# Kịch bản

Sam, người quản lý của một tổ chức, đã gọi đến đội pháp y sau một cuộc tấn công mạng

đã diễn ra. Nhóm an toàn thông tin của Sam đã tạo ra các hình ảnh pháp lý về

máy bị ảnh hưởng với mục đích tiết kiệm thời gian và công sức của nhóm pháp y.

Đội pháp y khi đến đã kiểm tra tính toàn vẹn của các tập tin hình ảnh và bây giờ họ

cần làm quen với file ảnh. Nhiệm vụ đầu tiên của họ là hiểu tập tin

hệ thống của tệp hình ảnh và tiến hành khôi phục tệp. Để điều tra một đĩa cứng, một điều tra viên pháp y phải có kiến ​​thức kỹ lưỡng hiểu biết về các loại hệ thống tập tin và cách phân tích chúng bằng nhiều công cụ khác nhau

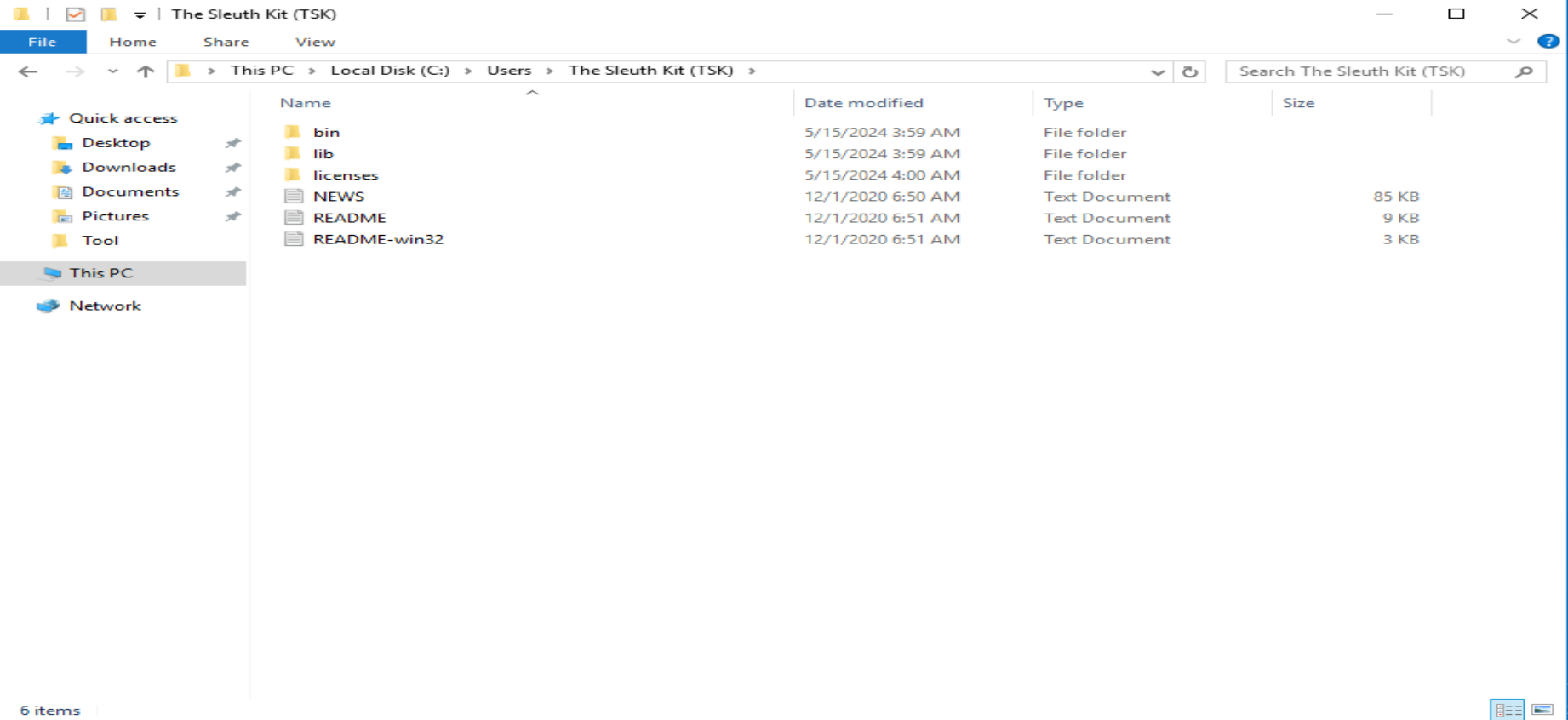
# Mục tiêu

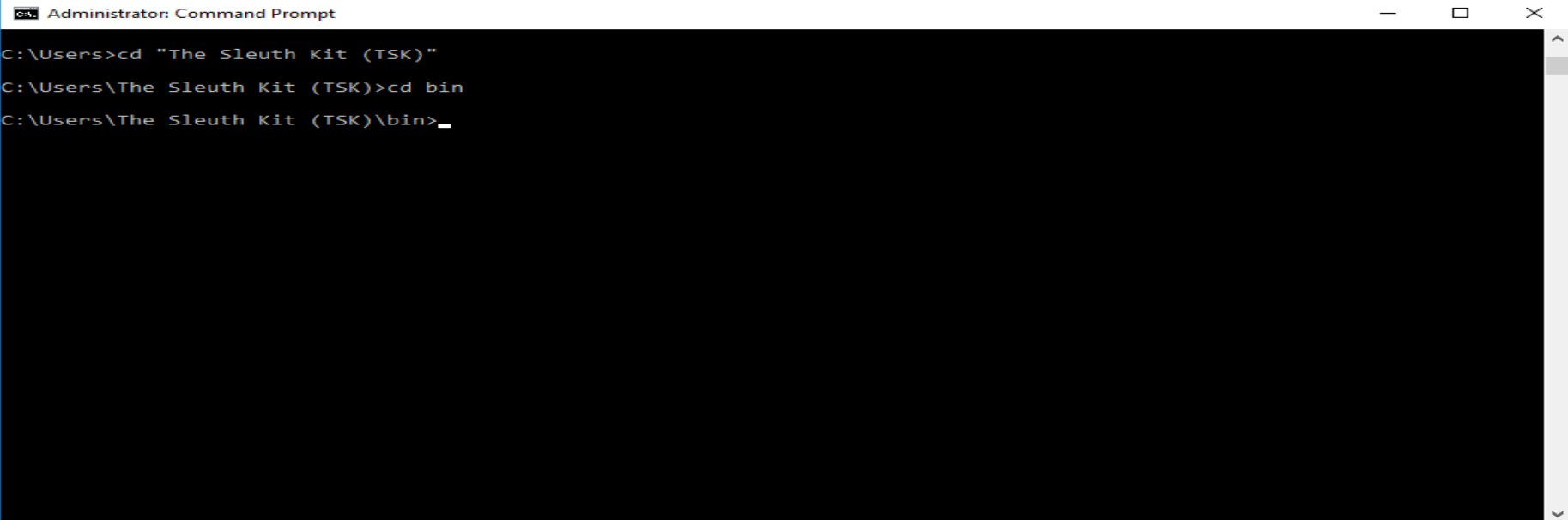
Mục tiêu của thí nghiệm này là giúp các nhà điều tra tìm hiểu và thực hiện phân tích hệ thống tệp sử dụng Bộ Sleuth. Bộ Sleuth (TSK) được sử dụng để có được những thông tin sau:

* Loại hệ thống tập tin
* Thông tin siêu dữ liệu
* Nội dung thông tin

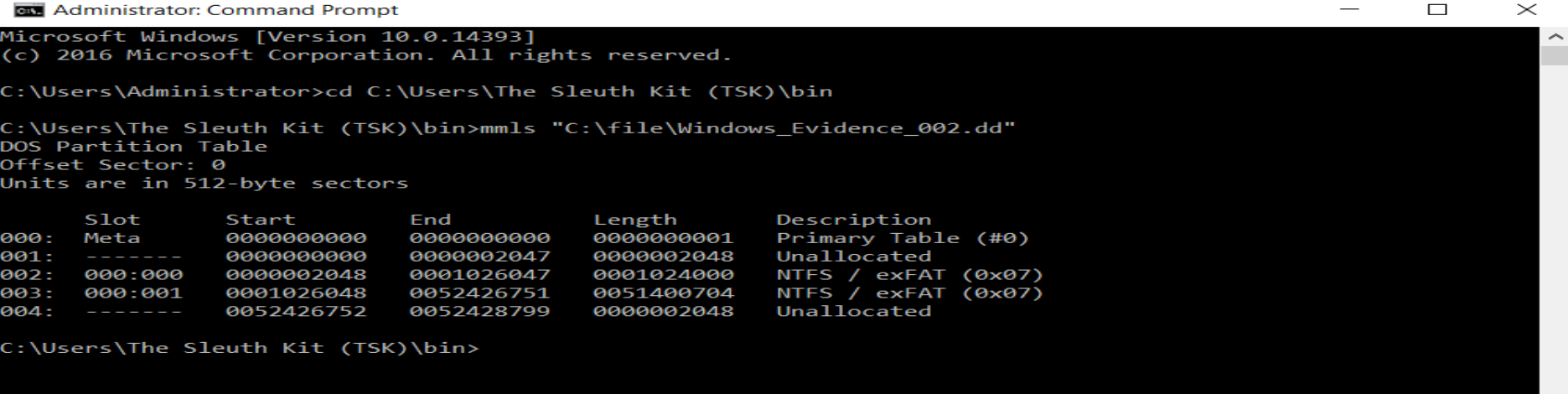
# Tổng quát

Lab này giúp bạn làm quen với việc phân tích hệ thống tệp bằng The Sleuth Kit. Nó giúp bạn hiểu cách tìm nạp thông tin từ một tệp hình ảnh, chẳng hạn như loại hệ thống tệp được sử dụng, nội dung tệp và thư mục trong hình ảnh và thông tin siêu dữ liệu liên quan đến bức hình.

