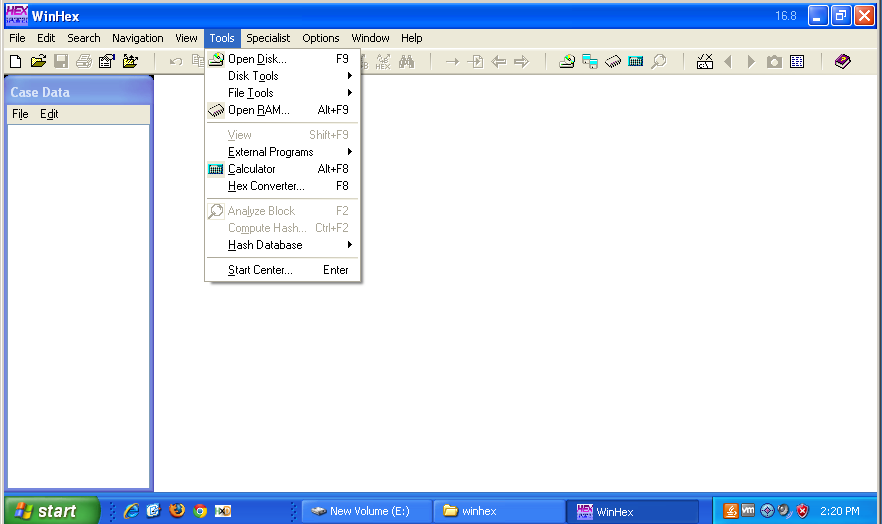
**SY486J: Cyber Crime Investigation: Lab Six**

**Linux Investigation**

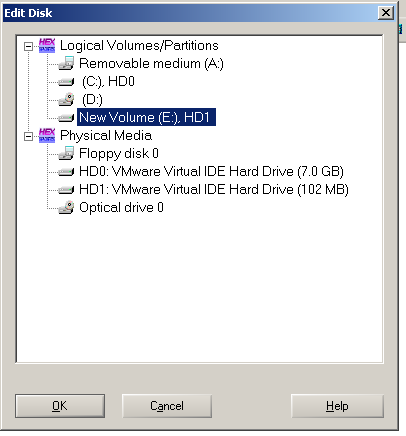
**Assigned: February 27,2019**

**Due Date: March 6,2019**

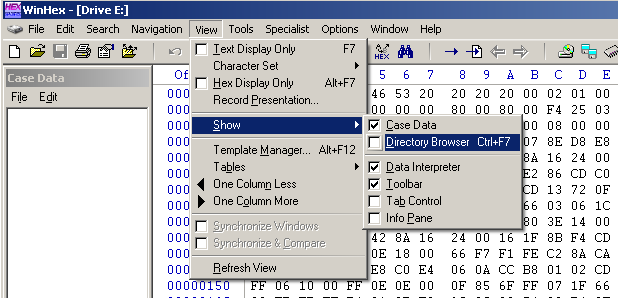
1. **Setting the drive**
   1. Right click on “This PC” 🡪Manage 🡪Disk Management
   2. Choose a drive to shrink by 4000MB (4GB)
   3. Now partition and format the new drive, right drive
   4. In Computer Management, in the lower right, right-click the "Unallocated" space on your new hard disk.
   5. In the context menu, click "New Volume...” as shown below.
   6. The "New Volume Wizard" opens, as shown below.
   7. Drag the FILE1.TXT and FILE2.TXT files from the Forensic Share and drop into the New Volume.
   8. From the Forensic Share, download WinHex.zip
   9. On your desktop, or wherever you saved the file, right-click the winhex.zip file and click "Extract All..."
   10. A folder with several files opens. Double-click the WinHex.exe file in the extracted folder.
   11. WinHex opens, as shown below.
2. **Viewing the data in WinHex**
   1. From the WinHex menu bar, click Tools, "Open Disk..."

