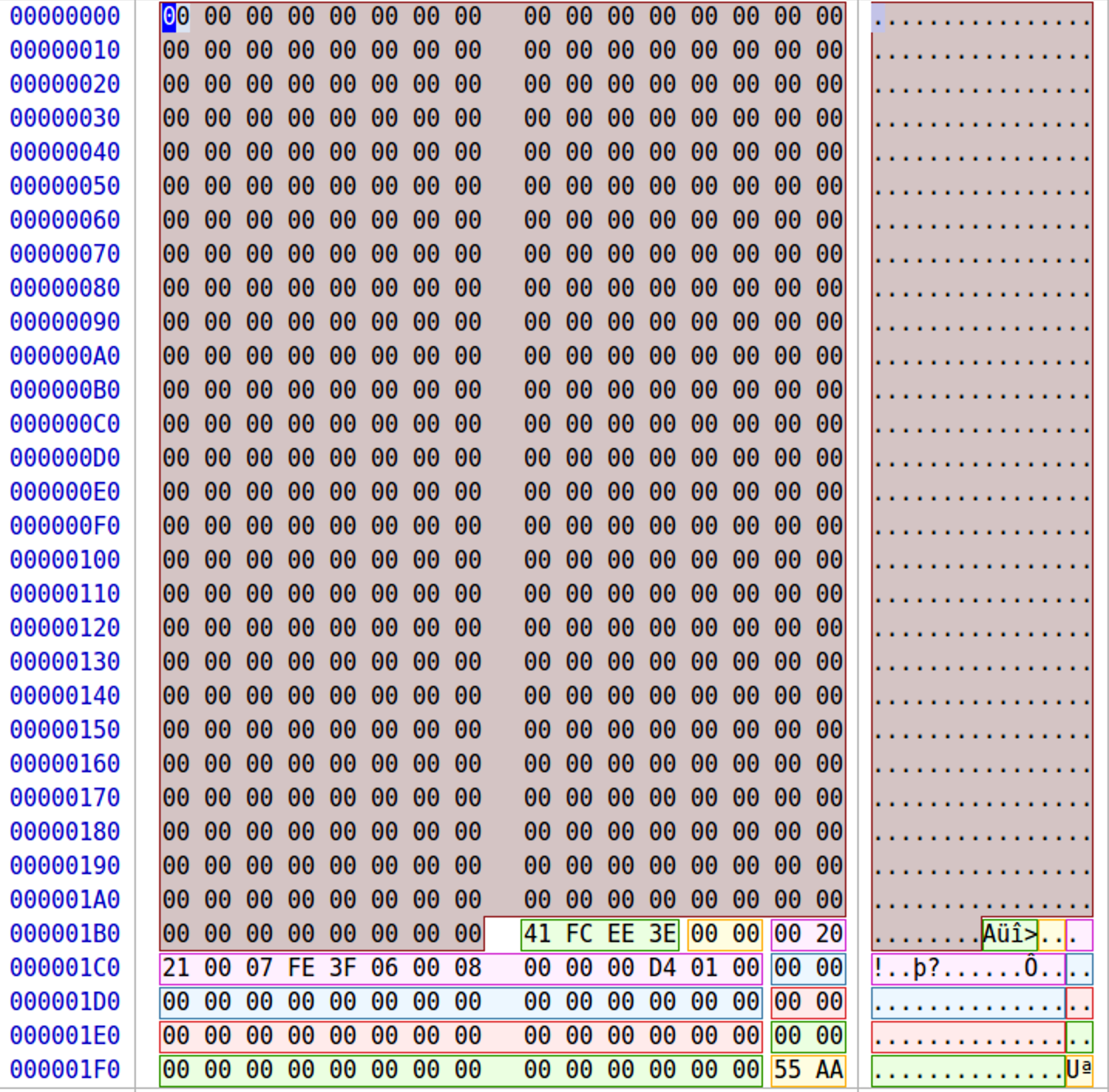
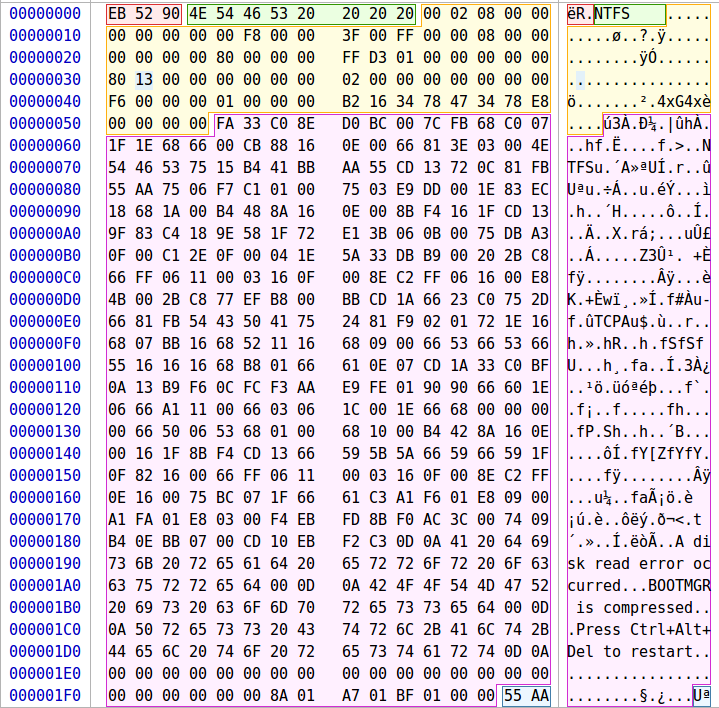
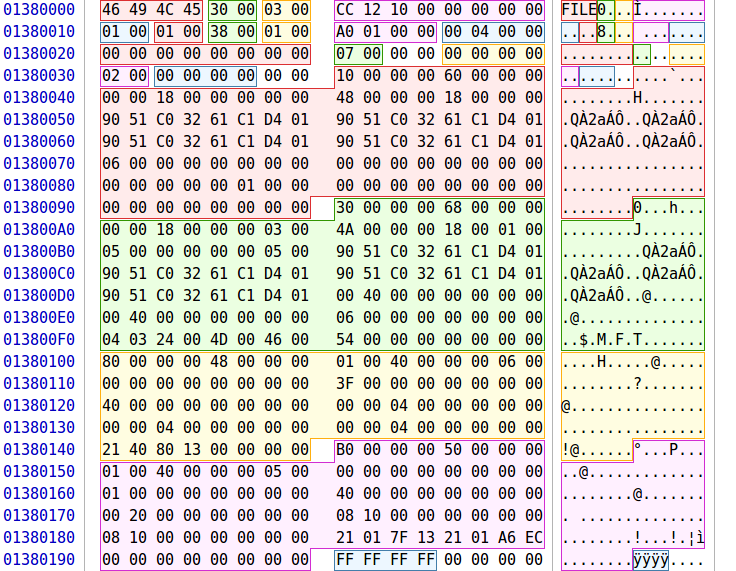
NTFS Image Findings Template



