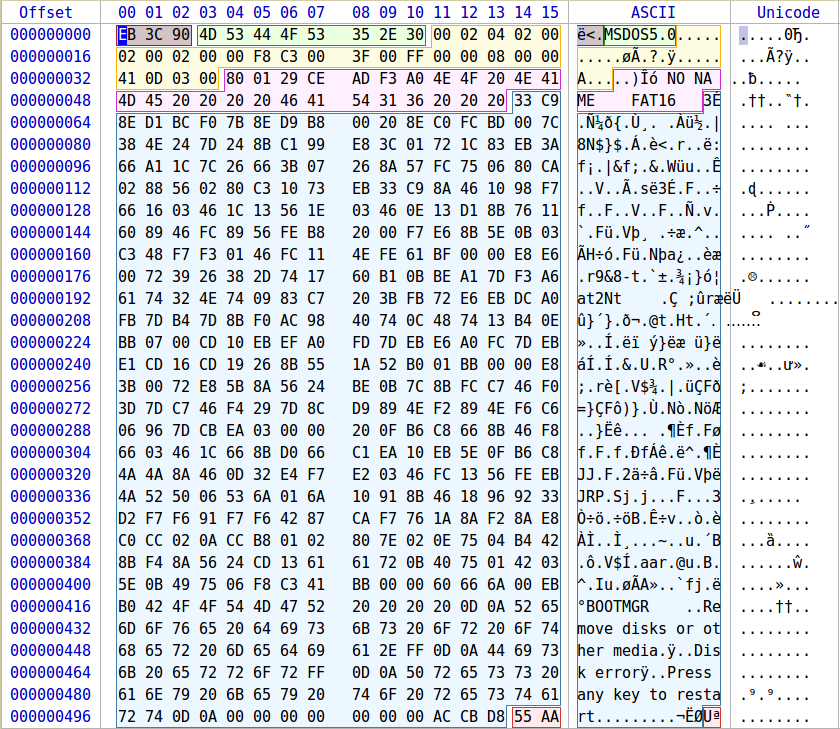


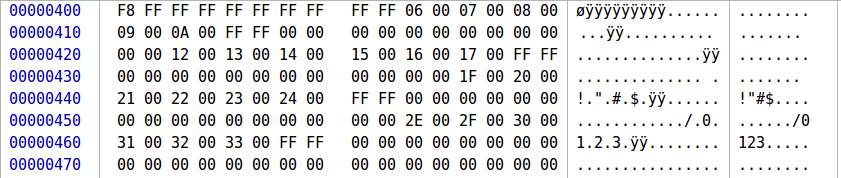
1. SEC PICS
   1. Structure Size Calculations
      1. Partition Offset
         1. 0x100000 = 1,048,576 bytes
      2. Bytes / Sector
         1. Offset 0x0B = 0x0200 = **512**
      3. Sectors / Cluster
         1. Offset 0x0D = 0x4 = **4**
      4. Bytes / Cluster
         1. 4 Sectors / Cluster \* 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 = **199,577** Sectors



