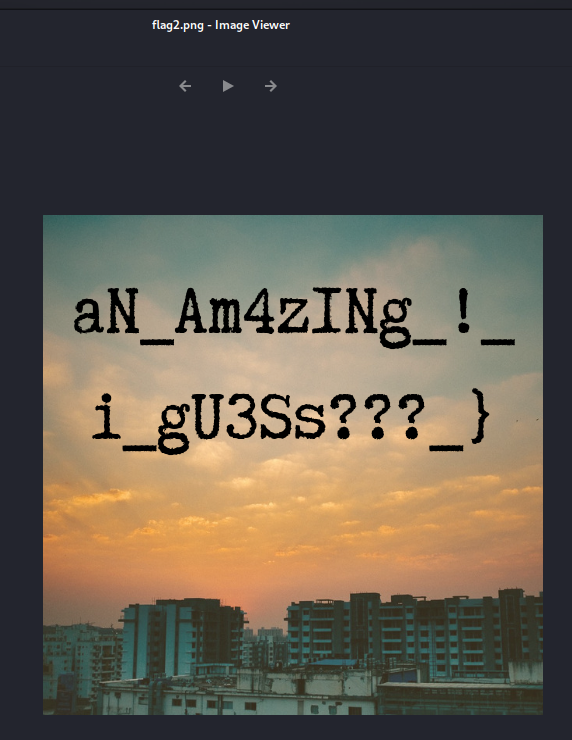
* Tiếp tục tìm flag khác, sẽ quay lại để giải nén tệp này sau khi ta có được password. Em dùng consoles để xem chi tiết lịch sử tiến trình cmd:



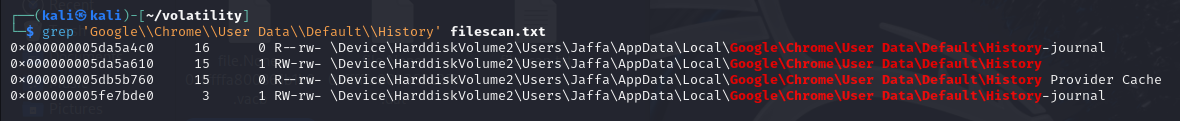
Kết quả cho thấy, lịch sử cmd có nhắc đến env, điều này gợi nhớ đến plugin envars dùng để xem các biến môi trường. Do đó, em sẽ chạy thử nó. Do cần tìm password cho file .rar nên biến môi trường cần tìm sẽ grep WinRAR.exe. Tìm được pass là “easypeasyvirus”:



Flag:



* Tiếp tục, đến chrome:



---

***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)