Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Khoa học tự nhiên
Khoa Công nghệ thông tin

Đồ án môn học

HỆ ĐIỀU HÀNH

Học kì 3
2020 – 2021

Quản Lý Hệ Thống Tập Tin Trên Windows

Lớp: 19CLC10
Giảng viên hướng dẫn: Ths.Lê Viết Long

Họ và tên	MSSV	Công việc	Hoàn thành
Phạm Nguyễn Anh Quốc	19127534	_Tìm tài liệu về FAT32 + NTFS, viết báo cáo	100%
Nguyễn Huy Anh Thư	19127569	_Lập trình phần đọc Boot Sector (FAT32) và đọc Partition Boot Sector (NTFS)	100%
Nguyễn Tiến Hùng	19127029	_Lập trình phần đọc cây thư mục con RDET/SRDET	100%

***Mức độ hoàn thành đồ án:** 85%

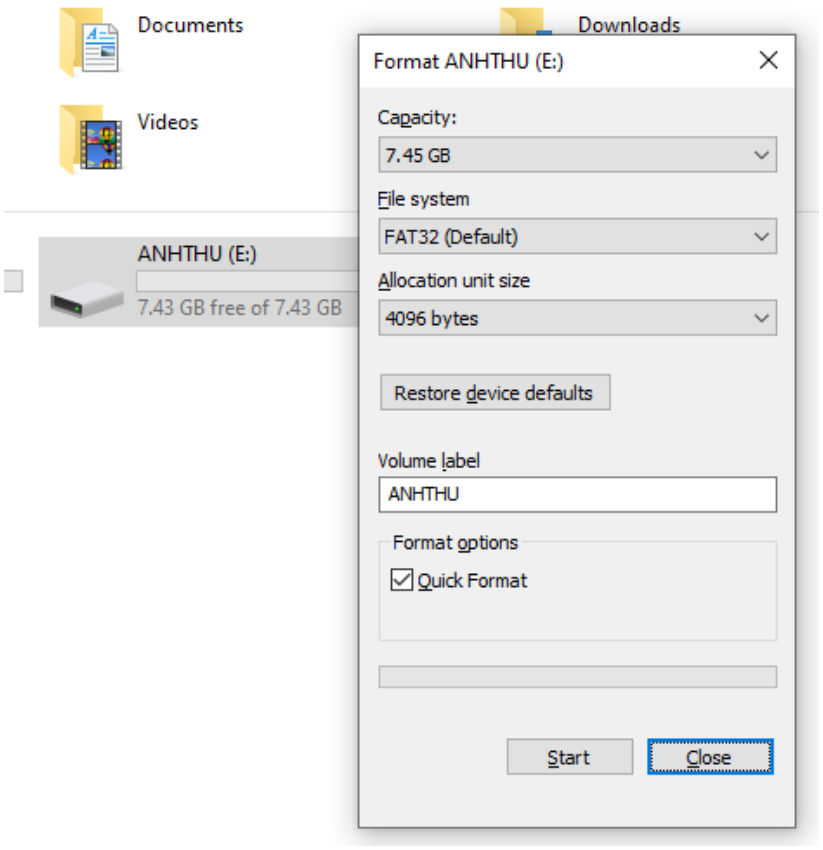
- Đọc thông tin Boot Sector và Partition Boot Sector (hoàn thành 100%)
- Đọc thông tin RDET của FAT32, đọc thông tin của thư mục con và thông tin nội dung tệp tin .txt (hoàn thành 100%)
- Đọc thông tin Master File Table của NTFS (chưa hoàn thành)

Ho Chi Minh , 2021

NỘI DUNG

1. Đọc thông tin của Boot Sector (FAT32)

Các bước thực hiện đọc thông tin Boot Sector(FAT32)



Tiến hành đọc thông tin bằng USB 8GB kiểu FAT32 tại ổ E:

- Trong đồ án này chủ yếu ta dùng cách đảo các bit lại và chuyển các bit từ hệ 16 sang hệ 10 để cho ra được các thông tin về số liệu (số byte, kích thước,...) hoặc đọc các bit từ hệ 16 sang các kí tự của bảng ASCII để cho ra được các thông tin về tên.
- Sau khi đọc được vào bảng Boot Sector của USB, ta có thể xác định được các thành phần của bảng như sau:
    + Kiểu bảng FAT: đọc 8 byte bắt đầu từ vị trí 0x036, với mỗi byte ta đem đối chiếu với ký tự của nó trong bảng ASCII, từ đó ra được thông tin về tên loại FAT như FAT16,... (nếu tất cả các byte cần đọc sẽ là 00 -> FAT32)
    + Kích thước bảng FAT (aka **SF**): đọc đảo 2 byte tại vị trí 0x016 rồi đổi sang hệ số 10. Nếu kết quả trước bằng 0 thì chuyển sang đọc đảo 4 byte tại vị trí 0x024 rồi đổi sang hệ số 10
    + Số byte của 1 sector: đọc đảo 2 byte tại vị trí 0x00B rồi đổi sang hệ số 10
    + Số sector của 1 cluster: đọc 1 byte tại vị trí 0x00D rồi đổi sang hệ số 10
    + Số sector tại vùng Boot Sector (aka **SB)**: đọc đảo 2 byte tại vị trí 0x00E rồi đổi sang hệ số 10
    + Số bảng FAT (aka **NF**): đọc 1 byte tại vị trí 0x010 rồi đổi sang hệ số 10
    + Số sector của RDET: đọc đảo 2 byte tại vị trí 0x011 rồi đổi sang hệ số 10 => ra được số entry, từ đó đổi sang số sector = entry * 32 / Số byte của 1 sector

      => **SRDET** = SB + SF / NF

+ Kích thước volume (aka SV): đọc đảo 2 byte tại vị trí 0x013 rồi đổi sang hệ số 10, nếu kết quả trước bằng 0 thì đọc đảo 4 byte tại vị trí 0x020 rồi đổi sang hệ số 10
+ Sector đầu tiên của bảng FAT = SB
+ Sector bắt đầu của RDET = SB + NF * SF
+ Sector bắt đầu của DATA = SRDET = SB + SF / NF

Demo chương trình:

```
1. READ BOOT SECTOR
        0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0x000  eb 58 90 4d 53 44 4f 53  35 2e 30 00 02 08 fc 08
0x010  02 00 00 00 00 f8 00 00  3f 00 ff 00 00 08 00 00
0x020  00 84 ee 00 82 3b 00 00  00 00 00 00 02 00 00 00
0x030  01 00 06 00 00 00 00 00  00 00 00 00 00 00 00 00
0x040  80 00 29 a0 63 1b 0a 4e  4f 20 4e 41 4d 45 20 20
0x050  20 20 46 41 54 33 32 20  20 20 33 c9 8e d1 bc f4
0x060  7b 8e c1 8e d9 bd 00 7c  88 56 40 88 4e 02 8a 56
0x070  40 b4 41 bb aa 55 cd 13  72 10 81 fb 55 aa 75 0a
0x080  f6 c1 01 74 05 fe 46 02  eb 2d 8a 56 40 b4 08 cd
0x090  13 73 05 b9 ff ff 8a f1  66 0f b6 c6 40 66 0f b6
0x0a0  d1 80 e2 3f f7 e2 86 cd  c0 ed 06 41 66 0f b7 c9
0x0b0  66 f7 e1 66 89 46 f8 83  7e 16 00 75 39 83 7e 2a
0x0c0  00 77 33 66 8b 46 1c 66  83 c0 0c bb 00 80 b9 01
0x0d0  00 e8 2c 00 e9 a8 03 a1  f8 7d 80 c4 7c 8b f0 ac
0x0e0  84 c0 74 17 3c ff 74 09  b4 0e bb 07 00 cd 10 eb
0x0f0  ee a1 fa 7d eb e4 a1 7d  80 eb df 98 cd 16 cd 19
0x100  66 60 80 7e 02 00 0f 84  20 00 66 6a 00 66 50 06
0x110  53 66 68 10 00 01 00 b4  42 8a 56 40 8b f4 cd 13
0x120  66 58 66 58 66 58 66 58  eb 33 66 3b 46 f8 72 03
0x130  f9 eb 2a 66 33 d2 66 0f  b7 4e 18 66 f7 f1 fe c2
0x140  8a ca 66 8b d0 66 c1 ea  10 f7 76 1a 86 d6 8a 56
0x150  40 8a e8 c0 e4 06 0a cc  b8 01 02 cd 13 66 61 0f
0x160  82 74 ff 81 c3 00 02 66  40 49 75 94 c3 42 4f 4f
0x170  54 4d 47 52 20 20 20 20  00 00 00 00 00 00 00 00
0x180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0x190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0x1a0  00 00 00 00 00 00 00 00  00 00 00 00 0d 0a 44 69
0x1b0  73 6b 20 65 72 72 6f 72  ff 0d 0a 50 72 65 73 73
0x1c0  20 61 6e 79 20 6b 65 79  20 74 6f 20 72 65 73 74
0x1d0  61 72 74 0d 0a 00 00 00  00 00 00 00 00 00 00 00
```