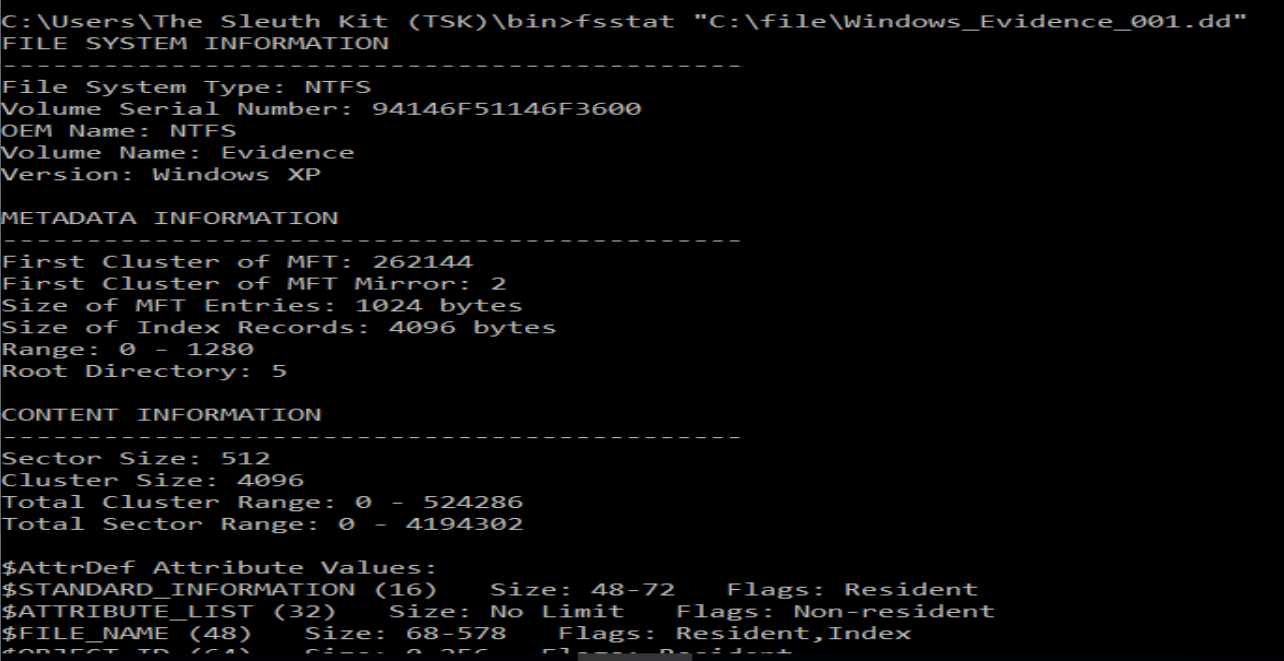




Xem các bảng phân vùng được liên kết với **Windows\_Evidence\_002.dd**

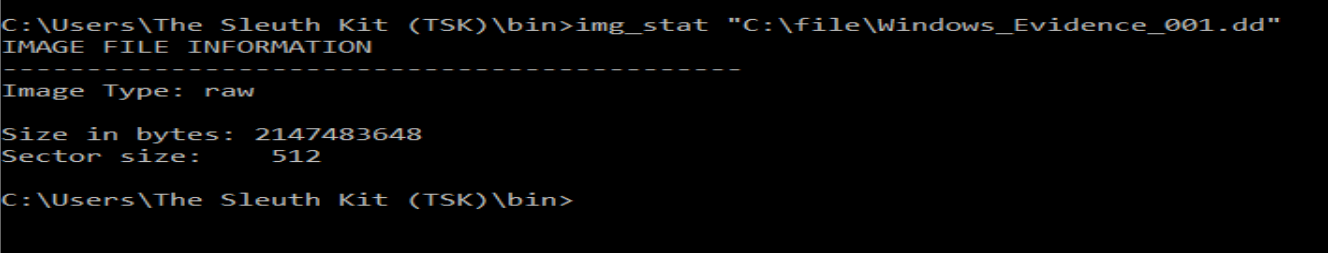
****

Xem loại hệ thống tệp và hệ điều hành liên quan đến hình ảnh

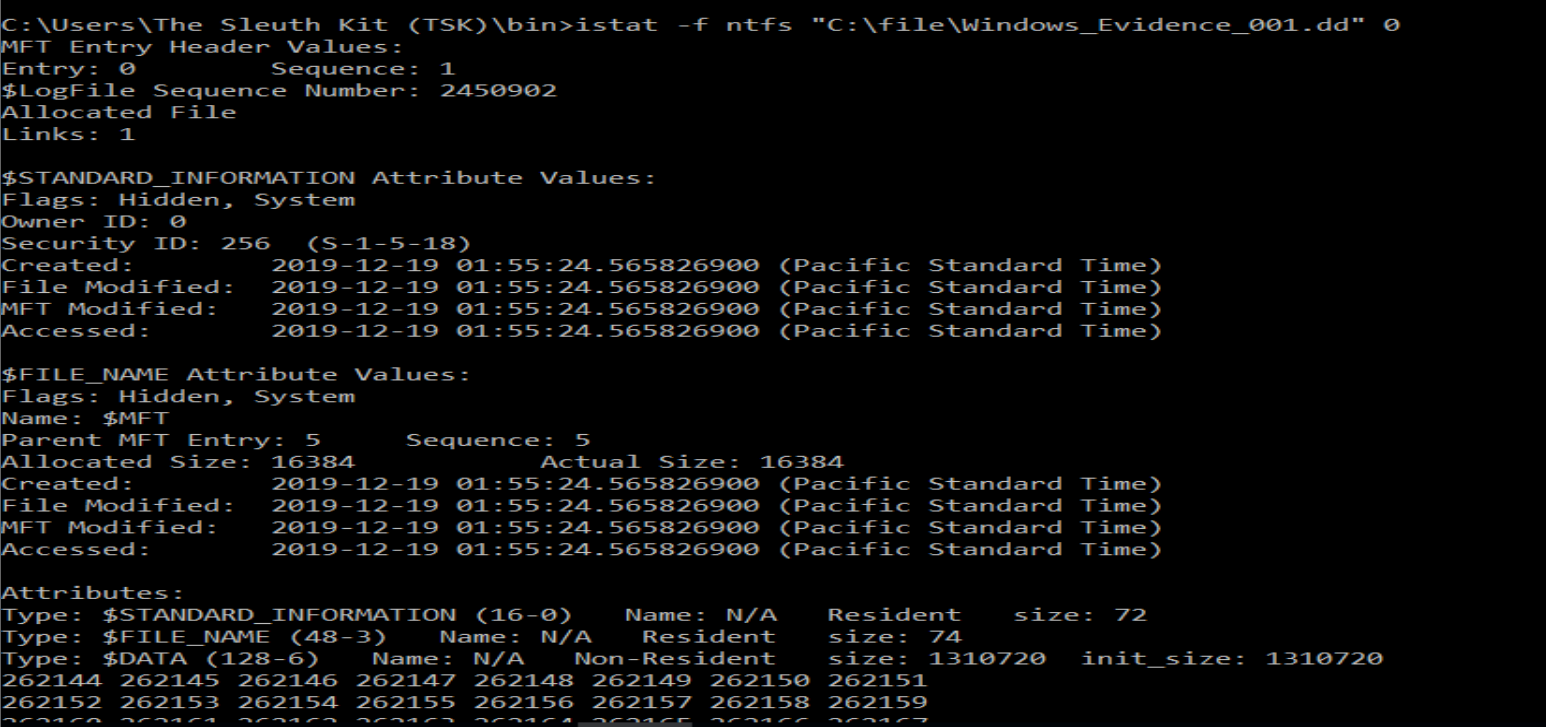


Từ ảnh chụp màn hình ở trên, có thể thấy rằng hệ thống tập tin là **NTFS** và hệ điều hành nguồn là **Windows XP.**