****

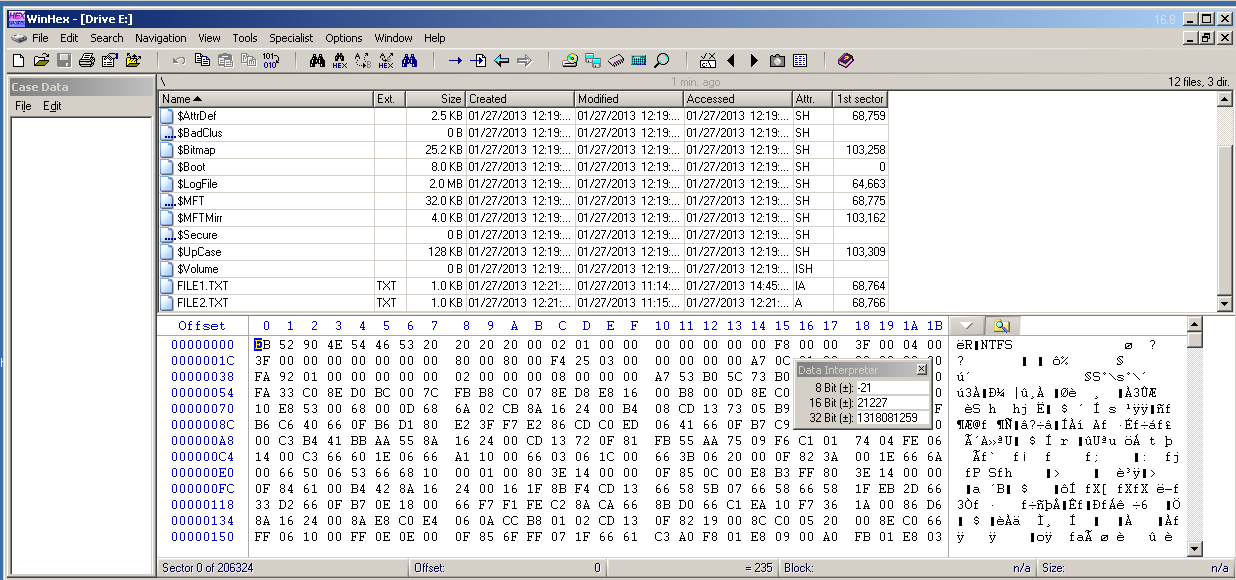
* 1. In the "Edit Disk" box, click "New Volume", as shown below, and then click the OK button



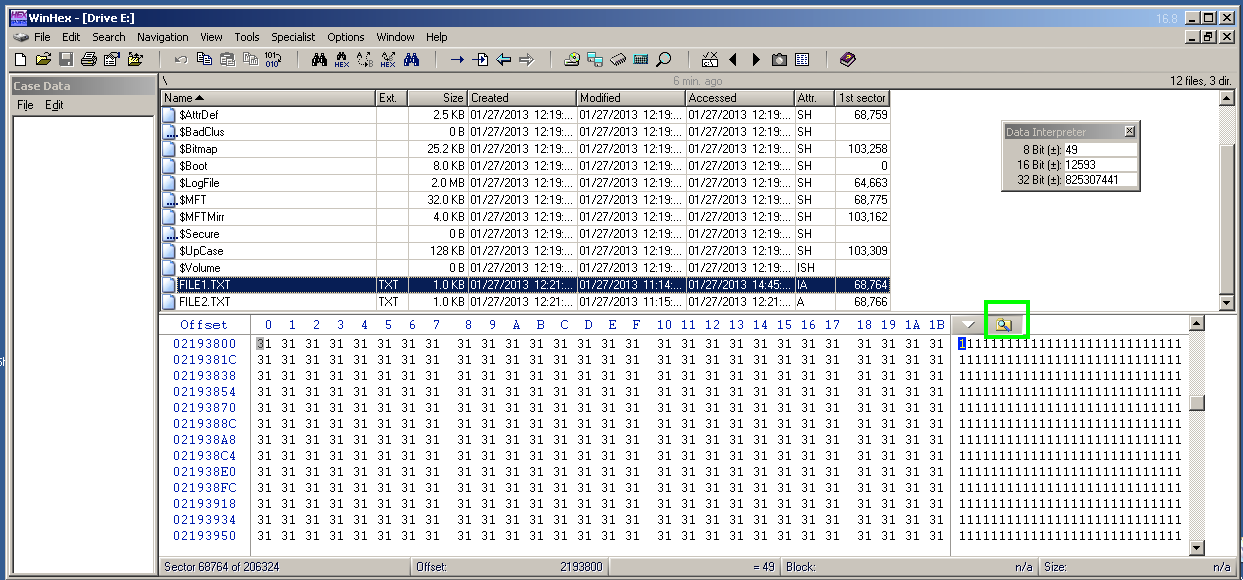
* 1. From the WinHex menu bar, click View, Show, "Directory Browser", as shown below.



