BÁO CÁO THỰC HÀNH

**Môn học: Pháp chứng kỹ thuật số**

**Lab 2: Hard drive Forensic**

*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)**

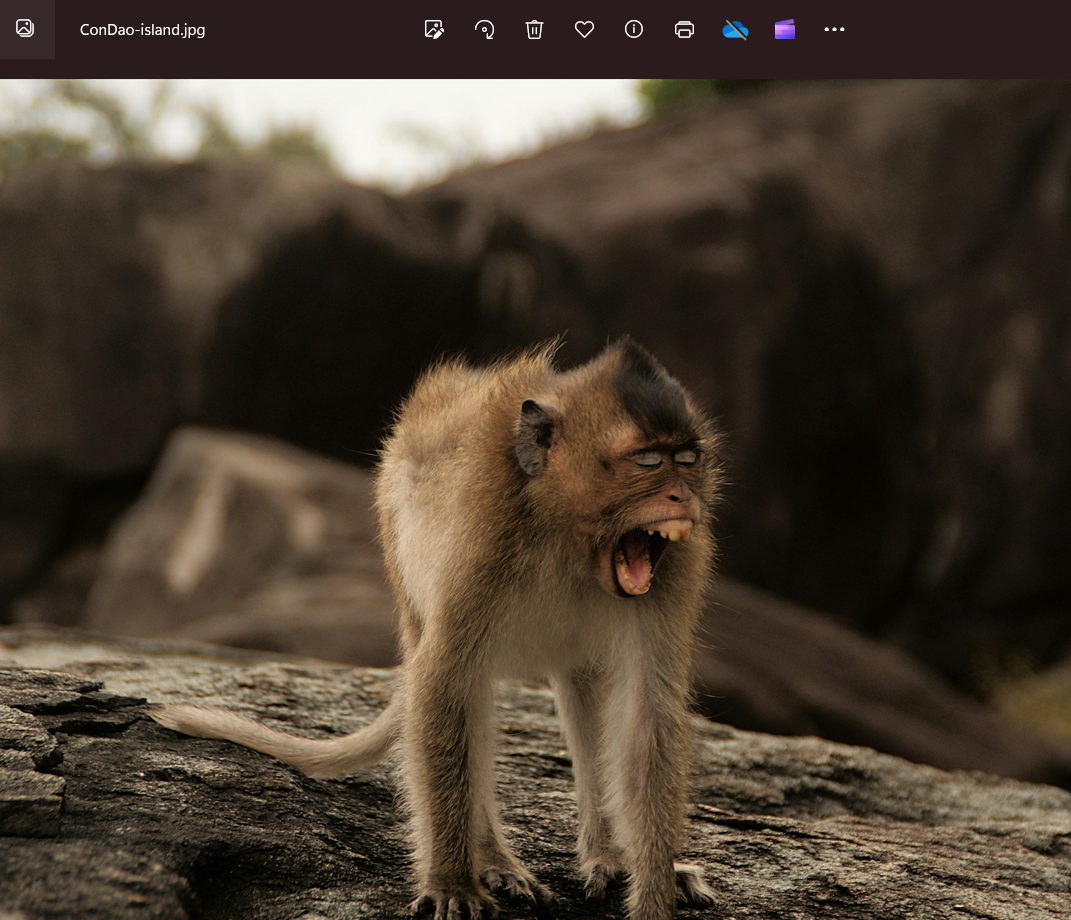
|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Kịch bản 1 (đã báo cáo ở lớp) | 100% |
| 2 | Kịch bản 2 (đã báo cáo ở lớp) | 100% |
| 3 | Kịch bản 3 | 80% |
| 4 | Kịch bản 4 | 100% |
| 5 | Kịch bản 5 (đã báo cáo ở lớp) | 100% |
| 6 | Kịch bản 6 | 100% |

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

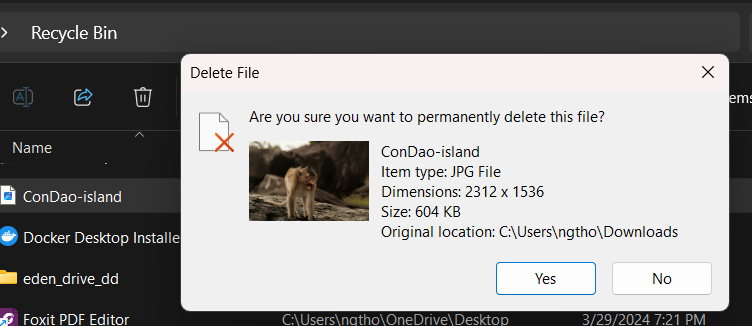
BÁO CÁO CHI TIẾT

**Kịch bản 03: Thực hiện phân tích theo kịch bản mô tả sau:**

* Trên máy tính/máy ảo windows thực hiện tải về hình ảnh và đặt tên ConDao-island. Liên kết tải: <https://unsplash.com/photos/uXPBXlruX5o>



* Thực hiện xóa file ảnh vừa tạo, xóa trong Recycle Bin.



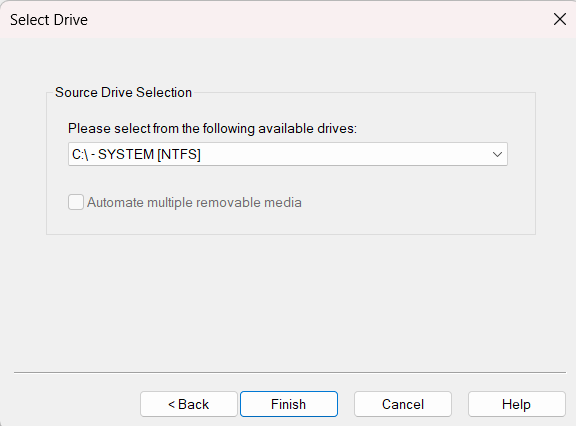
* Tạo một ảnh đĩa - định dạng Raw (dd) sau khi xóa file ảnh trên.

