

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:

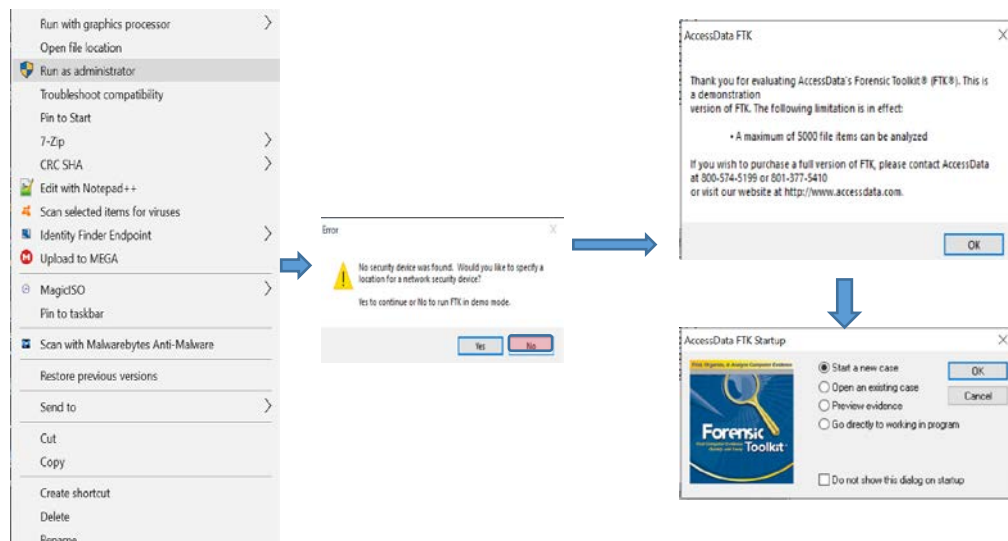
1. FTK Basics Quiz

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>

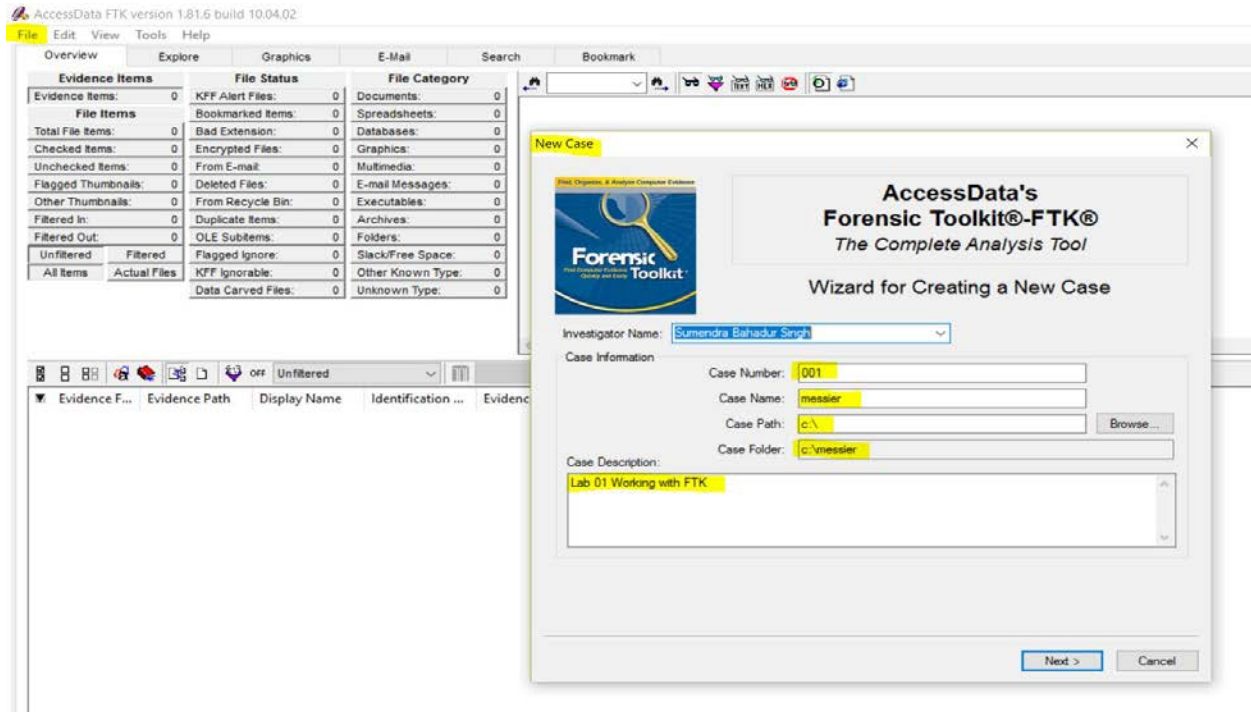
Lab Instructions:

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.

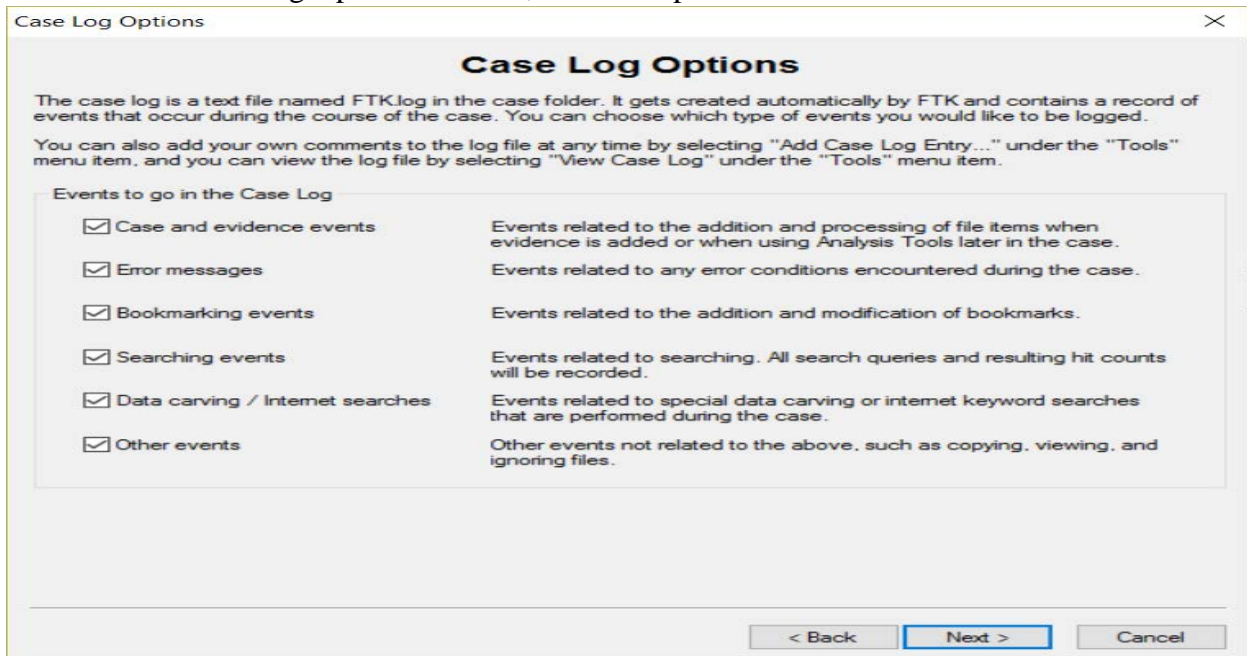


Steps:

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.

Processes to Perform

Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

- MD5 Hash An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
- SHA1 Hash A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
- KFF Lookup KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
- Entropy Test For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
- Full Text Index The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
- Store Thumbnails Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
- Decrypt EFS Files Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
- File Listing Database Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special. DB Options
- HTML File Listing Create an HTML version of the File Listing.
- Data Carve Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu. Carving Options
- Registry Reports Generate common registry reports during preprocessing.

