A close up of a sign

Description automatically generated

FAT and NTFS image recovery

Jordan Sosnowski, Demarcus Campbell, Grant Pinkert

March 1, 2019

# Executive Summary

This section should begin on a new page. The executive summary should include a table that answers all of the questions in project along with your findings. The line spacing default is double-spacing for academic reports.

We were tasked with analyzing two different disk image files: FAT.dd and FTFS.dd. With these images, we found the number of partitions and attempted to find existing and deleted files. For each file, we specified the hexadecimal address while also generating the FATs for the FAT image and we found the file attributes of each file in the NTFS image. We were able to recover a number of JPEG images as well as several PDFs while identifying several deleted files. However, he deleted files were overwritten and unrecoverable.

# Table of Contents

This section should begin on a new page. The table of contents below is generated using the "References" menu.

Table of Contents

[Executive Summary 2](#_Toc2380653)

[Table of Contents 3](#_Toc2380654)

[List of Figures 4](#_Toc2380655)

[List of Tables 5](#_Toc2380656)

[1 Introduction 6](#_Toc2380657)

[2 Background 6](#_Toc2380658)

[2.1 First Subheading 6](#_Toc2380659)

[2.2 Second Subheading 6](#_Toc2380660)

[2.2.1 First Sub-subheading 6](#_Toc2380661)

[2.2.2 Second Sub-subheading 7](#_Toc2380662)

[3 Methodology 7](#_Toc2380663)

3.1 FAT Image ……………………………………………………………………………………………………………………………… 7

3.2 NTFS Image…………………………………………………………………………………………………………………………… 11

[4 Results and discussion 12](#_Toc2380664)

4.1 FAT Image

4.1.1 Partition 1…………………………………………………………………………………………………………….

4.1.2 Partition 2………………………………………………………………………………………………………………….

4.1.3 Partition 3………………………………………………………………………………………………………………..

4.2 NTFS Image Partition 1…………………………………………………………………………………………………………………

[5 Conclusions and recommendations 25](#_Toc2380665)

[6 Acknowledgements 25](#_Toc2380666)

[7 References 25](#_Toc2380667)

[Appendix A: Place the title of appendix here 26](#_Toc2380668)

# List of Figures

[Figure 1 - fdisk Example 7](#_Toc2380586)

[Figure 2 - FAT Format 8](#_Toc2380587)

[Figure 3 - FTK Imager Visualization 8](#_Toc2380588)

[Figure 4 - FAT Directory Entry 10](#_Toc2380589)

[Figure 5 - NTFS Format 11](#_Toc2380590)

[Figure 6 - NTFS MBR using FTK Imager 11](#_Toc2380591)

[Figure 7 - NTFS MBR using FTK Imager 21](#_Toc2380592)

# List of Tables

[Table 1 - List of clusters and the cluster entry 9](#_Toc2380113)

[Table 2 - Partition 1 Directory Entries 14](#_Toc2380114)

[Table 3 - Partition 1 File Recovery Commands: 15](#_Toc2380115)

[Table 4 - FAT Partition 2 Directory Entries 17](#_Toc2380116)

[Table 5 - FAT Partition 2 File Recovery Commands 18](#_Toc2380117)

[Table 6 - Fat Partition 3 Directory Entries 20](#_Toc2380118)

[Table 7 – FAT Partition 3 File Recovery Commands………………………………………………………………………………. 20](#_Toc2380119)

# 1 Introduction

This section should begin on a new page. This should use "Heading 1" style font settings for the heading, then “Normal” style for the content.

# 2 Background

This section does not begin on a new page and should use "Heading 1" style font settings for the heading, then “Normal” style for the content.

## 2.1 First Subheading

Subheadings are sections beneath headings. These sections should use "Heading 2" style font settings.

Subheadings and sub-subheadings are not mandatory. However, if there is one subheading, there must be at least a second subheading. Otherwise, there is no reason for the subdivisions under the primary headings.

## 2.2 Second Subheading

This paragraph is repeated. Subheadings are sections beneath headings. These sections should use "Heading 2" style font settings.

Subheadings and sub-subheadings are not mandatory. However, if there is one subheading, there must be at least a second subheading. Otherwise, there is no reason for the subdivisions under the primary headings.

### 2.2.1 First Sub-subheading

This paragraph is repeated. Subheadings are sections beneath headings. These sections should use "Heading 3" style font settings.

Subheadings and sub-subheadings are not mandatory. However, if there is one subheading, there must be at least a second subheading. Otherwise, there is no reason for the subdivisions under the primary headings.

### 2.2.2 Second Sub-subheading

Avoid any further divisions under the sub-subheading. Otherwise, the number of divisions becomes distracting and difficult to follow.