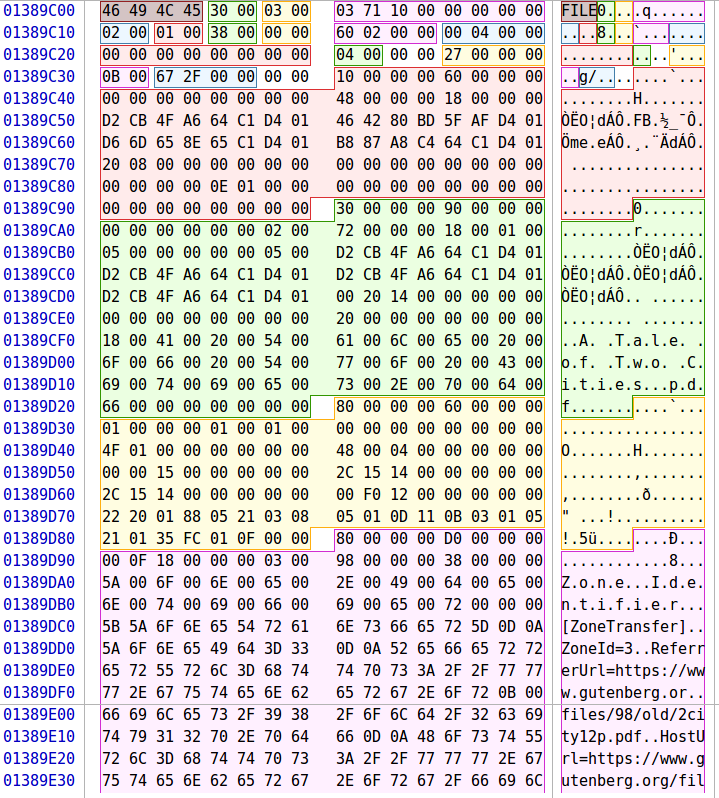
1. Disk Partition Information
   1. Sector Size = 512 bytes = 0x0200
   2. First Sector = Offset 0x01C6 = 0x0800 = 2048
   3. First Sector Address: 512 \* 2048 = 1,048,576 = 0x100000