< Back

Next >

Cancel

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

Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

Include All Items

Optimal Settings

Email Emphasis

Text Emphasis

Graphics Emphasis

Unconditionally Add

- File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
- Extract files from KFF ignorable containers

Conditionally Add

Add other items to the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria

- | | | |
|---|---|---|
| Deletion Status: | Encryption Status: | Email Status: |
| <input type="radio"/> Deleted | <input type="radio"/> Encrypted | <input type="radio"/> From email |
| <input type="radio"/> Not deleted | <input type="radio"/> Not encrypted | <input type="radio"/> Not from email |
| <input checked="" type="radio"/> Either | <input checked="" type="radio"/> Either | <input checked="" type="radio"/> Either |
| <input checked="" type="checkbox"/> Include Duplicate Files | <input checked="" type="checkbox"/> OLE Streams | |

File Type Criteria

- | | |
|--|---|
| <input checked="" type="checkbox"/> Documents | <input checked="" type="checkbox"/> Executables |
| <input checked="" type="checkbox"/> Spreadsheets | <input checked="" type="checkbox"/> Archives |
| <input checked="" type="checkbox"/> Databases | <input checked="" type="checkbox"/> Folders |
| <input checked="" type="checkbox"/> Graphics | <input checked="" type="checkbox"/> Other Known |
| <input checked="" type="checkbox"/> Multimedia | <input checked="" type="checkbox"/> Unknown |
| <input checked="" type="checkbox"/> Email msgs | |

< Back

Next >

Cancel

Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.

Unconditionally Index

File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)

Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)

KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)

Conditionally Index

Index other items in the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria

Deletion Status: Deleted Not deleted **Either**

Encryption Status: Encrypted Not encrypted **Either**

Email Status: From email Not from email **Either**

Include Duplicate Files OLE Streams

File Type Criteria

Documents Executables

Spreadsheets Archives

Databases Folders

Graphics Other Known

Multimedia Unknown

Email msgs

< Back
Next >
Cancel

- 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.

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

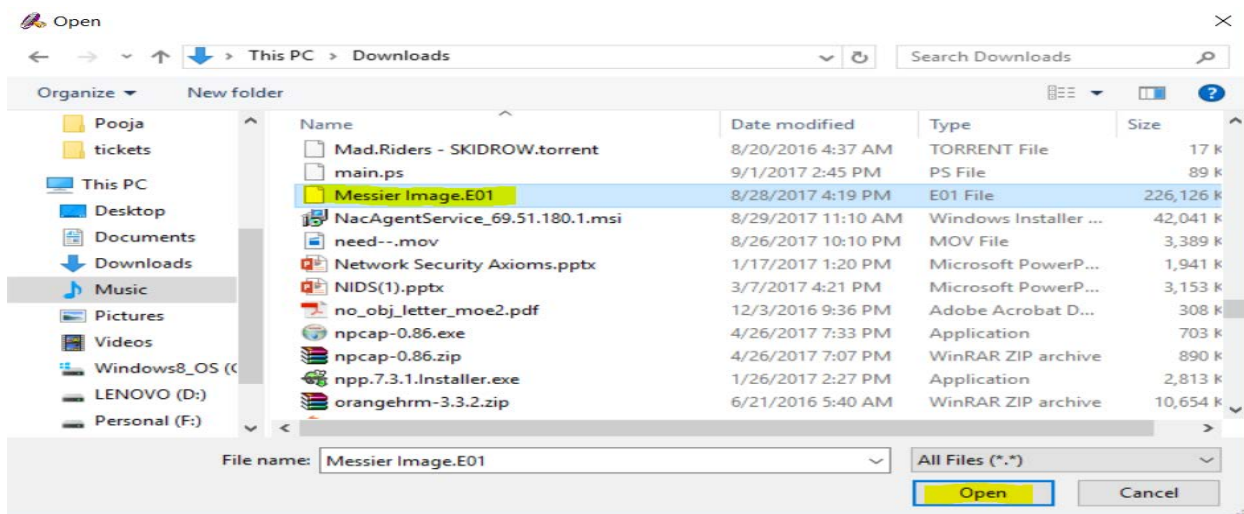
- Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
- Local drive: Can be a logical or physical drive
- Folder: Adds all files in the specified folder, including contents of subfolders
- Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