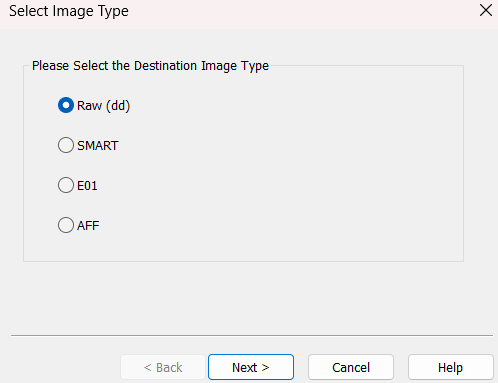
▪ Case Number: April\_0001

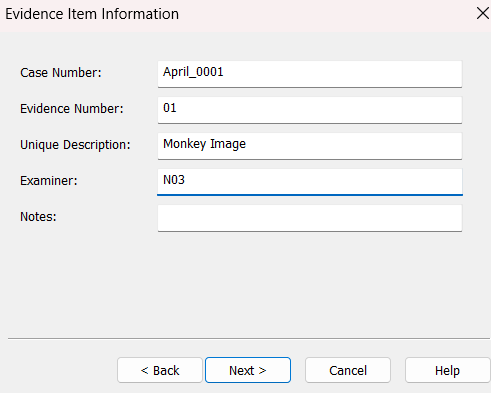
▪ Evidence Number: 01

▪ Unique Description: Monkey Image

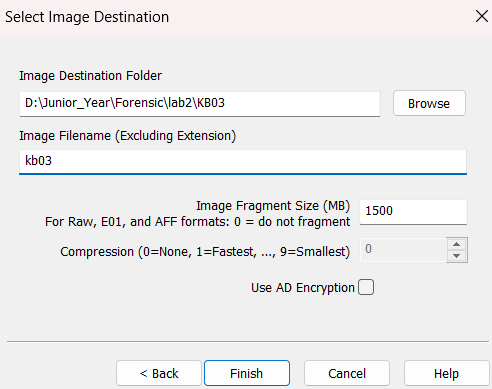
▪ Examiner: Your Name (tên của nhóm)

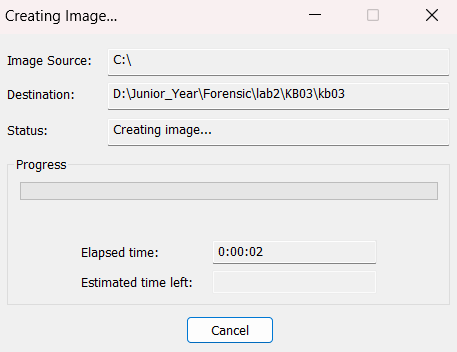


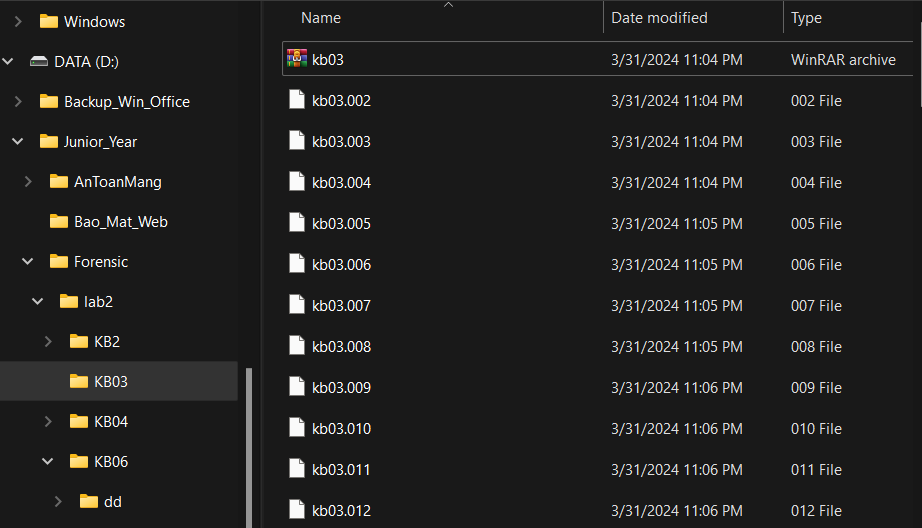




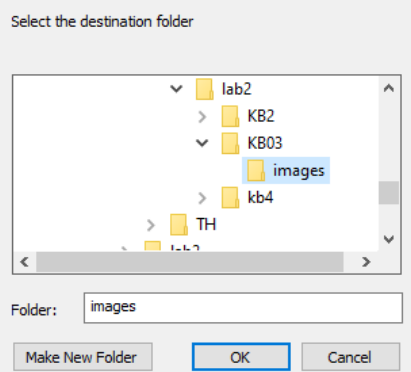
* Tạo một thư mục điều tra dùng cho kịch bản này: KB03, chứa ảnh đĩa đã tạo.







* Thực hiện điều tra, tìm ảnh đã bị xóa trên ổ đĩa bằng công cụ FTK Imager. Sử dụng tính năng phục hồi file ảnh đã bị xóa (tính năng Export Files), lưu trữ file này trong thư mục KB03\images.



* Kiểm tra giá trị hash MD5 của file ảnh vừa được phục hồi với file gốc ban đầu.

