Module B2: FTK Basics

Pre-requisite Knowledge and Skills:

1. Understand basic of computer operating skills

Learning Objectives

1. Be familiar to FTK basic functionalities.

Recommended Running Environment/Tools:

1. Windows OS
2. Forensic Toolkit 1.8.6.exe

Material:

1. Messier Image.E01 (a disk image file from AccessData)

Video Lecture:

1. N/A

Lab Assessment:

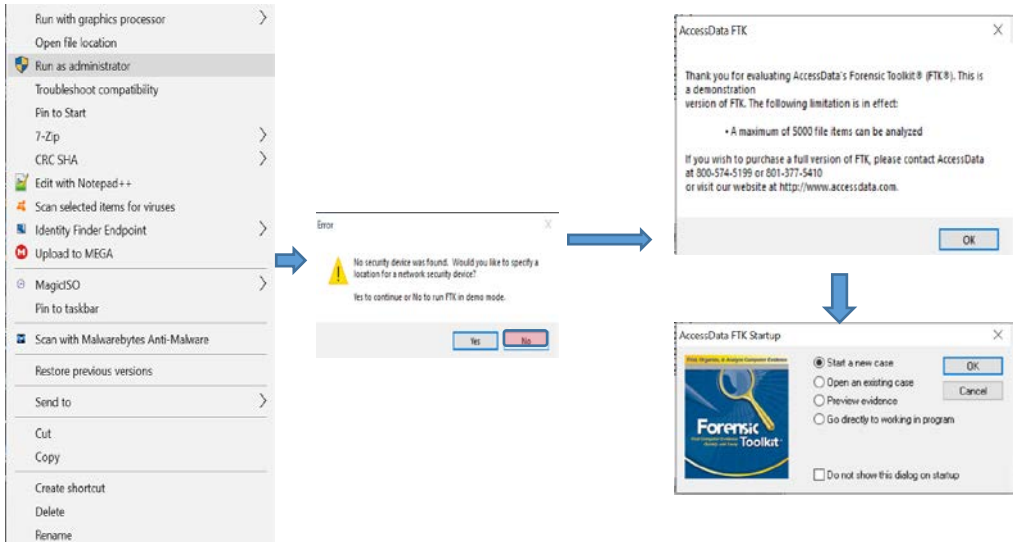
1. FTK Basics Quiz

Acknowledgement:

The Messier Image.E01 file is from AccessData and this module introduces how to use FTK tools, which is also from AccessData. https://www.accessdata.com

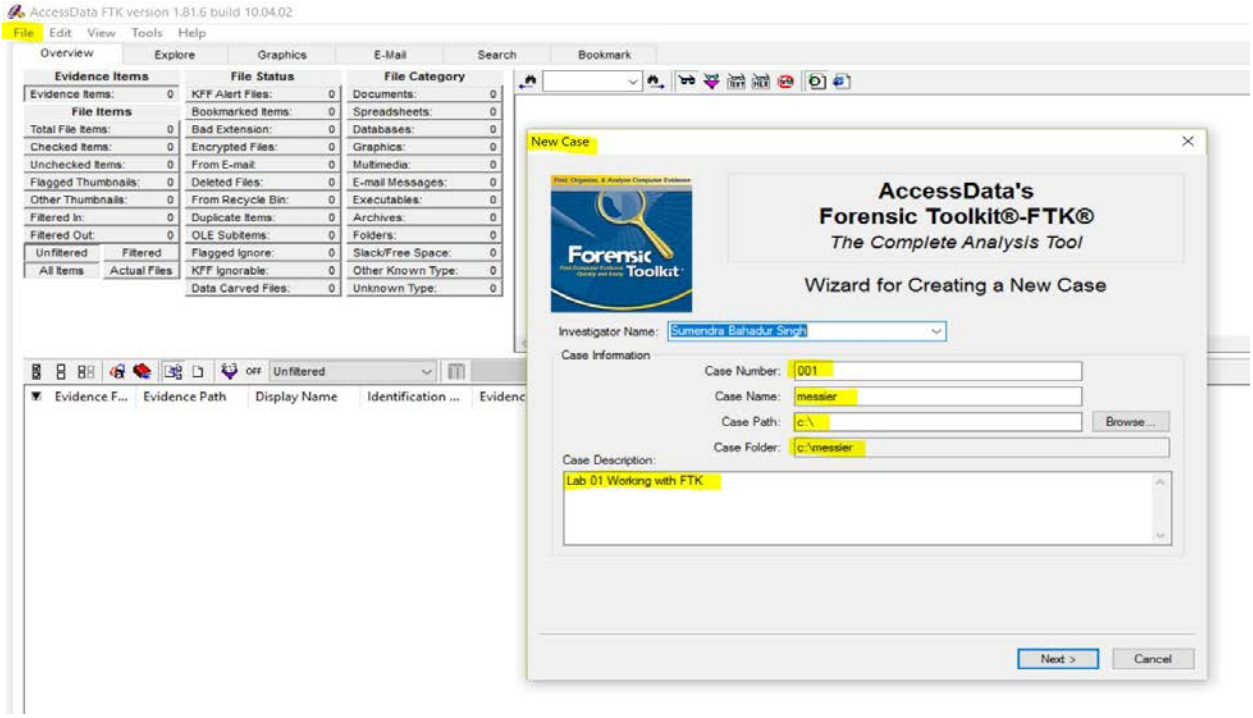
Lab Instructions:

Creating a new case by using FTK 1.8.6. start by run 1.8.6 from your computer by right click the FTK1.8.6 program icon, then choose the "**run as administrator**" option. after that, select the no to run FTK in **Demo mode** (no license), click ok to accept demo mode, and then start new case.

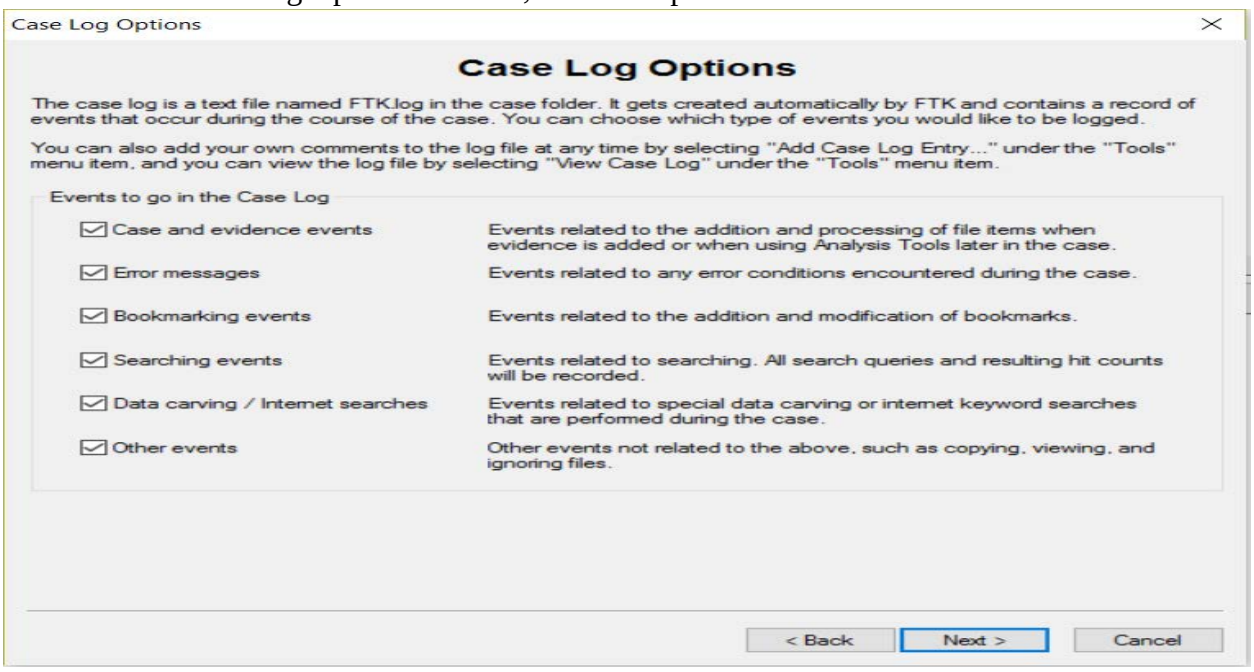


Steps:

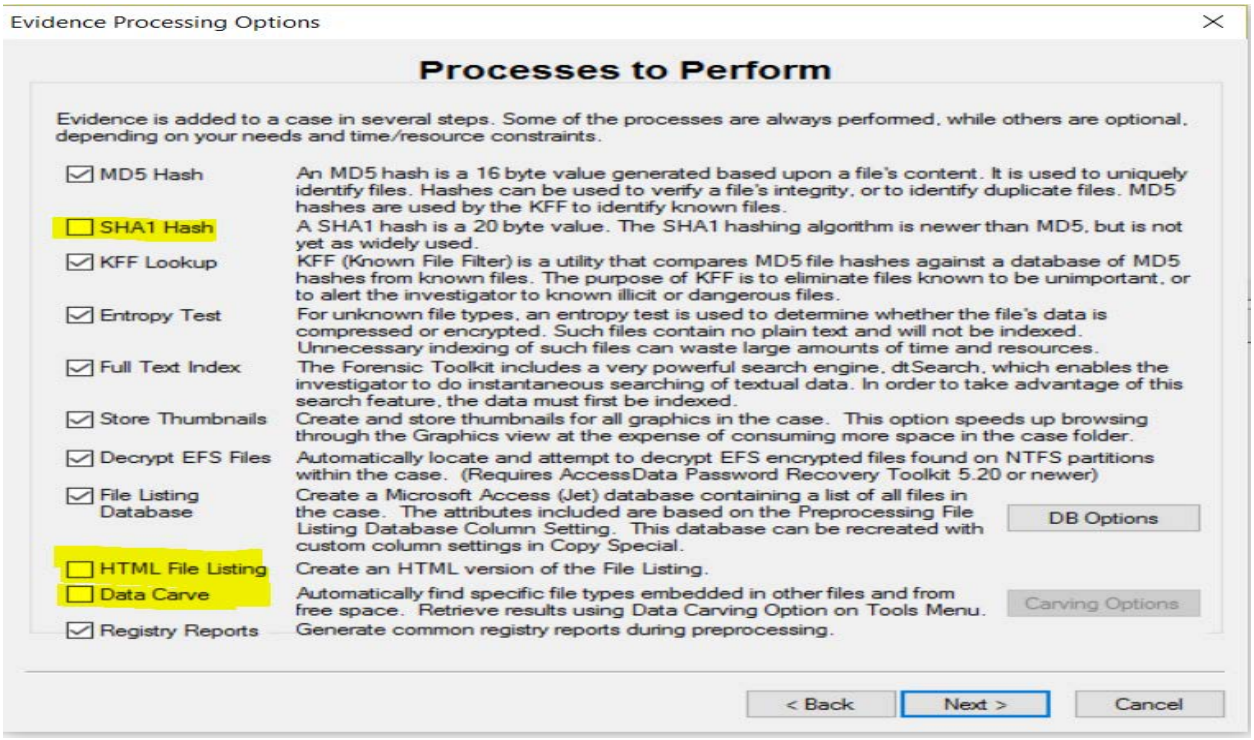
1. Following the steps above, or if the FTK is running with no case open, then you can also Click File> New Case.
2. In the New Case window, type case name.
3. Make sure the Case Path is drive:\Cases.



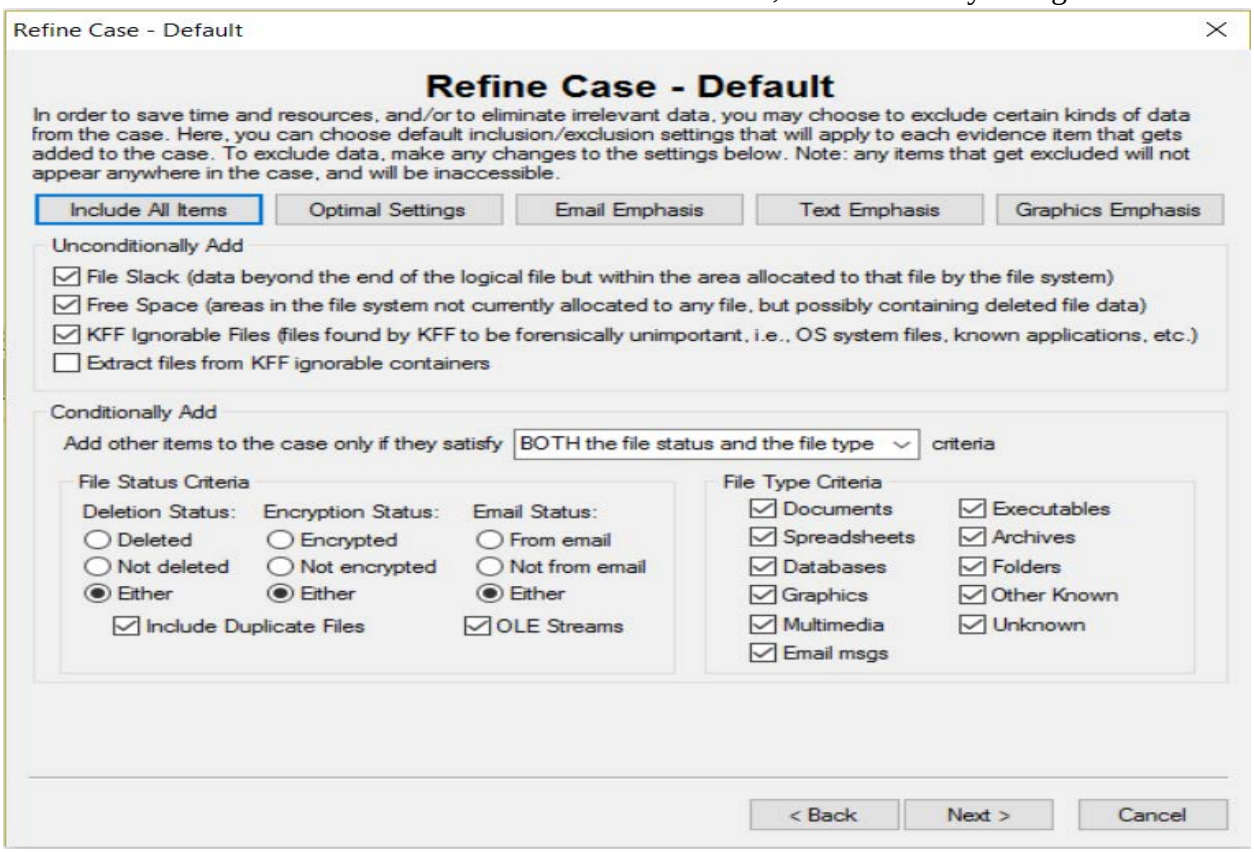
4. In the Case Log Options window, leave all options marked.

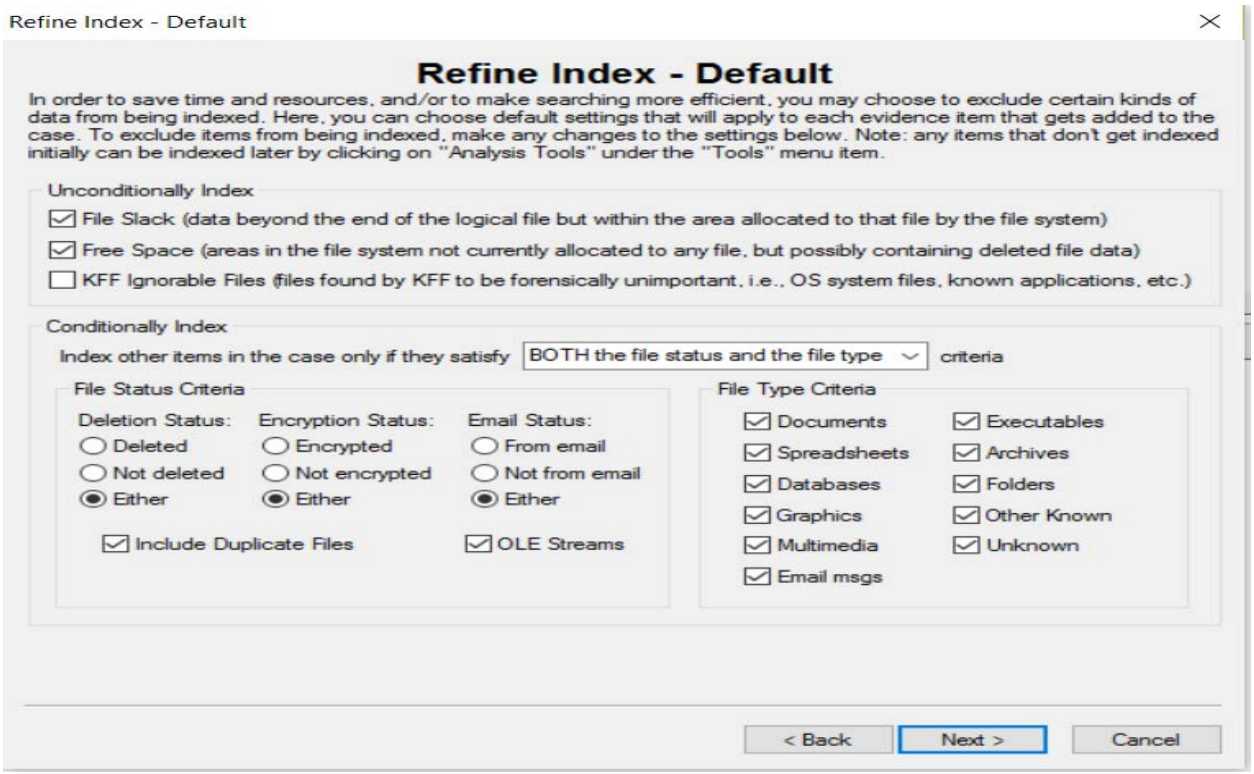


5. In the Evidence Processing Options window, mark all the options except SHAI Hash, Data Carving, and HTML File Listing.