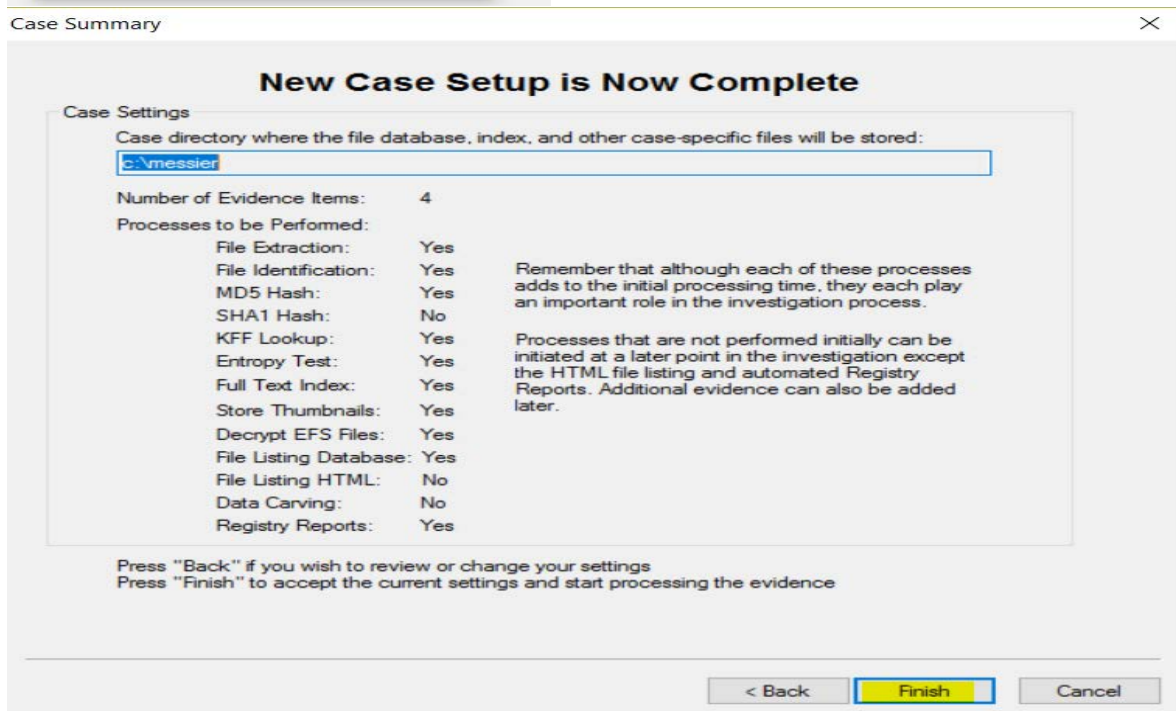
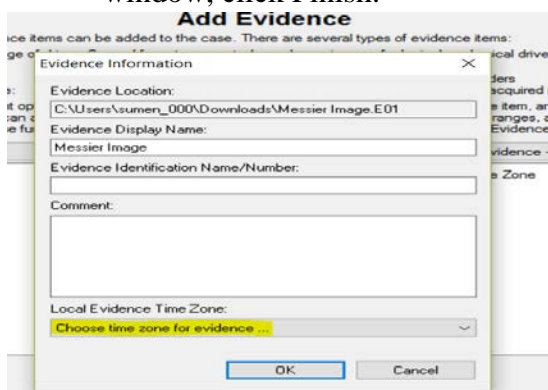
Add Evidence...
Edit Evidence...
Remove Evidence
Refine Evidence - Advanced...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
<div style="border: 1px solid gray; padding: 5px; margin: 10px auto; width: 80%;"> <p style="text-align: center;">Add Evidence to Case</p> <p>Type of Evidence to Add to Case</p> <p><input checked="" type="radio"/> Acquired Image of Drive</p> <p><input type="radio"/> Local Drive</p> <p><input type="radio"/> Contents of a Folder</p> <p><input type="radio"/> Individual File</p> <p style="text-align: right; margin-top: 10px;"> Continue... Cancel </p> </div>						