* 1. The Directory Browser pane appears in the upper center of the window.
  2. Scroll down to find FILE1.TXT and FILE2.TXT, as shown below.



* 1. In the Directory Browser, click FILE1.TXT.
  2. The lower pane shows the raw hex data in the first cluster containing data for FILE1.TXT, as shown below.



Notice the yellow icon marked with the green outline in the image above this text. (It's a magnifying glass on a folder). This icon toggles the display of Directory Browser. Click it now.

Directory Browser vanishes, so you can see more of the hex view, as shown below.

* 1. Scroll up a few rows in the hex view so you can see where the "1" characters start, as shown below.

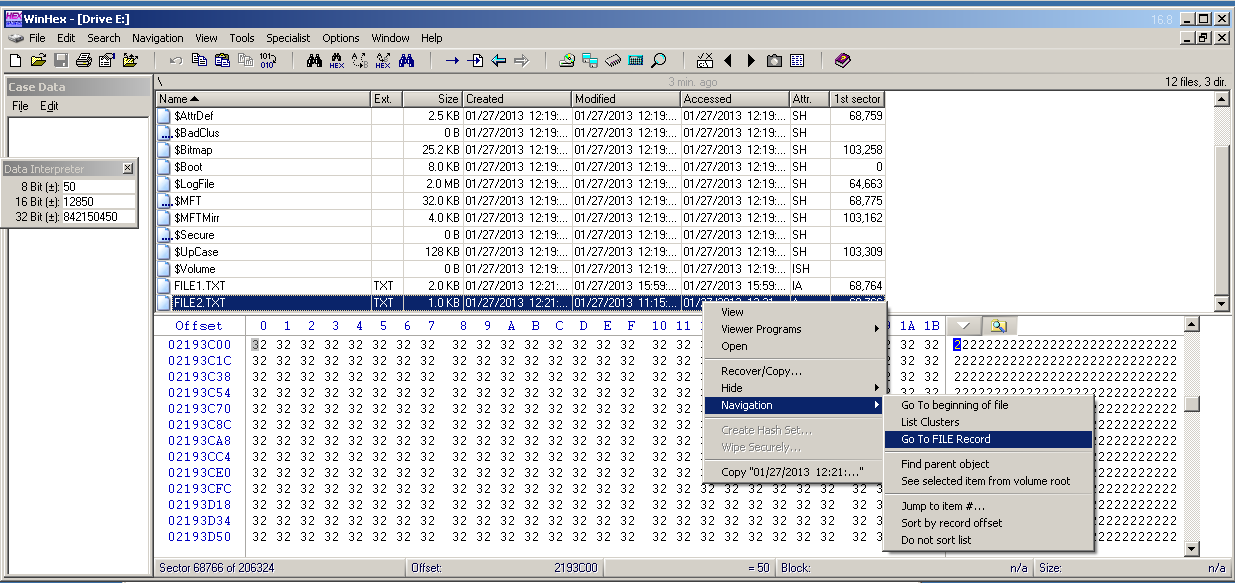
They start at the beginning of a sector. The sector number is shown at the lower left--in my case, it was Sector 68764.