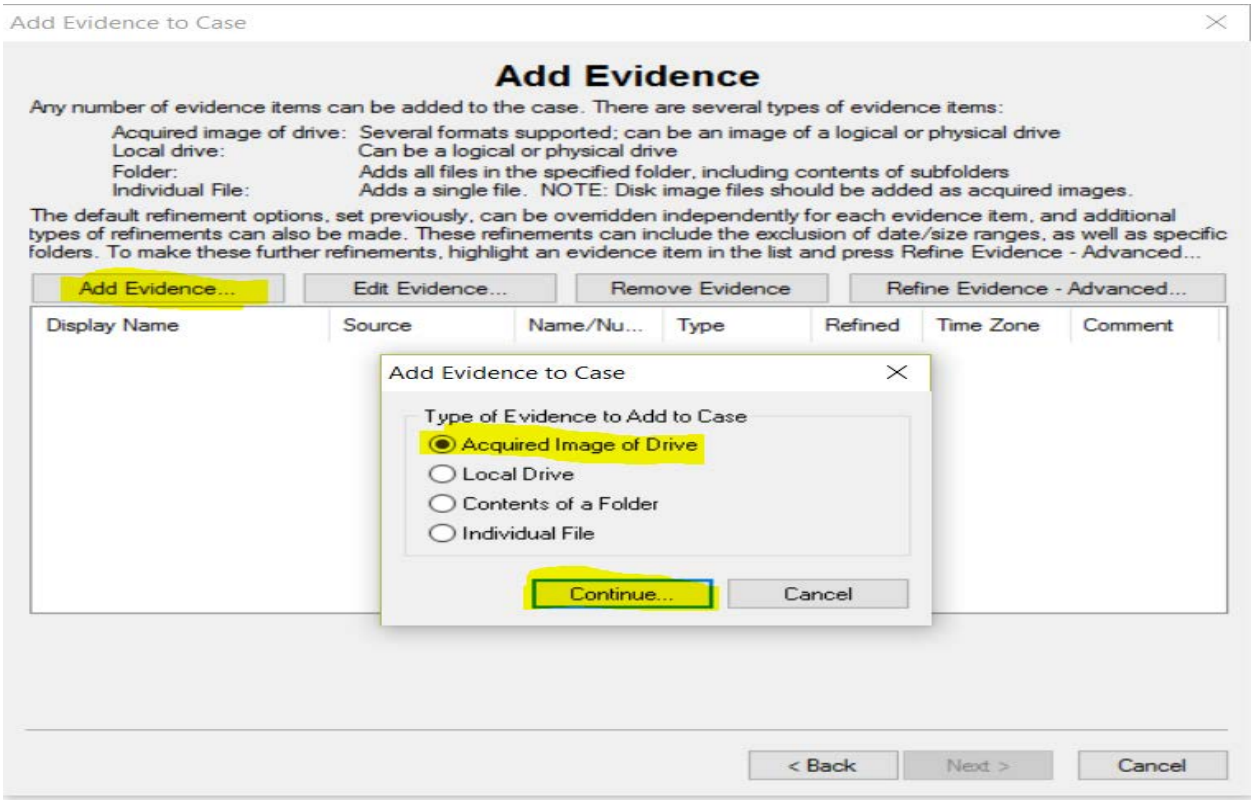


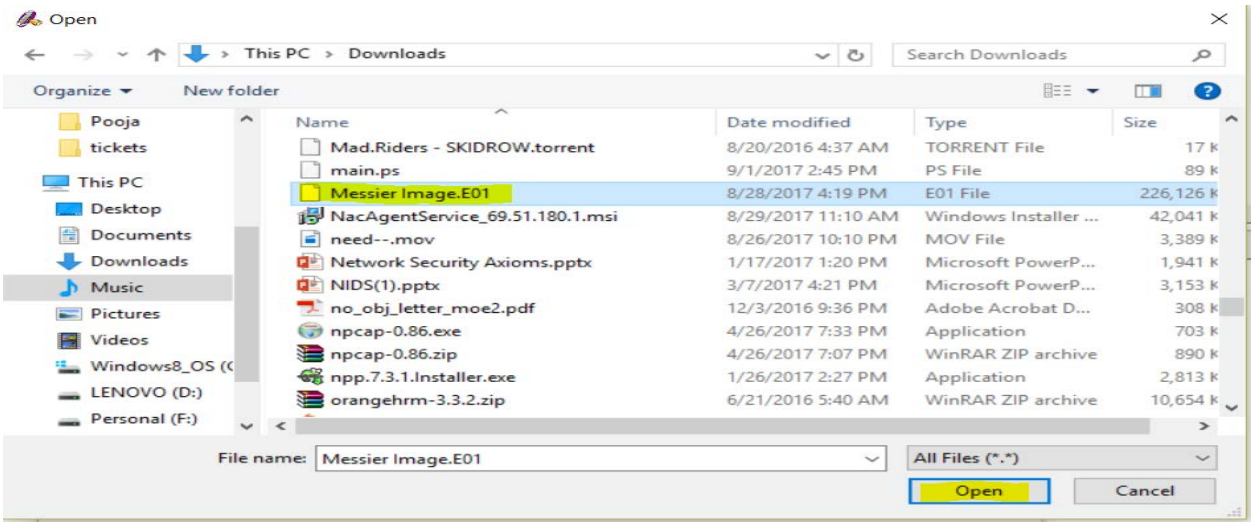
6. In the Refine Case and Refine Index default window, don't make any changes.



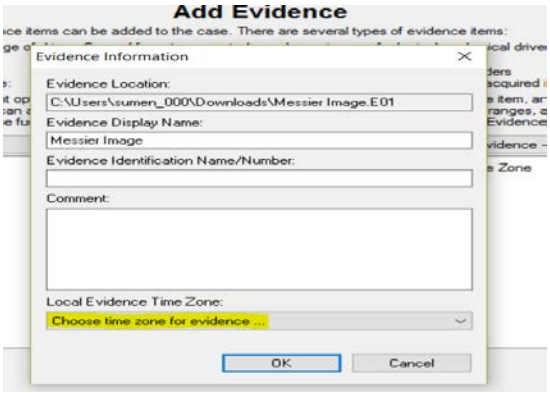


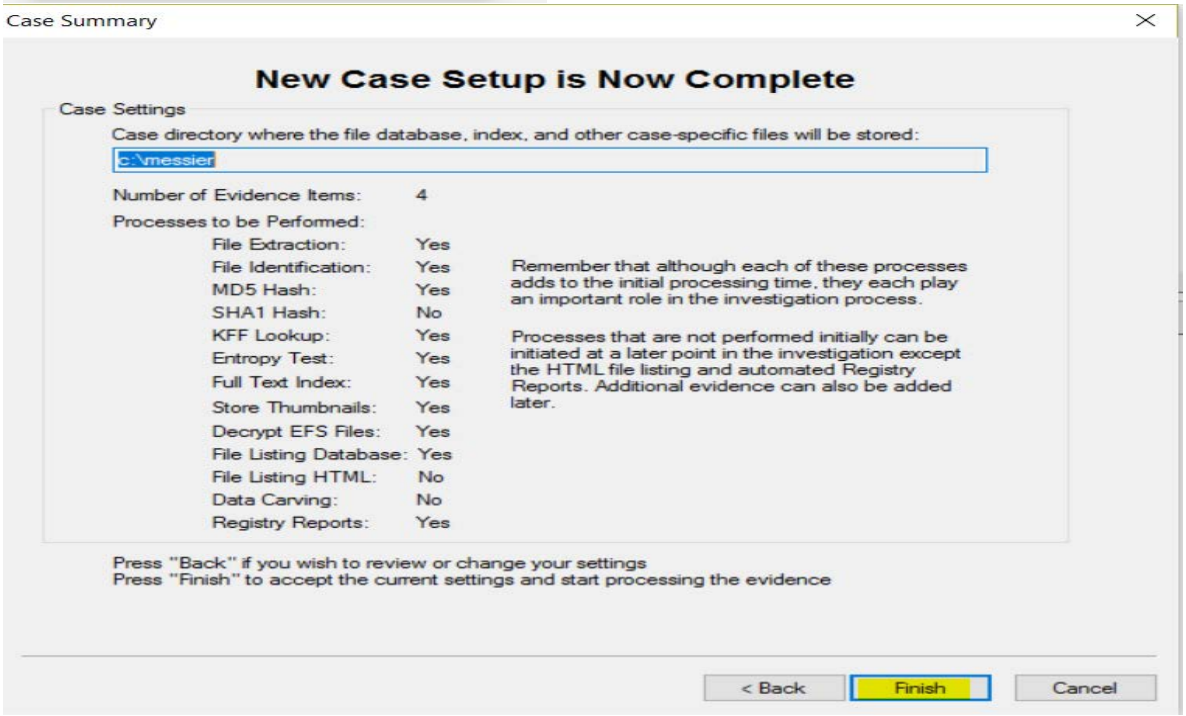
7. In the Add Evidence to Case window, click Add Evidence. Add case image from your drive with acquired image of drive option in our case. we need to download the image before we add the image file to the FTK.



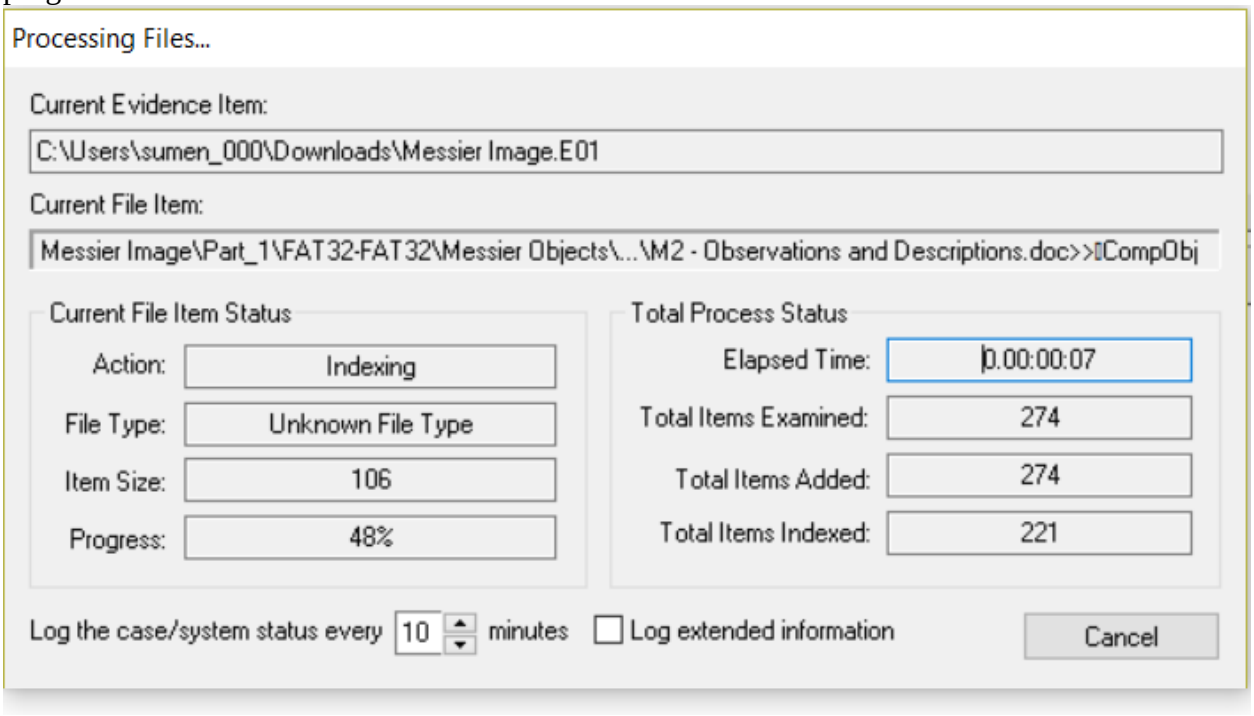


8. In the Evidence Information window, choose a time zone and in the Case Summary window, click Finish.



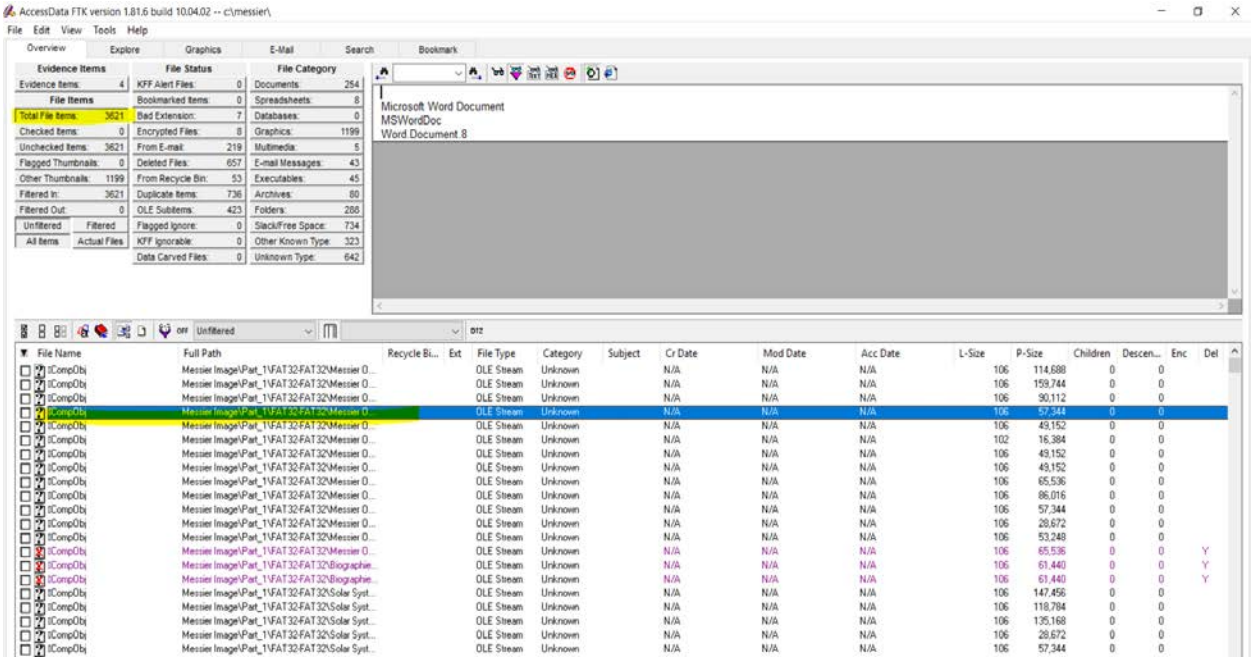


It will take few minutes to generate a case with the image a processing files windows will progress status.



Reviewing Menu Bar Options

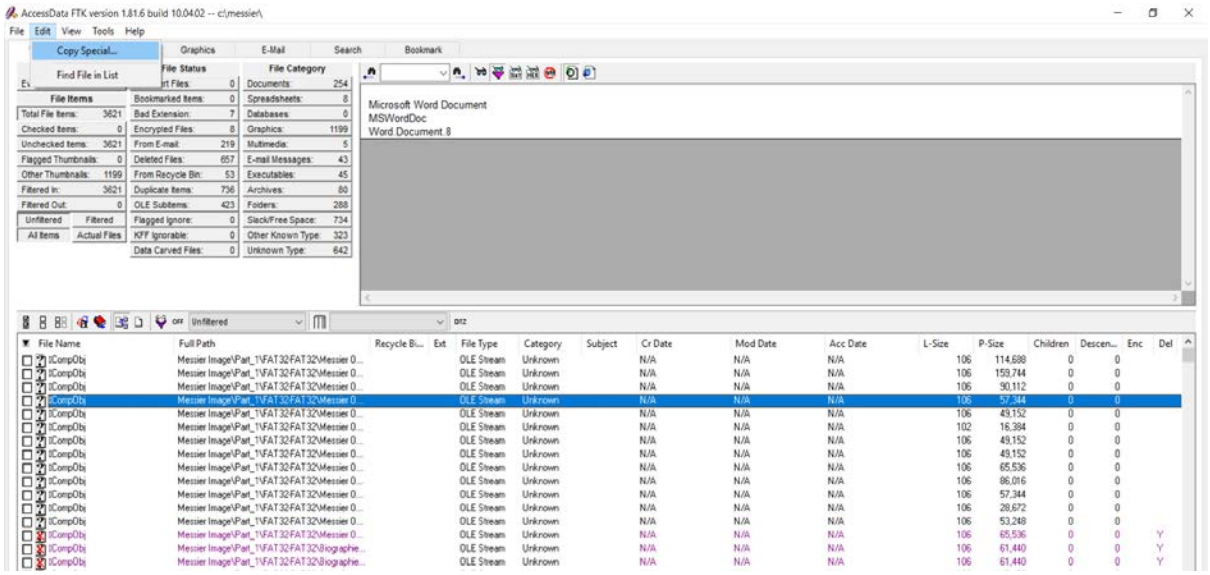
To select a file from the case, select the “Total File Items” and then the actual files for the windows at bottom.



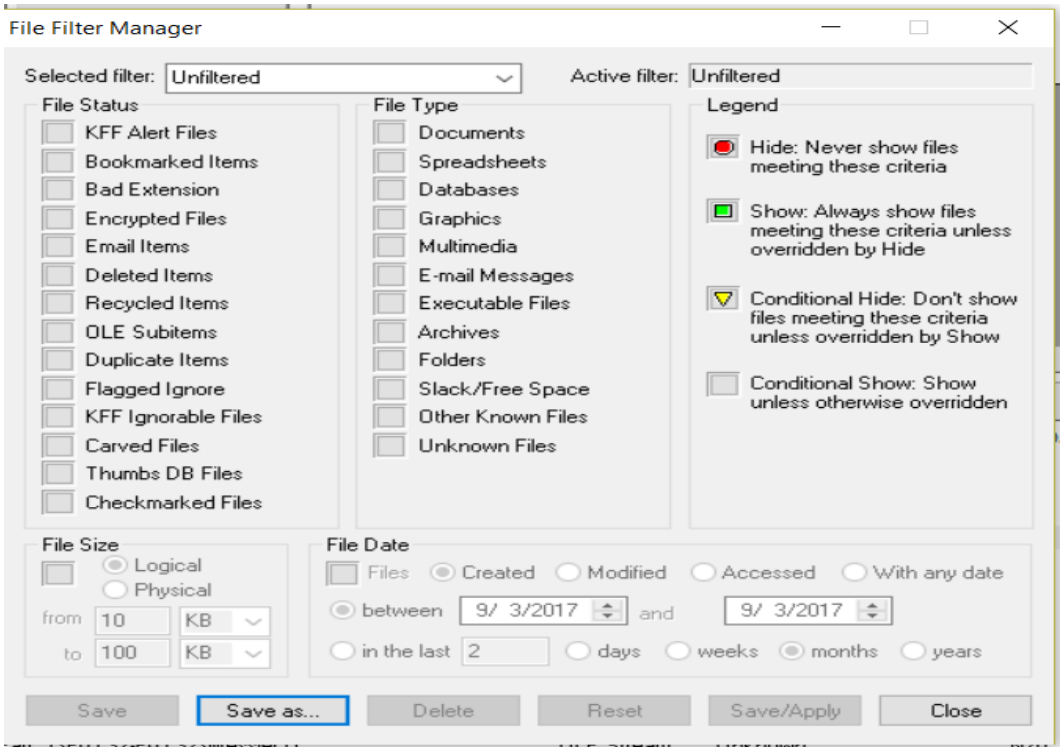
File and Edit Options

Steps:

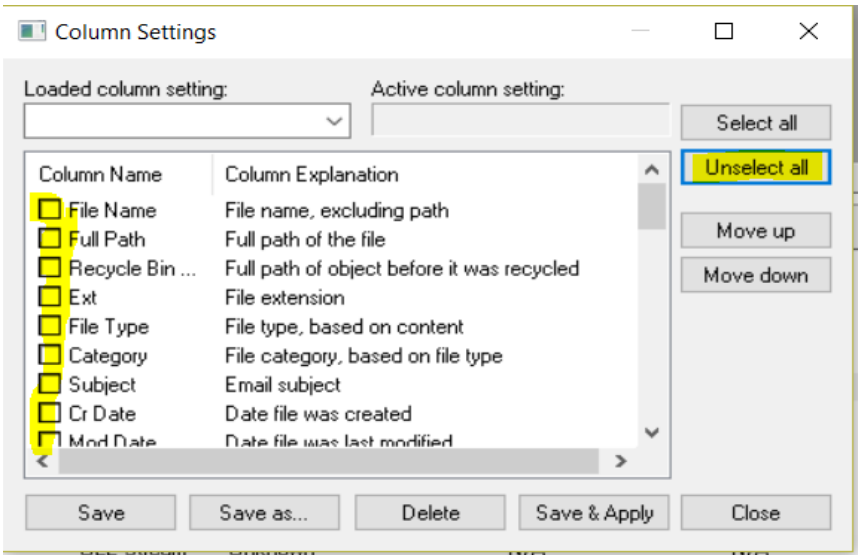
1. In the file list, select a file. On the menu bar, click File and note the options not previously discussed. Click Edit and note Copy Special and Find File in List.