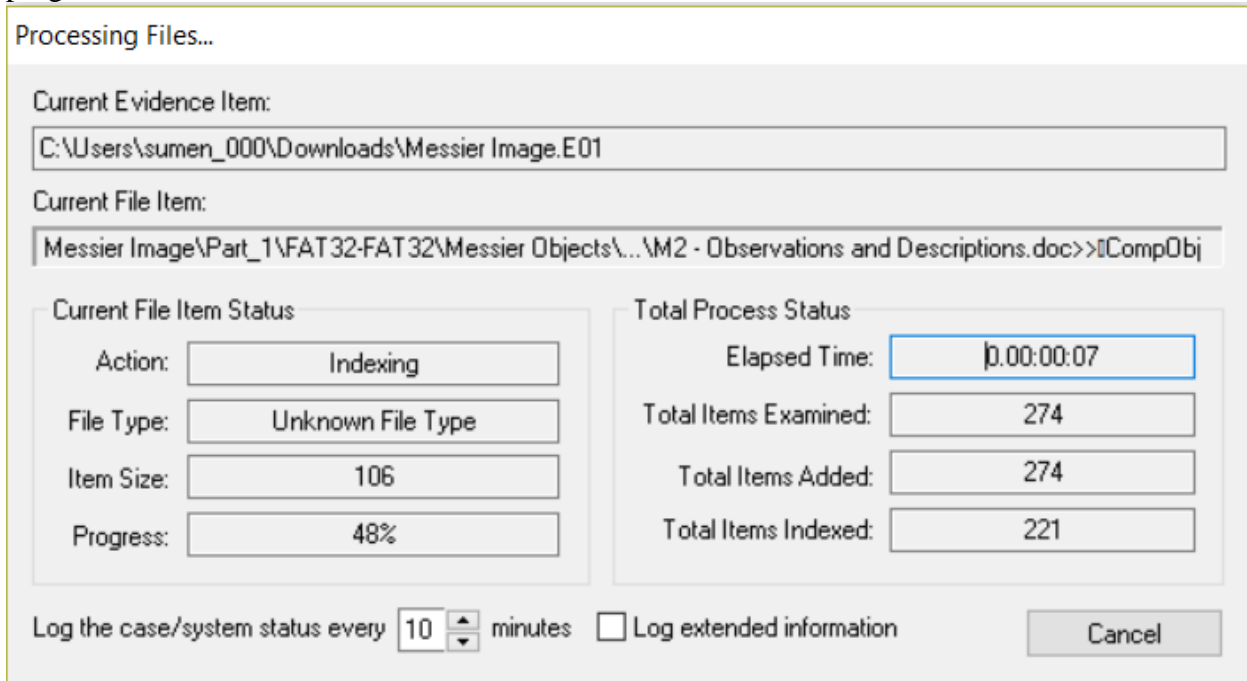
< Back
Next >
Cancel



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

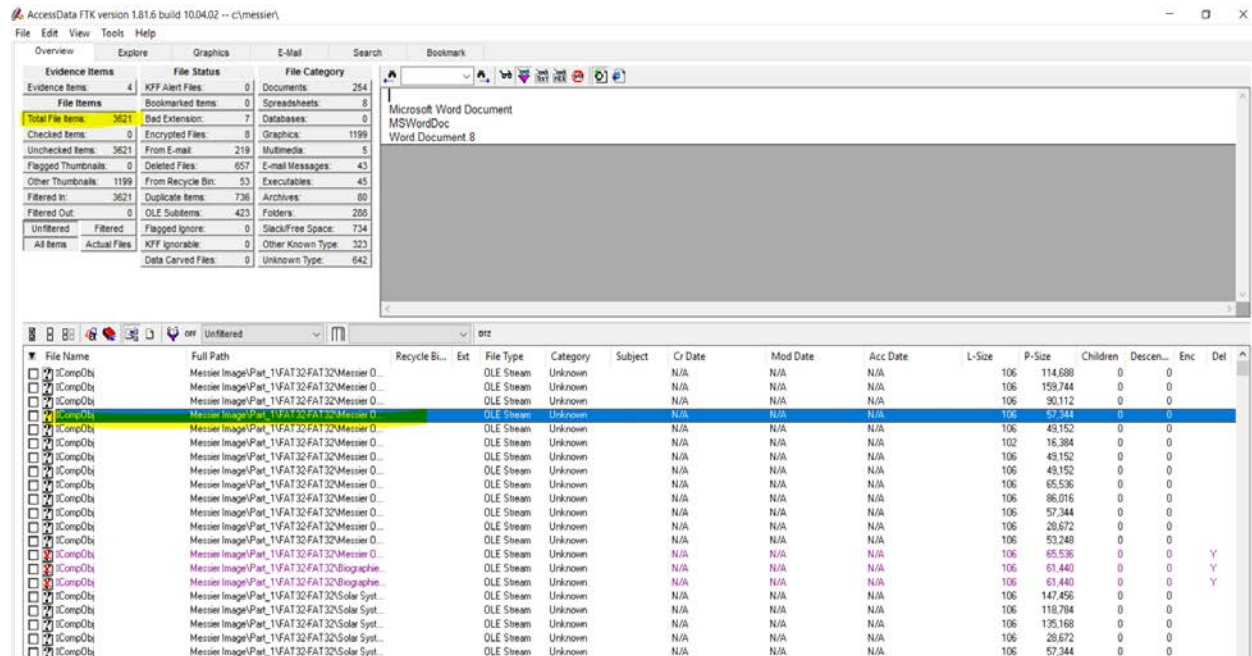


It will take few minutes to generate a case with the image a processing