**What is your sector number? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **Viewing an MFT Record**
   1. Click the little yellow icon to show Directory Browser again.

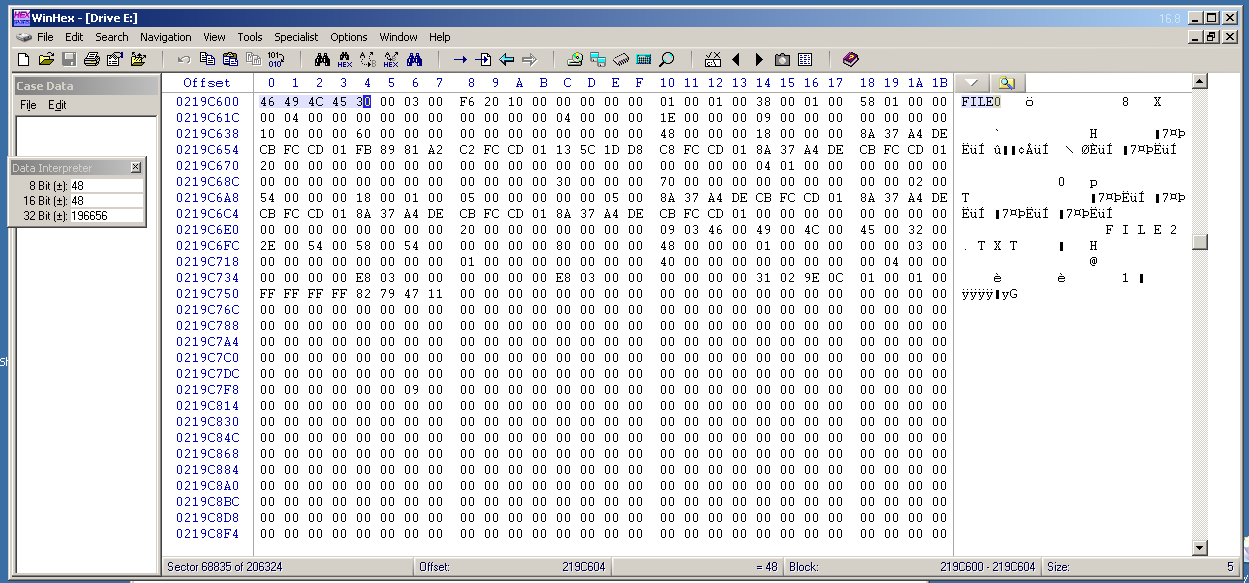
Scroll to the bottom.

* 1. Right-click FILE2.TXT.
  2. In the context menu, click Navigation, "Go To FILE Record", as shown below.



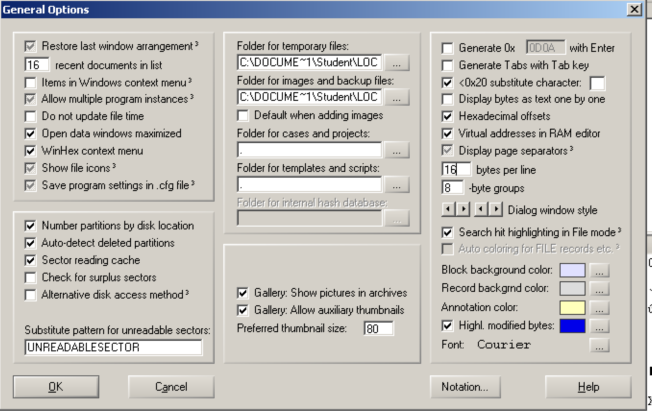
This is the Master File Table (MFT) record which contains information about FILE2.TXT. Each MFT record begins with the ASCII text "FILE0".