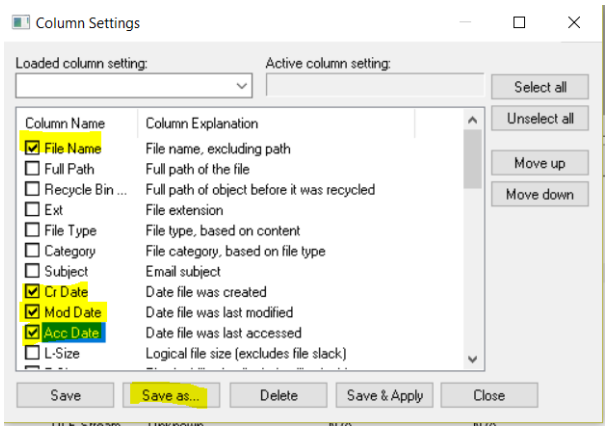
2. View Options > Click View > Click File Filter Manager or click  for different filter options.

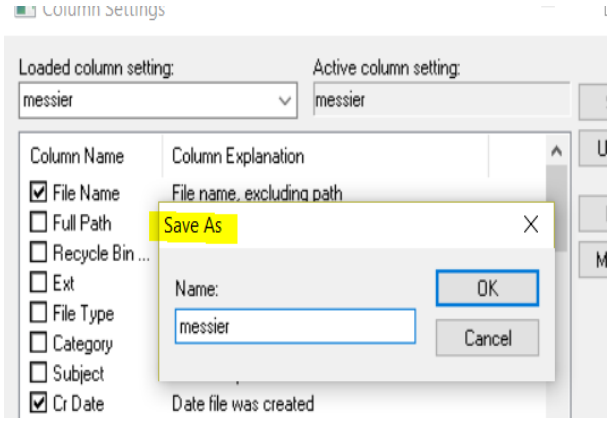


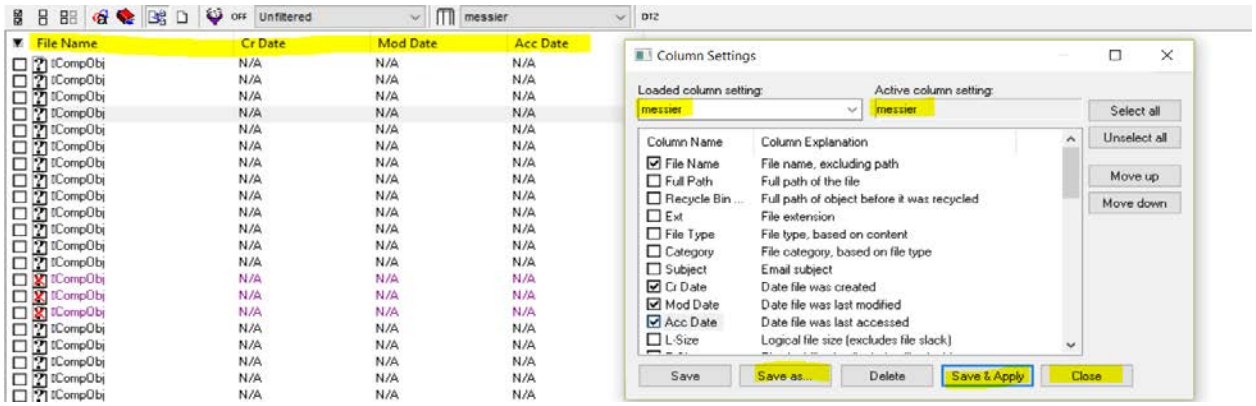
3. How to change file column view windows or customize the column view windows.
   a. Click View> Column Settings or  click > Click Unselect All.



b. In the Column Name list, mark the following: Filename, CrDate, Mod Date and Acc Date and click Save as. Name the column setting Date and Time and then click OK. In the Column Settings dialog, click Save, Apply and close the window.

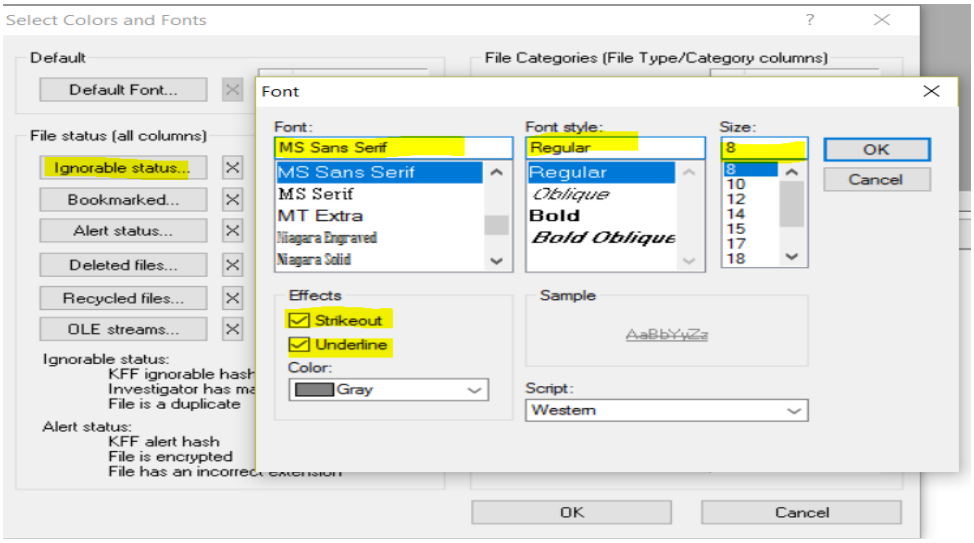




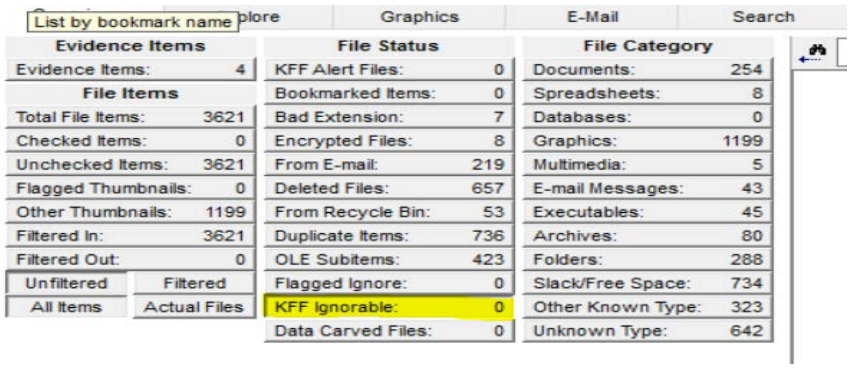


4. Click View> Colors and Fonts.

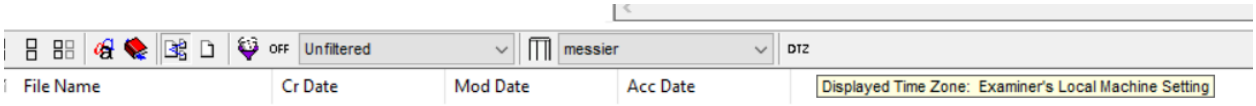
5. Change the display settings for Ignorable Status.
   a. In the File Status box, click Ignorable Status. In the Font menu, select a font, change the color, and mark, Strikeout or Underline. Then click OK.



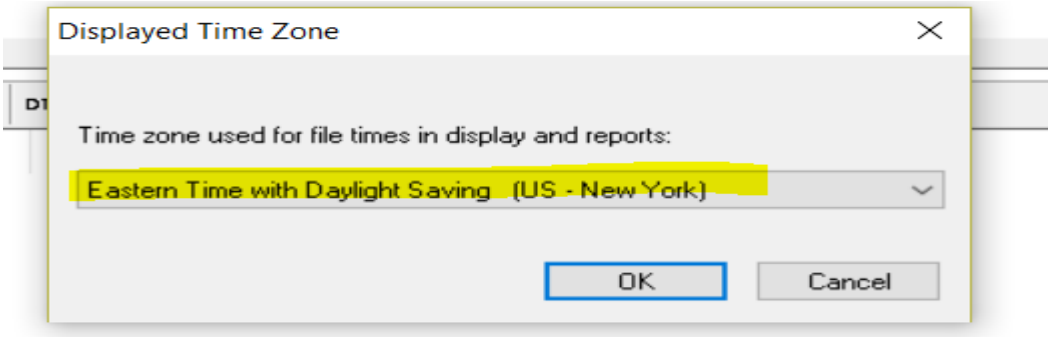
6. In the Overview tab, click the KFF Ignorable container to view the appearance of Ignorable Status.



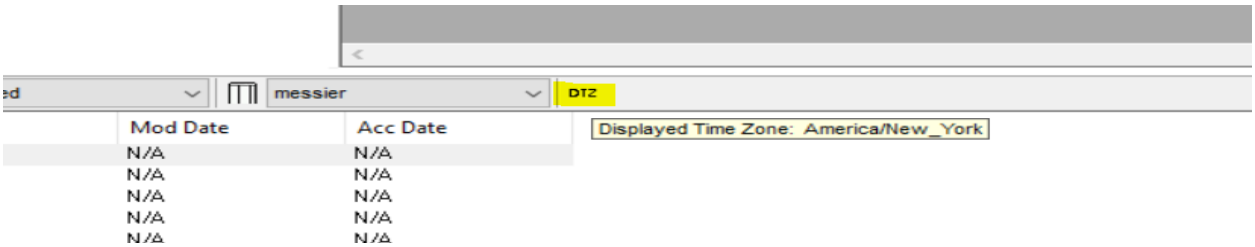
Mouse-over the DTZ symbol next to the Column Settings pull-down menu. Note that FfK is currently set to display times offset from GMT according to the examiner's machine settings.



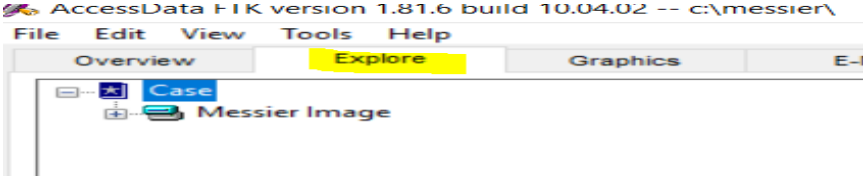
9. How to change the Time zone setting.
   a. Click View> Time Zone Display. Select a time zone different then the current machine settings. Then click OK. Note that the times in the file list dynamically update to the new settings. This ch~s also reflected in the case log.



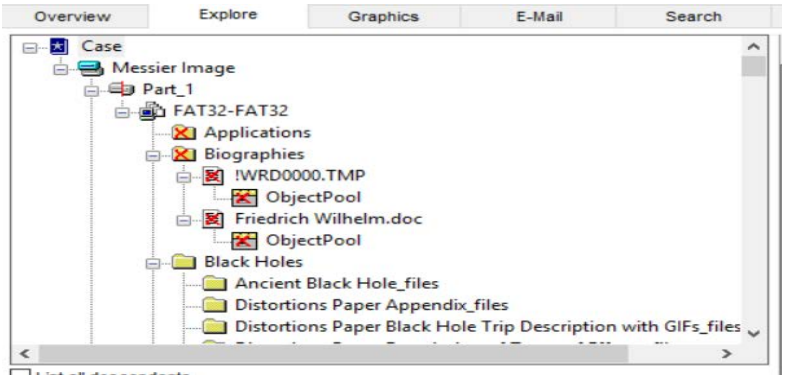
Mouse-over the DTZ symbol again and note the new settings.



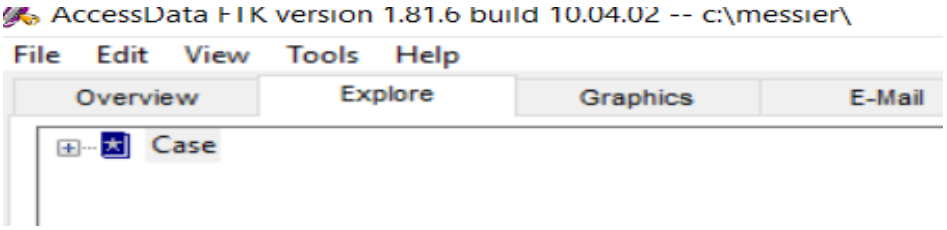
10. View Explore tab.
    a. Click the Explore tab.



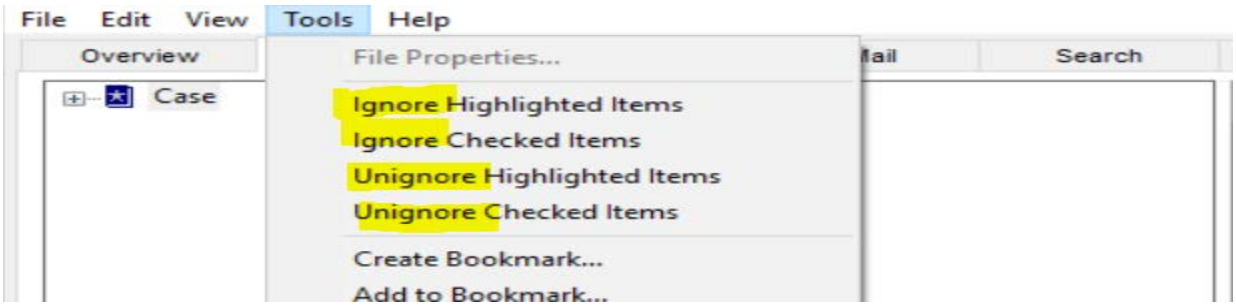
    b. Click View> Expand All. Note that the tree expands to show all items.



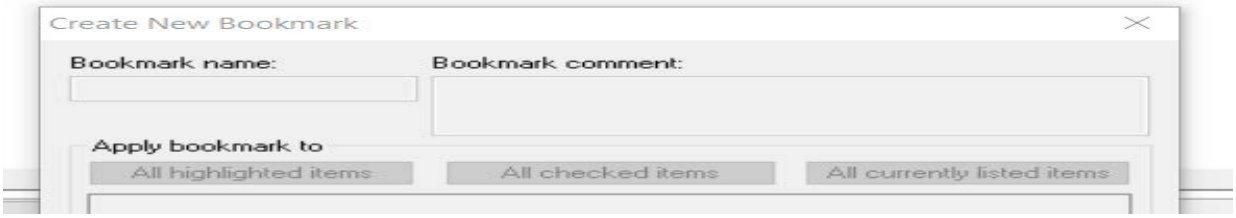
c. Click View> Contract All. Note that the tree hides all sub-items.



11. Exploring Tools Options
    a. On the menu bar, click Tools. Note the Ignore and Unignore options.

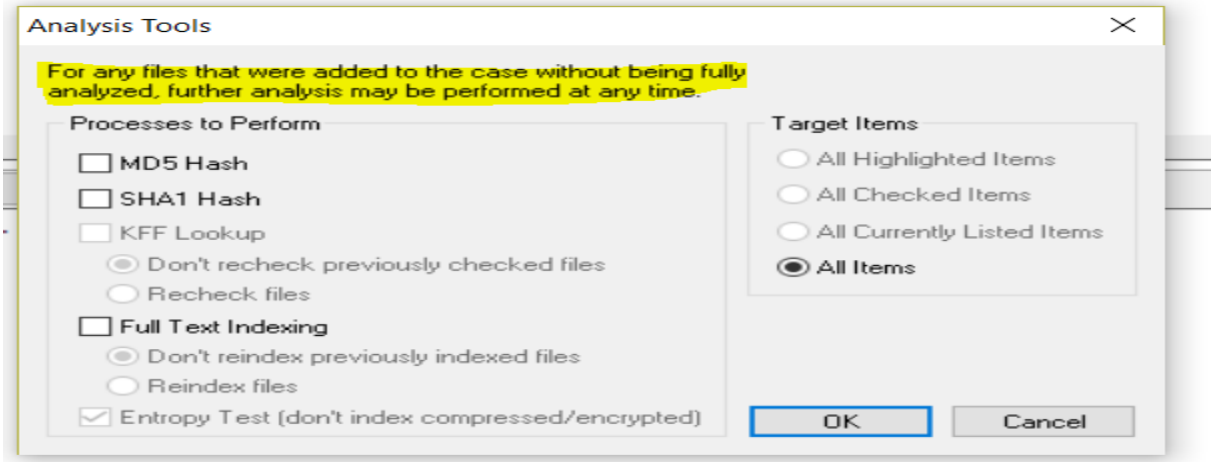


    b. Click Create Bookmark. Note the options in the Apply bookmark to box. Click Cancel to close the Create New Bookmark menu

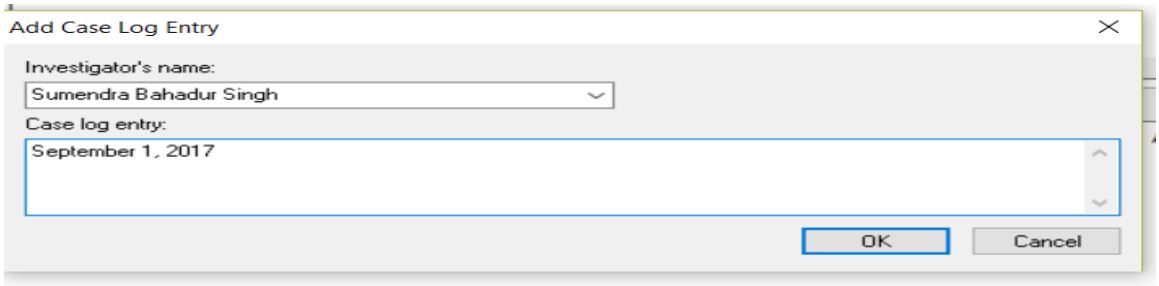


    c. Click Tools> Analysis Tools.

