**MASTER FILE TABLE**

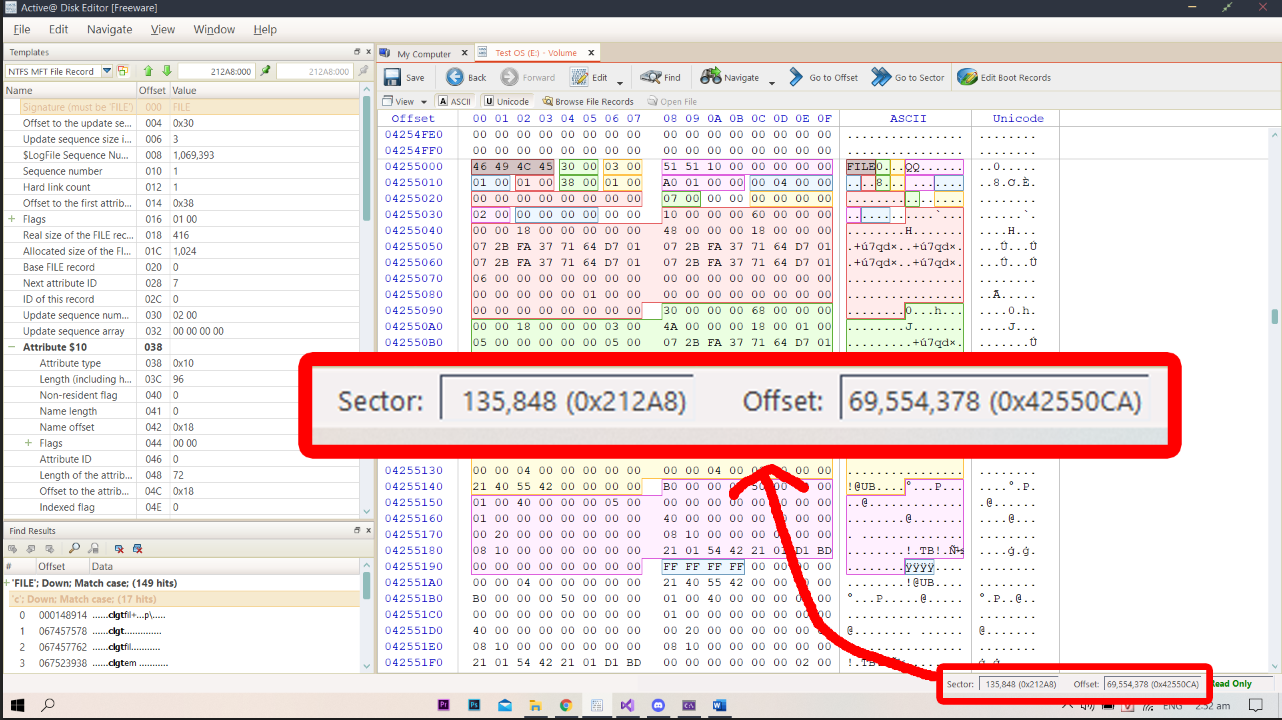
Ở đây tui dùng phần mềm [Disk Editor](https://www.disk-editor.org/index.html) để đọc thông tin trong ổ đĩa

Ở sector đầu tiên là phần thông tin của ổ đĩa ta thấy, Master file table $MFT sẽ bắt đầu tại cluster thứ 16,981 mà 1 cluster có 8 sector nên sector của $MFT sẽ là 16,981\*8 = 135,848

Ảnh có chứa bàn

Mô tả được tạo tự động

Ở đây tui đang xem xét sector thứ 135,848 sẽ bắt đầu tại Offset 69,554,176 con trỏ tui đang chỉ vào vị trí 0xCA nên nó hiển thị vị trí 69,554,378



- Muốn đọc sector thứ bao nhiêu thì set readPoint = 512 (kích thước 1 sector) \* sector thứ n

- ReadPoint ở đây có nghĩa là Byte thứ n trong file chứ không phải là sector thứ n

Ví dụ: muốn đọc sector 135,848 thì readPoint = 512 \* 135,848 = 69,554,176 (đây là vị trí bắt đầu của sector thứ 135,848)

- readPoint phải chính xác là offset bắt đầu của sector mới trả ra sector đó, không thì trả về sector đầu tiên (Partition Boot Sector)



- Có hai loại MFT entry:

+ MFT entry cho tập tin siêu dữ liệu (metadata file): chứa các thông tin mô tả về cấu trúc tổ chức của hệ thống NTFS.

