Báo Cáo Đồ Án Hệ Điều Hành

Project 01 – Quản lý hệ thống tập trên Windows

19127102 – Võ Hoàng Gia Bảo

19127406 – Ngô Huy Hoàng

19127457 – Nguyễn Tuấn Kiệt

Logo

Description automatically generated

Bộ môn Cơ sở trí tuệ nhân tạo

Khoa Công nghệ thông tin

Đại học Khoa học tự nhiên TP. HCM

I.Mục lục:

1. Bảng phân công công việc

2. Đánh giá mức độ hoàn thành trên từng yêu cầu và toàn bộ project

3. Mô tả các bước thực hiện

a. FAT32

b. NTFS

4. Hình ảnh (chụp màn hình) demo chương trình ứng với các trường yêu cầu

a. USB FAT32

b, USB NTFS

5. Nguồn tham khảo

a. Vùng FAT32

b. Vùng NTFS

II.Mô tả mức độ hoàn thành và quy trình thực hiện:

1.Bảng phân công công việc:

|  |  |  |  |
| --- | --- | --- | --- |
| MSSV | Họ tên | Chức vụ nhóm | Công việc phân công |
| 19127102 | Võ Hoàng Gia Bảo | Trưởng nhóm | FAT32 boot sector, RDET (100%) |
| 19127406 | Ngô Huy Hoàng | Thành viên | FAT32 SDET, in cây thư mục (100%) |
| 19127457 | Nguyễn Tuấn Kiệt | Thành viên | FAT32 đọc nội dung file text, NTFS boot sector (100%) |

Cả 3: + NTFS đọc RDET, SDET: 100%

+ NTFS hiển thị cây thư mục: 50%

+ NTFS đọc nội dung file text: 0%

2. Đánh giá mức độ hoàn thành trên từng yêu cầu và toàn bộ project:

|  |  |  |
| --- | --- | --- |
|  |  | Mức độ hoàn thành |
| 1.Đọc các thông tin chi tiết của một phân vùng | Với phân vùng FAT32 | 100% |
| Với phân vùng NTFS | 100% |
| 2. Hiển thị thông tin cây Thư mục của phân vùng | Với phân vùng FAT32 | 100% |
| Với phân vùng NTFS | 60% |

**Chức năng còn thiếu NTFS:**

+ Chưa sắp xếp cây thư mục theo trật tự

+ Chưa đọc được nội dung file text

3.Mô tả các bước thực hiện:

a. FAT32

Tạo các struct để dễ dàng đọc và lưu dữ liệu

A screenshot of a computer

Description automatically generated with medium confidenceGraphical user interface, text

Description automatically generatedText

Description automatically generated

Sau khi nhập thông tin của ổ đĩa cần đọc, chương trình sẽ đọc thông tin của boot sector của ổ đĩa FAT32

Text

Description automatically generated

Sau đó tiến hành copy số bytes từ sector vào các nội dung của boot sector

Text

Description automatically generated

Text

Description automatically generated

Tiến hành đọc cây thư mục gốc và bảng fat

Text

Description automatically generated

Text

Description automatically generated

Nối tên từ các entry phụ của entry chính

Text

Description automatically generated

Text

Description automatically generated

Tiến hành in các thông tin của tập tin / thư mục ( mặc định thư mục có size = 0)

Text

Description automatically generated

Sau khi đọc thông tin của tập tin / thư mục, nếu là thư mục thì sẽ đọc tiếp cây thư mục con, và nếu là tập tin file text thì sẽ in ra nội dung file text đó

Text

Description automatically generated

Hàm ReadSRDETFAT32 tương tự hàm ReadRDETFAT32 đọc cây thư mục gốc, lấy số cluster của thư mục và tra bảng fat để ra được cây thư mục con

b. NTFS

Sử dụng thư viện Sean Barrett’s data structures để mọi thứ đơn giản

Text

Description automatically generated

Hàm đọc từ 1 vị trí, giá trị truyền vào tên ổ đĩa, buffer lưu các bytes đọc, vị trí, số bytes cần đọc

Text

Description automatically generated

Sử dụng assert trong suốt quá trình thay vì kiểm tra lỗi, ta có thể muốn thay thế những thứ này sau, nhưng việc đọc trực tiếp từ MFT không phải là việc ta phải làm. Trình điều khiển hệ thống tệp có thể đang cập nhật MFT khi ta đọc nó, vì vậy có thể có conflicts trong dữ liệu thu được.

Tạo struct như bên FAT32 để lưu trữ boot sector

Text

Description automatically generated

Các trường cụ thể của header

Text

Description automatically generated with medium confidenceText

Description automatically generated with medium confidence

Có một số attributes bổ sung khác nhau cho các thuộc tính Non-Resident và Resident.

Bọc các cấu trúc này trong pragma để trình biên dịch không thêm phần padding.

MFT được chia nhỏ thành các phần bằng nhau gọi là MFT entry. Kích thước của một MFT entry được quy định trong BPB, thường là 1024 byte.