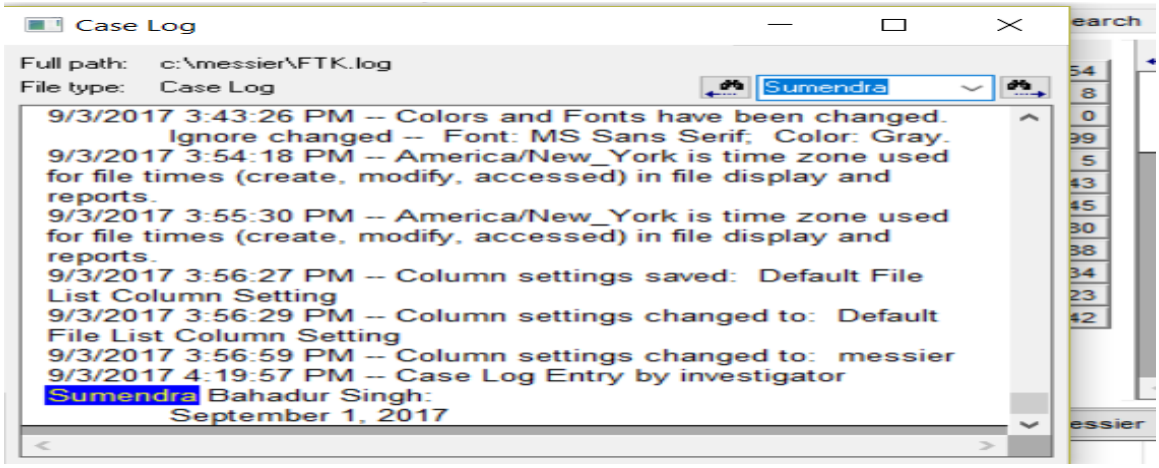
Note: The Analysis Tools menu allows you to process files that were added to the case without being fully analyzed. You can also reprocess files at any time. Click Cancel to close the Analysis Tools menu.



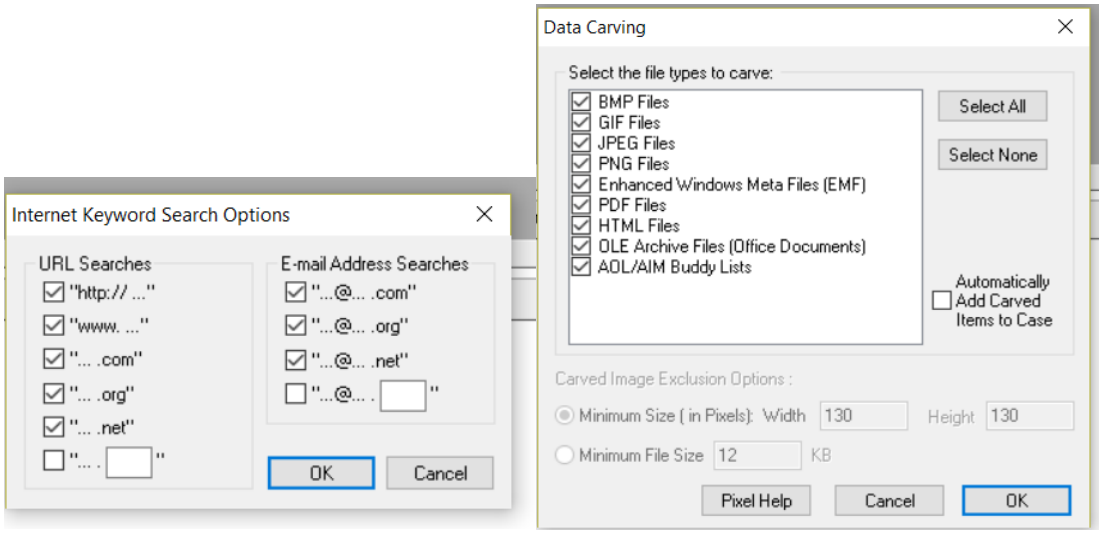
d. Click Tools> Add Case Log Entry. Type an investigator's name and case log entry and then click OK



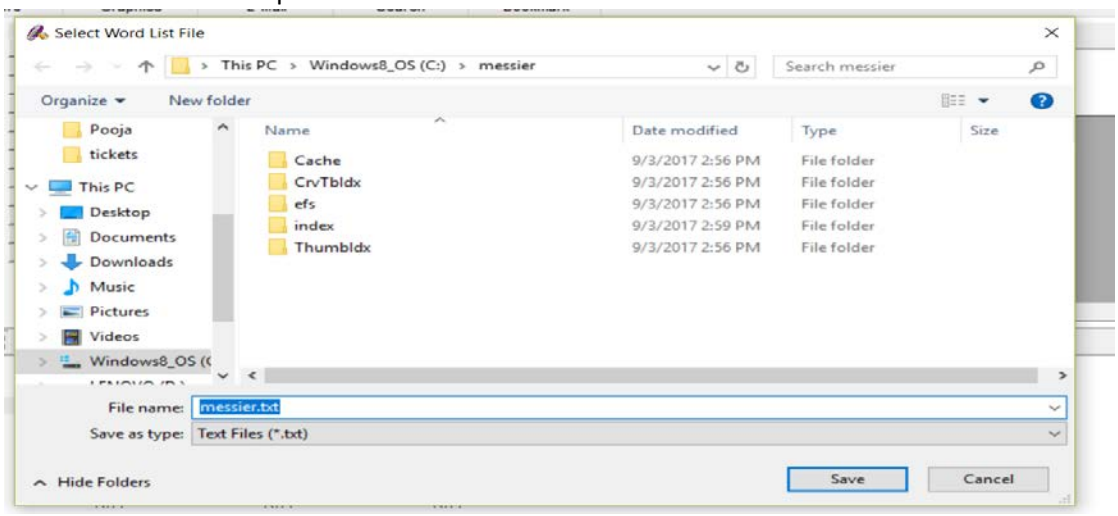
e. To view your entry, click Tools> View Case Log. Use the Search box to find your case log entry.



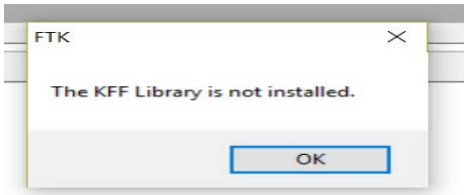
f. Click Tools and note Internet Keyword Search and Data Carving.



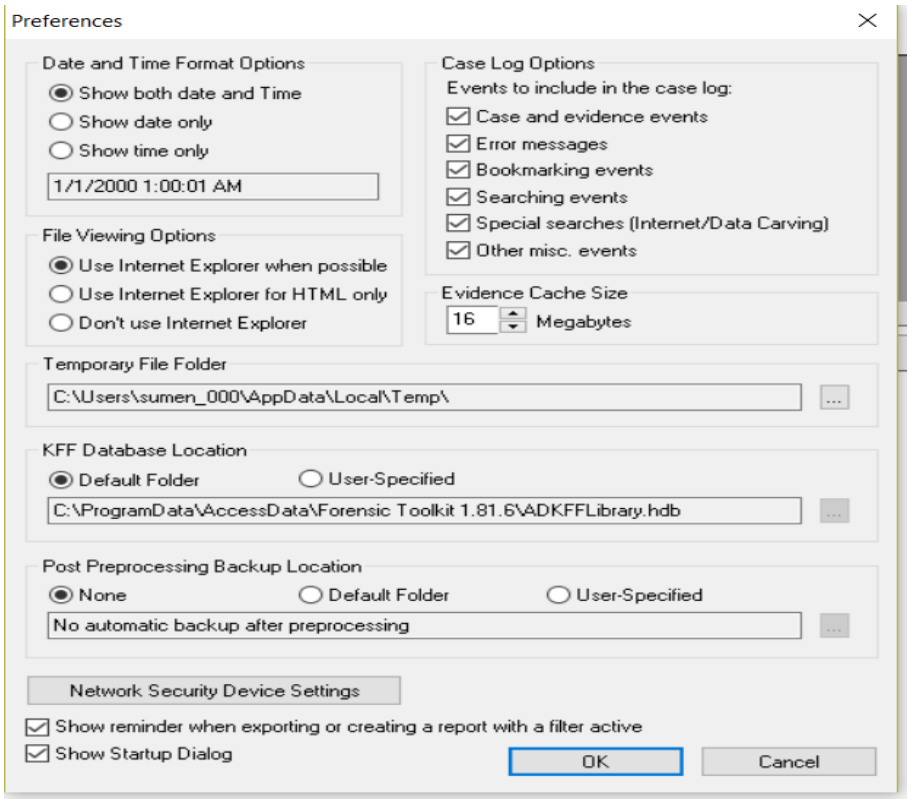
g. Click Tools and note Export Word List.



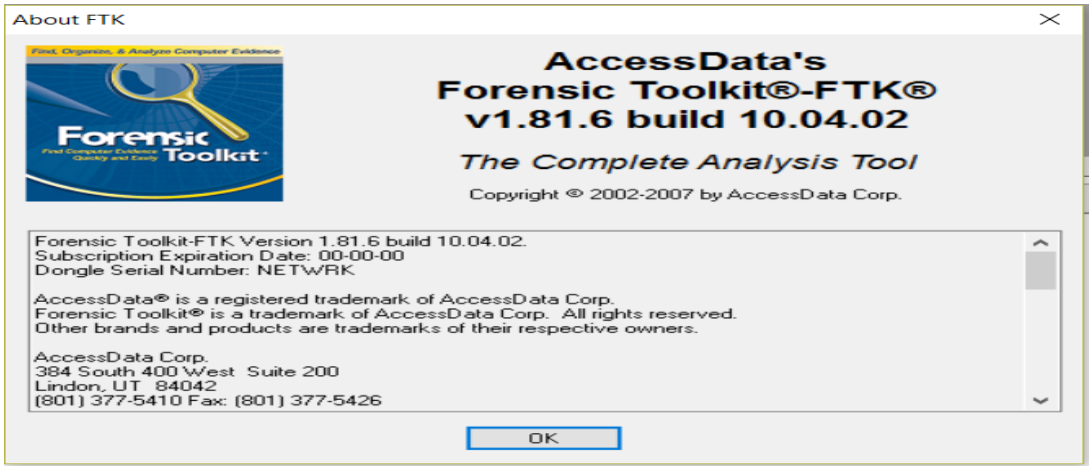
h. Click Tools> Import KFF Hashes. Note the types of hash sets you can import and click cancel if you don't want to make change.



i. Click Tools> Preferences and note the options.

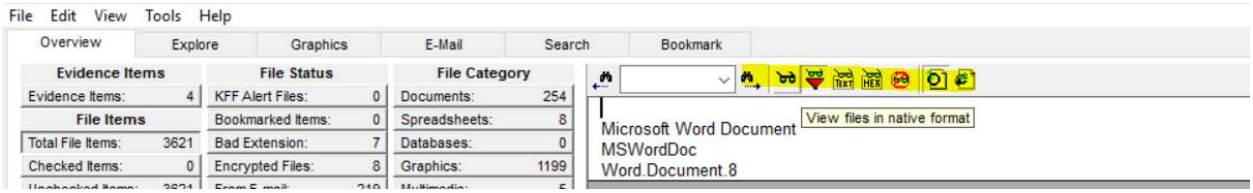


12. Exploring Help menu.
    a. On the menu bar, click Help. Click Help >AccessData LicenseManager. Note the dongle information. We don't have the license installed currently. We can note the software information from Help> About.



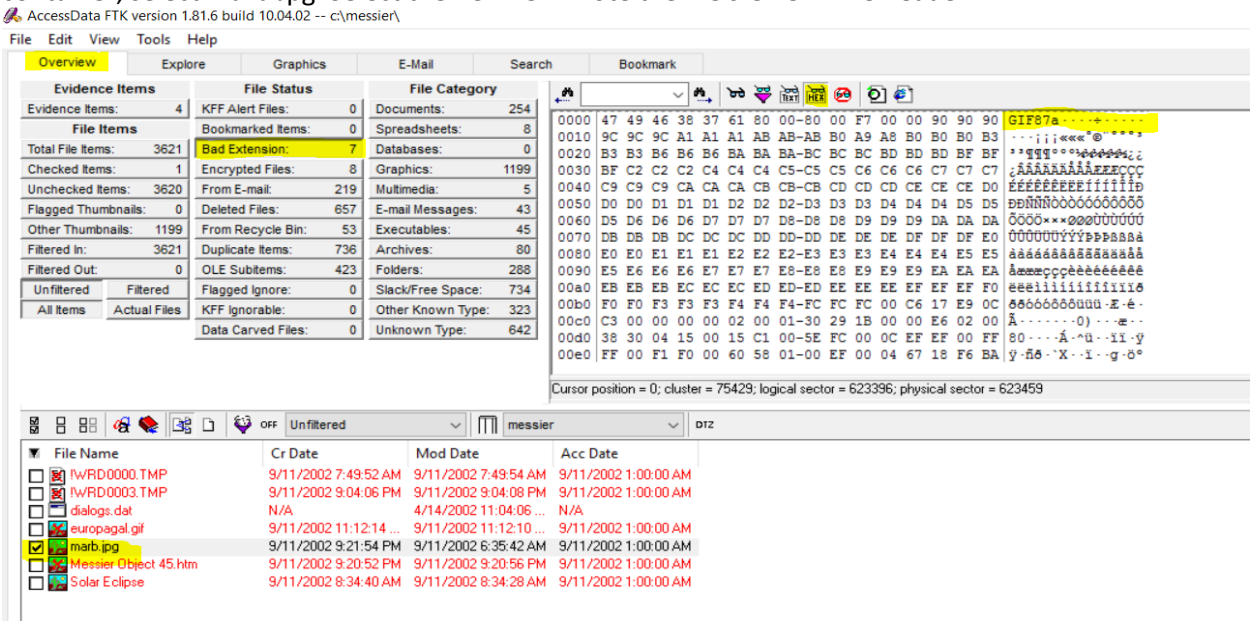
13. Reviewing Toolbar Buttons

We can review the toolbar shortcut, place your pointer over each toolbar button and view the tool tip that appears. Note the relationship of buttons to menu options.

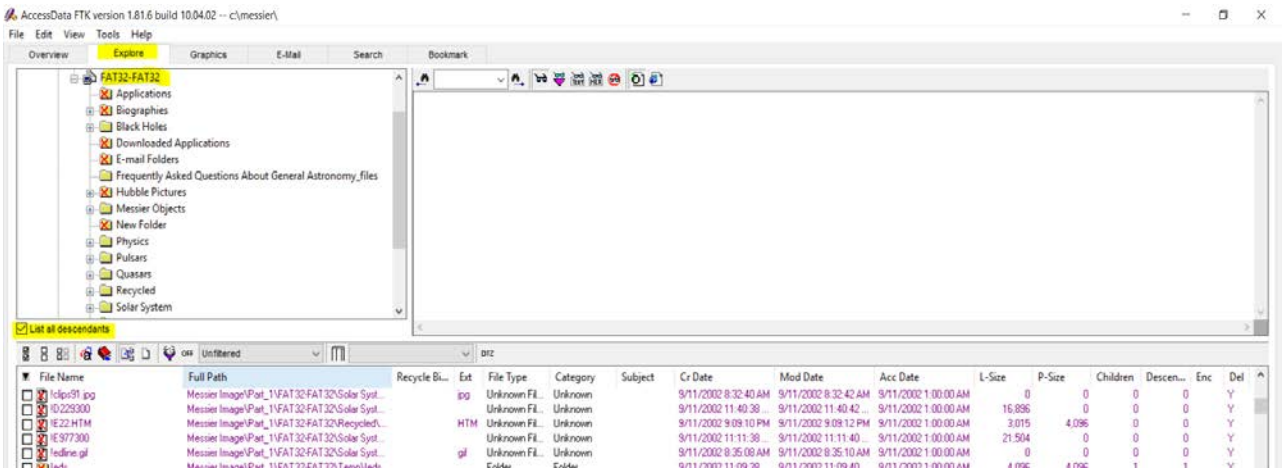


14. Reviewing FTK Tabs.

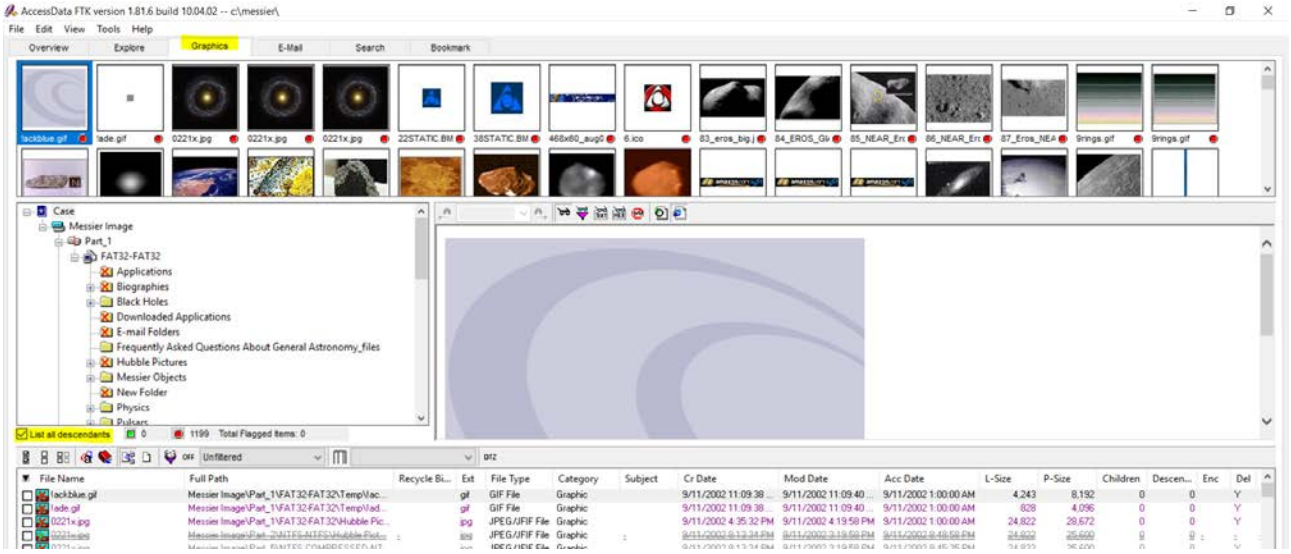
WithMessierImage.EO1 selected, click the Overview Tab. Note the Encrypted Files, Documents, and Bad Extension containers. Note the difference between All Items and Actual Files. In the Bad Extension container, select marb.Jpg. Select the hex view. Note the file's GIF87A file header.