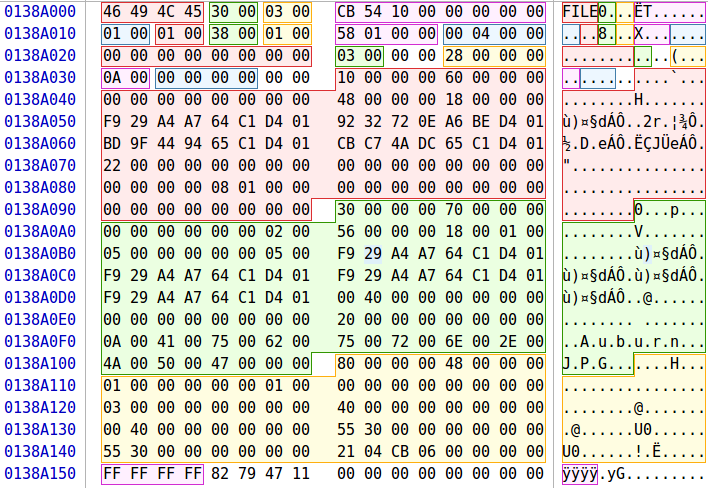
1. NTFS Disk Partition Information
   1. Bytes/Sector: Offset 0x0B = 0x0200 = 512
   2. Sectors/Cluster: Offset 0x0D = 0x08 = 8
   3. Bytes/Cluster: 8 \* 512 = 4096 bytes / cluster
   4. $MFT Cluster Number: Offset 0x30 = 0x1380 = 4,992
   5. $MFT Address: 0x13800000 = 20,447,232
2. $MFT Information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



1. User File Information – Offset 0x1389C00 (20,487,168)
   1. A tale of two cities
      1. List File Attributes:
         1. 0x10 - $STANDARD\_INFORMATION
         2. 0x30 - $FILE\_NAME
         3. 0x80 - $DATA
      2. Filename: Offset 0x0F2 = A Tale of Two Cities.pdf
      3. Allocated Size: Offset 0x150= 0x150000 = 1,376,256 bytes
      4. Data Start Cluster: Offset 0x170 = 0x0588 = 1,416
      5. Data Start Address
         1. 1,416 \* 4,096 = 5,799,936
      6. Unrecoverable: overwritten by auburn.jpg



* 1. Auburn
     1. List File Attributes:
        1. 0x10 - $STANDARD\_INFORMATION
        2. 0x30 - $FILE\_NAME
        3. 0x80 - $DATA
     2. Filename: Offset 0x0F2 = Auburn.jpg
     3. Allocated Size: Offset 0x130 = 0x4000 = 16,384 bytes
     4. Data Cluster Information
        1. 21 04 CB 06
        2. 2 bytes required for the first cluster address
        3. Number of continuous clusters for this file – 1 \* 4 = 4
        4. Start Cluster for Data: 0x06CB = 1,739
        5. Start Address for Data:
           1. 1,739 \* 4096 = 7,122,944



* 1. Avengers – Offset 0x138A3C0 (20,489,216)
     1. List File Attributes:
        1. 0x10 - $STANDARD\_INFORMATION
        2. 0x30 - $FILE\_NAME
        3. 0x80 - $DATA
     2. Filename: Offset 0x0F2 = Avengers.docx
     3. Allocated Size: Offset 0x138 = 0x100000 = 65,536 bytes
     4. Data Cluster Information
        1. 21 0D CF 06
           1. 2 bytes required for the first cluster address
           2. Number of continuous clusters for this file – 1 \* D = 13
           3. Start Cluster for Data: 0x06CF = 1,743
           4. Start Address for Data:

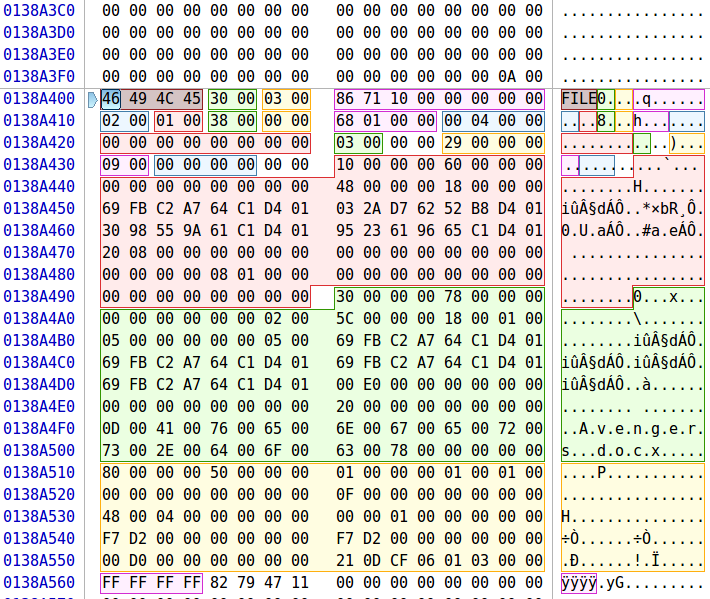
1,739 \* 4096 = 7,139,328

* + - * 1. Actual Offset

Partition Offset + Start Address

1,048,576 + 7,139,328 = 8,187,904

* + 1. Unrecoverable
       1. Overwritten by banana.gif



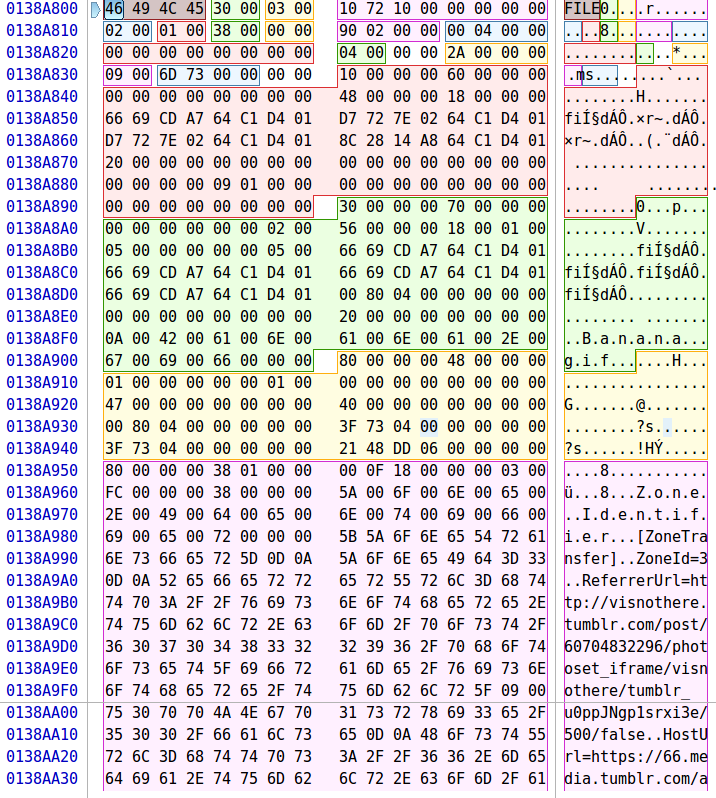
* 1. Banana – Offset 0x138A800 (20,490,240)
     1. List File Attributes:
        1. 0x10 - $STANDARD\_INFORMATION
        2. 0x30 - $FILE\_NAME
        3. 0x80 - $DATA
     2. Filename: Offset 0x0F2 = Banana.gif
     3. Allocated Size: Offset 0x130 = 0x048000= 294,912 bytes
     4. Data Cluster Information
        1. 21 48 DD 06
           1. 2 bytes required for the first cluster address
           2. Number of continuous clusters for this file – 0x1 \* 0x48 = 72
           3. Start Cluster for Data: 0x06DD = 1,757
           4. Start Address for Data:

1,757 \* 4096 = 7,196,672

* + - * 1. Actual Offset

Partition Offset + Start Address

1,048,576 + 7,196,672 = 8,245,248



* 1. Great Expectations – Offset 0x138AC00 (20,491,264)
     1. List File Attributes:
        1. 0x10 - $STANDARD\_INFORMATION
        2. 0x30 - $FILE\_NAME
        3. 0x80 - $DATA
     2. Filename: Offset 0x0F2 = Great Expectations.pdf
     3. Allocated Size: Offset 0x148 = 0x310000= 3,211,264 bytes
     4. Data Cluster Information
        1. 21 03 86 0A

For large files like the PDF the cluster information seems to continue

Assuming because it can’t hold the exact number of cluster sin one byte. But for example, this file is 784 clusters. Why not have this cluster information say 196 (xC4) and then have the number before it be 4 so its x4 \* xC4 = x310 = 784

* + - * 1. 2 bytes required for the first cluster address
        2. Number of continuous clusters for this file – 0x1 \* 0x3 = 3
        3. Start Cluster for Data: 0x0A86 = 2,694
        4. Start Address for Data:

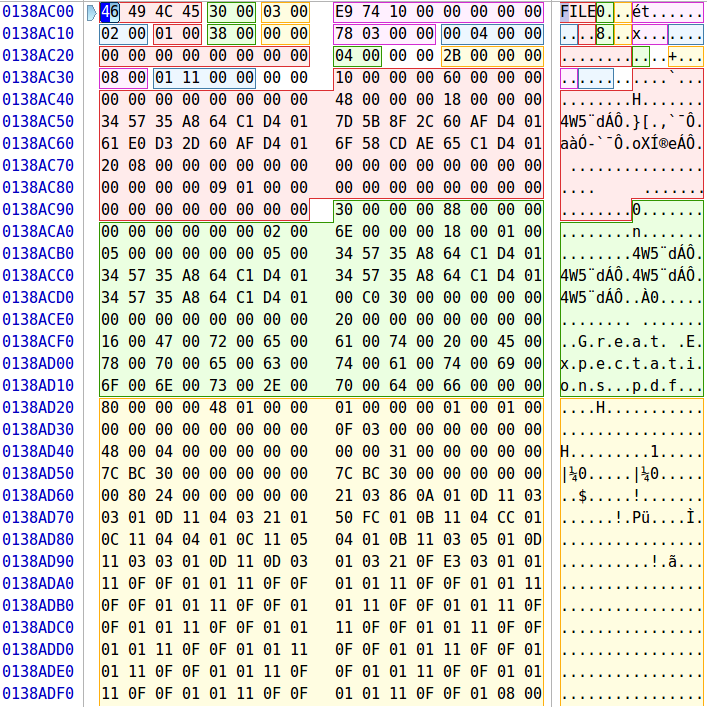
2,694 \* 4096 = 11,034,624

* + - * 1. Actual Offset

Partition Offset + Start Address

1,048,576 + 11,034,624 = 12,083,200

* + 1. Unrecoverable: zeroed out



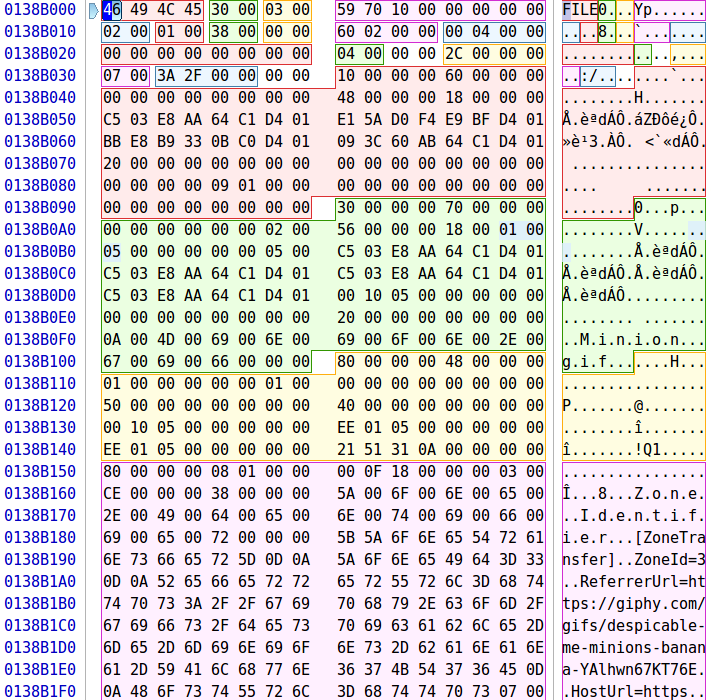
* 1. Minion – Offset 0x138B000 (20,492,288)
     1. List File Attributes:
        1. 0x10 - $STANDARD\_INFORMATION
        2. 0x30 - $FILE\_NAME
        3. 0x80 - $DATA
        4. 0x80 - $BITMAP