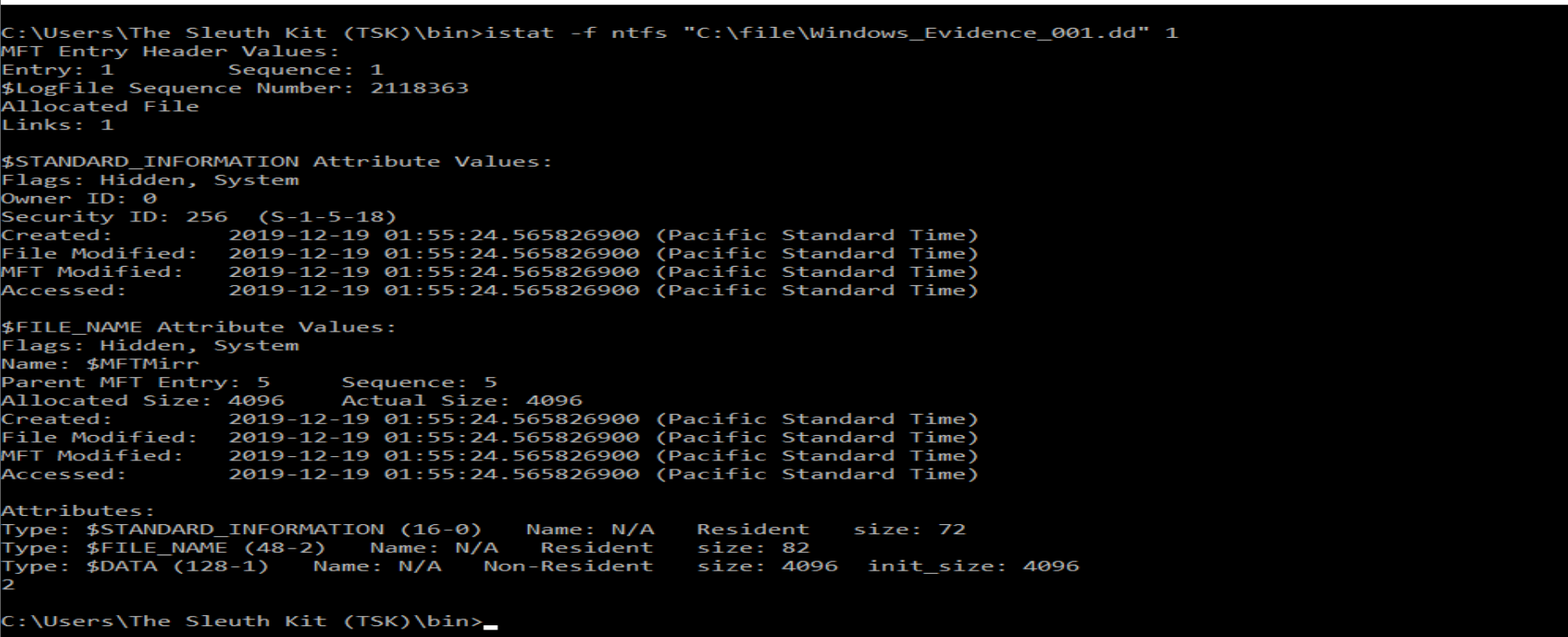
Xem chi tiết kiểu của hình ảnh đã chọn



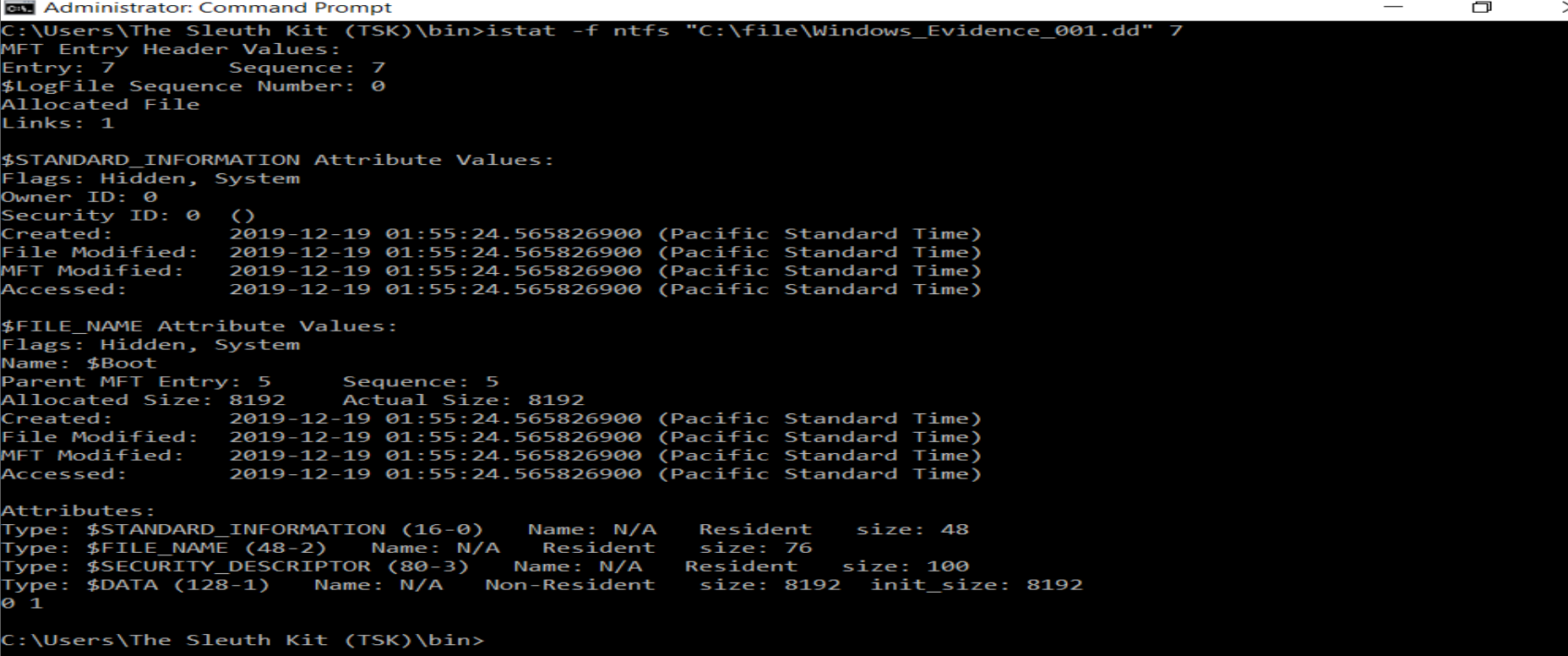
Sử dụng công cụ **istat** trong **The Sleuth Kit** để xem chi tiết cấu trúc metadata.