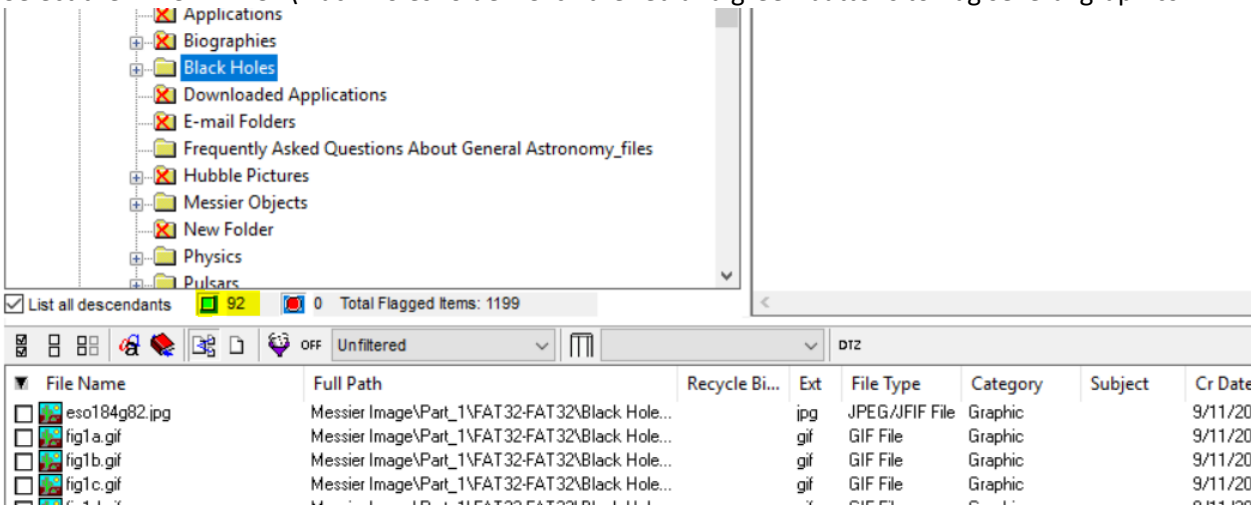
Click the Explore Tab. Select the FAT32-FAT32\Physics folder. Check List all descendants.



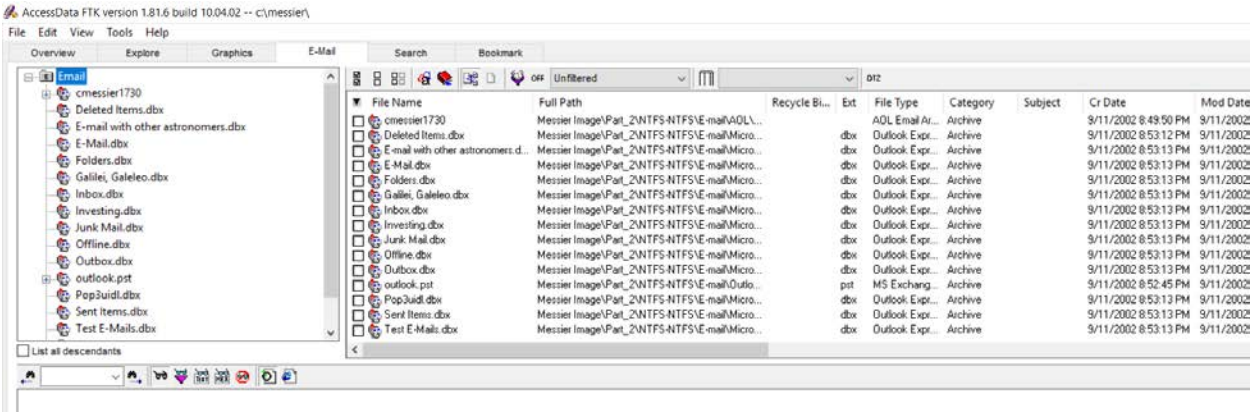
Click the Graphics Tab. Check List all descendants. Note that the List all Descendants feature is tab-independent.



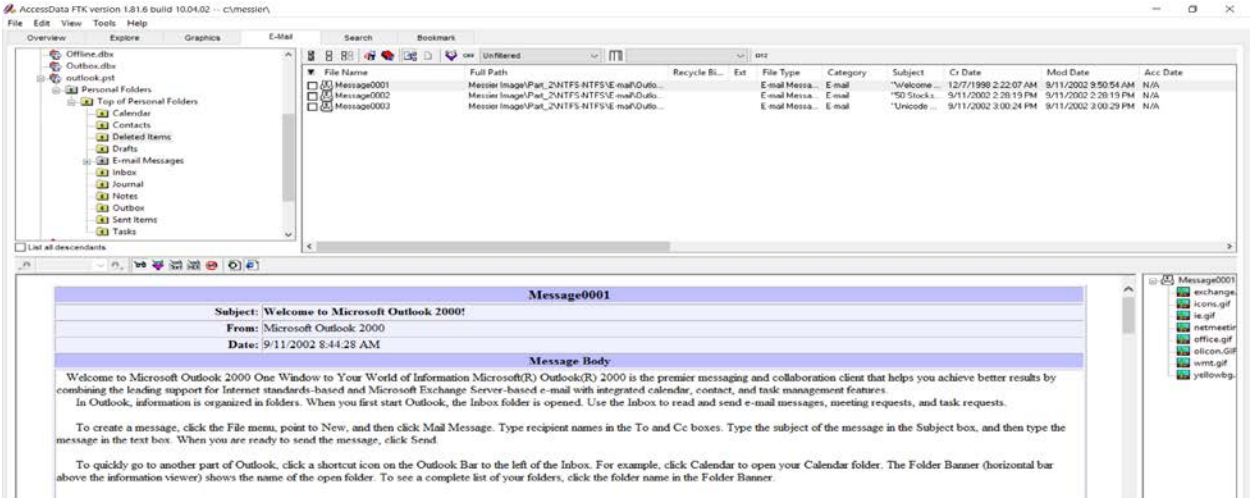
Select the FAT32-FAT32\Black Holes folder. Click the red and green buttons to flag several graphics.



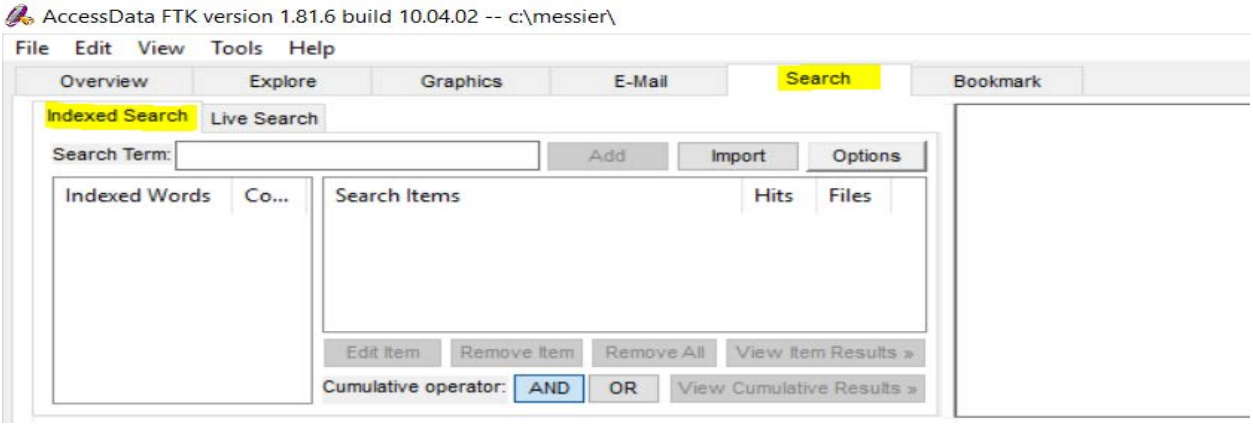
Click the E-Mail Tab. Note the different viewing panes. Several email file types are supported.



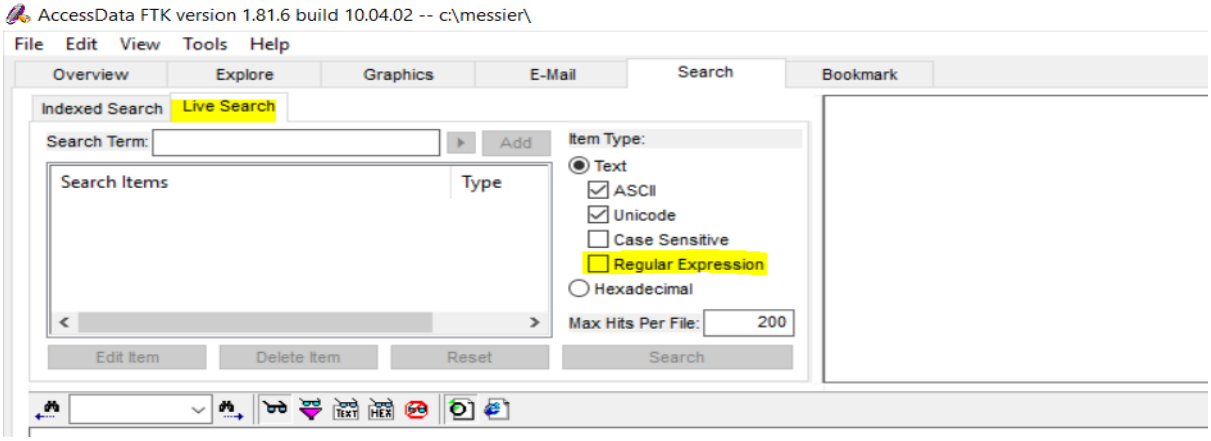
Navigate to the outlook.pst folder. View deleted message 001 in the Deleted Items folder.



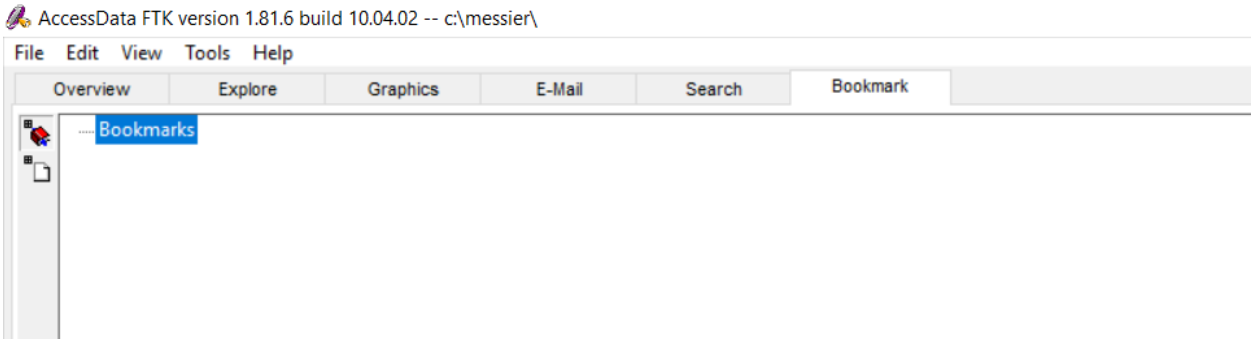
Click the Search Tab. Note the Indexed Search options. An indexed search uses the index file to find search terms. FTK uses the search engine, dtSearch, to perform indexed searches.



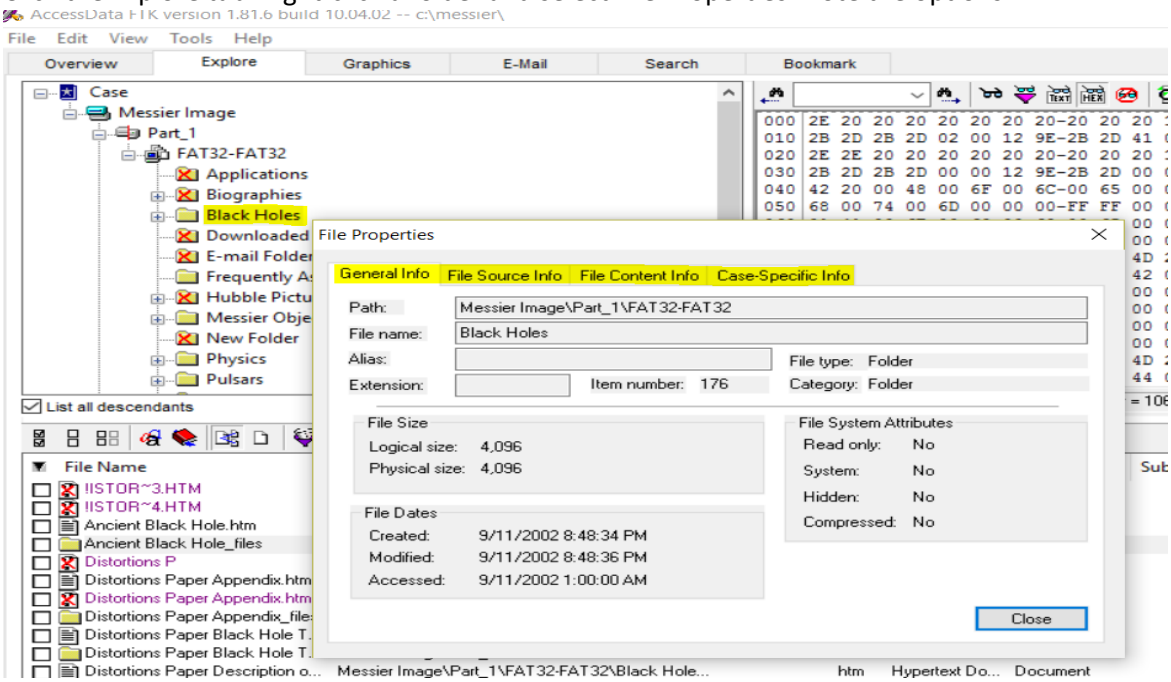
Click the Live Search Tab. Note the options. Live searches support regular expressions.



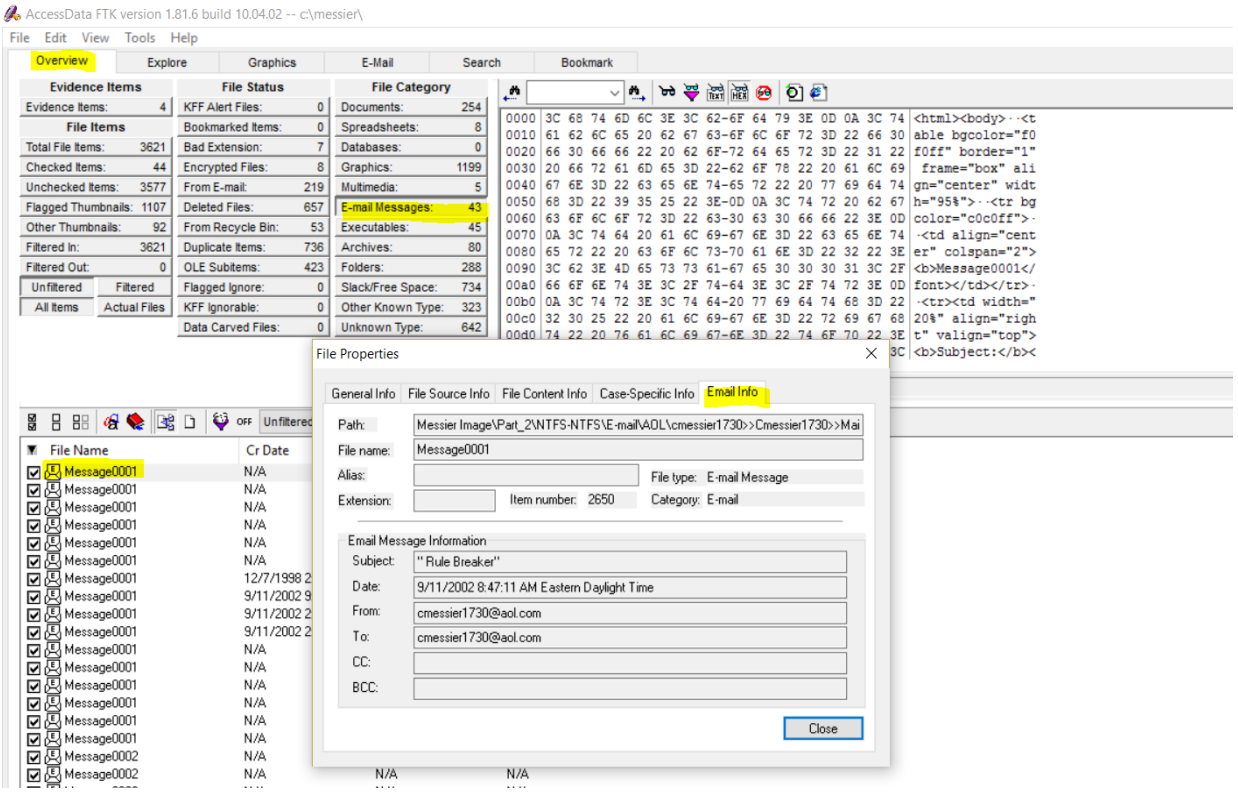
Click the Bookmark Tab. Note the Include in Report and Export file options.



