# Cách đọc ổ đĩa dạng NTFS

## Bước 1:

* Lấy tên ổ đĩa và cho chương trình đọc file hệ thống của ổ đĩa đó.
* Nếu không tồn tại thì thoát.

## Bước 2:

* Đọc 512-byte đầu tương ứng với VBR (Volume Boot Record)
* Và lưu cái thông số chính cần quan tâm:
  + OEM ID. (0x3 🡪 0xA)
  + Số bytes mỗi sector. (0xB, 0xC)
  + Số sector mỗi cluster. (0xD)
  + Số sectors dự trữ. (0xE, 0xF)
  + Tổng số sector. (0x28 🡪 0x2F)
  + Cluster bắt đầu của $MFT. (0x30 🡪 0x37)

(Quy đổi ra sector bằng cách nhân với số byte/sector và sector/cluster)

* + Cluster bắt đầu của $MFTMirr. (0x38 🡪 0x3F)
  + Số byte mỗi $MFT record (2 mũ với giá trị tại 0x40, đọc kiểu có dấu)

## Bước 3: Đọc MFT

* Nhảy đến vị trí bắt đầu của $MFT và đọc MFT đầu tiên.
* Lưu lại số lượng sector của tất cả cả $MFT record.

## Bước 4: Bắt đầu đọc các MFT record

* Tính số lượng $MFT record bằng cách lấy tổng số sector đã tính chia cho thương của byte/MFT record và byte/sector.
* Lần lượt duyệt qua từng record và đọc số byte tương ứng.
* Nếu dãy byte bắt đầu là “FILE” thì đọc tiếp, nếu không thì đọc tới record tiếp theo.
* Đọc các byte tại 0x2C 🡪 0x2F để lưu số hiệu của record này.

## Bước 5: Standard Information

* Đọc và tính vị trí bắt đầu của Standard Information ở byte thứ 0x14, 0x15 của MFT.
* Kiểm tra xem mã thuộc tính (4 bytes đầu tiên) có phải là 0x10 hay không.
* Lấy phân quyền của file tại 0x20 🡪 0x23 (tính từ đầu standard information).

## Bước 6: File name

* Nhảy qua hết phần Standard Information
* Kiểm tra mã thuộc có phải là 0x30 hay không, nếu không thì nhảy tiếp 1 lần nữa phần Attribute List.
* Đọc số hiệu của record cha tại 0x0 🡪 0x5 (tính từ vị trí bắt đầu của file name)
* Đọc phân quyền của file tại 0x38 🡪 0x3B.
* Đọc kiểu định dạng tên (0x41) và độ dài tên (0x40).
* Phần tên được lưu N bytes đã đọc từ 0x42.

## Bước 7: Data

* Tương tự như File Name, đọc và nhảy qua các thuộc tính tương ứng đến thuộc tính có mã là 0x80.
* Tại đây, nếu dữ lớn hơn 700 bytes sẽ được lưu dưới dạng non-resident, ngược lại là resident.
* Nếu thuộc tính này lưu dạng resident
  + Vị trí bắt đầu nội dung (0x14, 0x15)
  + Độ dài nội dung (0x10 🡪 0x13)
  + Phần nội dung đọc từ vị trí của vị trí bắt đầu nội dung đã tính trên.
* Nếu thuộc tính lưu dưới dạng non-resident, phần dữ liệu này sẽ được lưu dưới dạng các data-runs.

## Bước 8: Nối các record con đến record cha của nó

* Mỗi record được đọc đều được đánh số hiệu tương ứng.
* Lần lượt duyệt qua các record, các record con cha và con sẽ có lần lượt có số hiệu và số hiệu record cha giống nhau.
* Nếu record có số hiệu cha và chính nó giống nhau tức là vị trí gốc của thư mục.

# Cách đọc các data-runs

Lần lượt các data-run bao gồm phần header, length, offset.

Các data-run sẽ được xếp liền kề nhau.

Header có dạng 0xXY với:

* Y: số byte của phần length (bắt đầu từ sau header)
* X: số byte của phần offset (bắt đầu sau phần length)

Ví dụ, giả sử chúng ta có các dãy byte sau:

11 03 07 32 AD E1 4C 1A 01 00 00 ….

Ở đây chúng ta có 2 data-runs:

* Data-run 1:
  + 1 byte length, 03 clusters long.
  + 1 byte offset, cluster 07.
* Data-run 2:
  + 2 bytes length, AD E1 clusters long.
  + 3 bytes offset, cluster 4C 1A 01.

Phía sau data-run thứ 2 là 00, tức là không còn data-run nào khác nữa.