files windows will progress status.



Reviewing Menu Bar Options

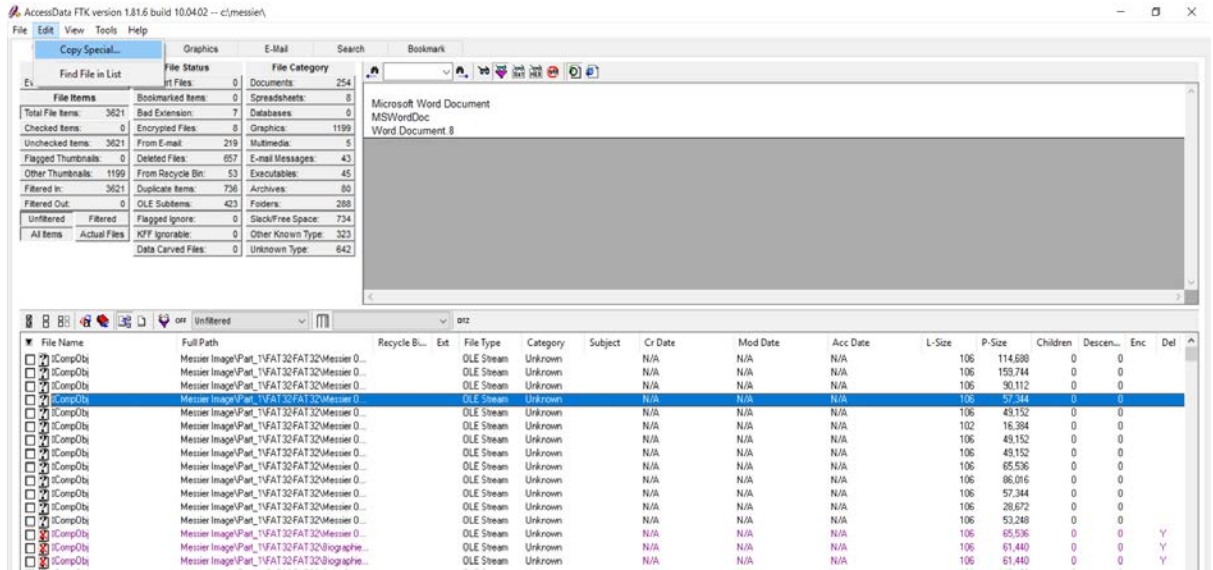
To select a file from the case, select the “Total File Items” and then the actual files for the windows at bottom.