* 1. FAT Structure

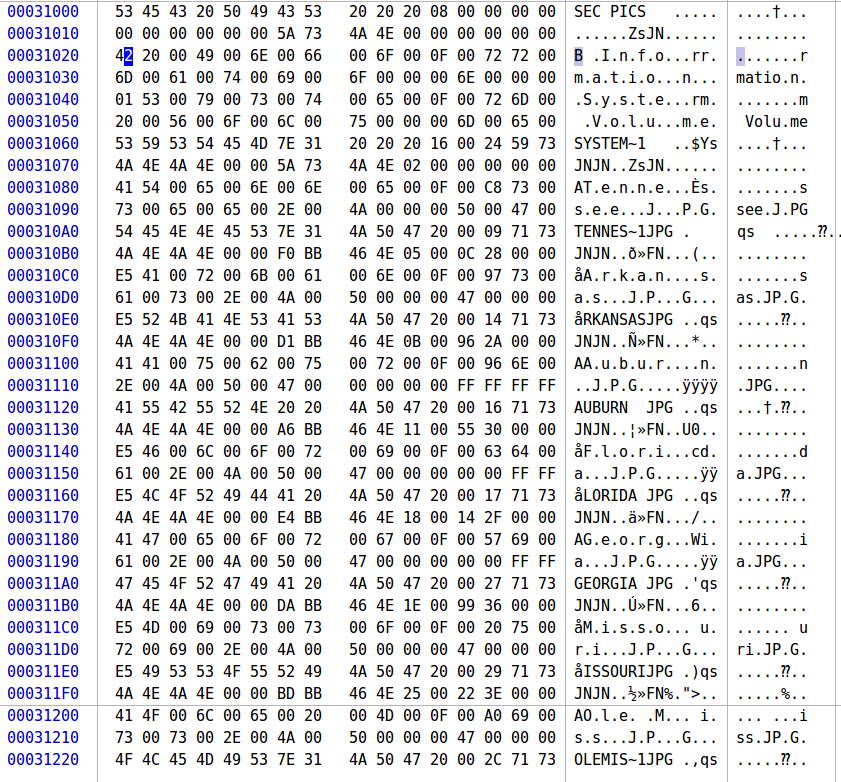
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2 | 195 | 195 | 32 | 199,577 |
| Reserved Sectors | 1st FAT Area | 2nd FAT Area | Root Directory | Data Area |

* 1. File Analysis
     1. File Allocation Table
        1. Located from sector 2 – 196
        2. Bytes 1024 – 100,352
        3. Address 0x400 – 0x18800

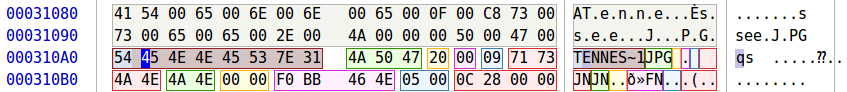


|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | 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 | |

* + 1. Root Directory Structure
       1. Sector 392 – 423
       2. Byte 200,704 – 216,576
       3. Address 0x31000 – 0x34E00



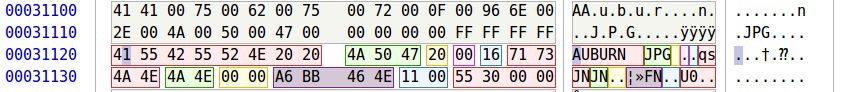
* + 1. Directory Entries
       1. Tennessee
          1. Status: 0x41 – Normal
          2. Filename: Tennessee
          3. Extension: JPG
          4. Attribute: 0x20 – Archive
          5. Modified date/time: 2/6/19 11:31 PM
          6. Cluster: 0x0005 – 5
          7. File Size: 0x0000280C – 10,252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



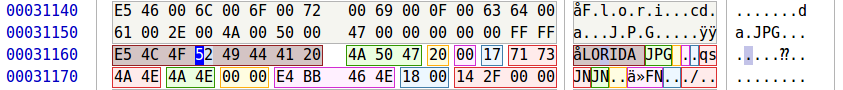
* + - 1. Arkansas
         1. Status: 0xE5 – Deleted
         2. Filename: Arkansas
         3. Extension: JPG
         4. Attribute: 0x20 – Archive
         5. Modified date/time: 2/6/19 11:30 PM
         6. Cluster: 0x000B – 11
         7. File Size: 0x00002A96 – 10,902 bytes



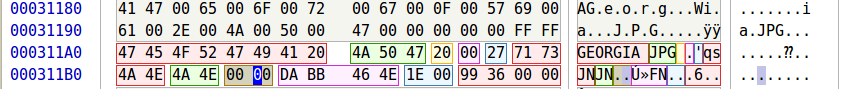
* + - 1. Auburn
         1. Status: 0x41 – Normal File
         2. Filename: Auburn
         3. Extension: JPG
         4. Attribute: 0x20 – Archive
         5. Modified data/time: 2/6/19 11:29 PM
         6. Cluster: 0x0011 – 17
         7. File Size: 0x00003055 – 12,373 bytes