Highlight that text, so your screen looks like the image below.



* 1. **MFT Record Header**

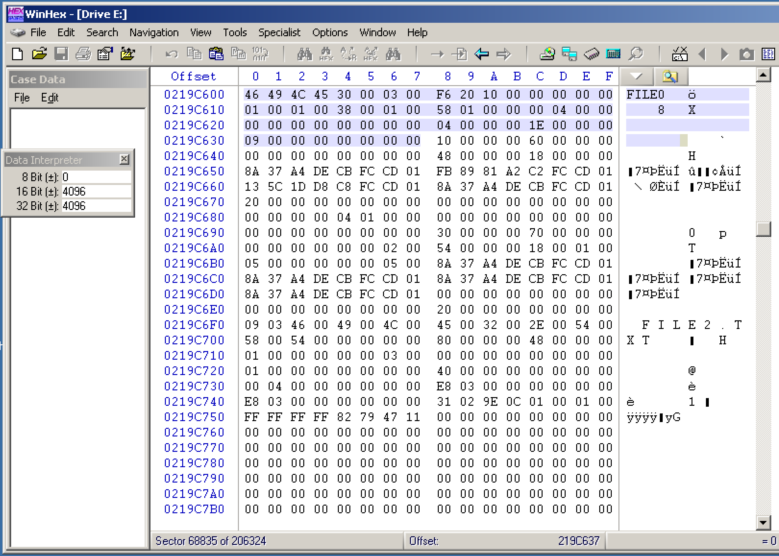
1. The MFT Record begins with a 56-byte header.
2. We need to count 56 bytes from this point. That will be a lot easier with only 16 bytes per row.
3. From the WinHex menu bar, click Options, General.
4. On the right side, in the center, enter 16 in the "bytes per line" box, as shown below.
5. Click OK.



1. WinHex now has only 16 bytes per line, labelled 0 though F in the "Offset" line at the top of the display, as shown below.
2. Click on the first byte: 46.
3. Hold down the Shift key and press the down-arrow on the keyboard three times. This selects three lines of 16 bytes for a total of 48 bytes.
4. Now, holding down the Shift key, press the right-arrow key until you have selected bytes 0 through 7 in that row.
5. This selects the entire 56 bytes of the MFT record header, as shown below.

Record the start and end offset for the header here:

**Start offset\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ end offset\_\_\_\_\_\_\_\_\_\_\_\_\_**

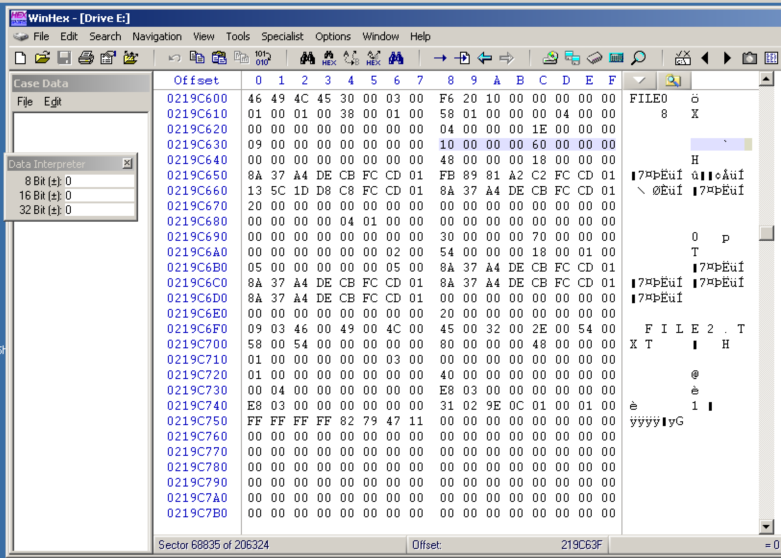


* 1. **Standard Information**

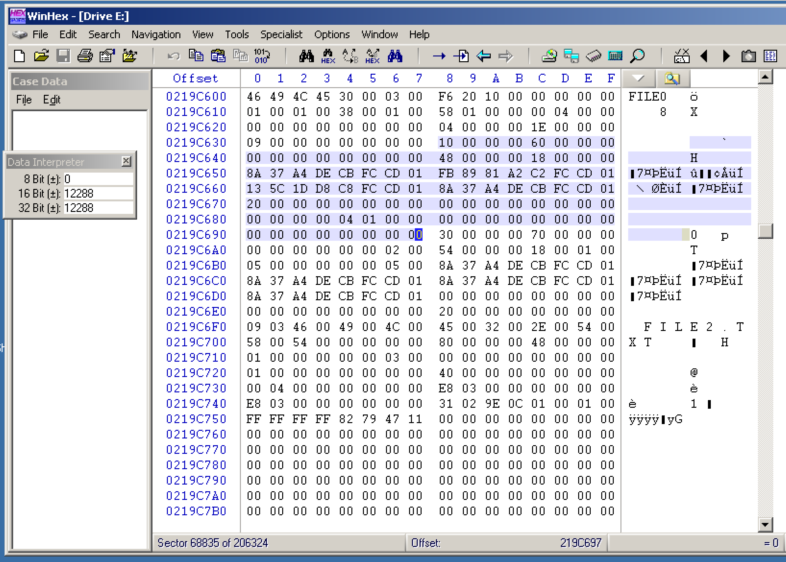
1. The next four bytes indicate the length of the section, in hexadecimal, with the least significant byte first.
2. Each standard information section of the MFT begins with a four-byte identifier--in this case 10 00 00 00.
3. **Record the start and end offset for the four-byte identifier:**

**Start offset\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ end offset\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. The next four bytes indicate the length of the section, in hexadecimal, with the least significant byte first.
2. **So the eight bytes highlighted below indicate that the Standard Information section is 60 bytes long (this is in hex). So this is equivalent to how many bytes in decimal \_\_\_\_\_\_\_\_\_\_\_\_\_\_**



1. Highlight the entire Standard Information section. It will be six entire rows of 16 bytes, as shown below.



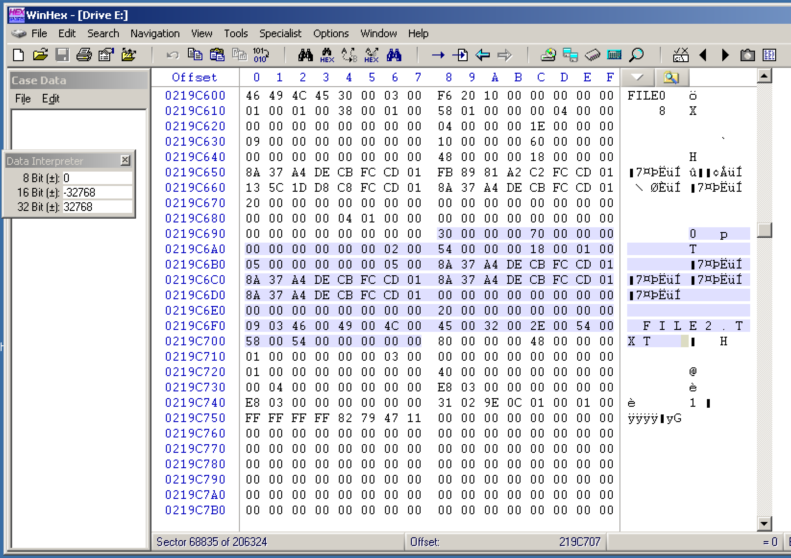
* 1. **File Name section**

The next section begins with 30 00 00 00 and is 70 (hex) bytes long, as shown below. Highlight the section. Notice the readable file name near the end of this section: FILE2.TXT.