# 3 Methodology

**3.1 FAT Image**

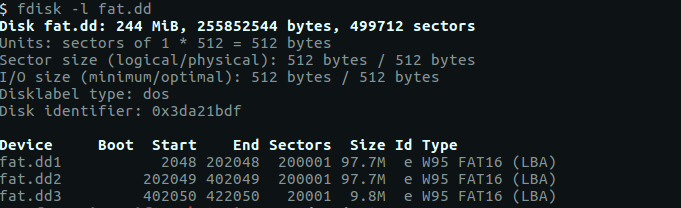


Figure - fdisk Example

Fdisk allowed us to find the size of the sectors, as well as the size of the different partitions on the image. Since the start of the first partition is located 2048 sectors in, we know that multiplying 2048 by 512 (the number of bytes per sector) will give us the offset of the first partition in bytes. We can also find the location of the reserved sectors, and since we know the FAT structure, we can then infer the offsets of reserved sectors, FATs, Root Directory, and the data area.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2 | 195 | 195 | 32 | 199,577 |
| Reserved Sectors | 1st FAT Area | 2nd FAT Area | Root Directory | Data Area |

Figure - FAT Format

For the first partition, we open FTK imager and jump to the offset of the first partition, as shown below.

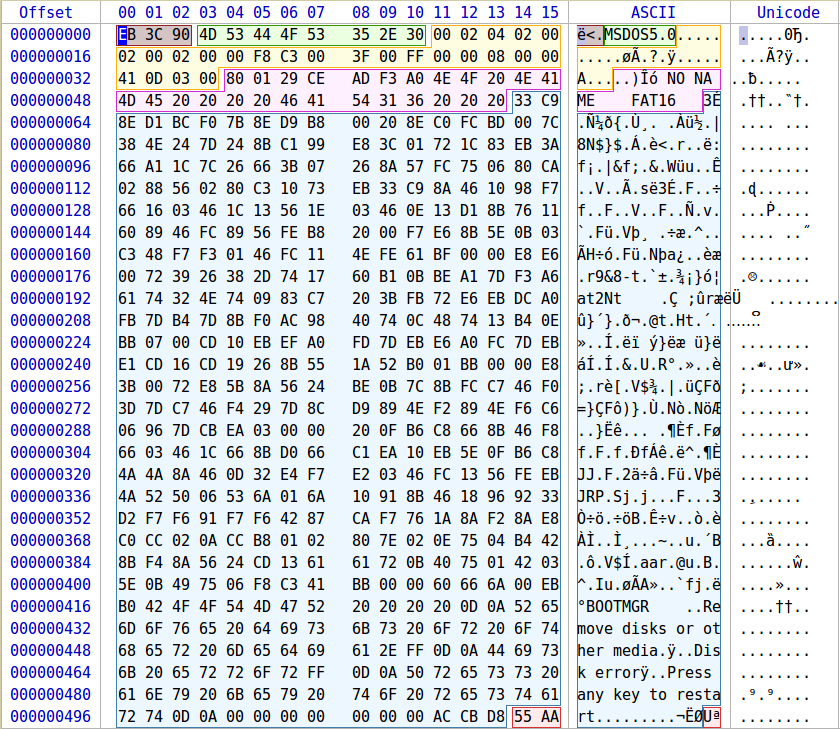


Figure - FTK Imager Visualization

From the File Allocation table, we can begin to see where the files are located via offsets in the partition.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Table List of clusters and the cluster entry   |  |  | | --- | --- | | Cluster | Next Cluster | | 0x0000 | 0xFFF8 | | 0x0001 | 0xFFFF | | 0x0002 | 0xFFFF | | 0x0003 | 0xFFFF | | 0x0004 | 0xFFFF | | 0x0005 | 0x0006 | | 0x0006 | 0x0007 | | 0x0007 | 0x0008 | | 0x0008 | 0x0009 | | 0x0009 | 0x000A | | 0x000A | 0xFFFF | | 0x000B | 0x0000 | | 0x000C | 0x0000 | | 0x000D | 0x0000 | | 0x000E | 0x0000 | | 0x000F | 0x0000 | | 0x0010 | 0x0000 | | 0x0011 | 0x0012 | | 0x0012 | 0x0013 | | 0x0013 | 0x0014 | | 0x0014 | 0x0015 | | 0x0015 | 0x0016 | | 0x0016 | 0x0017 | | 0x0017 | 0xFFFF | | 0x0018 | 0x0000 | | 0x0019 | 0x0000 | | |  |  | | --- | --- | | Cluster | Next Cluster | | 0x001A | 0x0000 | | 0x001B | 0x0000 | | 0x001C | 0x0000 | | 0x001D | 0x0000 | | 0x001E | 0x001F | | 0x001F | 0x0020 | | 0x0020 | 0x0021 | | 0x0021 | 0x0022 | | 0x0022 | 0x0023 | | 0x0023 | 0x0024 | | 0x0024 | 0xFFFF | | 0x0025 | 0x0000 | | 0x0026 | 0x0000 | | 0x0027 | 0x0000 | | 0x0028 | 0x0000 | | 0x0029 | 0x0000 | | 0x002A | 0x0000 | | 0x002B | 0x0000 | | 0x002C | 0x0000 | | 0x002D | 0x002E | | 0x002E | 0x002F | | 0x002F | 0x0030 | | 0x0030 | 0x0031 | | 0x0031 | 0x0032 | | 0x0032 | 0x0033 | | 0x0033 | 0xFFFF | |