*Yêu cầu: Các nhóm thực hiện chụp màn hình terminal sau khi hoàn thành điều tra bằng cách gõ các câu lệnh sau:*

dir D:\KB03 | findstr "ConDao-island"

date /t

echo "Tên nhóm"

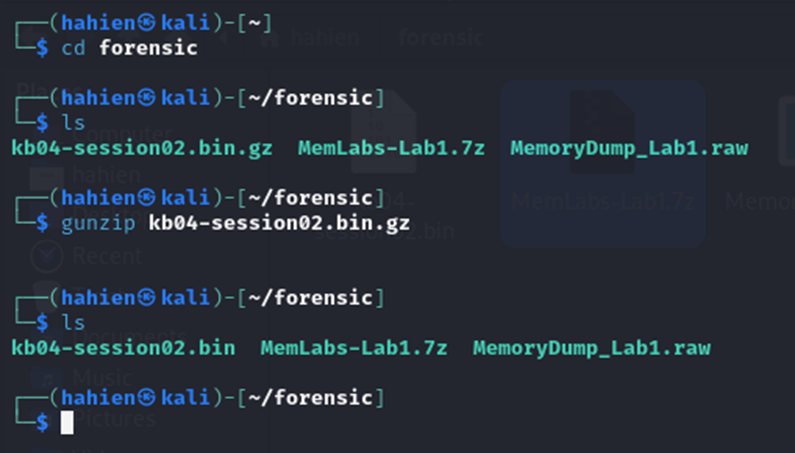
Thí dụ, echo "John, Dung, David, Kris"

**Kịch bản 04. Thực hiện phân tích:**

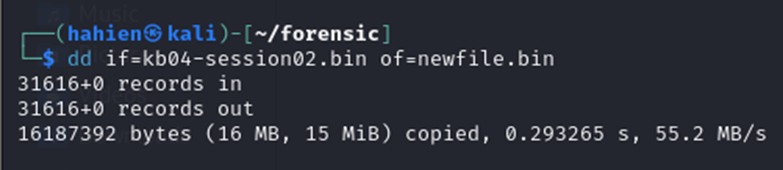
* Tài nguyên: kb04-session02.bin.gz
* Tìm thông tin có liên quan đến từ khóa “key” trong dữ liệu được cung cấp. *Gợi ý: Tìm hiểu các Master File Table (MFT), mmls, dd, strings, foremost/scalpel*

*Đáp án:*

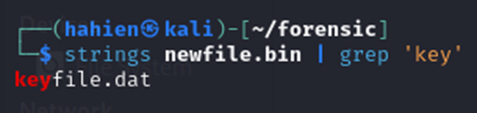
* Giải nén tệp:



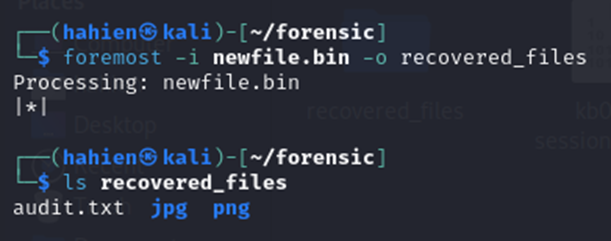
* Sử dụng dd để sao chép dữ liệu từ tệp này vào một tệp mới:

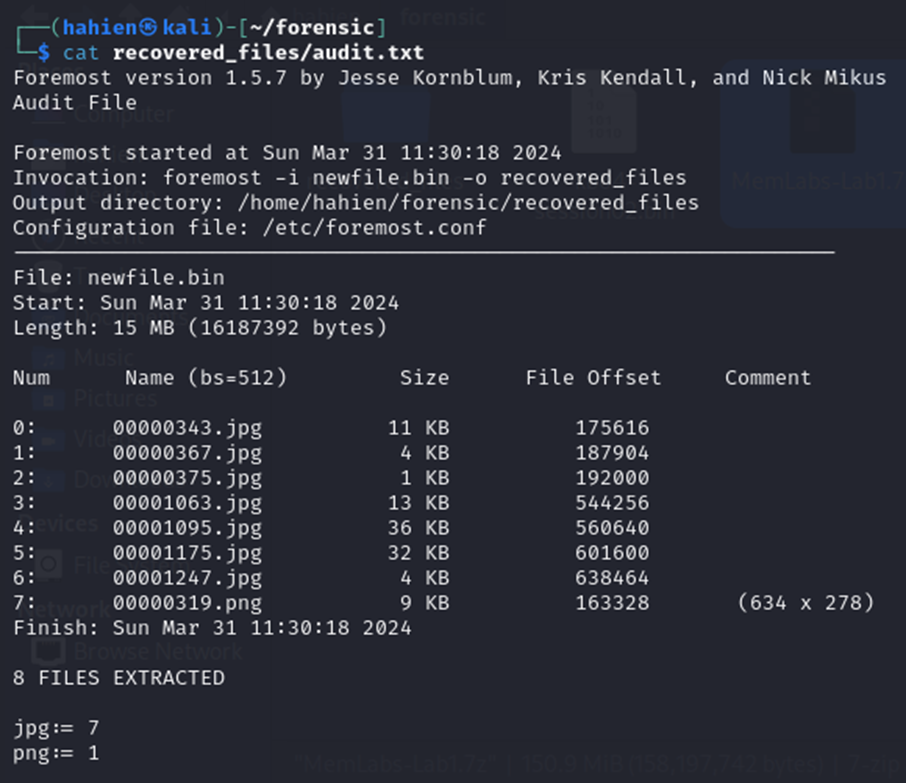


* Sử dụng strings để tìm các chuỗi có liên quan đến từ khóa "key"