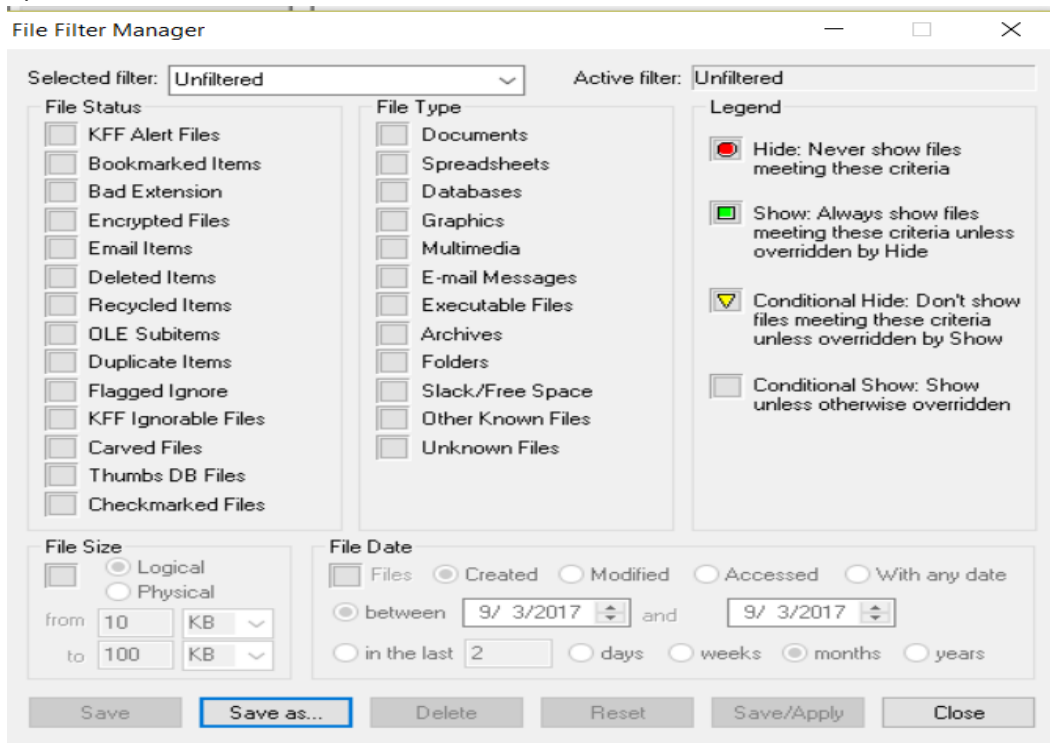
File and Edit Options


Steps:

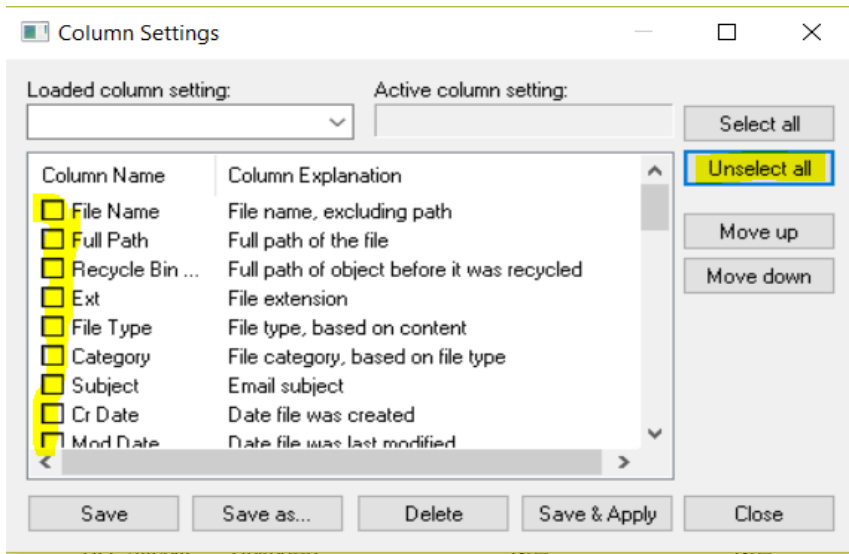
1. In the file list, select a file. On the menu bar, click File and note the options not previously discussed. Click Edit and note Copy Special and Find File in List.