These tables show the contents of the first FAT table and reserved sector. Each change of color indicated the end of one file and the start of another. A cluster ends when the entry is listed as 0xFFFF, and entries with 0x0000 indicated empty/deleted files.

The root table shows us directory entries, as well as all files, even those that are marked as deleted. Here, we find the filename, extension, attribute, modify date, cluster, and the file size, all of which is to be used to extract the file.

Example Directory Entry

* Tennessee

1. Status: 0x41 – Normal
2. Filename: Tennessee
3. Extension: JPG
4. Attribute: 0x20 – Archive
5. Modified date/time: 2/6/19 11:31 PM
6. Cluster: 0x0005 – 5
7. File Size: 0x0000280C – 10,252 bytes

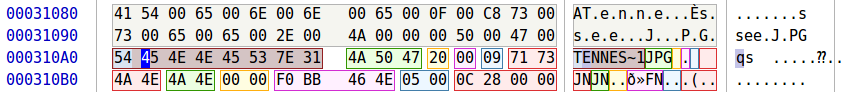


Figure - FAT Directory Entry

Using all of the information, now it is possible to create the files. To get a file, we use the dd command as follows:

**sudo dd if=image\_name of=filename bs=block\_size skip=blocks\_to\_skip count=blocks\_to\_grab**

The skip value is the starting position of the file. This is found by finding the cluster number for whichever file, subtracting two from it, multiplying cluster position by the value of bytes per cluster, adding the cluster offset to data offset, and then adding the file offset to partition offset. Using the root table, we can then find the length of the file of bytes, which is used for the count argument. Block size is set to 1 in case of a sector not using every byte of every sector.

This process is repeated for both partitions.

**3.2 NTFS Image**

Using the NTFS format:

|  |  |  |  |
| --- | --- | --- | --- |
| Master  Boot  Record | Master file Table | File Data Area | Master File Table Backup |

Figure - NTFS Format

We can easily infer the bytes per sector, sectors per cluster, bytes per cluster, $MFT Cluster Number, and the $MFT address as the MBR starts on the first sector of a partition, and using fdisk we can again see where the partitions are located.

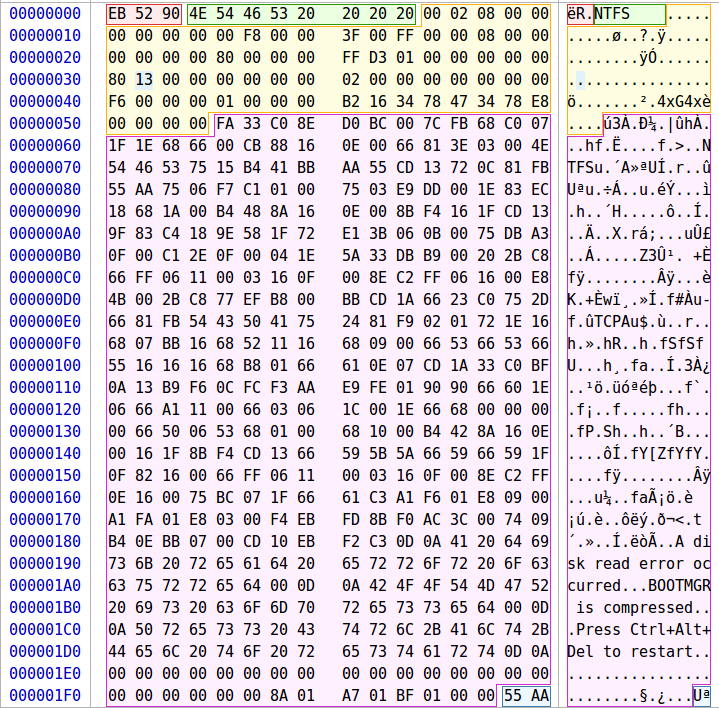


Figure - NTFS MBR using FTK Imager

Now that we know where the Master File Table is located, we can find the number of system files, the system files length, and the start of the user files. To find the start of the user files, we simply add the $MFT Address to the system files length. For each file, the attributes are located as follows:

1. 0x10 - $STANDARD\_INFORMATION
2. 0x30 - $FILE\_NAME
3. 0x80 - $DATA

Here, we find the file name, allocated size, and the data start cluster. Using this

information, we can begin to use the dd command to extract the files. Similar to the FAT files, we do this by using the partition offset, finding the start address for the data in the partition and using that as the offset. The block size is still 1, and the count is the length of the needed file.