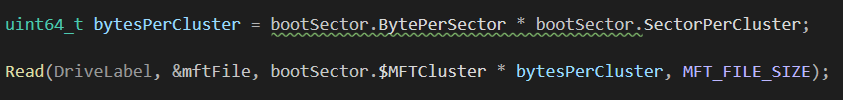
Text

Description automatically generated

Tiến hành đọc boot sector



Đọc 1KB đầu tiên của MFT (con trỏ bit đến các khối khác trong MFT)



Chúng tôi sẽ tìm kiếm thuộc tính $DATA trong FileRecord. Thuộc tính $DATA được sử dụng để lưu trữ nội dung của một tệp, vì vậy trong trường hợp của MFT, nó lưu trữ MFT. Vì toàn bộ MFT không thể nằm gọn trong một bản ghi tệp MFT, nên thuộc tính $DATA sẽ là non-resident. Điều đó có nghĩa là thay vào đó, thuộc tính sẽ liệt kê các khối liền kề có chứa MFT.

Text

Description automatically generated

Tiến hành parse các dữ liệu non-resident

Như đã mô tả ở trên, thuộc tính không cư trú liệt kê các khối liền kề tạo nên nội dung của thuộc tính. Do đó, với thuộc tính $DATA của MFT, chúng ta có danh sách các khối chứa MFT.

Mỗi khối được gọi là một lần chạy dữ liệu. Việc chạy dữ liệu phải bắt đầu và kết thúc ở ranh giới cụm (thường là mỗi 4KB - kích thước một cluster là: 8 x 512 = 4096 B = 4 KB)

Loop từng lần chạy dữ liệu trong thuộc tính $DATA

A picture containing text, screenshot, monitor, screen

Description automatically generated

Đối với mỗi lần chạy dữ liệu, ta cần tính toán độ dài và độ lệch tuyệt đối của nó (tức là từ đầu phân vùng). Sau đó, ta tính được số cluster và độ dài.

Tiến hành liệt kê các tệp

Đã đến lúc tải từng block MFT và quét file records. Bởi vì một khối MFT có thể khá lớn (hàng trăm MB), ta sẽ xử lý nó trong các khối 64MB

Text

Description automatically generated

Bỏ qua các file records đang không được sử dụng

Graphical user interface, text

Description automatically generated with medium confidence

Bây giờ ta cần tìm thuộc tính $FILENAME. (Thực tế có thể có nhiều thuộc tính $FILENAME - đó là cách các liên kết cứng hoạt động trong NTFS.) Code parse attribute giống như trước đó.

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Thuộc tính $FILE\_NAME chứa tên file trong nội dung của nó. Tên file có thể không quá dài, vì vậy thuộc tính này sẽ là resident.

Dùng struct File để lưu tên file và thư mục gốc của nó

Text

Description automatically generated

Đối với mỗi thuộc tính $FILE\_NAME, ta sẽ thêm 1 entry vào array.

Text

Description automatically generated

Ta cần lưu trữ tên file ở nơi khác, vì MFT buffer sẽ được sử dụng lại. Hàm sau phân bổ khoảng trắng cho tên tệp và chuyển đổi nó thành UTF-8. Ta nhóm các phân bổ lại với nhau thành các phần 16MB.

Text

Description automatically generated

Đối phần thông tin của các file, phần này sẽ in ra các thông tin của file

Text

Description automatically generated

4. Hình ảnh (chụp màn hình) demo chương trình ứng với các trường yêu cầu:

Đối với các ổ đĩa chính để không lỗi thì cần phải chạy visual studio dưới quyền admin, còn nếu đọc ổ đĩa rời như USB thì có thể chạy như bình thường. Ở đây sẽ demo đọc USB

a. USB FAT32

Đối với USB ở format FAT32 vui lòng chọn option 1

Text

Description automatically generated

Hãy chọn drive letter của ổ đĩa USB. Ở đây USB là ổ E

Text

Description automatically generated

Chương trình sẽ hiện thị thông tin cây thư mục gốc và cây thư mục con cho người dùng

Text

Description automatically generated

Text

Description automatically generated

Nếu tập tin có phần mở rộng là txt thì dòng content sẽ hiển thị nội dung của file text

Text

Description automatically generated

Text

Description automatically generated

b. USB NTFS

Đối với ổ đĩa định dạng NTFS, hãy chọn 2, sau đó chọn drive letter của ổ đĩa USB. Ở đây USB là ổ E

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

5. Nguồn tham khảo:

a.Vùng FAT32:

<https://www.codeguru.com/cpp/cpp/cpp_mfc/files/article.php/c13831/FAT-Root-Directory-Structure-on-Floppy-Disk-and-File-Information.htm>

<https://dev-notes.eu/2019/07/Convert-an-Array-of-Unsigned-Chars-to-an-int32_t-Value/>

<http://www.cs.fsu.edu/~cop4610t/lectures/project3/Week11/Slides_week11.pdf>

<https://www.cse.scu.edu/~tschwarz/COEN252_09/Lectures/FAT.html>

<http://www.disk-imager.com/data-recovery-blog/?p=1593>

<https://www.programmersought.com/article/8448841987/>

<https://stackoverflow.com/questions/29577114/read-boot-sector-using-c-on-windows8>

<https://lazytrick.wordpress.com/2015/12/27/khai-quat-ve-fat/>

b.Vùng NTFS:

<http://ntfs.com/ntfs_basics.htm>

<https://github.com/orkblutt/NTFS-Parser-Lib>

<http://inform.pucp.edu.pe/~inf232/Ntfs/ntfs_doc_v0.5/index.html>

<http://www.dewassoc.com/kbase/windows_nt/ntfs_directories_and_files.htm>

<https://www.file-recovery.com/recovery-understanding-file-system-ntfs.htm>

<https://slidetodoc.com/computer-forensics-ntfs-file-system-mbr-and-gpt/>

<https://handmade.network/wiki/7002-tutorial_parsing_the_mft>