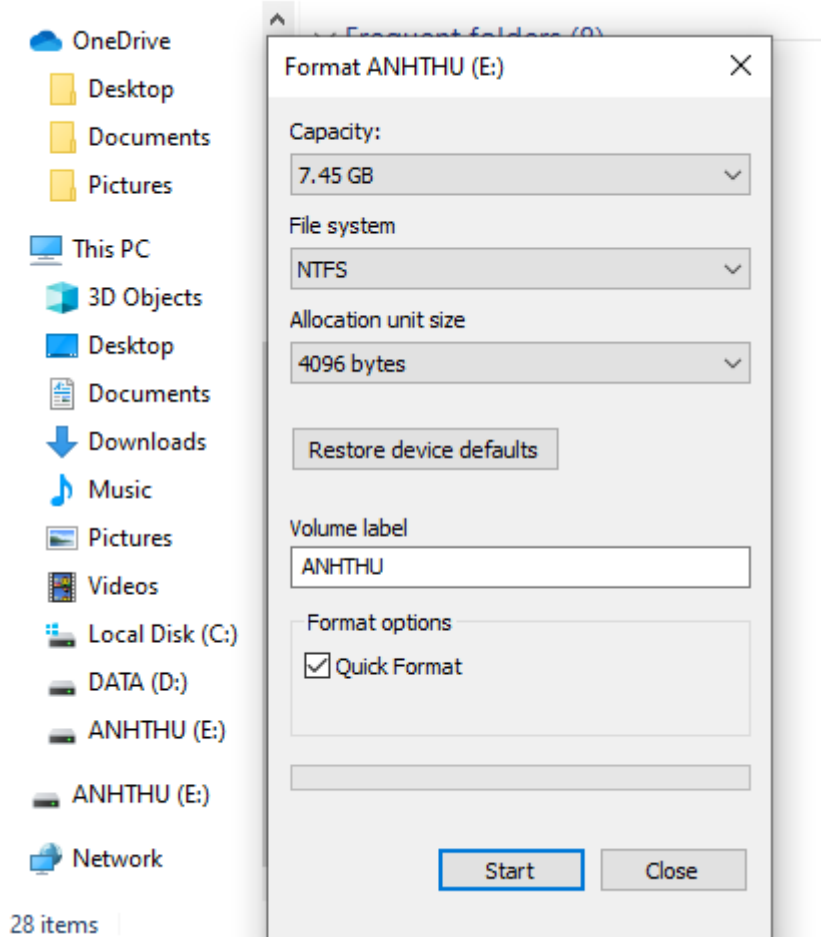
Ta có bảng Boot Sector được đọc từ USB

```
Kieu FAT: FAT32
Kich thuoc bang FAT : SF = 15234
So byte cho 1 sector: 512
So sector cho 1 cluster: 8
So sector tai vung boot sector: SB = 2300
So bang FAT: NF = 2
So sector cua RDET:0
1 entry = 32 byte --> 0 sector
Kich thuoc volume: SV = 15631360 sector
Sector dau tien cua bang FAT1: 2300
Sector bat dau cua RDET: 32768
Sector bat dau cua DATA: 32768
```

Kết quả thu được

2. Đọc thông tin của Partition Boot Sector (NTFS)

Các bước thực hiện đọc thông tin Partition Boot Sector(NTFS)



Tiến hành đọc thông tin bằng USB 8GB kiểu NTFS tại ổ E:

- Trong đồ án này chủ yếu ta dùng cách đảo các bit lại và chuyển các bit từ hệ 16 sang hệ 10 để cho ra được các thông tin về số liệu (số byte, kích thước,...) hoặc đọc các bit từ hệ 16 sang các kí tự của bảng ASCII để cho ra được các thông tin về tên
- Sau khi đọc được vào bảng Boot Sector của USB, ta có thể xác định được các thành phần của bảng như sau:
  + Số byte của 1 sector: đọc đảo 2 byte tại vị trí 0x00B rồi đổi sang hệ số 10
  + Số sector của 1 cluster: đọc 1 byte tại vị trí 0x00D rồi đổi sang hệ số 10
  + Loại đĩa: đọc 1 byte tại vị trí 0x015 (“F8” : Hard disk, “F0” : High density floppy)
  + Kích thước hiện tại của đĩa: đọc đảo 4 byte tại vị trí 0x028 rồi chuyển sang hệ 10 => số sector => kích thước = số sector * 512 / 10^9(GB)
  + Số mặt đĩa: đọc đảo 2 byte tại vị trí 0x02A rồi đổi sang hệ số 10
  + Sector bắt đầu của ổ đĩa logic: đọc đảo 8 byte tại vị trí 0x028 rồi chuyển sang hệ số 10
  + Cluster bắt đầu của MFT: đọc đảo 8 byte tại vị trí 0x030 rồi chuyển sang hệ số 10
  + Cluster bắt đầu của MFT dự phòng: đọc đảo 8 byte tại vị trí 0x038 rồi chuyển sang hệ số 10
  + Số cluster của 1 MFT: đọc 1 byte tại vị trí 0x040 rồi chuyển sang hệ số 10
  + Cluster per index buffer: đọc 1 byte tại vị trí 0x044 rồi chuyển sang hệ số 10
  + Volume serial number: đọc 8 byte tại vị trí 0x048

Demo chương trình:

```
1. READ PARTITION BOOT SECTOR OF NTFS
        0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0x000  eb 52 90 4e 54 46 53 20  20 20 20 00 02 08 00 00
0x010  00 00 00 00 00 f8 00 00  3f 00 ff 00 00 08 00 00
0x020  00 00 00 00 80 00 00 00  ff 83 ee 00 00 00 00 00
0x030  00 00 0c 00 00 00 00 00  02 00 00 00 00 00 00 00
0x040  f6 00 00 00 01 00 00 00  1e 88 47 ba 9a 47 ba 84
0x050  00 00 00 00 fa 33 c0 8e  d0 bc 00 7c fb 68 c0 07
0x060  1f 1e 68 66 00 cb 88 16  0e 00 66 81 3e 03 00 4e
0x070  54 46 53 75 15 b4 41 bb  aa 55 cd 13 72 0c 81 fb
0x080  55 aa 75 06 f7 c1 01 00  75 03 e9 dd 00 1e 83 ec
0x090  18 68 1a 00 b4 48 8a 16  0e 00 8b f4 16 1f cd 13
0x0a0  9f 83 c4 18 9e 58 1f 72  e1 3b 06 0b 00 75 db a3
0x0b0  0f 00 c1 2e 0f 00 04 1e  5a 33 db b9 00 20 2b c8
0x0c0  66 ff 06 11 00 03 16 0f  00 8e c2 ff 06 16 00 e8
0x0d0  4b 00 2b c8 77 ef b8 00  bb cd 1a 66 23 c0 75 2d
0x0e0  66 81 fb 54 43 50 41 75  24 81 f9 02 01 72 1e 16
0x0f0  68 07 bb 16 68 52 11 16  68 09 00 66 53 66 53 66
0x100  55 16 16 16 68 b8 01 66  61 0e 07 cd 1a 33 c0 bf
0x110  0a 13 b9 f6 0c fc f3 aa  e9 fe 01 90 90 66 60 1e
0x120  06 66 a1 11 00 66 03 06  1c 00 1e 66 68 00 00 00
0x130  00 66 50 06 53 68 01 00  68 10 00 b4 42 8a 16 0e
0x140  00 16 1f 8b f4 cd 13 66  59 5b 5a 66 59 66 59 1f
0x150  0f 82 16 00 66 ff 06 11  00 03 16 0f 00 8e c2 ff
0x160  0e 16 00 75 bc 07 1f 66  61 c3 a1 f6 01 e8 09 00
0x170  a1 fa 01 e8 03 00 f4 eb  fd 8b f0 ac 3c 00 74 09
0x180  b4 0e bb 07 00 cd 10 eb  f2 c3 0d 0a 41 20 64 69
0x190  73 6b 20 72 65 61 64 20  65 72 72 6f 72 20 6f 63
0x1a0  63 75 72 72 65 64 00 0d  0a 42 4f 4f 54 4d 47 52
0x1b0  20 69 73 20 63 6f 6d 70  72 65 73 73 65 64 00 0d
0x1c0  0a 50 72 65 73 73 20 43  74 72 6c 2b 41 6c 74 2b
```