# 4 Results and discussion

**4.1 FAT Results**

**4.1.1 Partition 1**

Structure Size Calculations

* 1. Partition Offset
     1. 0x100000 = 1,048,576 bytes
  2. Bytes / Sector
     1. Offset 0x0B = 0x0200 = **512**
  3. Sectors / Cluster
     1. Offset 0x0D = 0x4 = **4**
  4. Bytes / Cluster
     1. 4 Sectors / Cluster \* 512 Bytes / Sector = **2048**
  5. Reserved Sectors
     1. Offset 0x000E = 0x0002 = **2**
  6. Number of FATs
     1. Offset 0x0010 = 0x02 = **2**
  7. 1st FAT Area Size
     1. Offset 0x0016 = 0x00C3 = **195** sectors
  8. 2nd FAT Area Size
     1. Offset 0x0016 = 0x00C3 = **195** sectors
  9. Root Directory
     1. Directory Entries
        1. Offset 0x0011 = 0x0200 = 512 entries
     2. 512 \* 32 bytes = 16,384 bytes / 512 (bytes/sector) = **32** sectors
  10. Data Area
      1. Total Sectors
         1. Offset 0x0020 = 0x00030D41 = 200,001 Sectors
      2. Data Area = Total Sectors – End of Root
         1. 200,001 – 424 = **199579** Sectors

Directory Entries

1. Tennessee
   * 1. Status: 0x41 – Normal
     2. Filename: Tennessee
     3. Extension: JPG
     4. Attribute 0x20 – Archive
     5. Modified Date/time: 2/6/19 11:31 PM
     6. Cluster: 0x0005 – 5
     7. File Size: 0x0000280C – 10,252 bytes
2. Arkansas
   * 1. Status: 0xE5 – Deleted
     2. Filename: Arkansas
     3. Extension: JPG
     4. Attribute: 0x20 – Archive
     5. Modified date/time: 2/6/19 11:30 PM
     6. Cluster: 0x000B – 11
     7. File Size: 0x00002A96 – 10,902 bytes
3. Auburn
   * 1. Status: 0x41 – Normal File
     2. Filename: Auburn
     3. Extension: JPG
     4. Attribute: 0x20 – Archive
     5. Modified data/time: 2/6/19 11:29 PM
     6. Cluster: 0x0011 – 17
     7. File Size: 0x00003055 – 12,373 bytes
4. Florida
   * 1. Status: 0xE5 – Deleted
     2. Filename: Florida
     3. Extension: JPG
     4. Attribute: 0x20 – Archive
     5. Modified date/time: 2/6/19 11:31 PM
     6. Cluster: 0x0018 – 24
     7. File Size: 0x00002F14 – 12,052
5. Georgia
   * 1. Status: 0x41 – Normal File
     2. Filename: Georgia
     3. Extension: JPG
     4. Attribute: 0x20 – Archive
     5. Modified date/time: 2/6/19 11:30 PM
     6. Cluster: 0x001E – 30
     7. File size: 0x00003699 – 13,977 bytes
6. Missouri
   * 1. Status: 0xE5 – Deleted
     2. Filename: Missouri
     3. Extension: JPG
     4. Attribute: 0x20 – Archive
     5. Modified date/time: 2/6/19 11:29 PM
     6. Cluster: 0x0025 – 37
     7. File size: 0x00003E22 – 15,906 bytes
7. Ole Miss
   * 1. Status: 0x41 – Normal File
     2. Filename: Ole Miss
     3. Extension: JPG
     4. Attribute: 0x20 – Archive
     5. Modified date/time: 2/6/19 11:30 PM
     6. Cluster: 0x002D – 45
     7. File size: 0x0000339B – 13,211 bytes