+ MFT entry cho tập tin dữ liệu (data file): chứa thông tin mô tả cho các tập tin dữ liệu, có thể chứa cả phần dữ liệu của tập tin.

Ảnh có chứa văn bản

Mô tả được tạo tự động

**CẤU TRÚC CỦA 1 ENTRY MFT**

Gồm có 1 header của entry, nhiều Attribute và 1 End Mark

- Header 42 byte đầu

- Attribute các byte còn lại (1 file entry luôn có 2 attribute $STANDARD\_INFOMATION và $FILE\_NAME)

- End Mark: FF FF FF FF đánh dấu kết thúc Entry

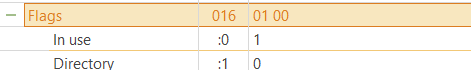
Ảnh có chứa bàn

Mô tả được tạo tự động

**HEADER**

4 byte đầu (0x00 – 0x03) [signature] luôn là 46 49 4C 45 là FILE (thể hiện đó là 1 file)

2 byte 22 và 23 (0x16 – 0x17) là cờ báo hiệu đó là file hay thư mục hoặc là file đã bị xóa



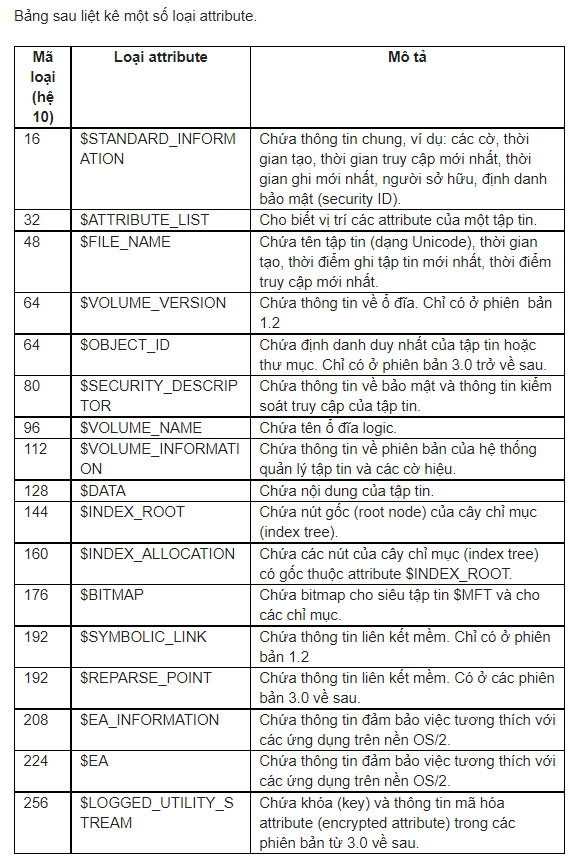
Giá trị: - 01 00: Entry đã được sử dụng

- 02 00: Là 1 thư mục đã xóa

- 03 00: Là 1 thư mục hiện còn được sử dụng

**Chú ý:** nếu xóa file/thư mục rồi nhưng Flat vẫn là 01 00 có hoặc 03 00 nghĩa là nó vẫn còn được sử dụng và nó hiện đang ở trong Recycle Bin, 1 khi đã xóa file đó trong Recycle Bin thì Flat sẽ hạ 00 00

**ATTRIBUTE**



Ở đây đang xét dãy byte của attribute có bắt đầu từ byte 0

- Loại Attribute: 4 byte đầu của attribute đó (little endian)