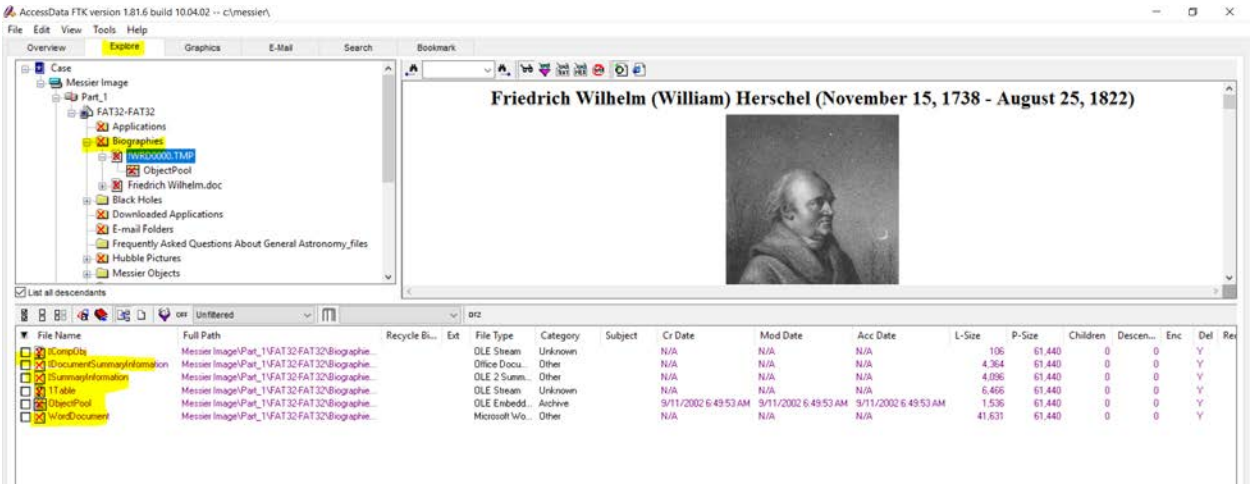
15. Viewing File and Folder Properties
    a. Click the Explore tab. Right-click a folder and select File Properties. Note the options.



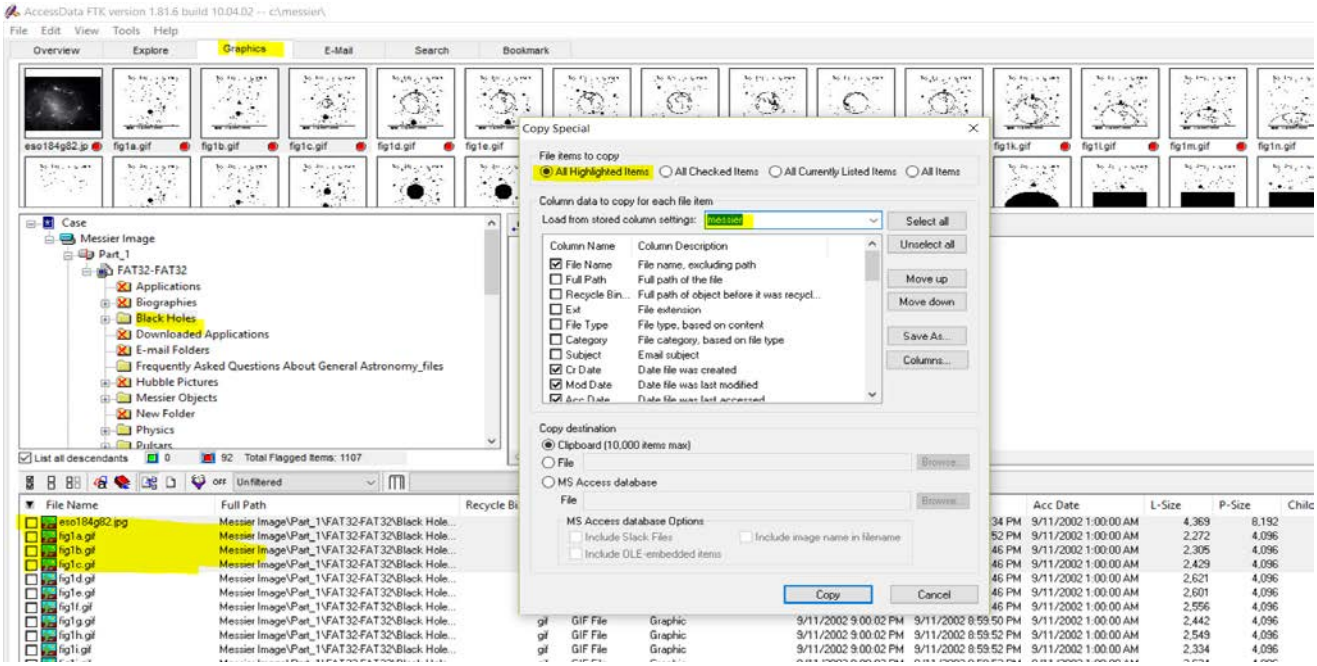
b. Go to the E-Mail Messages container in the Overview Tab. Select All Items so you can view the items within the PST container. Right-click an email file and select File Properties. Note the options, particularly, the E-Mail Info tab.



16. Viewing Metadata
    a. Click the Explore tab. In the FAT32-FAT32\Biographies folder, select the !WRDOOOO.tmp file from the Directory Tree. View the supported metadata in the file list pane by clicking on each item.

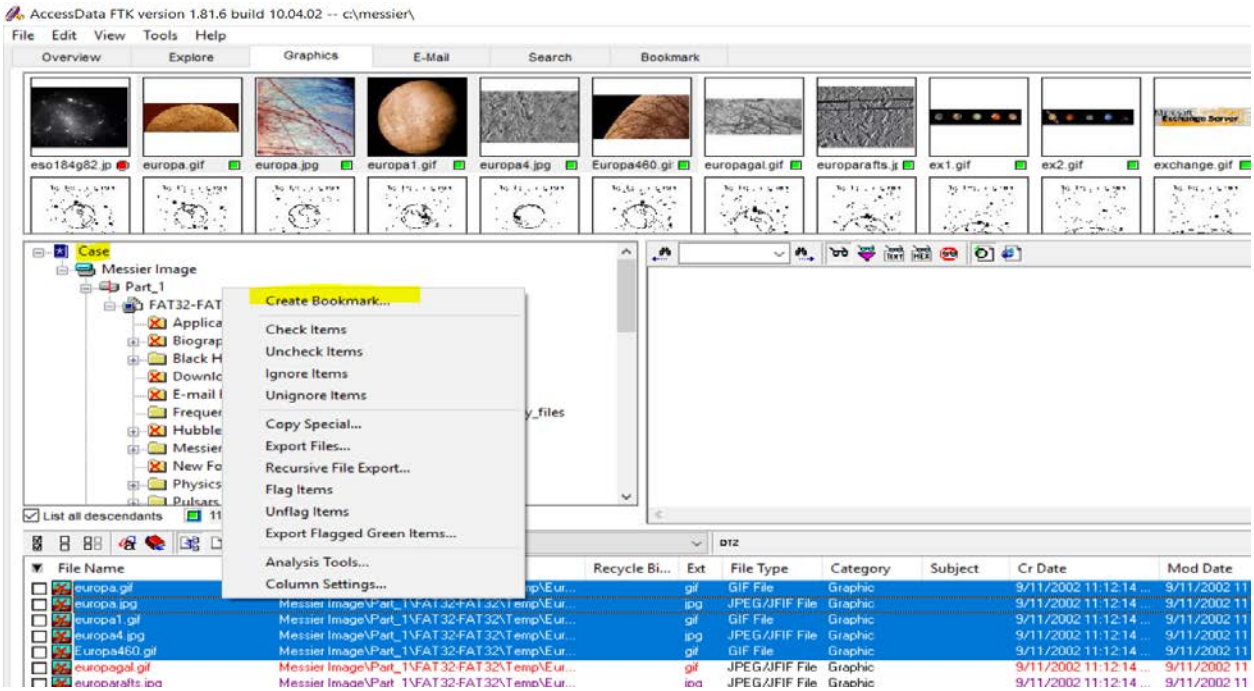


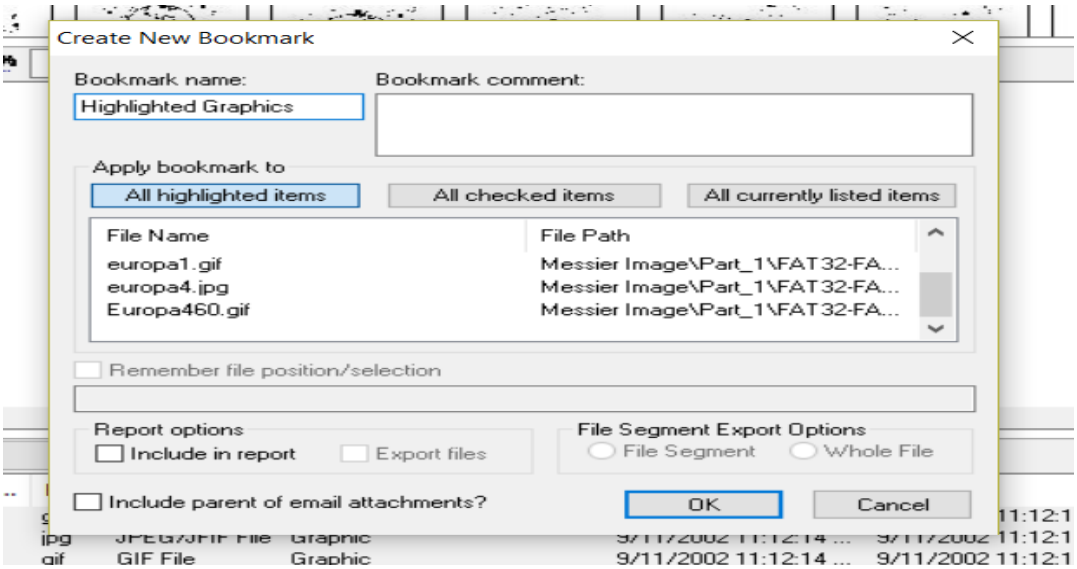
17. Creating a Date and Time Export List
    a. Click the Graphics Tab. Select a folder, Highlight several files. Right-click the files and select Copy Special. Under File Items to Copy, select All Highlighted Items. Select the Date and Time column setting you created earlier.



18. Working with Graphics.
    a. Bookmark the highlighted files.

       Click the Graphics tab. In the tree view, click Case. Make sure no filters are applied. Make sure List all descendants are marked and highlight few graphics files. Right click the graphics and create Bookmarks. In the Create New Bookmark menu, name the bookmark Highlighted Graphics. Then select All highlighted items and click okay.



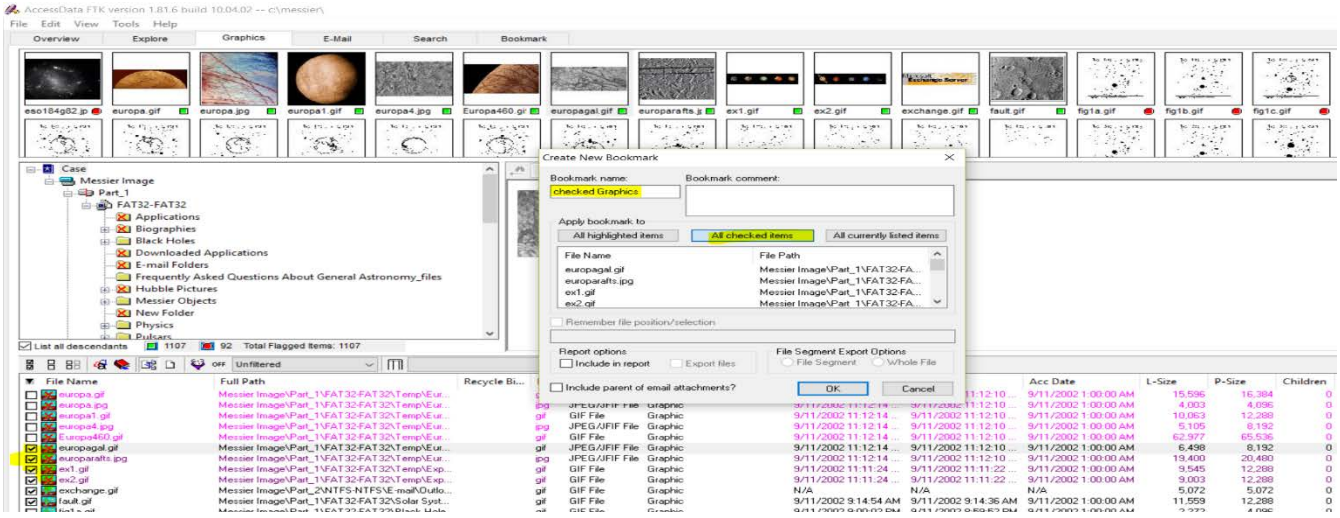


b. Adding comment on Bookmark.

Go to the Bookmark Tab. Select the Highlighted Graphics bookmark. Add a comment in the Bookmark Comment field. Then click Save Changes.

c. Bookmark the checked files.

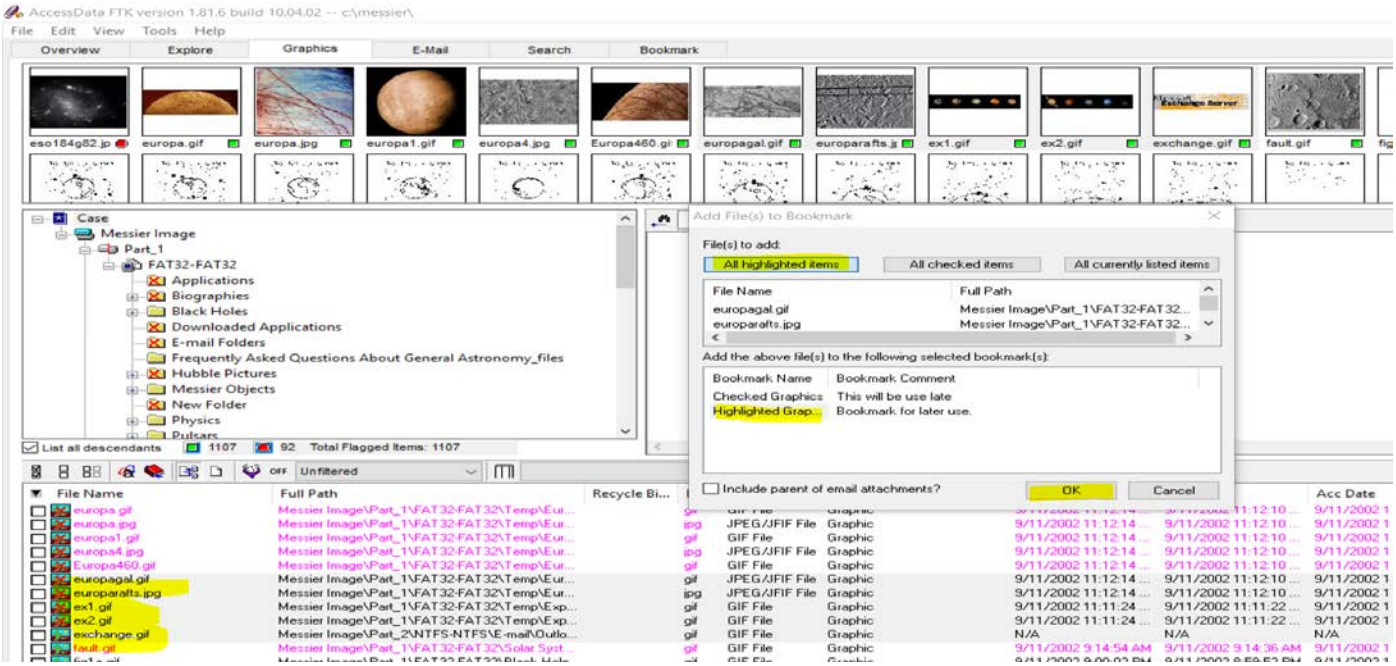
Click the Graphics tab. In the tree view, click Case. Make sure no filters are applied. Make sure List all descendants are marked and checked mark few graphics files. Right click the



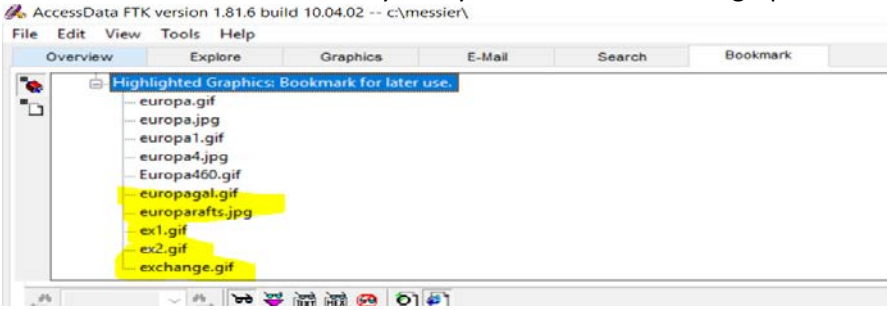
graphics and create Bookmarks. In the Create New Bookmark menu, name the bookmark Checked Graphics. Then select All highlighted items and click okay. Add the comment on the bookmarked file from Bookmark tab, add comment and save.

d. Adding file to existing bookmark.