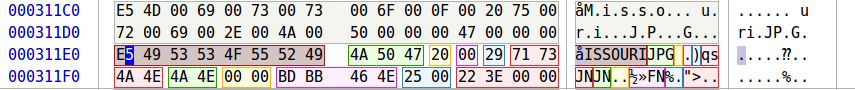
* + - 1. Florida
         1. Status: 0xE5 – Deleted
         2. Filename: Florida
         3. Extension: JPG
         4. Attribute: 0x20 – Archive
         5. Modified date/time: 2/6/19 11:31 PM
         6. Cluster: 0x0018 – 24
         7. File Size: 0x00002F14 – 12,052



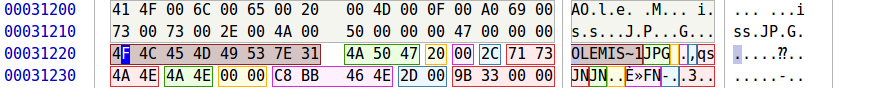
* + - 1. Georgia
         1. Status: 0x41 – Normal File
         2. Filename: Georgia
         3. Extension: JPG
         4. Attribute: 0x20 – Archive
         5. Modified date/time: 2/6/19 11:30 PM
         6. Cluster: 0x001E – 30
         7. File size: 0x00003699 – 13,977 bytes



* + - 1. 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



* + - 1. 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



* + 1. All 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 | 12,373 | 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 |

* + 1. File Recovery
       1. Constant Info
          1. ***Partition Offset 0x100000 (2048 sectors/ 1,048,576 bytes)***
          2. ***Data Offset 0x35000 (217,088 bytes)***
          3. Command