Ta có bảng Partition Boot Sector được đọc từ USB

```
So byte cua 1 sector: 512
So sector cua 1 cluster: 8
Loai dia: Hard disk
Kich thuoc hien tai cua dia: 15631359 sectors => 8.00326 GB
So mat dia (head hoac side): 238
Sector bat dau cua o dia logic: 0
So sector cua o dia logic: 15631359
Cluster bat dau cua MFT: 786432
Cluster bat dau cua MFT du phong: 2
Cluster per MTF: 246 clusters
Cluster per index buffer: 1
The volume serial number: 1e 88 47 ba 9a 47 ba 84
```

Kết quả thu được

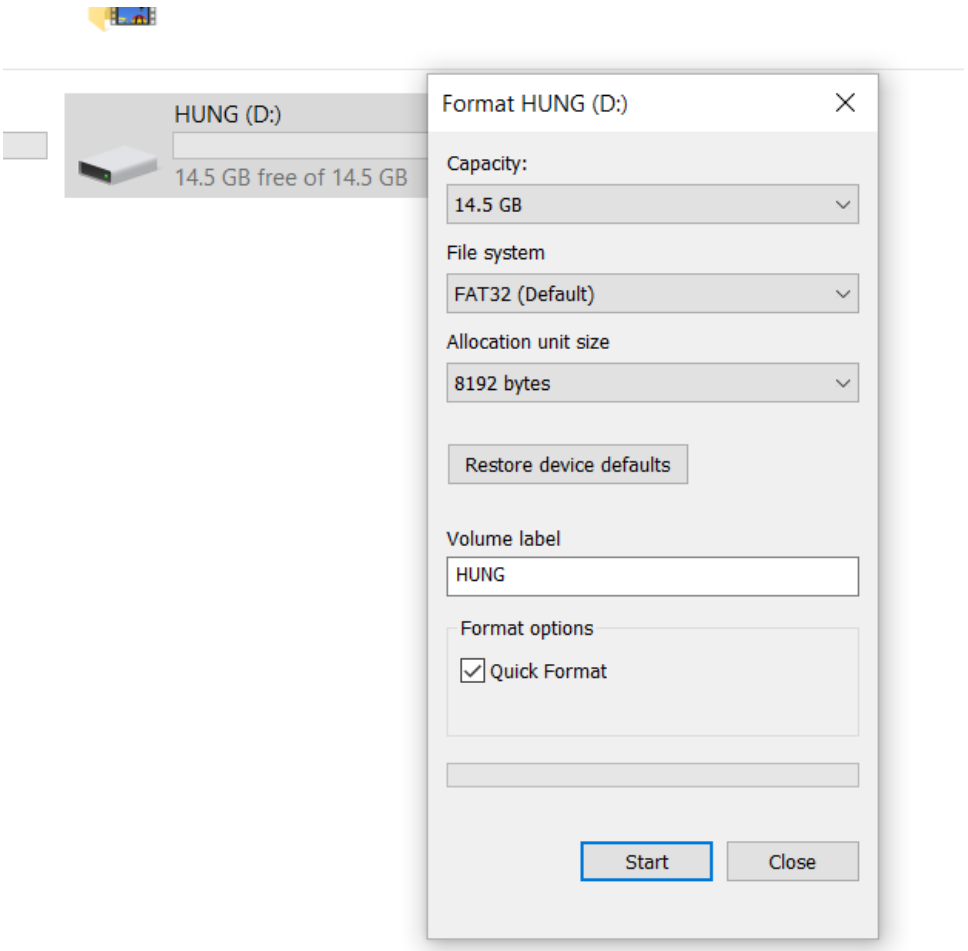
3. Đọc thông tin và phân tích bảng RDET + FAT đối với hệ thống FAT32