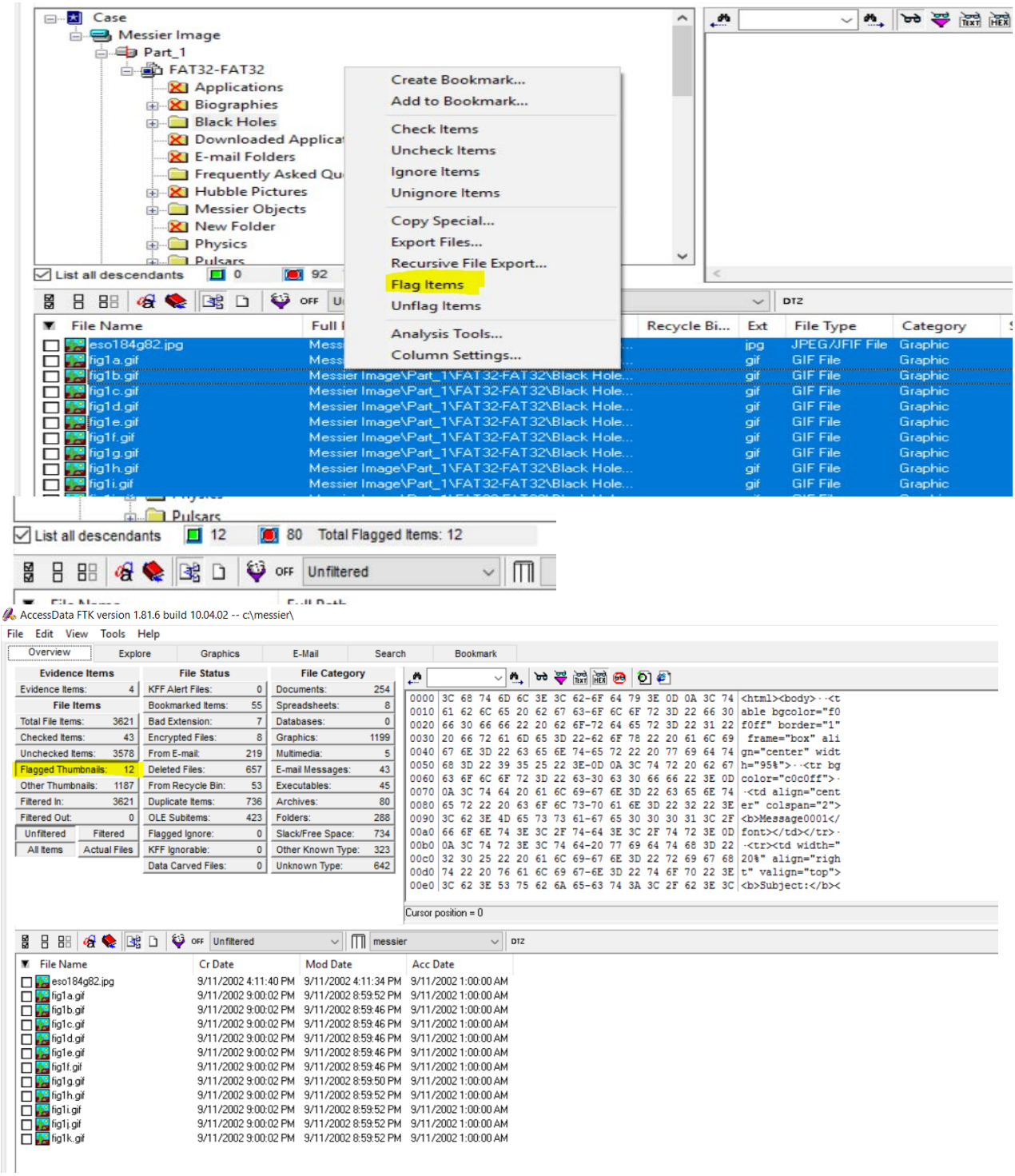
Click the Graphics Tab. Highlight five more graphics. Right-click the graphics and select Add to Bookmark. In the Add Files to Bookmark menu, select Highlighted Graphics. Then click OK.



Go to the Bookmark tab to verify that you have a total of ten graphics in the bookmark.

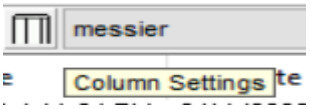


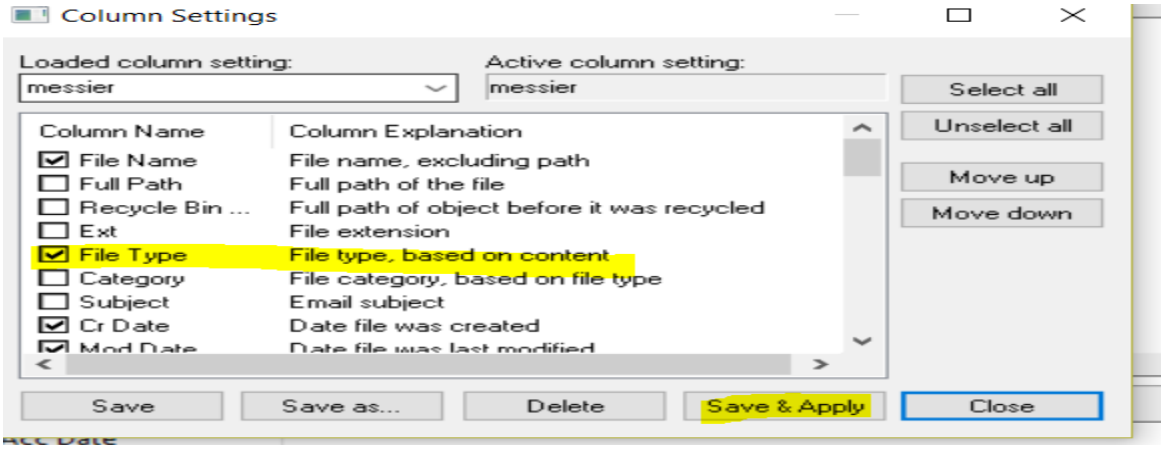
e. Flag the files on graphics. Click the Graphics Tab. Flag twelve graphics green (click the red circles), these will be used later. Go to the Overview tab and select the Flagged Thumbnails container to verify that the graphics you just flagged are included.



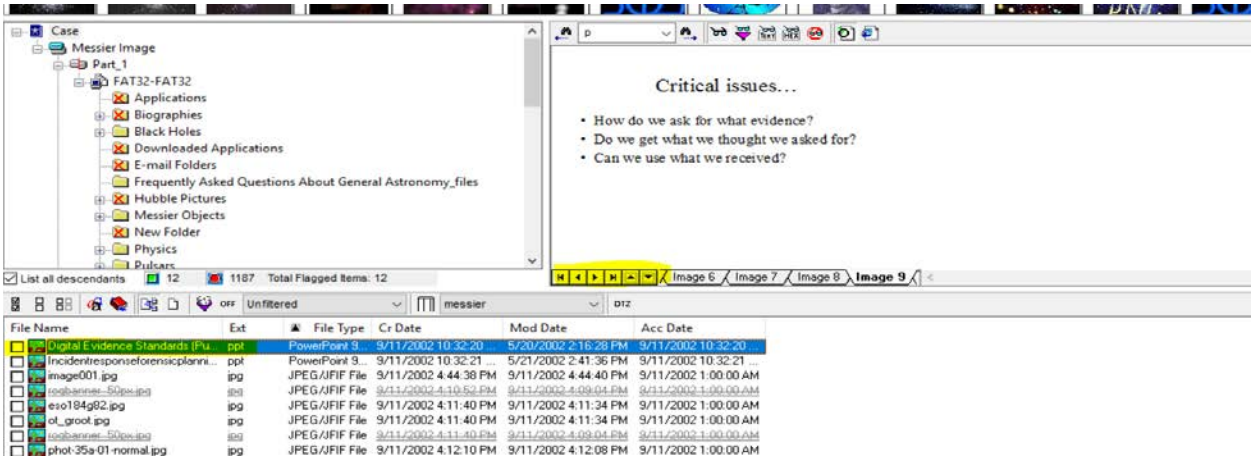
19. Add File Type to the Date and Time column settings.

Note:The column settings are tab-independent.
Click the Column Settings button on the toolbar Mark File Type. Click Save and Apply.

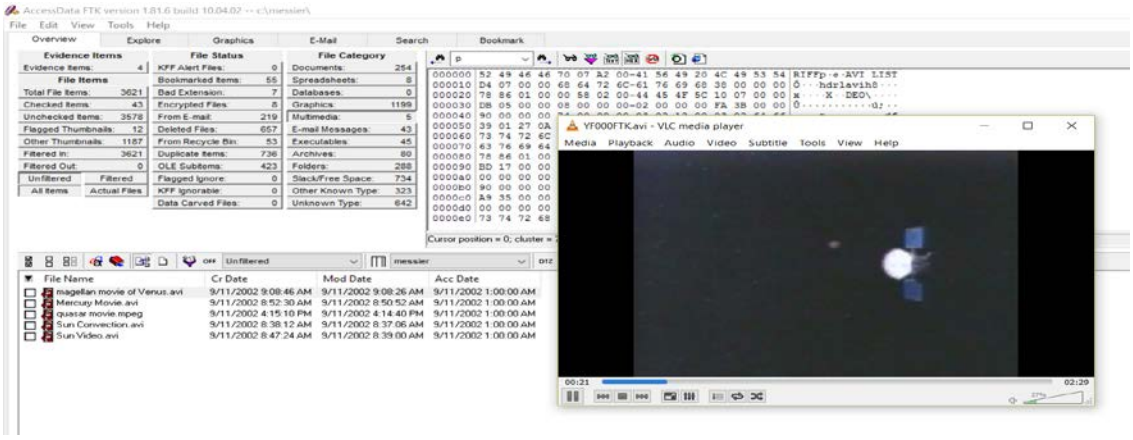




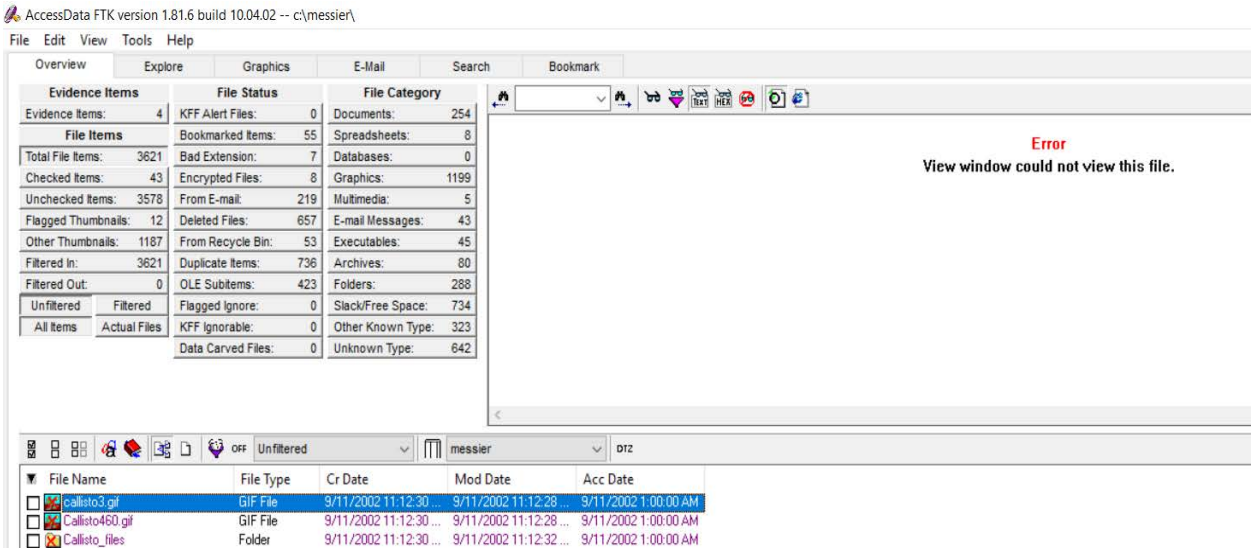
Click the File Type column heading to sort the files by file type. Type "p" on the keyboard to go to that selection alphabetically. Select the Digital Evidence Standards (Public).ppt file. Use the navigation buttons to view the slide show in the viewer.



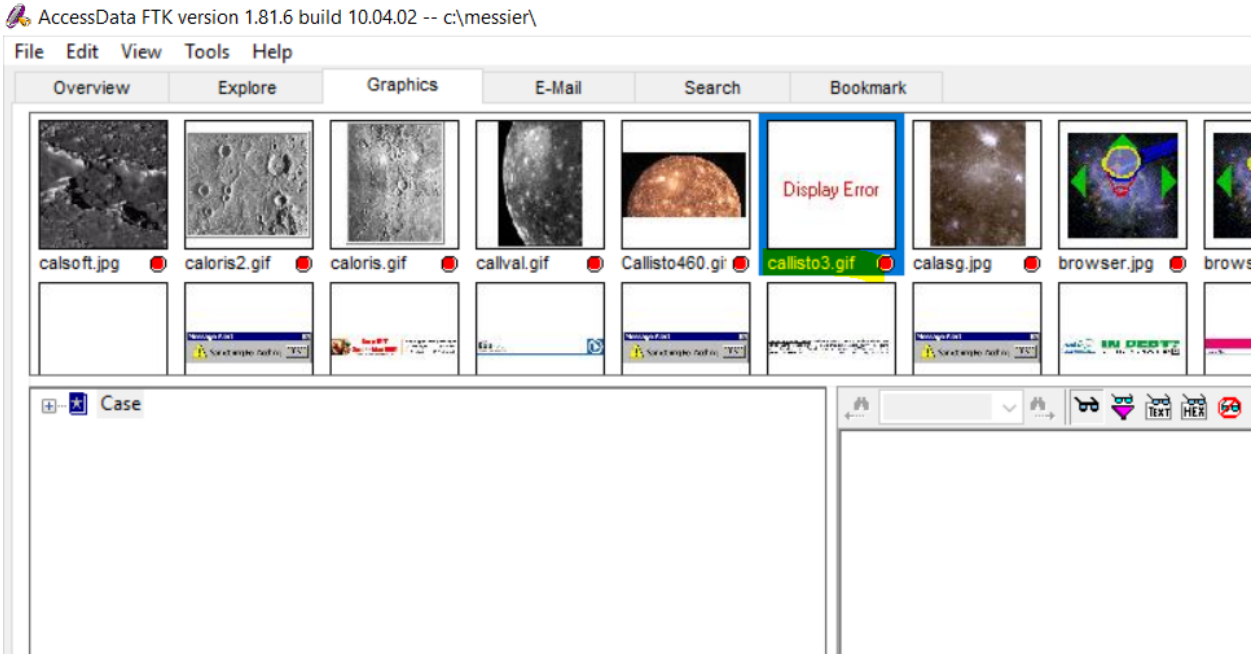
Select the Magellan movie of Venus.avi. Right-click and select Launch Associated Program.



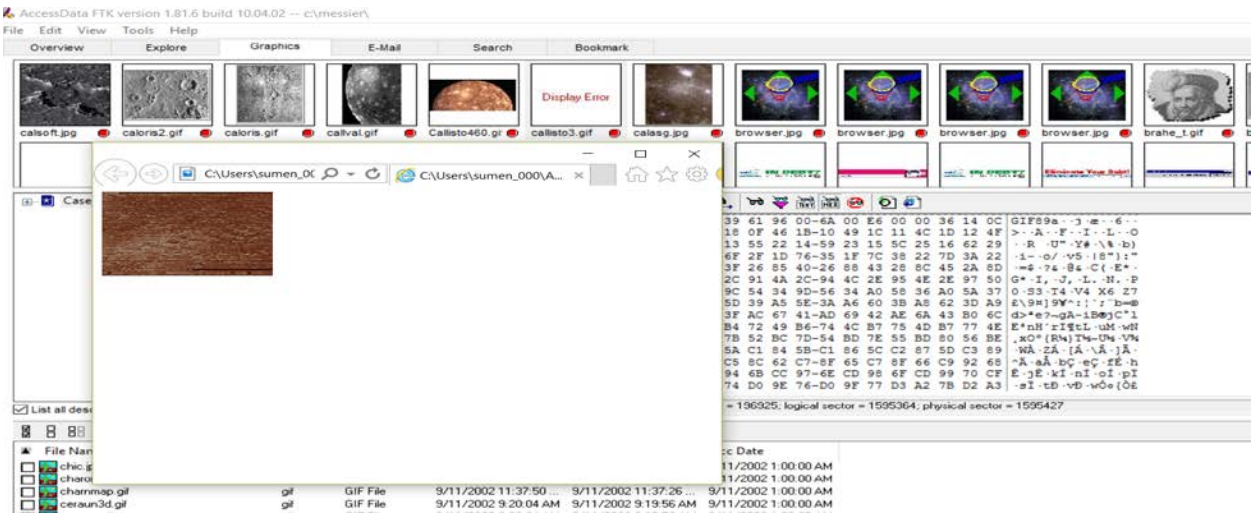
View CALLIST03.GIF, In the thumbnail view, note the me shows as "display error."



Select the graphic. Notice it can still be viewed in the viewer.

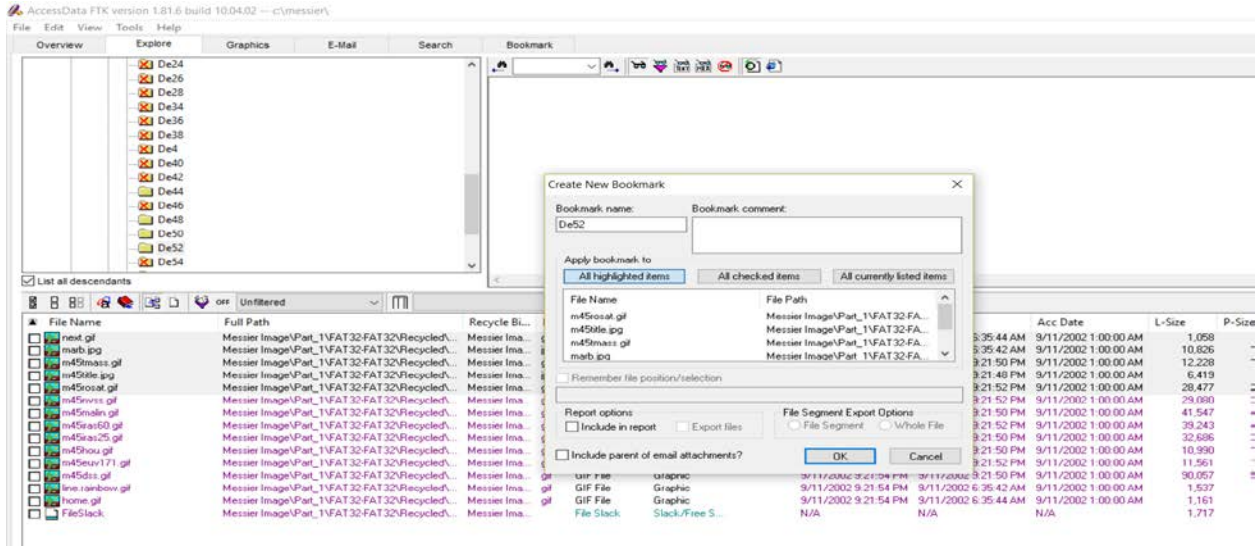


Right-click the thumbnail and view with your browser.