Table - Partition 1 Directory Entries

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Filename | Extension | Attribute | Time | Date | Cluster | File Size | Status |
| Tennessee | JPG | Archive | 11:31 | 2/6/19 | 5 | 10,252 | Normal file |
| Arkansas | JPG | Archive | 11:30 | 2/6/19 | 11 | 10,902 | Deleted |
| Auburn | JPG | Archive | 11:29 | 2/6/19 | 17 | 12,273 | Normal File |
| Florida | JPG | Archive | 11:31 | 2/6/19 | 24 | 12,502 | Deleted |
| Georgia | JPG | Archive | 11:30 | 2/6/19 | 30 | 13,977 | Normal File |
| Missouri | JPG | Archive | 11:29 | 2/6/19 | 37 | 15,906 | Deleted |
| Ole Miss | JPG | Archive | 11:30 | 2/6/19 | 45 | 13,211 | Normal File |

Table - 1. Partition 1 File Recovery Commands:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Filename** | **Cluster** | **File Length** | **Cluster Offset** | **File Offset** | **Actual Offset** | **Command to Retrieve File** |
| TENNESSE.JPG | 5 | 10,252 | 6144 | 223,232 | 1,271,808 | sudo dd if=fat.dd of=TENNESSE.JPG bs=1 skip=1271808 count=10252 |
| ARKANSAS.JPG | 11 | 10902 | 18432 | 235,520 | 1,284,096 | sudo dd if=fat.dd of=ARKANSAS.JPG bs=1 skip=1284096 count=10902 |
| AUBURN.JPG | 17 | 12273 | 30720 | 247,808 | 1,296,384 | sudo dd if=fat.dd of=AUBURN.JPG bs=1 skip=1296384 count=12273 |
| FLORIDA.JPG | 24 | 12502 | 45056 | 262,144 | 1,310,720 | sudo dd if=fat.dd of=FLORIDA.JPG bs=1 skip=1310720 count=12502 |
| GEORIGA.JPG | 30 | 13977 | 57344 | 274,432 | 1,323,008 | sudo dd if=fat.dd of=GEORIGA.JPG bs=1 skip=1323008 count=13977 |
| MISSOURI.JPG | 37 | 15906 | 71680 | 288,768 | 1,337,344 | sudo dd if=fat.dd of=MISSOURI.JPG bs=1 skip=1337344 count=15906 |
| OLEMISS.JPG | 45 | 13211 | 88064 | 305,152 | 1,353,728 | sudo dd if=fat.dd of=OLEMISS.JPG bs=1 skip=1353728 count=13211 |

* + 1. **Partition 2**

Structure Size Calculations

* 1. Partition Offset = 0x62A8200 = 103,449,088 bytes
  2. Bytes / Sector
     1. Offset 0x0B = 0x0200 = **512**
  3. Sectors / Cluster
     1. Offset 0x0D = 0x4 = **4**
  4. Bytes / Cluster
     1. 4 Sectors / Cluster \* 512 Bytes / Sector = **2048**
  5. Reserved Sectors
     1. Offset 0x000E = 0x0002 = **2**
  6. Number of FATs
     1. Offset 0x0010 = 0x02 = **2**
  7. 1st FAT Area Size
     1. Offset 0x0016 = 0x00C3 = **195** sectors
  8. 2nd FAT Area Size
     1. Offset 0x0016 = 0x00C3 = **195** sectors
  9. Root Directory
     1. Directory Entries
        1. Offset 0x0011 = 0x0200 = 512 entries
     2. 512 \* 32 bytes = 16,384 bytes / 512 (bytes/sector) = **32** sectors
  10. Data Area
      1. Total Sectors
         1. Offset 0x0020 = 0x00030D41 = 200,001 Sectors
      2. Data Area = Total Sectors – End of Root
         1. 200,001 – 424 = **199579** Sectors

File Analysis

File Allocation Table

1. Located from sector 2 – 196
2. Bytes 1024 – 100,352
3. Address 0x400 – 0x18800

Root Directory Structure

1. Sector 392 – 423
2. Byte 200,704 – 216,576
3. Address 0x31000 – 0x34E00

Directory Entries

1. Great Expectations
   1. Status: 0x42
   2. Filename: Great Expectations
   3. Extension: PDF
   4. Attribute: 0x20 – Archive
   5. Modified date/time: 2/10/19 2:28 PM
   6. Cluster: 0x0005 – 5
   7. File Size: 0x0000280C – 3,193,980 bytes
2. Pride and Prejudice
3. Status: 0xE5 – Deleted
4. Filename: Pride and Prejudice
5. Extension: PDF
6. Attribute: 0x20 – Archive
7. Modified date/time: 1/18/19 1:01 PM
8. Cluster: 0x061D – 1,565
9. File Size: 0x000C303B – 798,779 bytes
10. War and Peace
    1. Status: 0xE5 – Deleted
    2. Filename: War and Peace
    3. Extension: PDF
    4. Attribute: 0x20 – Archive
    5. Modified date/time: 2/10/19 11:15 AM
    6. Cluster: 0x07A4 – 1956
    7. File Size: 0x009BC0F7 – 10,207,479
11. Tale of Two Cities
    1. Status: 0xE5
    2. Filename: Tale of Two Cities
    3. Extensions: PDF
    4. Attribute: 0x20 – Archive
    5. Modified date/time: 1/18/19 12:58 PM
    6. Cluster: 0x1B1D – 6,941
    7. File Size: 1,316,140 bytes