Các bước thực hiện đọc cây thư mục :

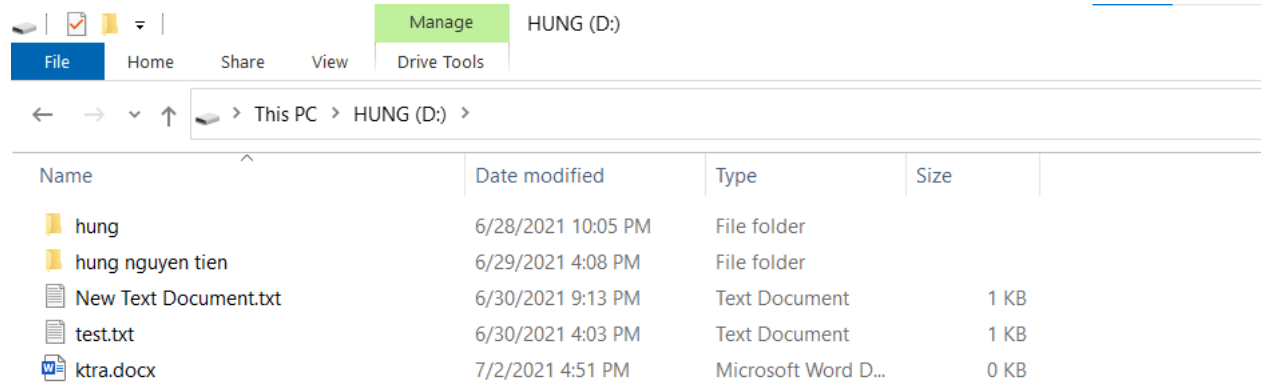
- Đầu tiên chúng ta thực hiện đọc từng entry (mỗi entry có 32 byte) , dựa vào byte đầu tiên trong mỗi entry để xác định entry đó đã xóa (có giá trị là 0xe5) hay chưa và entry đó có rỗng không (có giá trị là 0x00).
- Tiếp theo chúng ta kiểm tra nó là entry chính hay entry phụ bằng cách xác định nếu ở vị trí 0B = 0x0f thì nó là entry phụ chúng ta sẽ lưu lại giá trị ASCII ở các vị trí 0x01 (đọc 10 byte), vị trí 0x0E (đọc 12 byte) , vị trí 0x1C (đọc 4 byte) .

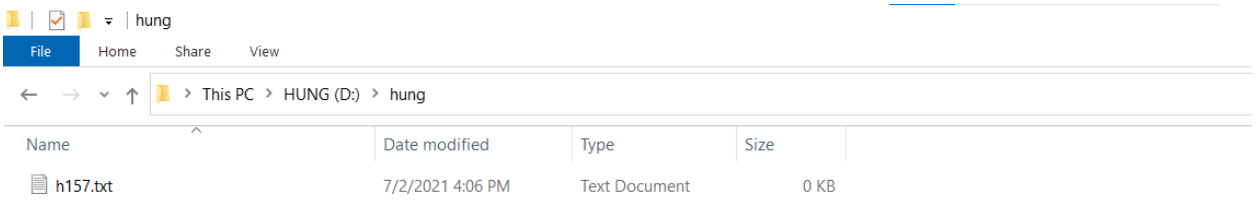
- Khi gặp được entry chính , khi này chúng ra sẽ in ra tên của tập tin thư mục của entry chính là các giá trị ASCII của những entry phụ ta đã lưu khi nãy và reset lại biến phụ để lưu tiếp.
- Nếu chỉ có 1 entry chính chúng ta thực hiên đọc tên của chúng ở vị tri : 0x00 (đọc 8 byte) và phần mở rộng ở vị trí 0x08 (đọc 3 byte).
- Sau đó chúng ta đọc lần lượt các thông tin của cây thư mục : kích thước ở vị trí 0x1C (đọc 4 byte) , trạng thái ở vị trí 0X0B (đọc 1 byte và chuyển thành binary để đọc),cluster bắt đầu ở vị trí 0x14 (2 byte đầu của cluster cao) và vị trí 0x1A(2 byte của cluster thấp)
- Kiểm tra nó là loại gì :
    + Nếu là tập tin thì ktra xem nó có phải là txt không : nếu phải thì thực hiện đọc nội dung bên trong ra và nếu không phải thì ghi sử dụng chương trình khác để đọc.
    + Nếu là thư mục thì tiến hành đọc thư mục con dựa vào cluster bắt đầu để tìm ra sector bắt đầu của thư mục con . Bỏ qua 2 entry đầu vì nó chưa thông tin của thư mục cha và thư mục này.