Ví dụ: 10 00 00 00h sẽ tương ứng 16d -> là attribute $STANDARD\_INFOMATION

- 4 byte tiếp theo (byte[4] – byte[7]) độ dài của attribute đó (bao gồm cả header của attribute đó) dùng để tính toán nhảy qua các attribute khác khi đã đọc hết thông tin trong attribute đó

**$FILE\_NAME**

- File attribute để biết là loại file gì từ byte[80]-byte[83] (hệ thống, ẩn, thư mục,…)

Từ đó có thể lọc ra các file hệ thống như $MFT, $MFTMirr,…

**Ảnh có chứa văn bản, máy tính, ảnh chụp màn hình

Mô tả được tạo tự động**

- Tên file byte[90] đến hết attribute

- Phần nội dung bắt đầu từ byte[24]-byte[31] của attribute $FILE\_NAME là địa chỉ của folder cha (file reference)

Ảnh có chứa bàn

Mô tả được tạo tự động

**NỘI DUNG CỦA FILE**

Xét attribute $DATA

Xét non-resident flat tại byte[8] nếu giá trị là 0 thì là file Resident (phần nội dung file nhỏ nên được ghi trực tiếp trong entry) và ngược lại

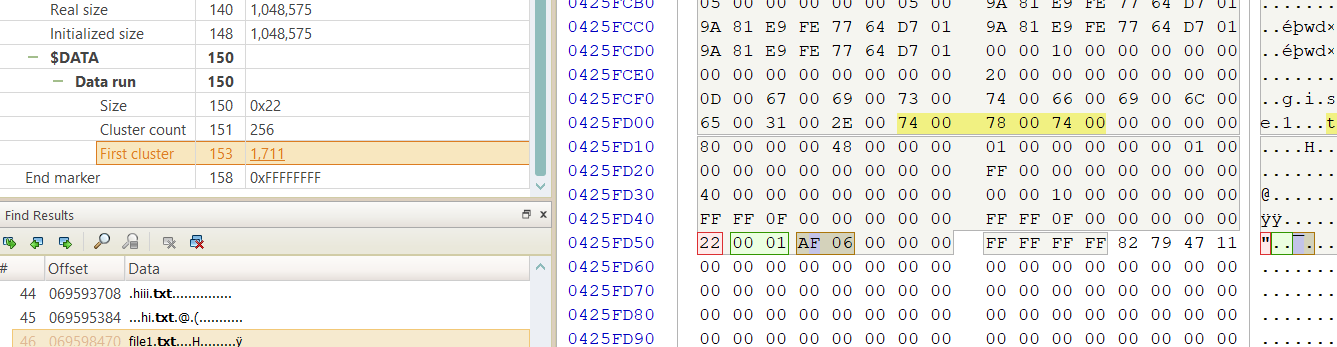
**Trường hợp**

**Non-resident flat: 0**

Phần nội dung Byte[24] đến hết

**Non-resident flat: 1**

Trong $DATA sẽ có phần First cluster byte[67-68] trong data run là cluster bắt đầu chứa dữ liệu ở đây First clusterl;à 1,711 -> sector 13,688



Di chuyển đến sector 13,688 đây là nội dung của file đọc đến khi thấy 00 00 00

Ảnh có chứa văn bản, máy tính, trong nhà, máy tính xách tay

Mô tả được tạo tự động

**$INDEX\_ROOT**

Nếu Entry là 1 folder sẽ có attribute $INDEX\_ROOT

Các file con sẽ là sector nằm sau đó (đọc trong phần Data run sẽ ra sector entry của file đó)

Check nếu File reference chính xác là vị trí sector folder cha thì in ra

**REFERENCE**

<https://flatcap.org/linux-ntfs/ntfs>

<https://legiacong.blogspot.com/2014/04/he-thong-quan-ly-tap-tin-ntfs-6-mft-mft.html?fbclid=IwAR0C07fR7LhSMi4xxa-VahdaAaAR0Z-mXGobDzUpRccC7sU4HR-Zci3AgPE>

<https://www.ntfs.com/ntfs-mft.htm>