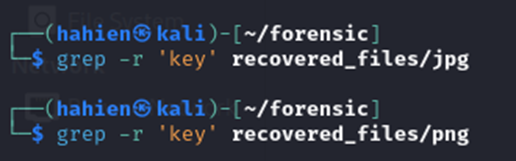


* Sử dụng foremost để phục hồi tệp

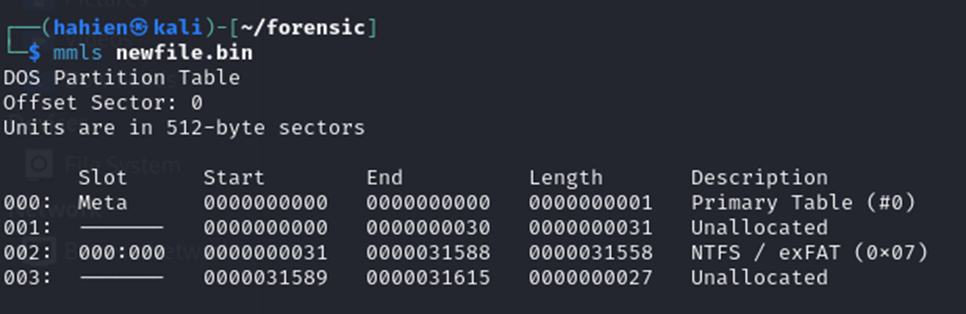




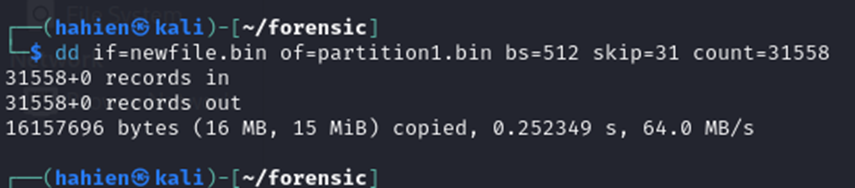
* Có vẻ như không có thứ mà chúng ta muốn tìm



* Thử dùng mmls để xem phân vùng



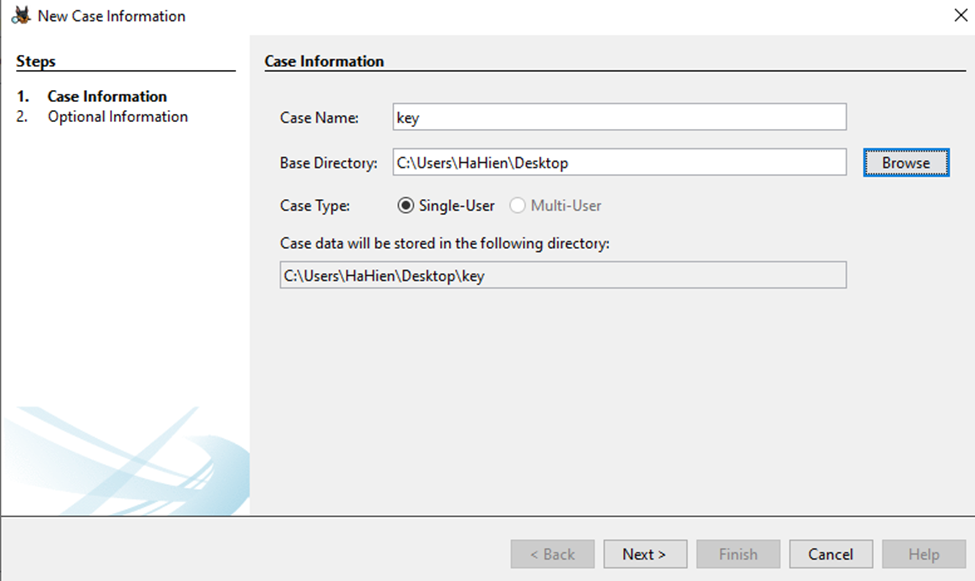
* Dựa trên kết quả của lệnh mmls, có vẻ như newfile.bin chứa một bảng phân vùng DOS với một phân vùng NTFS / exFAT. Phân vùng này bắt đầu từ sector 31 và kết thúc ở sector 31588.
* Để tiếp tục phân tích, ta có thể trích xuất phân vùng này bằng cách sử dụng dd.

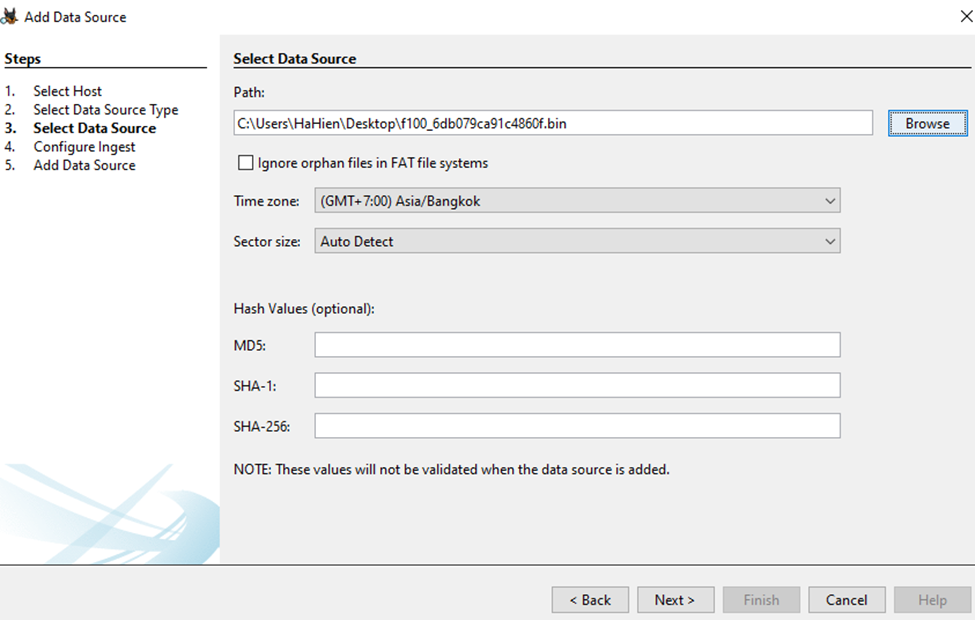


* Lệnh trên sẽ sao chép dữ liệu bắt đầu từ sector 31 và kéo dài 31558 sectors từ newfile.bin vào tệp mới có tên là partition1.bin.
* Không tìm thấy ‘key’ ở phân vùng này.