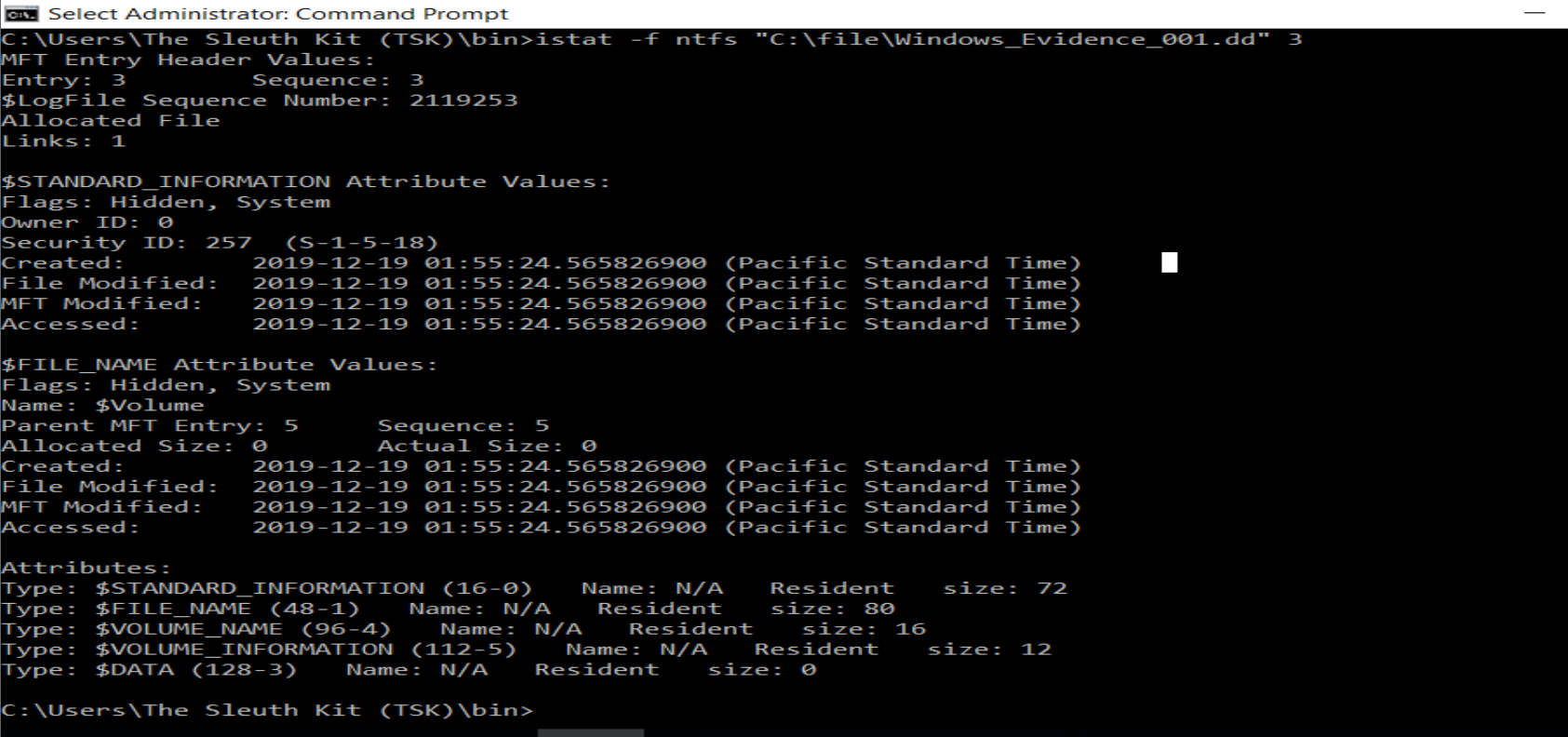
Hiển thị Tổng quan về tệp **MFTMirr**



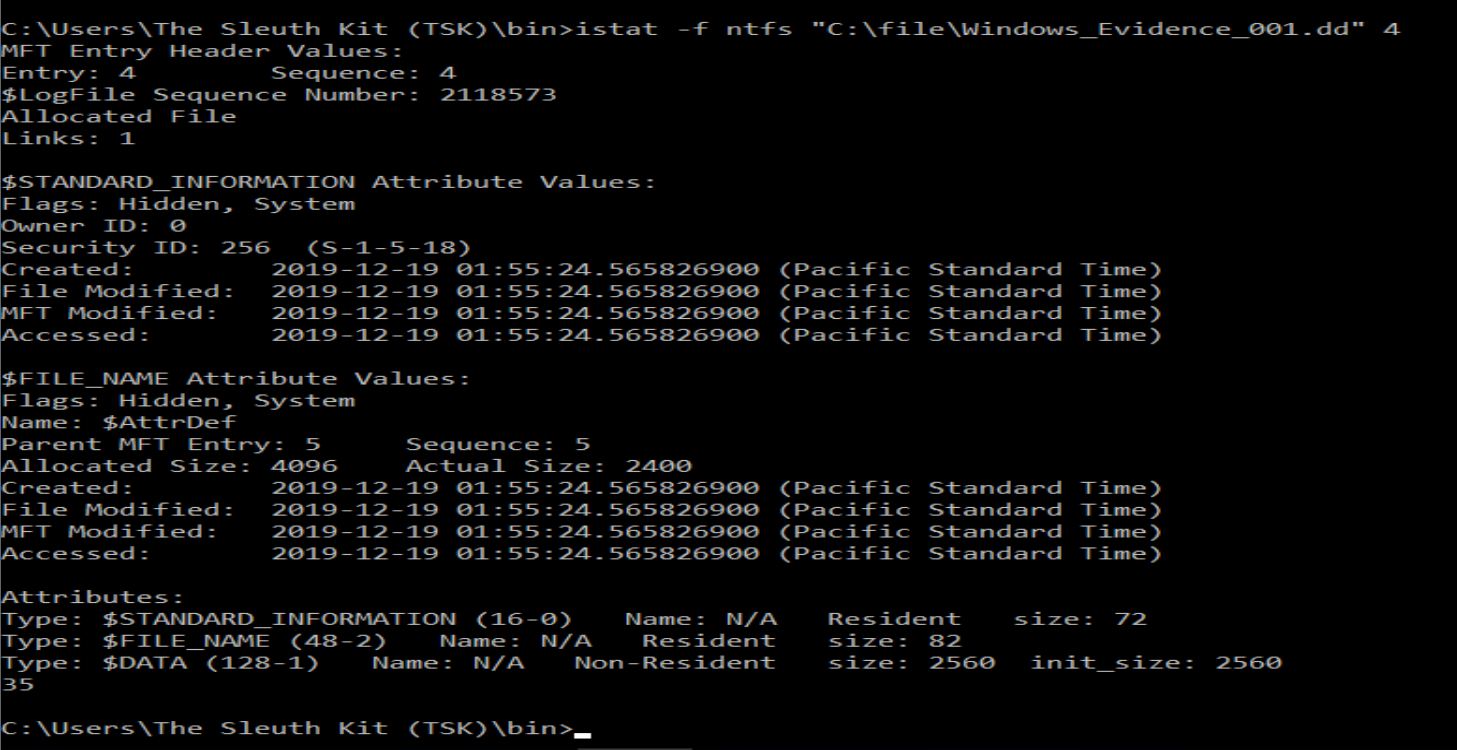