**How long is the file name section in decimal? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

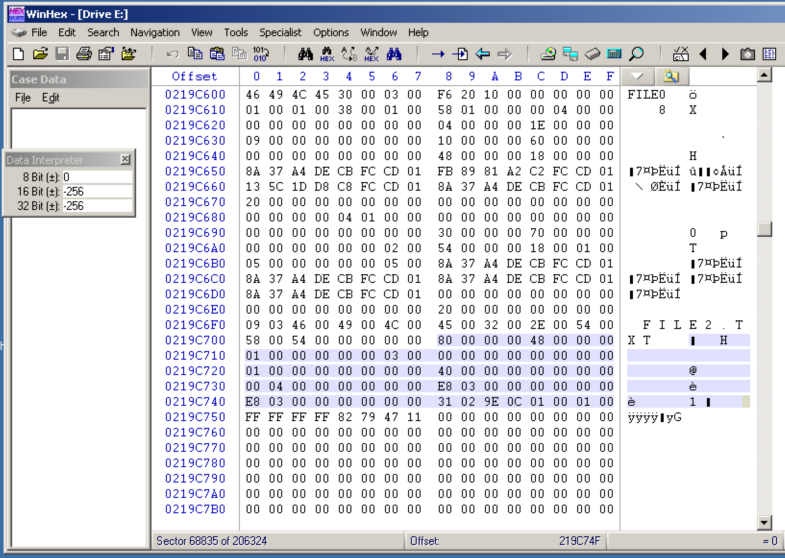
**Record the start and end offset for the file name section:**

**Start offset\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ end offset\_\_\_\_\_\_\_\_\_\_\_\_\_**



* 1. **Data Section**

1. The next section begins with 80 00 00 00 and is 48 bytes long, as shown below.
2. This section indicates where the data is actually stored on the disk.
3. Highlight the section.

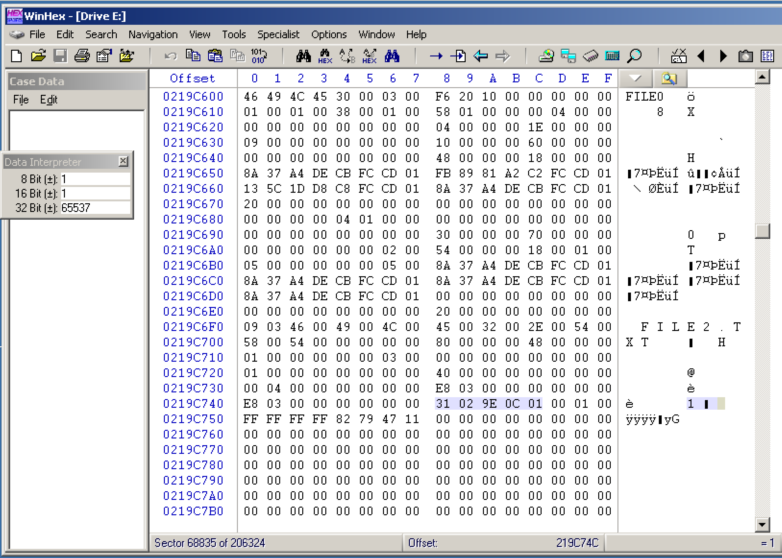


The last eight bytes of this section contain the "Data Run", as highlighted below.

**How long is the data section in decimal? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Record the start and end offset for the data section:**

**Start offset\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ end offset\_\_\_\_\_\_\_\_\_\_\_\_\_**



In this case, the Data Run is

31 02 9E 0C 01

The first byte should be read as two individual hexadecimal values:

3: the last 3 bytes contain the starting cluster number

1: The first 1 byte contains the length of this portion of the file, in clusters.

The cluster # bytes are in "Little Endian" notation, so they must be reversed in order, resulting in Cluster number 01 0c 9E.

Lets go over the same process for FILE1.TXT – writing the offsets next to each other and labeling them clearly.