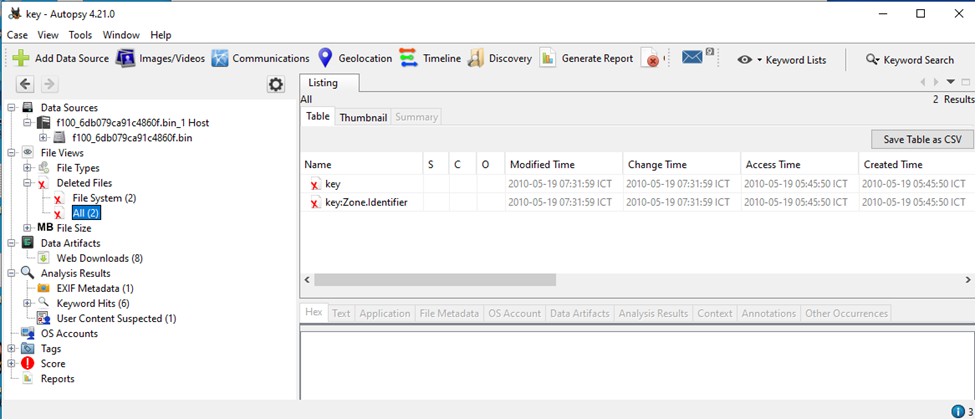


* Tương tự, tìm cấc phân vùng còn lại cũng không có phát hiện gì.
* Tiến hành dùng Autospy

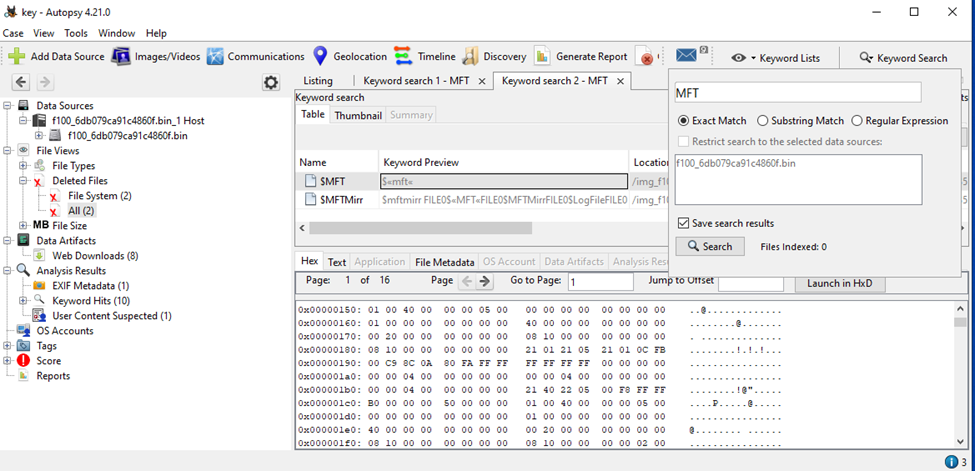




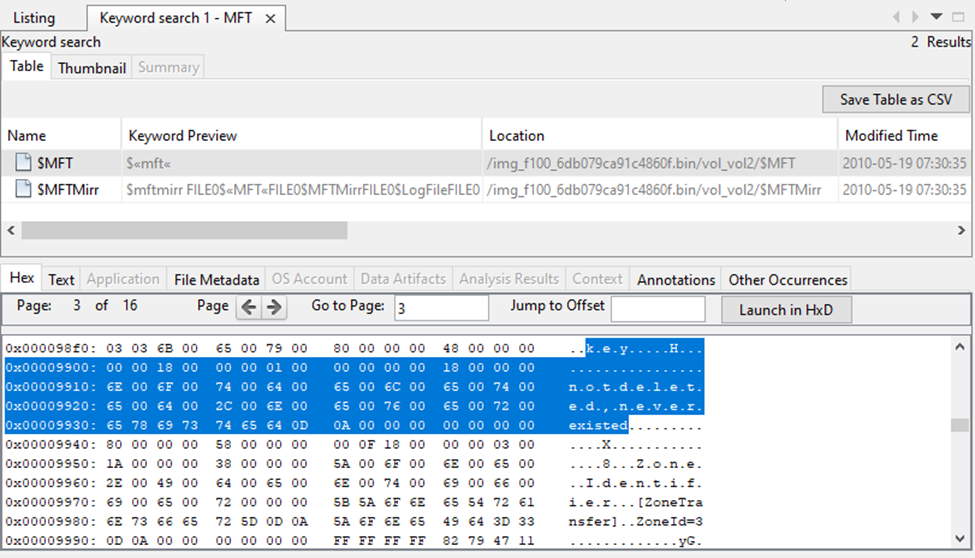
* Phát hiện file key đã bị xóa



* Tuy nhiên, NTFS có một thành phần thú vị: Master File Table (MFT) , được hiển thị trong hệ thống tệp NTFS dưới dạng $ MFT . Tiến hành xem xét nó vì nó có thể vẫn chứa các phần của tệp đã xóa.



* Tìm kiếm Key xem sao



* Tìm được nội dung của file key: “notdeleted, neverexisted”

**Kịch bản 06. Thực hiện phân tích:**

* Tài nguyên: kb06-session02.pdf
* Hãy điều tra các thông tin liên quan đến vụ án này theo một số câu hỏi gợi ý sau: Eden

▪ Thông tin đăng nhập của tài khoản truyền thông xã hội của Eden là gì?

▪ Tìm tập tin có nội dung liên quan đến nơi Eden học tập và làm việc? Ai là người viết nội dung trong đó?