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

* + - 1. Recovering a FAT File
         1. Calculate Skip Value

Generate Cluster Offset

Find Cluster Number for File and subtract 2 from it

Multiply cluster position by the value of bytes / cluster

Generate File Offset

Add cluster offset to data offset

Generate Actual Offset

Add file offset to partition offset

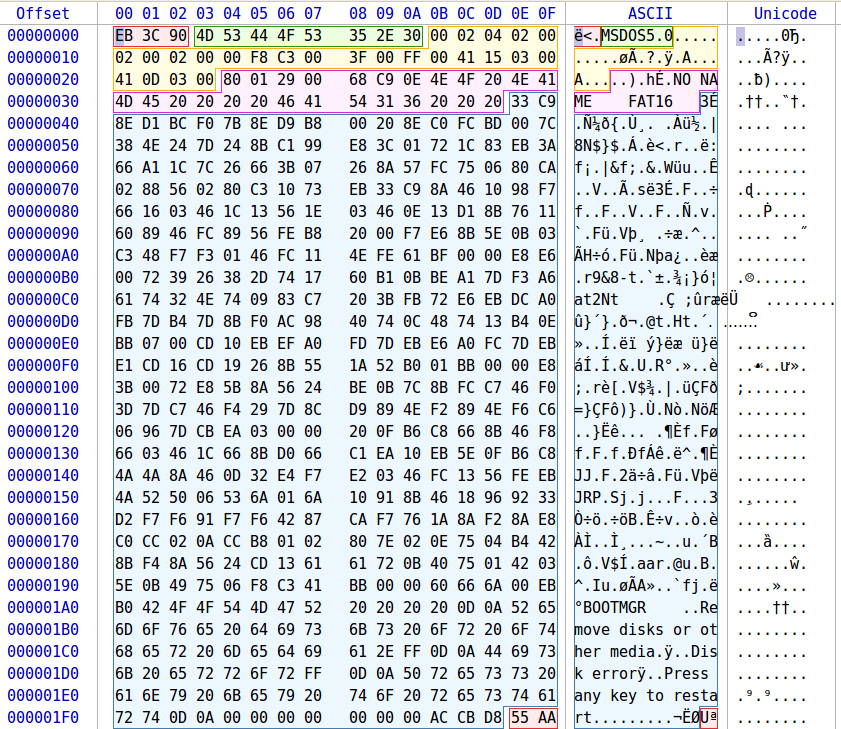
* + - * 1. Calculate Count Value

Number of bytes of the file

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Filename** | **Cluster** | **File Length** | **Cluster Offset** | **File Offset** | **Actual Offset** | **Command To Retrieve File** |
| Tennessee.JPG | 5 | 10,252 | 6,144 | 223,232 | 1,271,808 | sudo dd if=fat.dd of='Tennessee.JPG' bs=1 skip=1271808 count=10252 status=progress |
| Arkansas.JPG | 11 | 10,902 | 18,432 | 235,520 | 1,284,096 | sudo dd if=fat.dd of='Arkansas.JPG' bs=1 skip=1284096 count=10902 status=progress |
| Auburn.JPG | 17 | 12,373 | 30,720 | 247,808 | 1,296,384 | sudo dd if=fat.dd of='Auburn.JPG' bs=1 skip=1296384 count=12373 status=progress |
| Florida.JPG | 24 | 12,502 | 45,056 | 262,144 | 1,310,720 | sudo dd if=fat.dd of='Florida.JPG' bs=1 skip=1310720 count=12502 status=progress |
| Georgia.JPG | 30 | 13,977 | 57,344 | 274,432 | 1,323,008 | sudo dd if=fat.dd of='Georgia.JPG' bs=1 skip=1323008 count=13977 status=progress |
| Missouri.JPG | 37 | 15,906 | 71,680 | 288,768 | 1,337,344 | sudo dd if=fat.dd of='Missouri.JPG' bs=1 skip=1337344 count=15906 status=progress |
| Ole Miss.JPG | 45 | 13,211 | 88,064 | 305,152 | 1,353,728 | sudo dd if=fat.dd of='Ole Miss.JPG' bs=1 skip=1353728 count=13211 status=progress |

1. Classics Partition
   1. 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
   2. FAT Structure

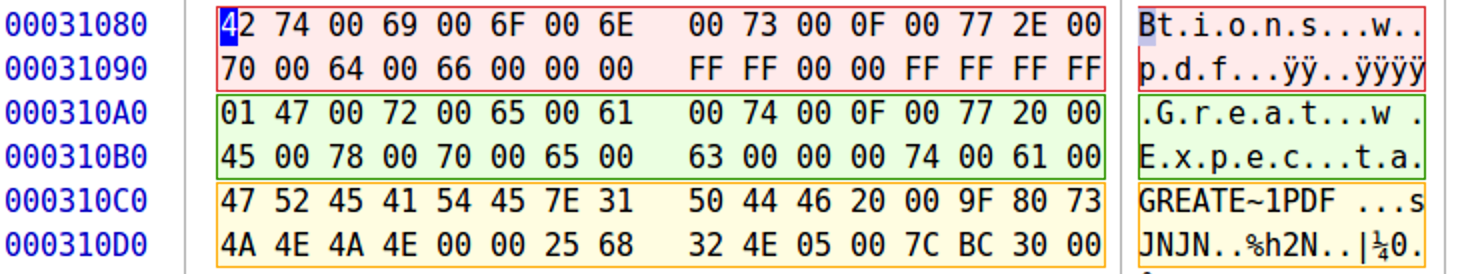
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2 | 195 | 195 | 32 | 199,577 |
| Reserved Sectors | 1st FAT Area | 2nd FAT Area | Root Directory | Data Area |



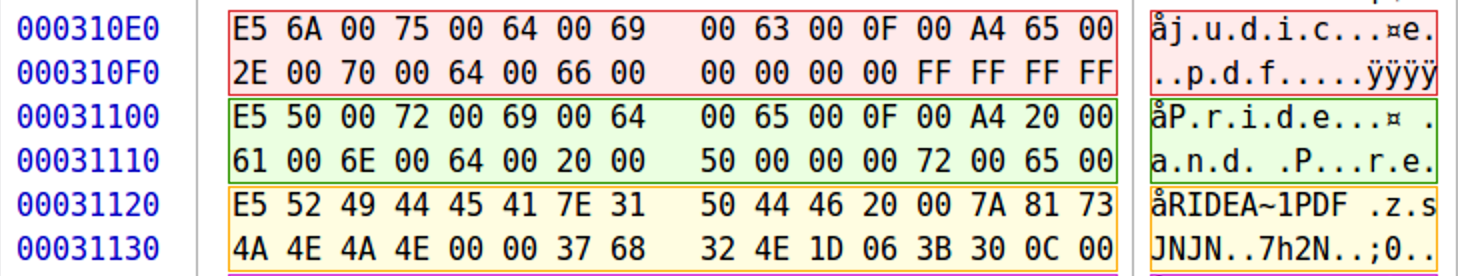
* 1. File Analysis
     1. File Allocation Table
        1. Located from sector 2 – 196
        2. Bytes 1024 – 100,352
        3. Address 0x400 – 0x18800