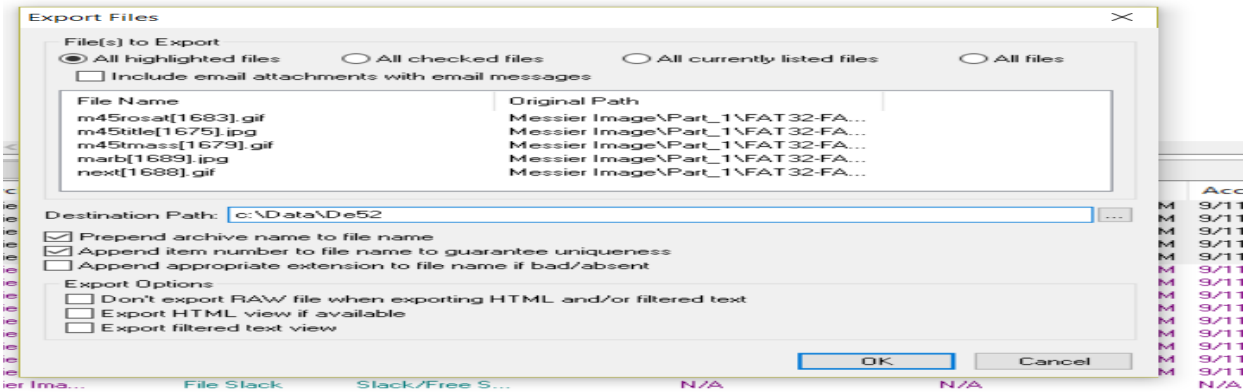


PRACTICAL: IDENTIFYING, BOOKMARKING, AND EXPORTING GRAPHICS FILES

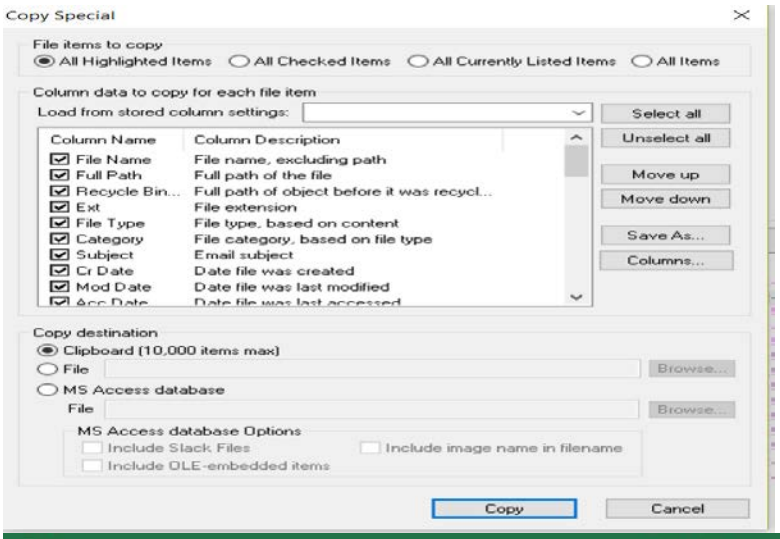
1. Navigate to \Recyclecf\J)e52 on FAT32-FAT32. Select at least five graphics. Create a bookmark name De52 add those graphics to the bookmark.

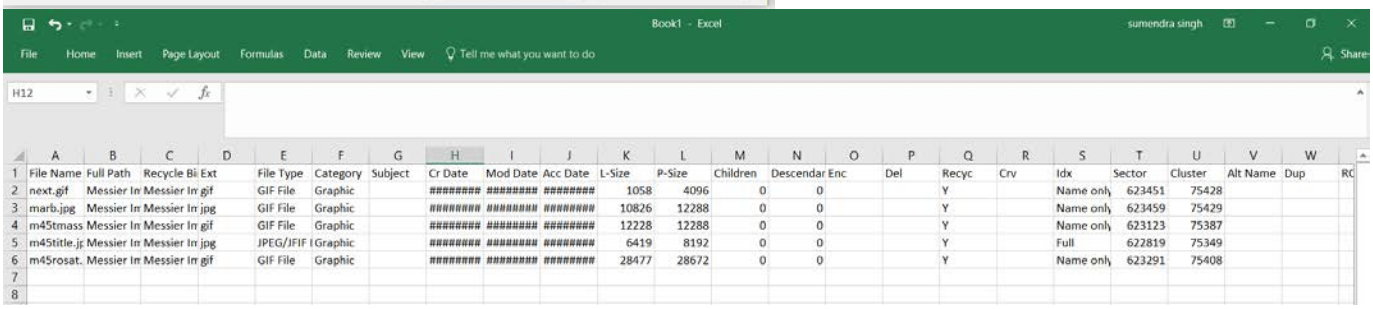


Export the files to drive:\Data\De52.

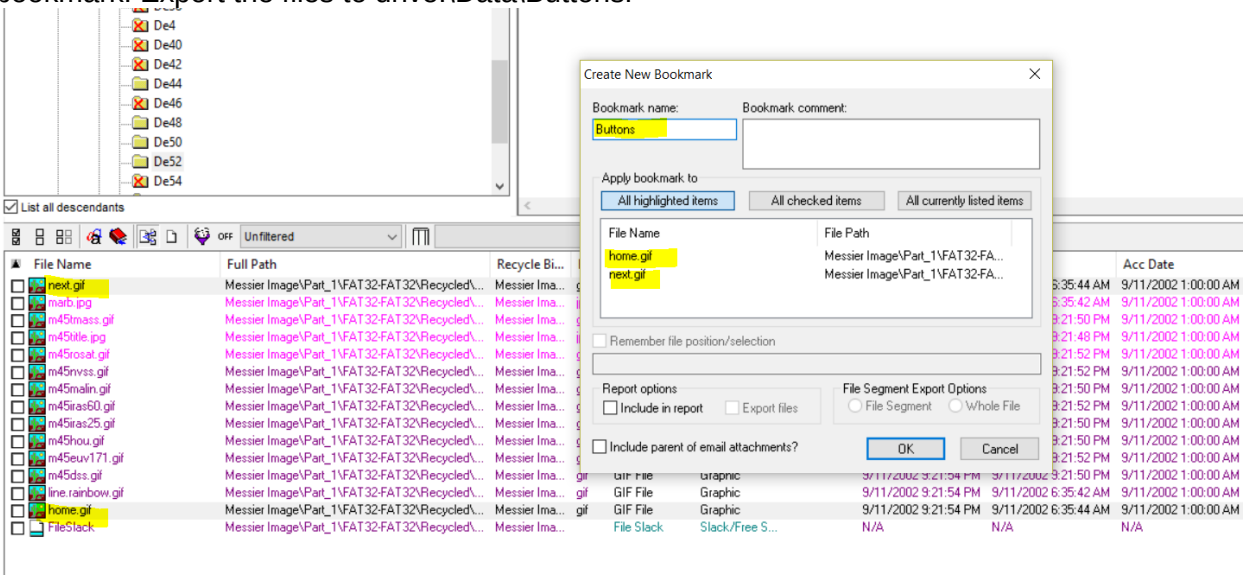


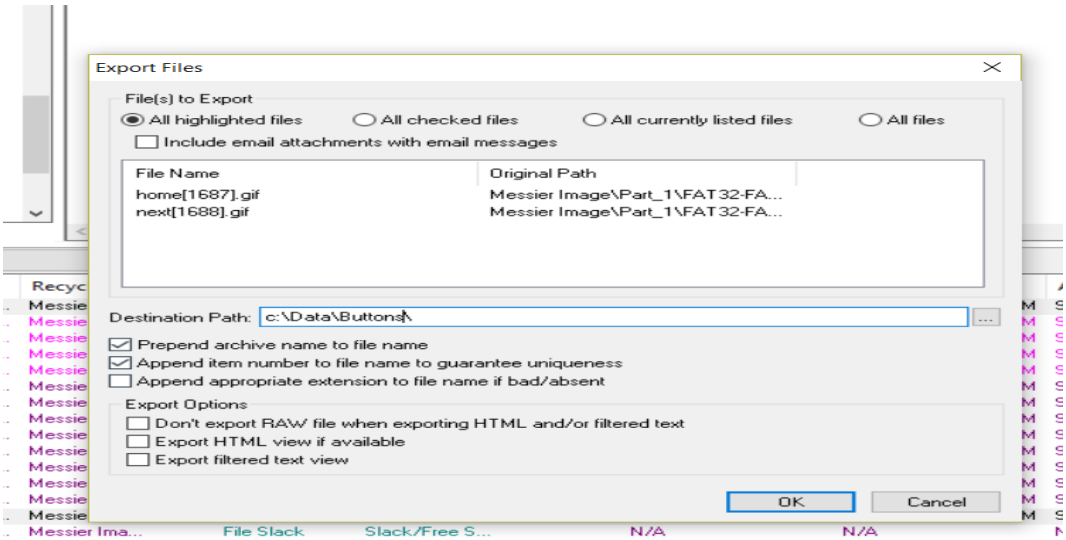
Use Copy Special to copy a list of the dates and times associated with the exported files to the clipboard. Then paste this data into Microsoft Excel.



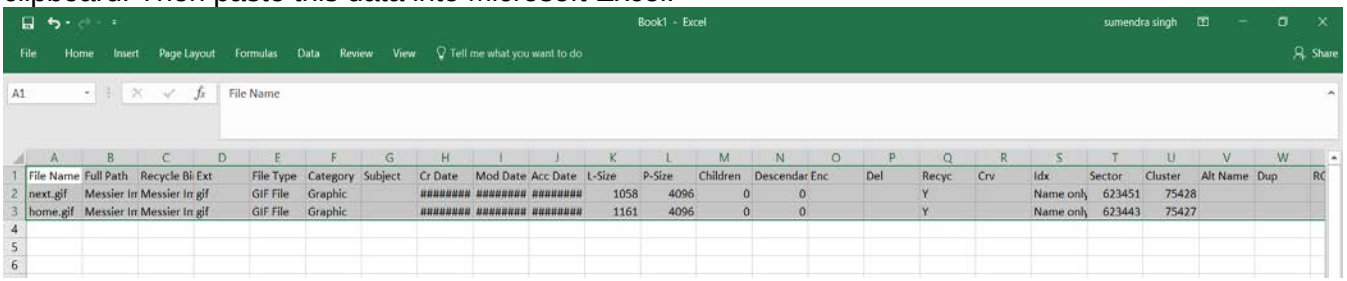


Select next.gif and home.gif. Create a bookmark named Buttons and add those graphics to the bookmark. Export the files to drive:\Data\Buttons.

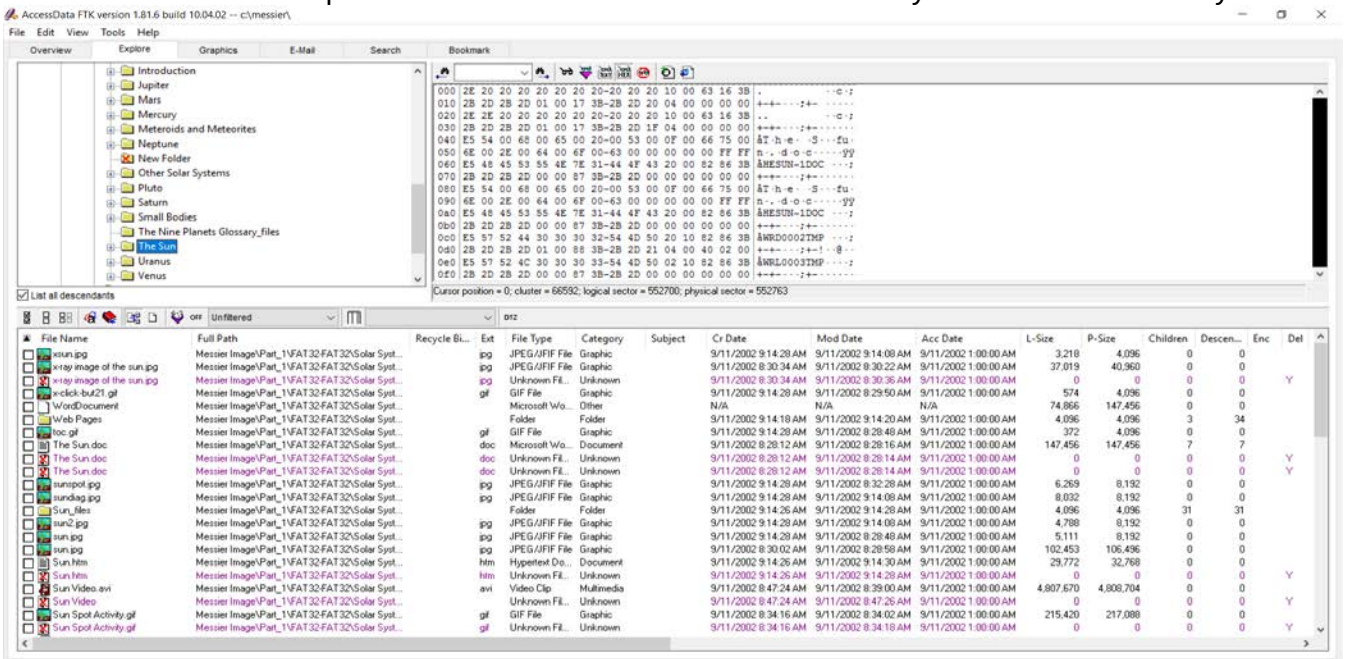




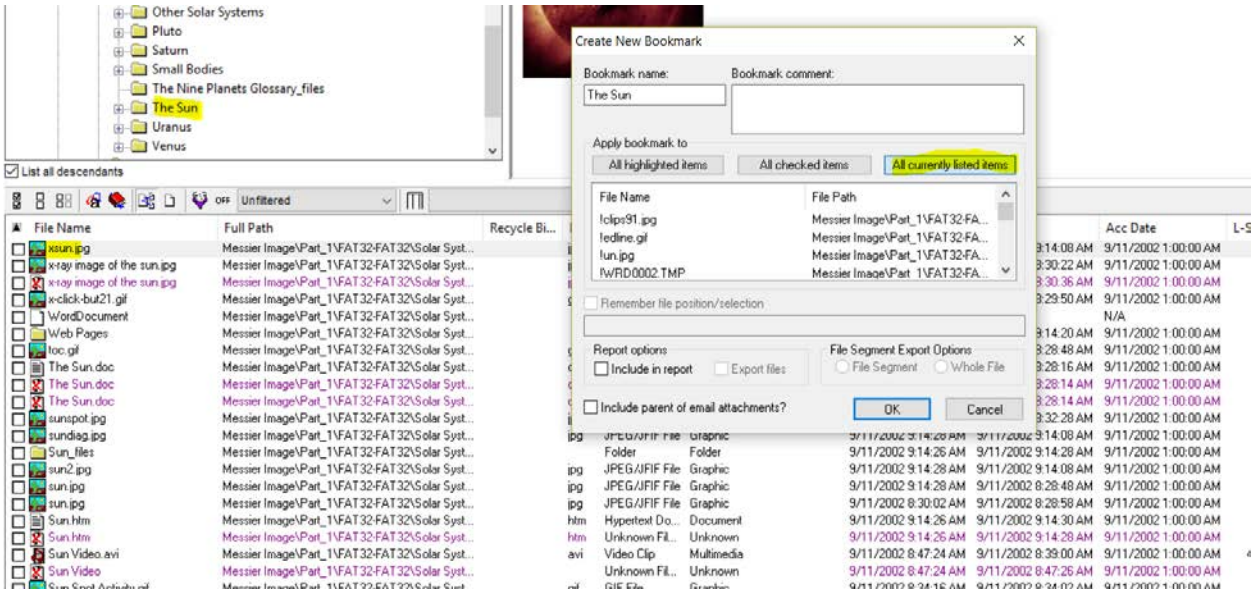
Use Copy Special to copy a list of the dates and times associated with the exported files to the clipboard. Then paste this data into Microsoft Excel.



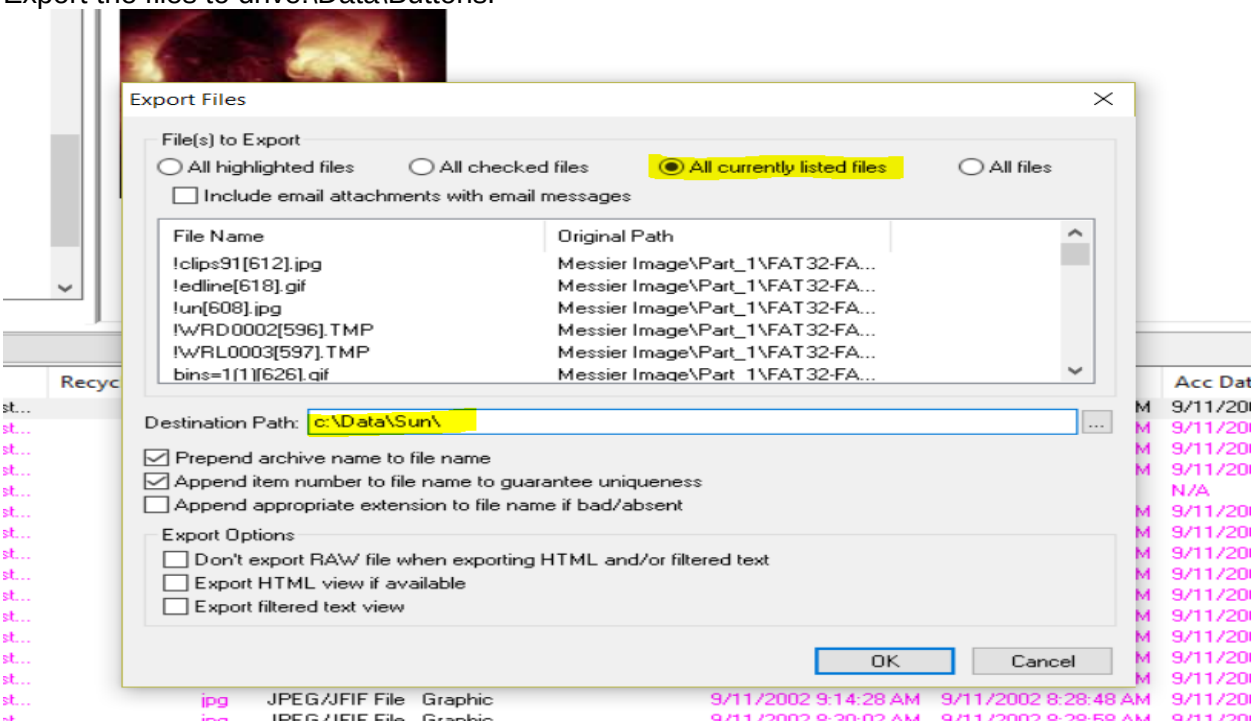
Go to the FAT32-FAT32 partition and select all the files in the \Solar System\The Sun directory.



Create a bookmark named The Sun and add the files to the bookmark.



Export the files to drive:\Data\Buttons.



Use Copy Special to copy a list of the dates and times associated with the exported files to the clipboard. Then paste this data into Microsoft Excel.