Hiển thị tổng quan về **Boot File**

****

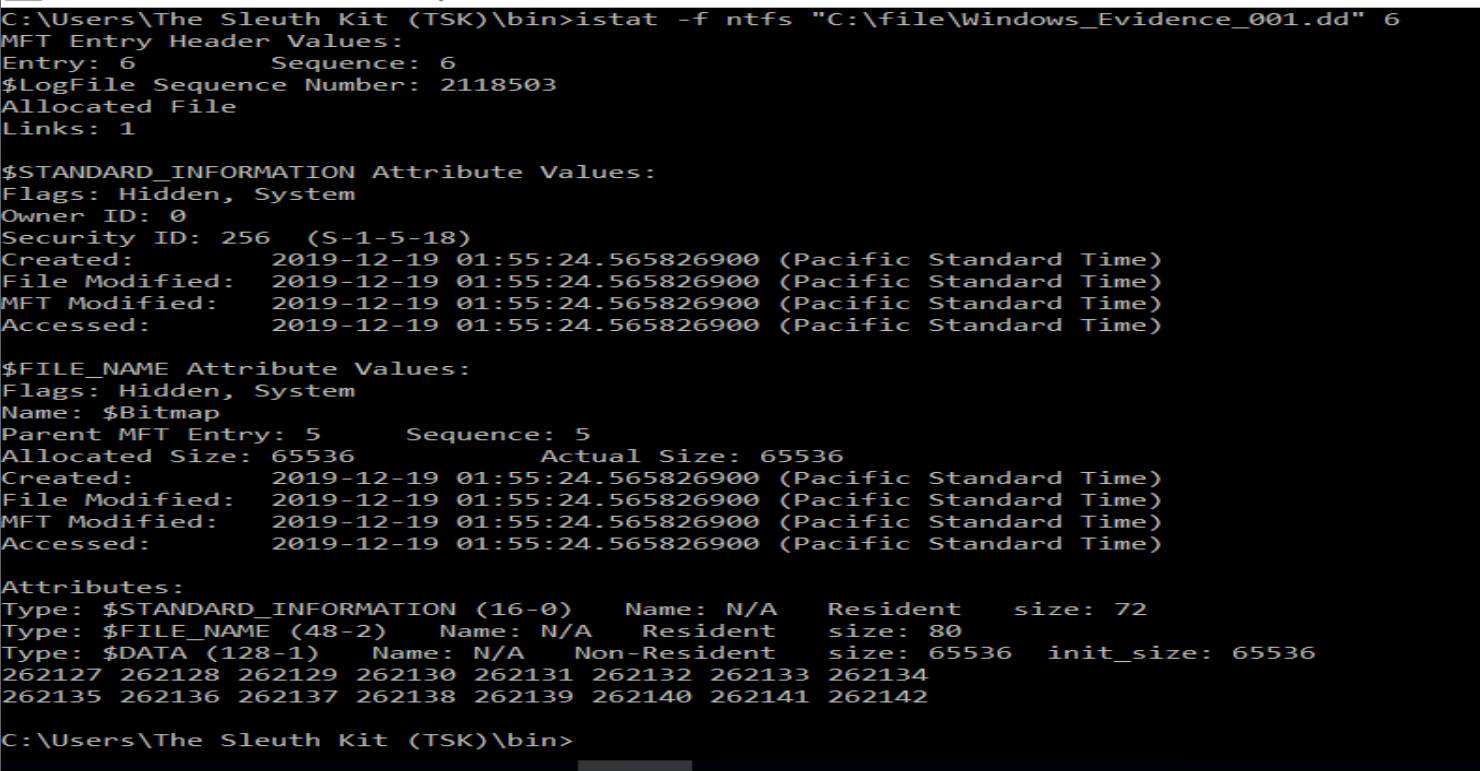
Hiển thị tổng quan về tệp **File hệ thống Metadata**