|  |  |
| --- | --- |
| Sector | Next Sector |
| 0x0000 | 0xFFF8 |
| 0x0001 | 0xFFFF |
| 0x0002 | 0xFFFF |
| 0x0003 | 0xFFFF |
| 0x0004 | 0xFFFF |
| 0x0005 | 0x0006 |
| 0x0006 | 0x0007 |
| 0x0007 | 0x0008 |
| 0x0009 | 0x000A |
| ... | |
| 0x061B | 0x061C |
| 0x061C | 0xFFFF |

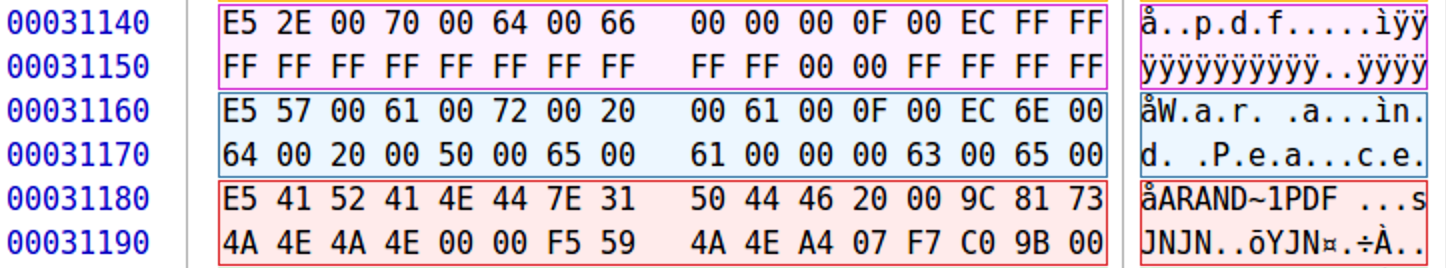
* + 1. Root Directory Structure
       1. Sector 392 – 423
       2. Byte 200,704 – 216,576
       3. Address 0x31000 – 0x34E00
    2. Directory Entries
       1. Great Expectations
          1. Status: 0x42
          2. Filename: Great Expectations
          3. Extension: PDF
          4. Attribute: 0x20 – Archive
          5. Modified date/time: 2/10/19 2:28 PM
          6. Cluster: 0x0005 – 5
          7. File Size: 0x0000280C – 3,193,980 bytes



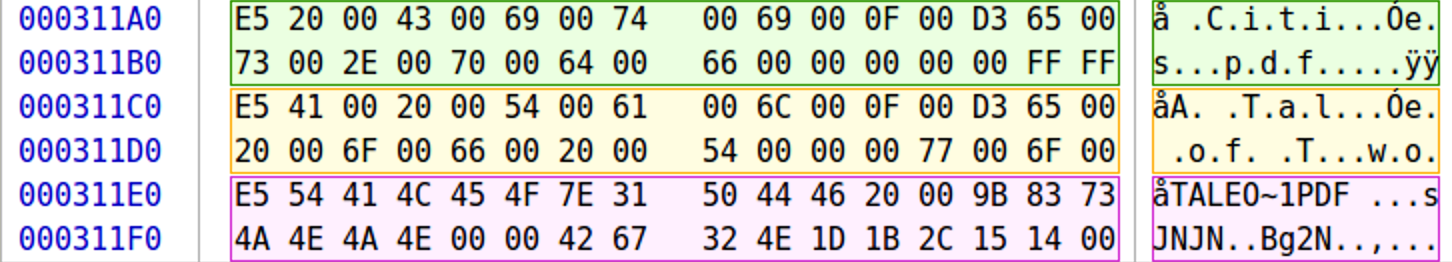
* + - 1. Pride and Prejudice
         1. Status: 0xE5 – Deleted
         2. Filename: Pride and Prejudice
         3. Extension: PDF
         4. Attribute: 0x20 – Archive
         5. Modified date/time: 1/18/19 1:01 PM
         6. Cluster: 0x061D – 1,565
         7. File Size: 0x000C303B – 798,779 bytes