     2. Filename: Offset 0x0F2 = Minion.gif
     3. Allocated Size: Offset 0x130 = 0x051000 = 331,776 bytes
     4. Data Cluster Information
        1. 21 05 31 0A
           1. 2 bytes required for the first cluster address
           2. Number of continuous clusters for this file – 0x1 \* 0x5 = 5
           3. Start Cluster for Data: 0x0A31 = 2,609
           4. Start Address for Data:

2,609 \* 4096 = 10,686,464

* + - * 1. Actual Offset

Partition Offset + Start Address

1,048,576 + 10,686,464 = 11,735,040



* 1. War and Peace – Offset 0x138B000 (20,492,288)
     1. List File Attributes:
        1. 0x10 - $STANDARD\_INFORMATION
        2. 0x30 - $FILE\_NAME
        3. 0x80 - $DATA
        4. 0x80 - $BITMAP
     2. Filename: Offset 0x0F2 = War and Peace.pdf
     3. Allocated Size: Offset 0x140 = 0x9C0000 = 10,223,616 bytes
     4. Real Size: Offset 0x148 = 0x9BC0F7 = 10,207,479 bytes
     5. Data Cluster Information
        1. 22 90 08 E0 1A
           1. 2 bytes required for the first cluster address
           2. 2 bytes required for cluster counter

0x0890 = 2,192

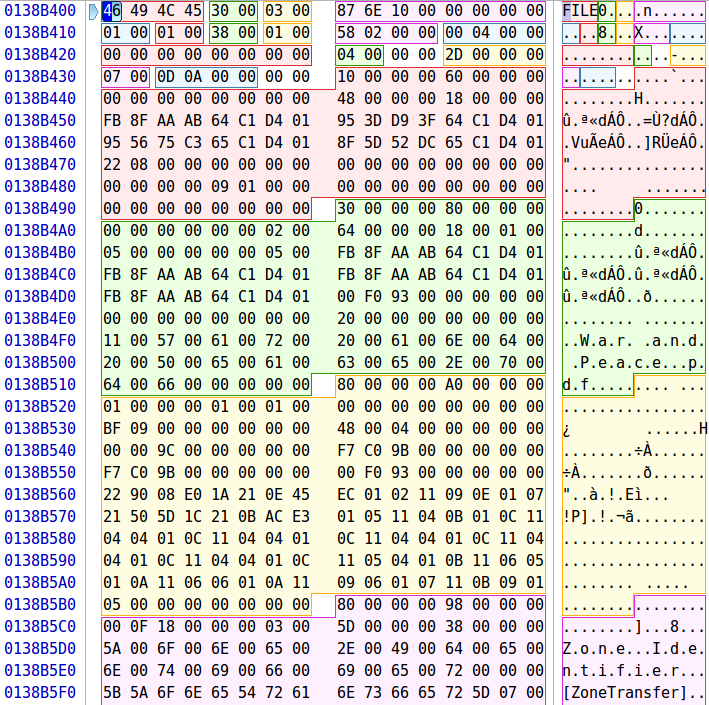
* + - * 1. Start Cluster for Data: 0x1AE0 = 6,880
        2. Start Address for Data:

6,880 \* 4096 = 28,180,480

* + - * 1. Actual Offset

Partition Offset + Start Address

1,048,576 + 28,180,480 = 29,229,056



1. Recover File Command:
   1. sudo dd if=/dev/sdX of=<13> bs=1 skip=<15> count=<14>