▪ Giao dịch (transaction) cũ nhất được ghi lại vào ngày nào? Tìm trong mục Credit card, ghi thông tin ngày tháng gần nhất là được.

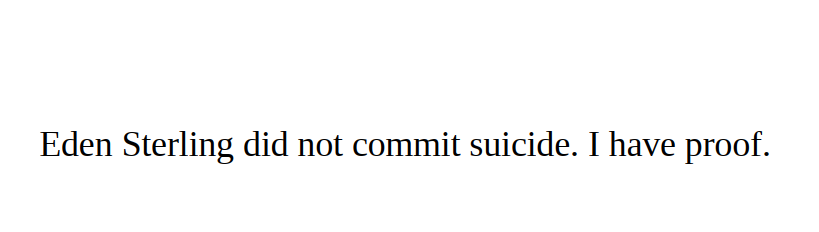
▪ Tìm tài khoản ngân hàng?

▪ Tìm file secret.txt và đọc nội dung mà Eden để lại.

▪ Tìm tấm hình Nobias.

*Đáp án:*

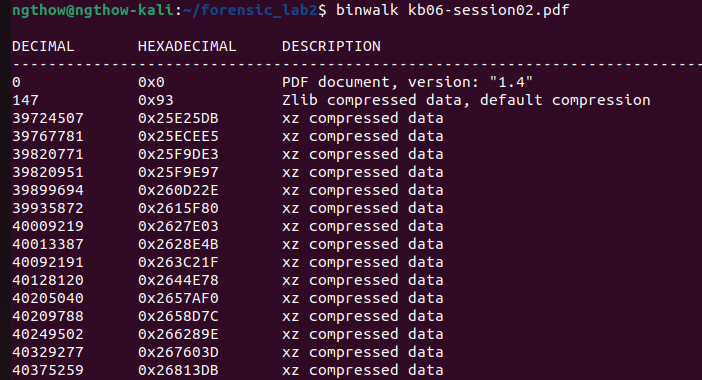
* + Mở file pdf, có nội dung như sau “Eden Sterling không tự sát. Tôi có bằng chứng.”:



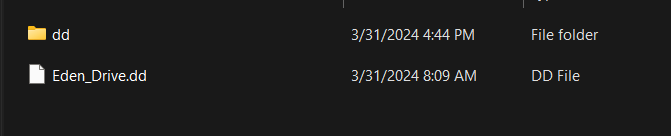
* + Dùng Autopsy để kiểm tra pdf, em thấy rằng bên trong file pdf còn chứa file nén là Eden.Drive, và giải nén ra có thể là fle Eden\_Drive.dd:



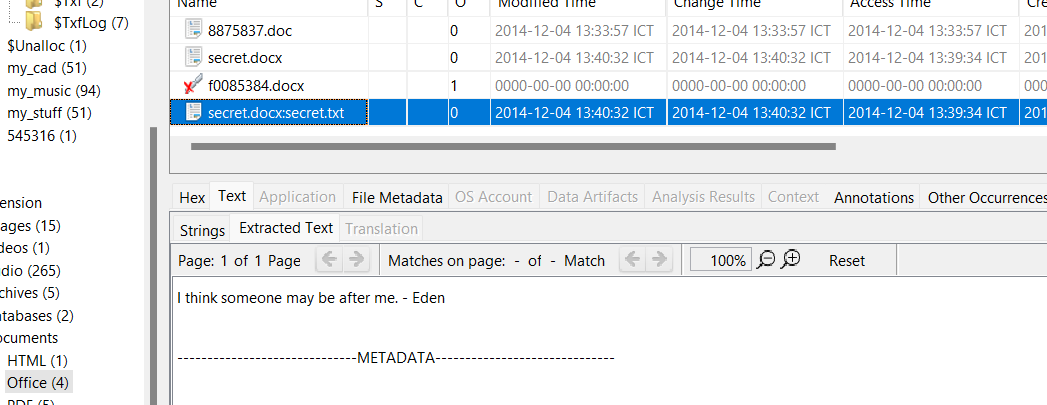
* + Kiểm tra bằng binwalk cho chắc, thì được kết quả:



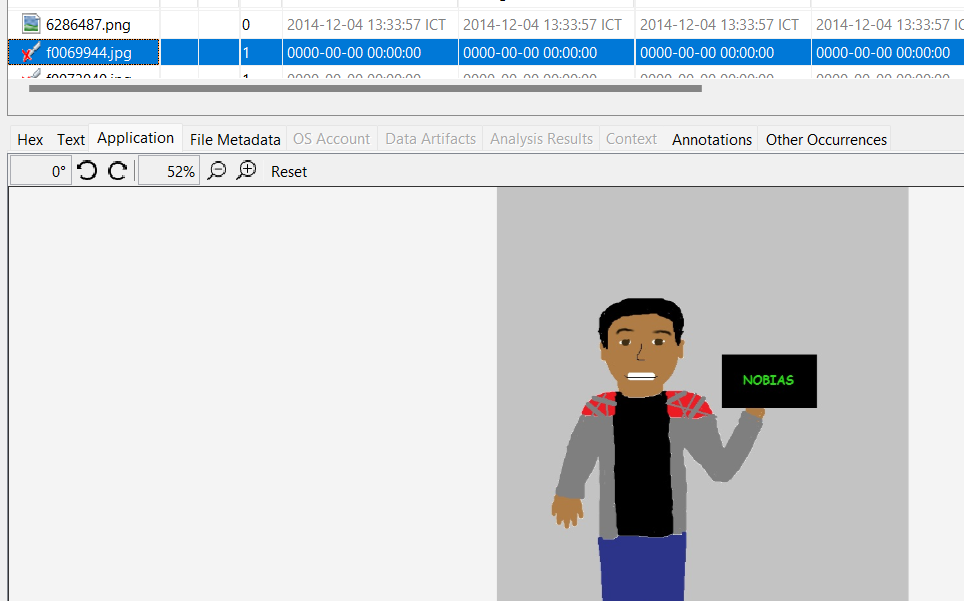
* Do đó cần giải nén tệp pdf, em sẽ sử dụng tính năng extract của Autospy, tìm được file Eden\_Drive.dd, sau đó sẽ tiếp tục dùng file này để tool phân tích:



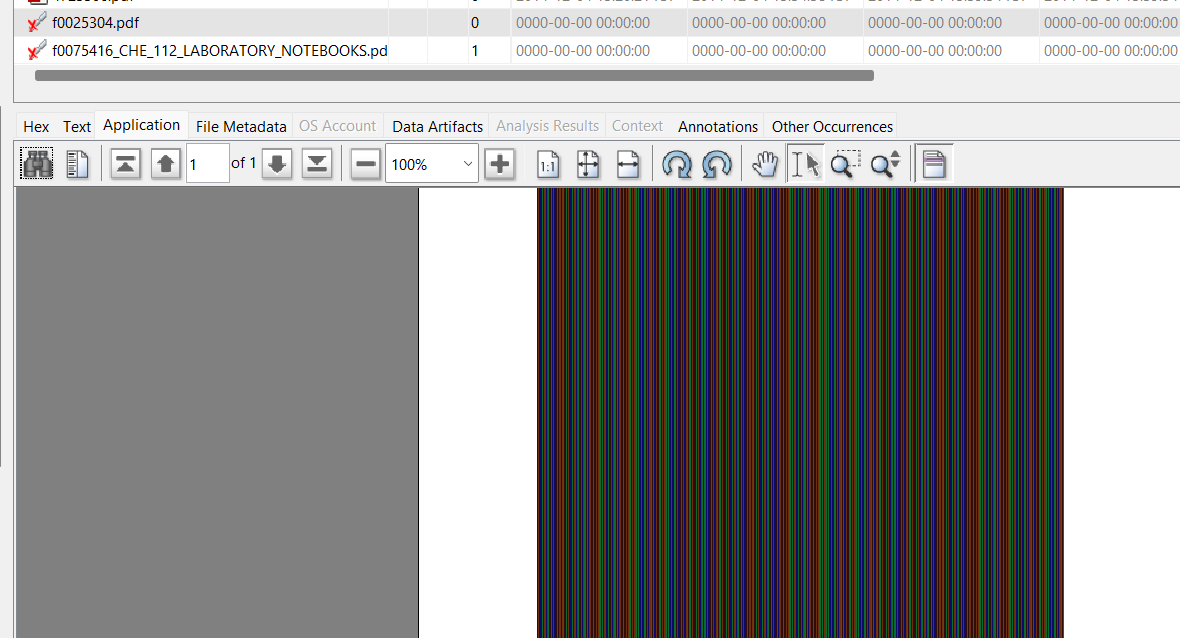
* Tìm file secret.txt và đọc nội dung mà Eden để lại:



* Tìm tấm hình Nobias:



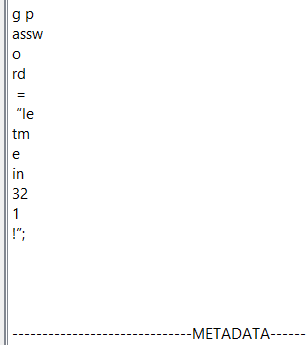
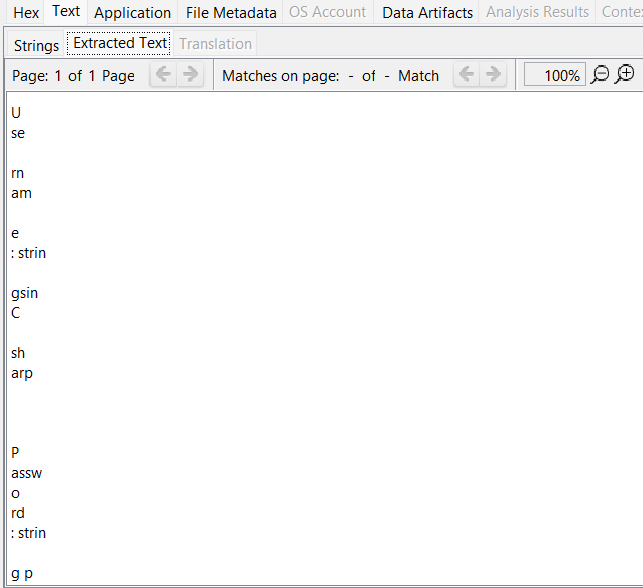
* Thông tin đăng nhập của tài khoản truyền thông xã hội của Eden là gì? Trong hình này:



Tìm được Username: stringCsharp

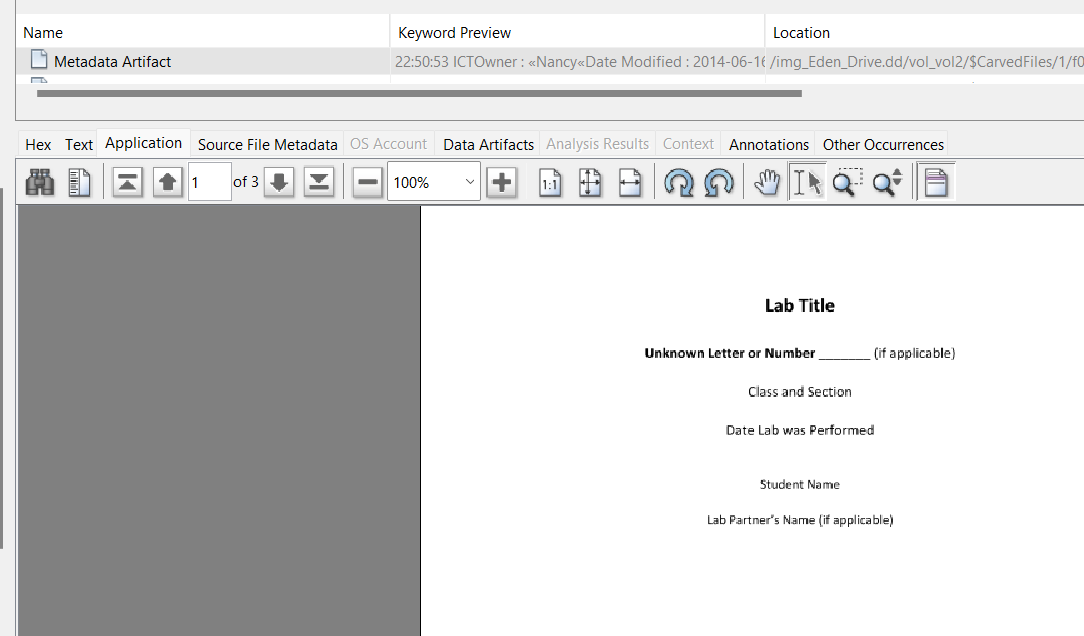
Password: letmein321!

Em tìm được cái này em thấy có động lực để làm tiếp ghê thầy ạ=))))

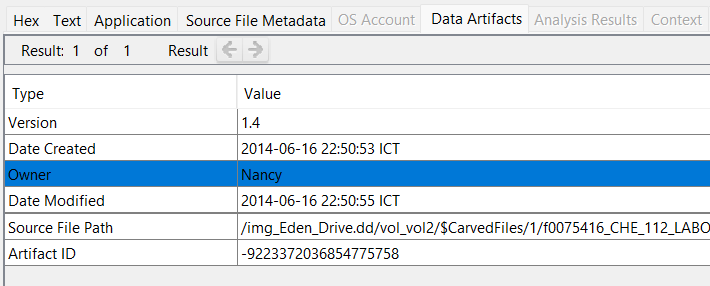


* Tìm tập tin có nội dung liên quan đến nơi Eden học tập và làm việc? Ai là người viết nội dung trong đó?

Tìm được các file chứa hình ảnh là dạng như đề thi:

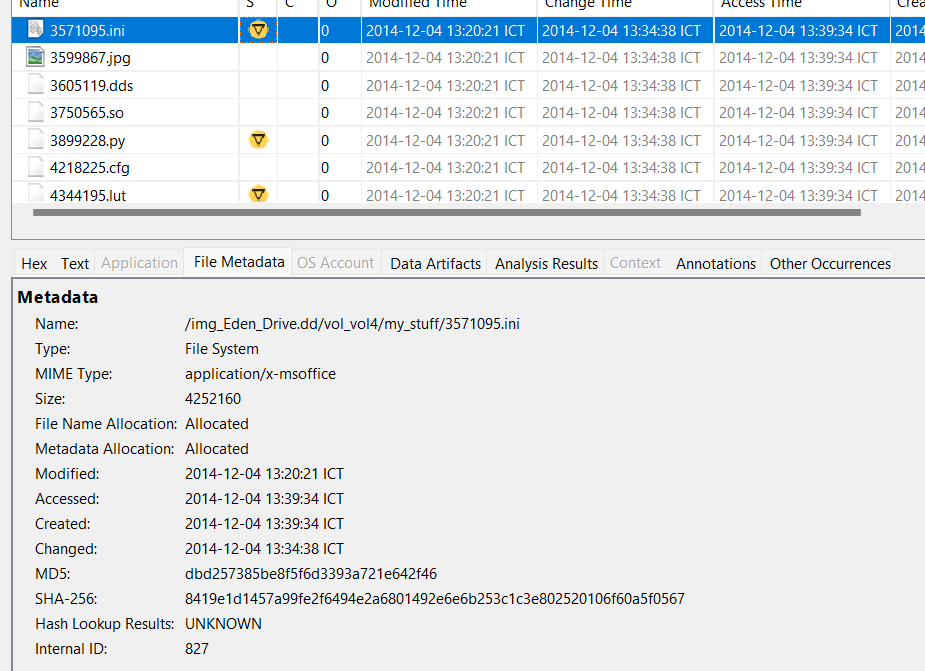


Để xem ai viết nội dung đó, sử dụng “Data Artifacts”, kết quả tác giả file là Nancy



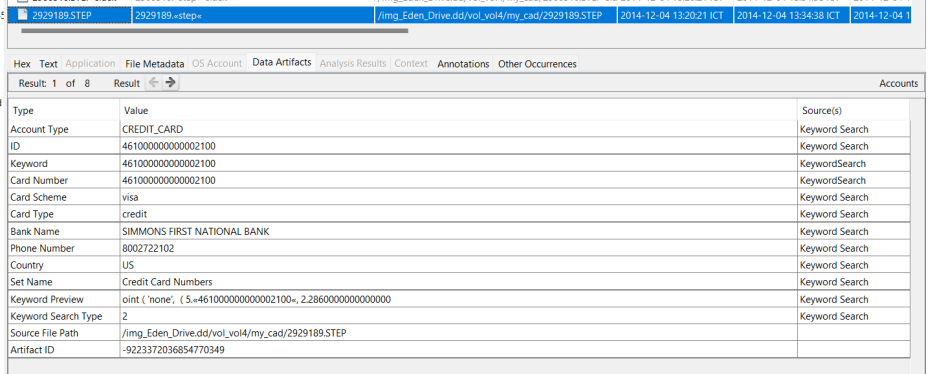
* Giao dịch (transaction) cũ nhất được ghi lại vào ngày nào? Tìm trong mục Credit card, ghi thông tin ngày tháng gần nhất là được.

Em tìm key word là “transaction”, được kết quả là 12/04/2014:





* Tìm tài khoản ngân hàng?



---

***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)