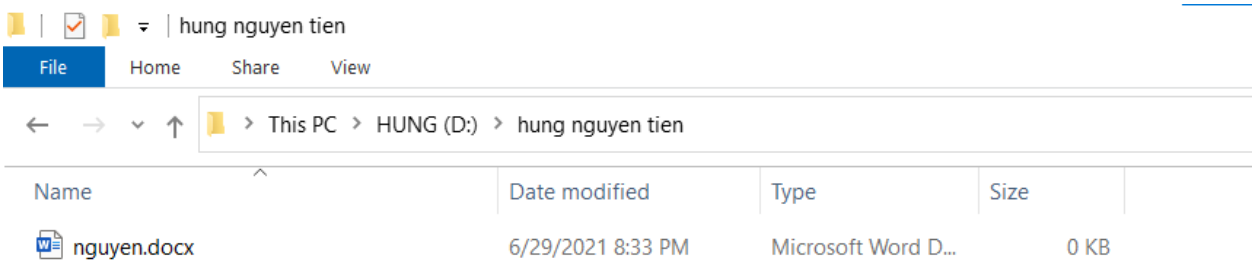
Demo chương trình:



Tiến hành đọc USB đang ở dạng FAT32 và trong máy tính hiện tại là ổ đĩa D:







Ở đây chúng ta thực hiện demo với 2 thư mục bao gồm thư mục tên dài và thư mục tên ngắn và thực hiện demo với 3 tập tin với 2 tập tin txt và 1 tập tin docx.

```
ten thu muc :HUNG
kich thuoc : 0
trang thai : vollabel
cluster bat dau : 0
```

```
ten thu muc tep tin :hung nguyen tien
kich thuoc : 0
trang thai : directory
cluster bat dau : 7
Chiem cac sector :4294934608 4294934609 4294934610 4294934611 429
tap tin thu muc con :
        ten tap tin thu muc :nguyen.docx
        kich thuoc : 0
        trang thai : archive
        cluster bat dau : 0

        dung chuong trinh khac de doc
```

```
ten thu muc :HUNG
kich thuoc : 0
trang thai : directory
cluster bat dau : 6
Chiem cac sector :4294934592 4294934593 4294934594 4294934595 4294934596 4294934597
tap tin thu muc con :
        ten tap tin  thu muc :H157
        phan mo rong :TXT
        kich thuoc : 0 bytes
        trang thai : archive
        cluster bat dau : 0
```

```
ten thu muc tep tin:TEST
phan mo rong :TXT
kich thuoc : 76 bytes
trang thai : archive
cluster bat dau : 8
Chiem cac sector :4294934624 4294934625 4294934626 4294934627 4294934628 429493

        hung ngueyengaghaighiasguahigjiadhgiuhidoguahsifhjsnigfhdajghidsahughi
```

```
ten thu muc tep tin :New Text Document.txt
kich thuoc : 7
trang thai : archive
cluster bat dau : 9
Chiem cac sector :4294934640 4294934641 4294934642 4294934643 4294934644 42949346
        huynggg
```

```
ten thu muc tep tin :ktra.docx
kich thuoc : 0
trang thai : archive
cluster bat dau : 0
dung chuong trinh khac de doc
```

Ngoài những thư mục hay tập tin có thể thấy thì còn những tập tin hệ thống bị ẩn :

```
ten thu muc tep tin :System Volume Information
kich thuoc : 0
trang thai : hidden system directory
cluster bat dau : 3
Chiem cac sector :4294934544 4294934545 4294934546 4294934547 4294934548 4294934549
```

TÀI LIỆU THAM KHẢO

1. https://wiki.osdev.org/FAT#Following_Cluster_Chains
2. http://ntfs.com/ntfs-partition-boot-sector.htm
3. https://www.cse.scu.edu/~tschwarz/COEN252_09/Lectures/NTFS.html