**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:

A computer screen shot of text

Description automatically generated

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

A computer screen shot of a computer code

Description automatically generated

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

A computer screen with white text

Description automatically generated

* Sử dụng foremost để phục hồi tệp

A computer screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

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

A computer code on a black background

Description automatically generated

* Thử dùng mmls để xem phân vùng

A screenshot of a computer

Description automatically generated

* 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.

A screen shot of a computer program

Description automatically generated

* 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.

A computer code on a dark background

Description automatically generated

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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

* Phát hiện file key đã bị xóa

A screenshot of a computer

Description automatically generated

* 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.

A screenshot of a computer

Description automatically generated

* Tìm kiếm Key xem sao

A screenshot of a computer

Description automatically generated

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