* + - 1. 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



* + - 1. 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



* + 1. All 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 |

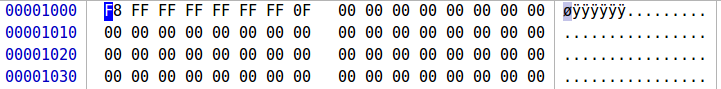
* + 1. Recovering Files

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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. GIFS
   1. Structure Size Calculations
      1. Partition Offset
         1. 0xC450400 = **205,849,600**
      2. Bytes / Sector
         1. Offset 0x0B = 0x0200 = **512**
      3. Sectors / Cluster
         1. Offset 0x0D = 0x8 = **8**
      4. Bytes / Cluster
         1. 8 Sectors / Cluster \* 512 Bytes / Sector = **4096**
      5. Reserved Sectors
         1. Offset 0x000E = 0x0008= **8**
      6. Number of FATs
         1. Offset 0x0010 = 0x2 = **2**
      7. 1st FAT Area Size
         1. Offset 0x0016 = 0x8 = **8** sectors
      8. 2nd FAT Area Size
         1. Offset 0x0016 = 0x8 = **8** 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 0x0013= 0x4E21 = 20,001 Sectors
          2. Data Area = Total Sectors – End of Root
             1. 20,001 – 56 = **19,945** Sectors
   2. FAT Structure

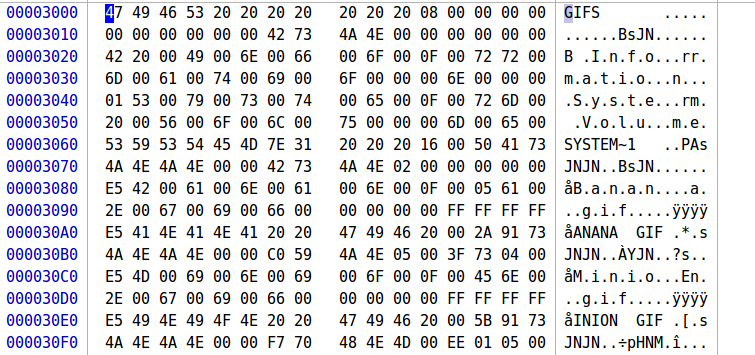
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8 | 8 | 8 | 32 | 19,945 |
| Reserved Sectors | 1st FAT Area | 2nd FAT Area | Root Directory | Data Area |

* 1. 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

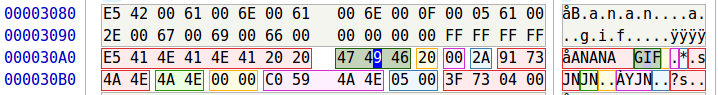


|  |  |
| --- | --- |
| Sector | Next Sector |
| 0x0000 | 0xFFF8 |
| 0x0001 | 0xFFFF |
| 0x0002 | 0xFFFF |
| 0x0003 | 0xFFFF |
| 0x0004 | 0xF0FF |

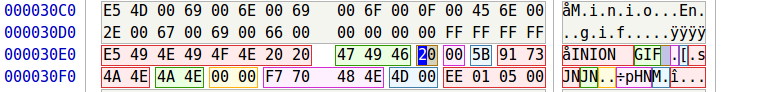
* + 1. Root Directory Structure
       1. Sector 24 – 55
       2. Byte 12,288 – 28,160
       3. Address 0x3000 – 0x6E00



* + 1. File Recovery
       1. Banana
          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



* + - 1. 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



* + 1. All 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 |

* + 1. Recovering Files

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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 |