**BÁO CÁO ĐỒ ÁN**

**HỆ THỐNG TẬP TIN WINDOWS**

1. **Bảng phân công công việc**

|  |  |  |
| --- | --- | --- |
| **MSSV** | **Họ và tên** | **Công việc** |
| 20120224 | Trần Thị Mỹ Trinh |  |
| 20120228 | Trần Quốc Trung |  |
| 20120231 | Phan Huy Trường |  |
| 20120247 | Nguyễn Phương Anh |  |
| 20120328 | Hoàng Đức Nhật Minh |  |

1. **Đánh giá mức độ hoàn thành**

Đánh giá mức độ hoàn thành trên toàn bộ project:

Đánh giá mức độ hoàn thành trên từng yêu cầu:

|  |  |  |
| --- | --- | --- |
| **Phân vùng** | **Yêu cầu** | **Mức độ hoàn thành** |
| FAT32 | Đọc Boot Sector | 100% |
| Hiển thị cây thư mục gốc gồm tên tập tin/ thư mục, trạng thái, kích thước, chỉ số sector lưu trữ trên đĩa cứng |  |
| Truy xuất thông tin trên cây thư mục |  |
| NTFS | Đọc Partition Boot Sector | 100% |
| Hiển thị cây thư mục gốc gồm tên tập tin/ thư mục, trạng thái, kích thước, chỉ số sector lưu trữ trên đĩa cứng |  |
| Truy xuất thông tin trên cây thư mục |  |

1. **Mô tả các bước thực hiện**
2. **Quá trình thực hiện hệ thống tập tin FAT32**
3. **Quá trình thực hiện hệ thống tập tin NTFS**
   1. **Đọc thông tin trong Partition Boot Sector**

BPB (Bios Parameter Block) bắt đầu tại offset 0xB tới offset 0x53 trong VBR, có kích thước 73 byte. BPB chứa một số thông tin mô tả về tổ chức của một ổ đĩa logic và hệ thống quản lý tập tin. Từ BPB, nhóm em đọc được một số thông tin trong PBS như sau:

Các hàm phụ trợ:

* + - Hàm là hàm chuyển đổi hệ thập lục phân ra hệ thập phân không dấu (tham số nhận vào là một chuỗi).
    - Hàm là hàm chuyển đổi hệ thập lục phân ra hệ thập phân có dấu (tham số nhận vào là một chuỗi).

Thông tin trong PBS:

+ Kích thước một sector (đơn vị byte): địa chỉ offset 0B và kích thước 2bytes bytes\_per\_sector=HexLittleEndianToUnsignedDecimal(string[11:11+2])

Vì kích thước một sector là một số nguyên không dấu, bắt đầu từ vị trí và dài 2 bytes nên: [11:11+2]

+ Số sector trong một cluster: địa chỉ offset 0D và kích thước 1byte sectors\_per\_cluster=HexLittleEndianToUnsignedDecimal(string[13:13+1])

và dài 1byte nên: [13:13+1]

+ Số sector chưa sử dụng: địa chỉ offset 0E và kích thước 2bytes reserved\_sectors=HexLittleEndianToUnsignedDecimal(string[14:14+2])

và dài 2 bytes nên: [14:14+2]

+ Mã xác định loại đĩa: địa chỉ offset 15 và kích thước 1byte media\_descriptor=string[21:21+1].hex()

và dài 1byte nên: [21:21+1]

+ Số sector/track: địa chỉ offset 18 và kích thước 2bytes sectors\_per\_track=HexLittleEndianToUnsignedDecimal(string[24:24+2])

và dài 2 bytes nên: [24:24+2]

+ Số mặt đĩa (head): địa chỉ offset 1A và kích thước 2bytes numbers\_of\_heads=HexLittleEndianToUnsignedDecimal(string[26:26+2])

và dài 2 bytes nên: [26:26+2]

+ Sector bắt đầu của ổ đĩa logic: địa chỉ offset 1C và kích thước 4bytes hidden\_sectors=HexLittleEndianToUnsignedDecimal(string[28:28+4])

và dài 4 bytes nên: [28:28+4]

+ Số sector của ổ đĩa logic: địa chỉ offset 28 và kích thước 8bytes total\_sectors=HexLittleEndianToUnsignedDecimal(string[40:40+8])

và dài 8 bytes nên: [40:40+8]

+ Cluster bắt đầu của MFT: địa chỉ offset 30 và kích thước 8bytes mft\_cluster\_number=HexLittleEndianToUnsignedDecimal(string[48:48+8])

và dài 8 bytes nên: [48:48+8]

+ Cluster bắt đầu của MFT dự phòng (MFTMirror): offset 38, kích thước 8bytes mftmirr\_cluster\_number=HexLittleEndianToUnsignedDecimal(

string[56:56+8])

và dài 8 bytes nên: [56:56+8]

+ Kích thước của một bản ghi trong MFT (MFT entry): offset 40, 1byte bytes\_per\_file\_record\_segment=2\*\*abs(HexLittleEndianToSignedDecimal(

string[64:64+1]))

và dài 1byte nên: [64:64+1]

0xF6 là một số có dấu, 0xF6 = 1111 0110 (dạng bù 2), tính ra được giá trị hệ thập phân = -10. Kích thước của một bản ghi MFT tính bằng 2 ^ |-10| = **1024 byte**.

+ Số cluster của Index Buffer: offset 44, kích thước 4 bytes cluster\_per\_index=HexLittleEndianToUnsignedDecimal(string[68:68+4])

và dài 4 bytes nên: [68:68+4]

+ Số seri của ổ đĩa (volume serial number): offset 48, kích thước 8 bytes volume\_serial\_number=string[72:72+8].hex())

và dài 8 bytes nên: [72:72+8]

Từ Cluster bắt đầu của MFT, nhóm em tính được vị trí bắt đầu của MFT:

mft\_cluster\_number \* sectors\_per\_cluster

Đọc và phân tích các MFT entry (thường là 1024 byte) để xác định các tập tin thư mục.

* 1. **Hiển thị cây thư mục gốc**
  2. **Truy xuất thông tin trên cây thư mục**

1. **Demo chương trình**
2. **Demo FAT32**
3. **Demo NTFS**
4. **Tài liệu tham khảo**

[**https://legiacong.blogspot.com/2014/04/he-thong-quan-ly-tap-tin-ntfs-4-vbr-bpb.html**](https://legiacong.blogspot.com/2014/04/he-thong-quan-ly-tap-tin-ntfs-4-vbr-bpb.html)

[**https://iamtoet.blogspot.com/2014/06/file-system-forensics-ntfs-concepts.html?fbclid=IwAR2Dj8r2cuCXsxrSHIB-NCTIihbiS6bx-DQeceb\_1iZ01Ysmvf6ZVtXu\_BM**](https://iamtoet.blogspot.com/2014/06/file-system-forensics-ntfs-concepts.html?fbclid=IwAR2Dj8r2cuCXsxrSHIB-NCTIihbiS6bx-DQeceb_1iZ01Ysmvf6ZVtXu_BM)