****

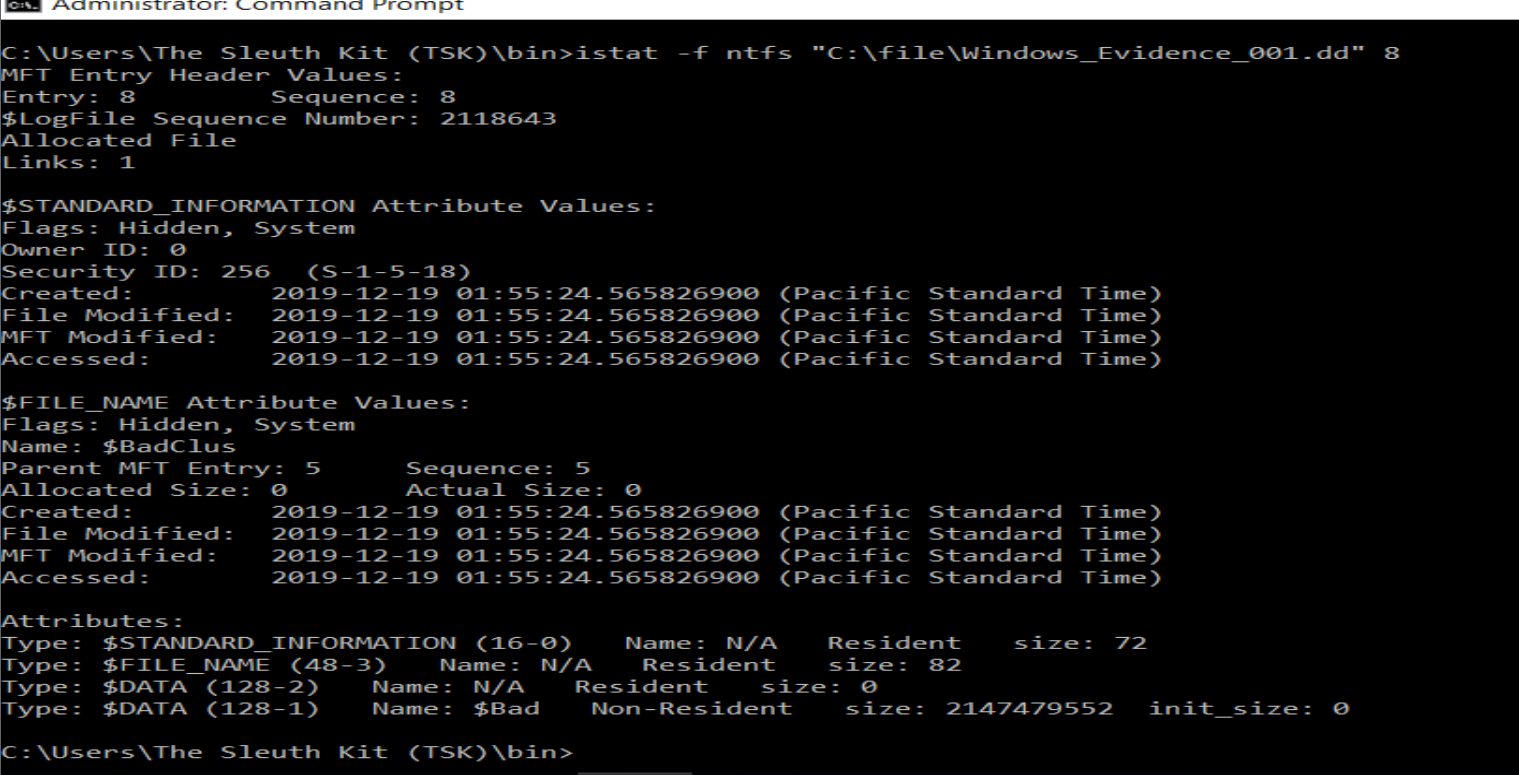
Hiển thị tổng quan về tệp **AttrDef**



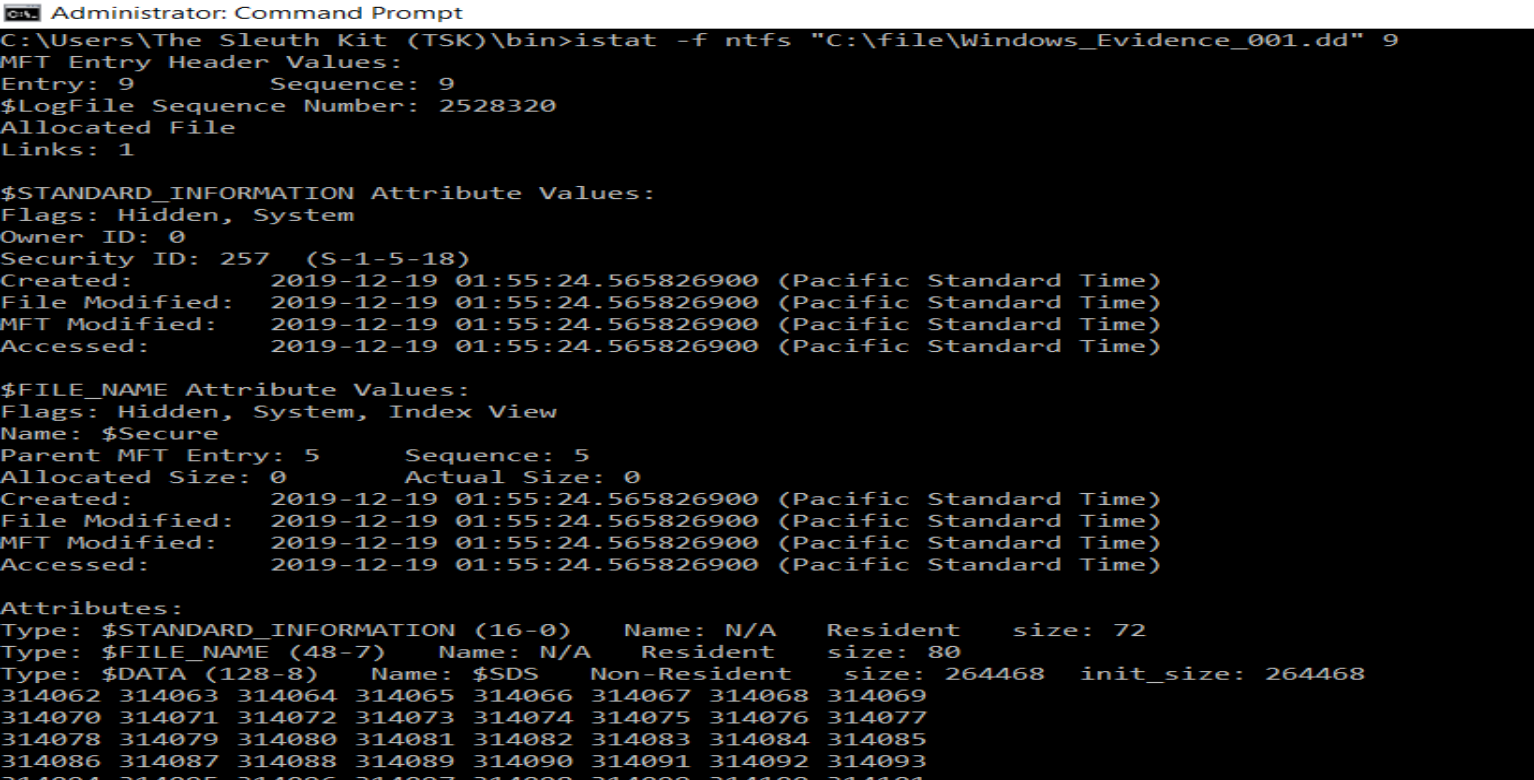
Hiển thị tổng quan về tệp **Bitmap**



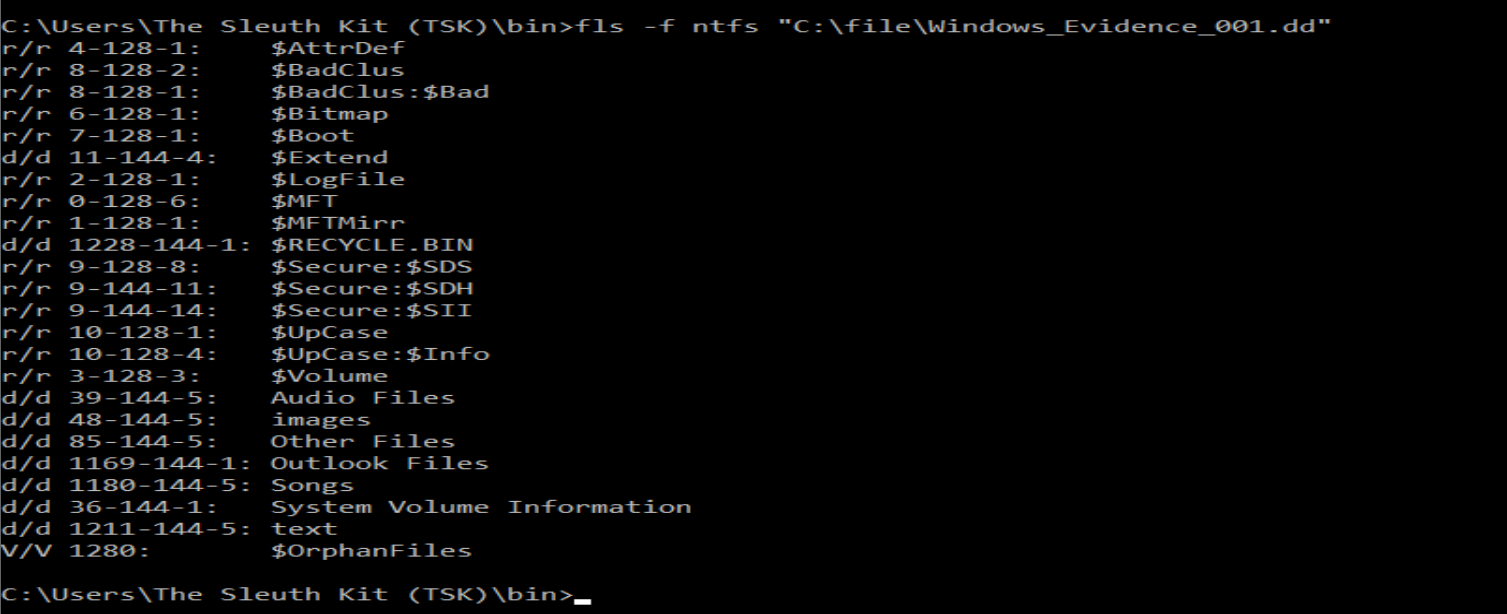
Hiển thị tổng quan về tệp **BadClus**



Hiển thị tổng quan về tệp **Secure**

****

Sử dụng công cụ dòng lệnh fls của TSK để liệt kê các tệp và tên thư mục.



Bây giờ, chúng ta sẽ khôi phục các tệp này từ hình ảnh bằng module **tsk\_recover**. Trước khi chạy **module** này, bạn cần tạo một thư mục có tên là **Retrieved Files by SleuthKit** trên Desktop.

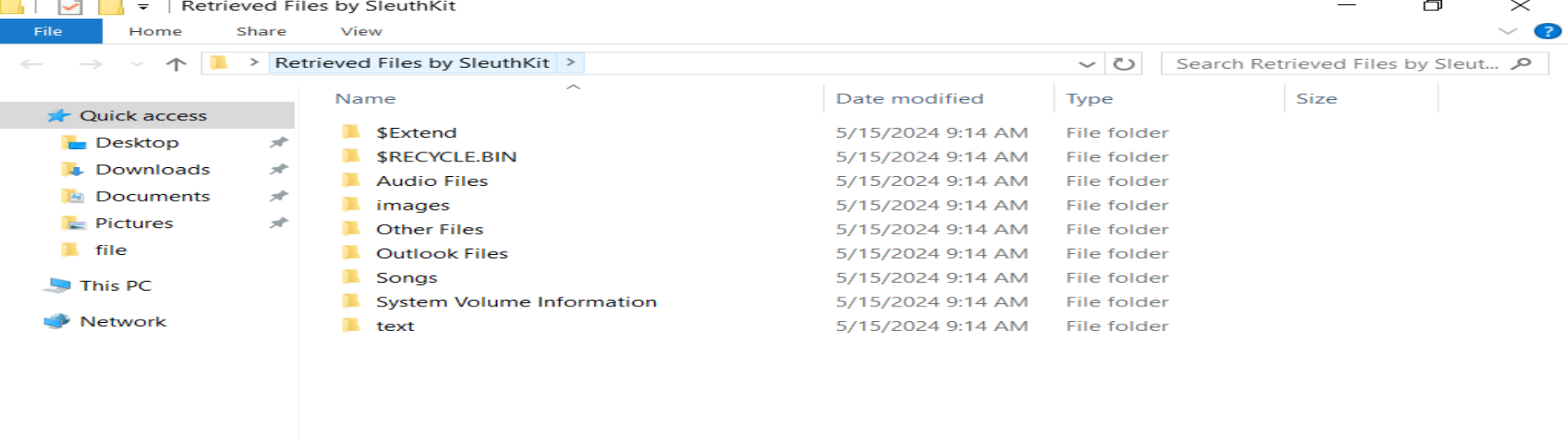
Chạy lệnh:

***tsk\_recover -i raw -e "C:\file\Windows\_Evidence\_001.dd" "C:\Users\Administrator\Desktop\Retrieved Files by SleuthKit"***

Khi hoàn tất, nó sẽ trả về một thông báo hiển thị số lượng tệp được khôi phục



Mở thư mục Retrieved Files by SleuthKit, ta có thể thấy các tệp và thư mục đã truy xuất:



Bằng cách này, ta có thể sử dụng **The Sleuth Kit** để lấy thông tin liên quan đến dữ liệu có trong tệp hình ảnh và truy xuất các tệp và thư mục từ đó.

# Kết luận

Bài lab phân tích các thuộc tính tệp và hệ thống tệp của hình ảnh phân vùng đĩa và ghi lại các kết quả liên quan đến bài tập trong phòng thí nghiệm.