Table - FAT Partition 2 Directory Entries

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Filename | Extension | Attribute | Time | Date | Cluster | File Size | Status |
| Great Expectations | PDF | Archive | 11:31 | 2/6/19 | 5 | 10,252 | Normal file |
| Pride and Prejudice | PDF | Archive | 11:30 | 2/6/19 | 11 | 10,902 | Deleted |
| War and Peace | PDF | Archive | 11:29 | 2/6/19 | 17 | 12,273 | Deleted |
| Tale of Two Cities | PDF | Archive | 11:31 | 2/6/19 | 24 | 12,502 | Deleted |

Table - FAT Partition 2 File Recovery Commands

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Filename** | **Cluster** | **File Length** | **Cluster Offset** | **File Offset** | **Actual Offset** | **Command To Retrieve File** |
| Great Expectations.pdf | 5 | 3,193,980 | 6144 | 223,232 | 103,672,320 | sudo dd if=fat.dd of= ‘Great Expectations.pdf' bs=1 skip=103672320 count=3193980 status=progress |
| Pride and Prejudice.pdf | 1,565 | 798,779 | 3201024 | 3,418,112 | 106,867,200 | sudo dd if=fat.dd of= ’Pride and Prejudice.pdf ' bs=1 skip=106867200 count=798779 status=progress |
| War and Peace.pdf | 1,956 | 10,207,479 | 4001792 | 4,218,880 | 107,667,968 | sudo dd if=fat.dd of=' War and Peace.pdf’ bs=1 skip=107667968 count=10207479 status=progress |
| Tale of Two Cities.pdf | 6,941 | 1,316,140 | 14211072 | 14,428,160 | 117,877,248 | sudo dd if=fat.dd of=' Tale of Two Cities.pdf’ bs=1 skip=117877248 count=1316140 status=progress |
|  |  |  |  |  |  |  |

* + 1. **Partition 3**

1. Structure Size Calculations
2. Partition Offset
   * + 1. 0xC450400 = 205,849,600
3. Bytes / Sector
4. Offset 0x0B = 0x0200 = **512**
5. Sectors / Cluster
6. Offset 0x0D = 0x8 = **8**
7. Bytes / Cluster
8. 8 Sectors / Cluster \* 512 Bytes / Sector = **4096**
9. Reserved Sectors
10. Offset 0x000E = 0x0008= **8**
11. Number of FATs
12. Offset 0x0010 = 0x2 = **2**
13. 1st FAT Area Size
14. Offset 0x0016 = 0x8 = **8** sectors
15. 2nd FAT Area Size
16. Offset 0x0016 = 0x8 = **8** sectors
17. Root Directory
18. Directory Entries
    * + - 1. Offset 0x0011 = 0x0200 = 512 entries
19. 512 \* 32 bytes = 16,384 bytes / 512 (bytes/sector) = **32** sectors
20. Data Area
21. Total Sectors
22. Offset 0x0013= 0x4E21 = 20,001 Sectors
23. Data Area = Total Sectors – End of Root
24. 20,001 – 56 = **19,945** Sectors

File Analysis

* 1. File Allocation Table
     1. Located from sector 8 – 15
     2. Bytes 4096 – 7,680
     3. Address 0x1000 – 0x1E00
  2. No files in file analysis since they are all deleted

Root Directory Structure

1. Sector 24 – 55
2. Byte 12,288 – 28,160
3. Address 0x3000 – 0x6E00

File Recovery

1. Great Expectations
   * + - 1. Status: 0xE5 – Deleted
         2. Filename: Banana
         3. Extension: GIF
         4. Attribute: 0x20 – Archive
         5. Modified date/time: 2/10/19 11:14 AM
         6. Cluster: 0x0005 – 5
         7. File Size: 0x0000280C – 291,647 bytes
2. Minions
   * + - 1. Status: 0xE5 – Deleted
         2. Filename: Minion
         3. Extension: GIF
         4. Attribute: 0x20 – Archive
         5. Modified date/time: 2/8/19 2:07 PM
         6. Cluster: 0x007A – 77
         7. File Size: 0x0000280C – 328,174 bytes

Table - Fat Partition 3 Directory Entries

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Filename | Extension | Attribute | Time | Date | Cluster | File Size | Status |
| Banana | GIF | Archive | 11:14 AM | 2/8/19 | 5 | 291,647 | Deleted |
| Minion | GIF | Archive | 2:07 PM | 2/8/19 | 77 | 328,174 | Deleted |

Table – FAT Partition 3 File Recovery Commnds

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Filename** | **Cluster** | **File Length** | **Cluster Offset** | **File Offset** | **Actual Offset** | **Command To Retrieve File** |
| Banana.GIF | 5 | 291647 | 12288 | 40960 | 205890560 | sudo dd if=fat.dd of='Banana.GIF' bs=1 skip=205890560 count=291647 status=progress |
| Minions.GIF | 77 | 328174 | 307200 | 335872 | 206185472 | sudo dd if=fat.dd of='Minions.GIF' bs=1 skip=206185472 count=328174 status=progress |

* 1. **NTFS Image Partition 1**

1. NTFS Disk Partition Information
2. Bytes/Sector: Offset 0x0B = 0x0200 = 512
3. Sectors/Cluster: Offset 0x0D = 0x08 = 8
4. Bytes/Cluster: 8 \* 512 = 4096 bytes / cluster
5. $MFT Cluster Number: Offset 0x30 = 0x1380 = 4,992
6. $MFT Address: 0x13800000 = 20,447,232
7. $MFT Information – Offset 0x1380000 (20,447,232)
8. MFT Entry Size:1024
9. Number of System Files: 39
10. MFT System Files Length: 1024 \* 39 = 0x9C00
11. Start of User Files:
12. $MFT Address + System Files Length
13. 0x13800000 + 0x9C00 = 0x1389C00 = 20,487,168

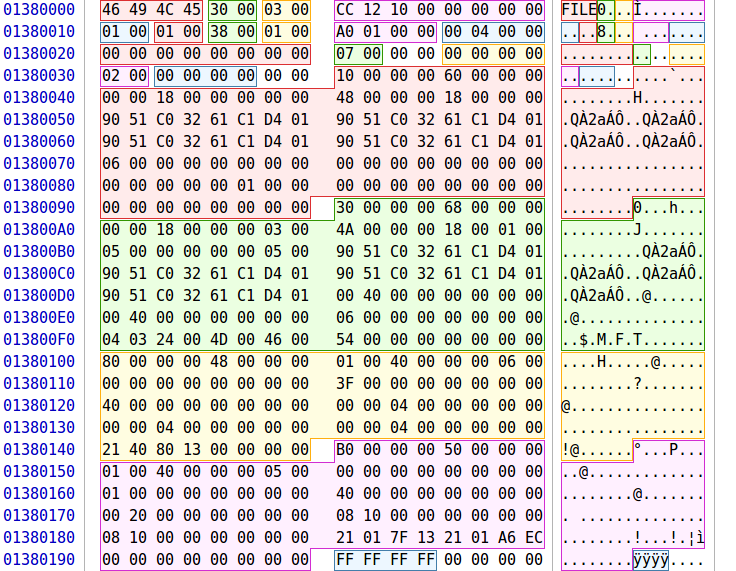


Figure - NTFS MBR using FTK Imager

1. User File Information – Offset 0x1389C00 (20,487,168)
2. A tale of two cities
3. List File Attributes:
4. 0x10 - $STANDARD\_INFORMATION
5. 0x30 - $FILE\_NAME
6. 0x80 - $DATA
7. Filename: Offset 0x0F2 = A Tale of Two Cities.pdf
8. Allocated Size: Offset 0x150= 0x150000 = 1,376,256 bytes
9. Data Start Cluster: Offset 0x170 = 0x0588 = 1,416
10. Data Start Address
11. 1,416 \* 4,096 = 5,799,936
12. Unrecoverable: overwritten by auburn.jpg
13. Auburn
14. List File Attributes:
15. 0x10 - $STANDARD\_INFORMATION
16. 0x30 - $FILE\_NAME
17. 0x80 - $DATA
18. Filename: Offset 0x0F2 = Auburn.jpg
19. Allocated Size: Offset 0x130 = 0x4000 = 16,384 bytes
20. Data Cluster Information
21. 21 04 CB 06
22. 2 bytes required for the first cluster address
23. Number of continuous clusters for this file – 1 \* 4 = 4
24. Start Cluster for Data: 0x06CB = 1,739
25. Start Address for Data:
26. 1,739 \* 4096 = 7,122,944
27. Avengers – Offset 0x138A3C0 (20,489,216)
28. List File Attributes:
29. 0x10 - $STANDARD\_INFORMATION
30. 0x30 - $FILE\_NAME
31. 0x80 - $DATA
32. Filename: Offset 0x0F2 = Avengers.docx
33. Allocated Size: Offset 0x138 = 0x100000 = 65,536 bytes
34. Data Cluster Information
35. 21 0D CF 06
36. 2 bytes required for the first cluster address
37. Number of continuous clusters for this file – 1 \* D = 13
38. Start Cluster for Data: 0x06CF = 1,743
39. Start Address for Data:
40. 1,739 \* 4096 = 7,139,328
41. Actual Offset
42. Partition Offset + Start Address
43. 1,048,576 + 7,139,328 = 8,187,904
44. Unrecoverable
45. Overwritten by banana.gif
46. Banana – Offset 0x138A800 (20,490,240)
47. List File Attributes:
48. 0x10 - $STANDARD\_INFORMATION
49. 0x30 - $FILE\_NAME
50. 0x80 - $DATA
51. Filename: Offset 0x0F2 = Banana.gif
52. Allocated Size: Offset 0x130 = 0x048000= 294,912 bytes
53. Data Cluster Information
54. 21 48 DD 06
55. 2 bytes required for the first cluster address
56. Number of continuous clusters for this file – 0x1 \* 0x48 = 72
57. Start Cluster for Data: 0x06DD = 1,757
58. Start Address for Data:
59. 1,757 \* 4096 = 7,196,672
60. Actual Offset
61. Partition Offset + Start Address
62. 1,048,576 + 7,196,672 = 8,245,248
63. Great Expectations – Offset 0x138AC00 (20,491,264)
64. List File Attributes:
65. 0x10 - $STANDARD\_INFORMATION
66. 0x30 - $FILE\_NAME
67. 0x80 - $DATA
68. Filename: Offset 0x0F2 = Great Expectations.pdf
69. Allocated Size: Offset 0x148 = 0x310000= 3,211,264 bytes
70. Data Cluster Information
71. 21 03 86 0A
72. 2 bytes required for the first cluster address
73. Number of continuous clusters for this file – 0x1 \* 0x3 = 3
74. Start Cluster for Data: 0x0A86 = 2,694
75. Start Address for Data:
76. 2,694 \* 4096 = 11,034,624
77. Actual Offset
78. Partition Offset + Start Address
79. 1,048,576 + 11,034,624 = 12,083,200
80. Unrecoverable: zeroed out
81. Minion – Offset 0x138B000 (20,492,288)
82. List File Attributes:
83. 0x10 - $STANDARD\_INFORMATION
84. 0x30 - $FILE\_NAME
85. 0x80 - $DATA
86. 0x80 - $BITMAP
87. Filename: Offset 0x0F2 = Minion.gif
88. Allocated Size: Offset 0x130 = 0x051000 = 331,776 bytes
89. Data Cluster Information
90. 21 05 31 0A
91. 2 bytes required for the first cluster address
92. Number of continuous clusters for this file – 0x1 \* 0x5 = 5
93. Start Cluster for Data: 0x0A31 = 2,609
94. Start Address for Data:
95. 2,609 \* 4096 = 10,686,464
96. Actual Offset
97. Partition Offset + Start Address
98. 1,048,576 + 10,686,464 = 11,735,040
99. War and Peace – Offset 0x138B000 (20,492,288)
100. List File Attributes:
101. 0x10 - $STANDARD\_INFORMATION
102. 0x30 - $FILE\_NAME
103. 0x80 - $DATA
104. 0x80 - $BITMAP
105. Filename: Offset 0x0F2 = War and Peace.pdf
106. Allocated Size: Offset 0x140 = 0x9C0000 = 10,223,616 bytes
107. Real Size: Offset 0x148 = 0x9BC0F7 = 10,207,479 bytes
108. Data Cluster Information
109. 22 90 08 E0 1A
110. 2 bytes required for the first cluster address
111. 2 bytes required for cluster counter
112. 0x0890 = 2,192
113. Start Cluster for Data: 0x1AE0 = 6,880
114. Start Address for Data:
115. 6,880 \* 4096 = 28,180,480
116. Actual Offset
117. Partition Offset + Start Address
118. 1,048,576 + 28,180,480 = 29,229,056

# 5 Conclusions and recommendations

This project allowed us to delve into a FAT and a NTFS file system. In doing so, we gained a better understanding of how the formats are structured, where data is stored, and how the file systems take care of deleted files.

# 6 Acknowledgements

This section allows authors to acknowledge contributors and other sources that are not appropriate to list in the references section.

# 7 References

This is the last section of the report, prior to any appendices. The references should not be double-spaced, but single-spaced. For a technical report, use the CSE style.

[1] Reference 1 information.

[2] Reference 2 information.

[3] Reference 3 information.

# Appendix A: Place the title of appendix here

Provide appropriate appendices as necessary. Each appendix should begin on a new page.