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

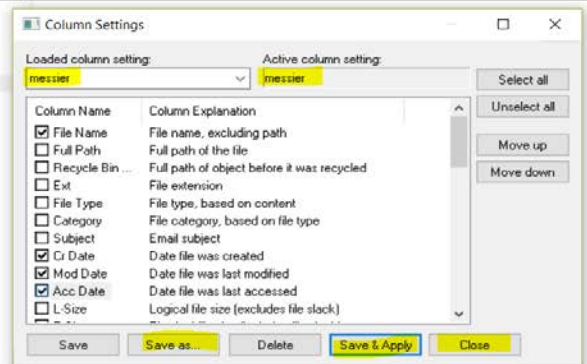
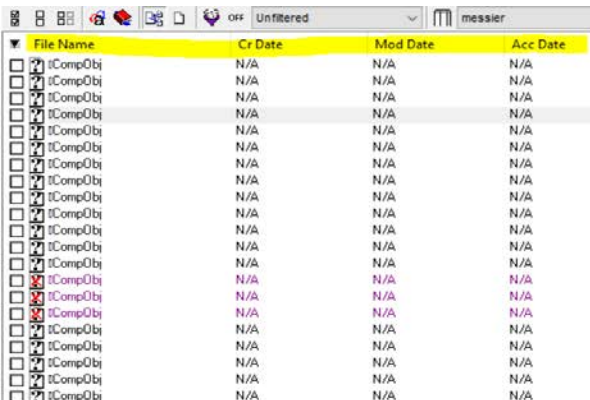
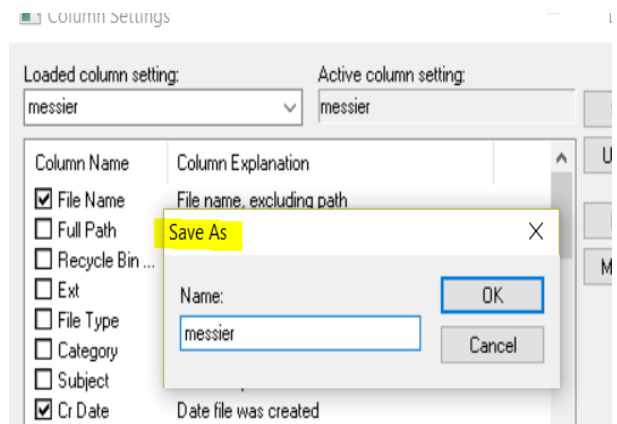
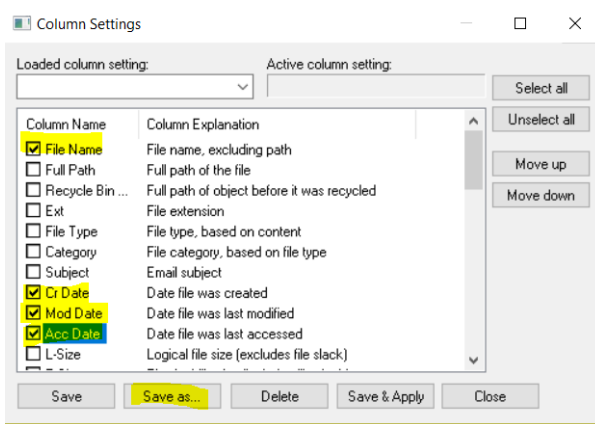


3. How to change file column view windows or customize the column view windows.
 - a. Click View > Column Settings or  click > Click Unselect All.

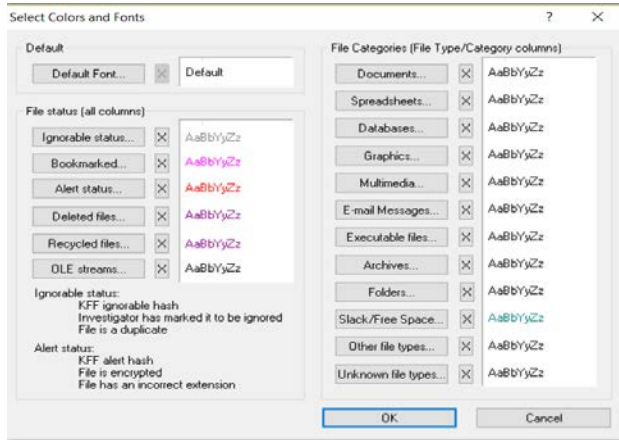


b. In the Column Name list, mark the following: Filename, CrDate,

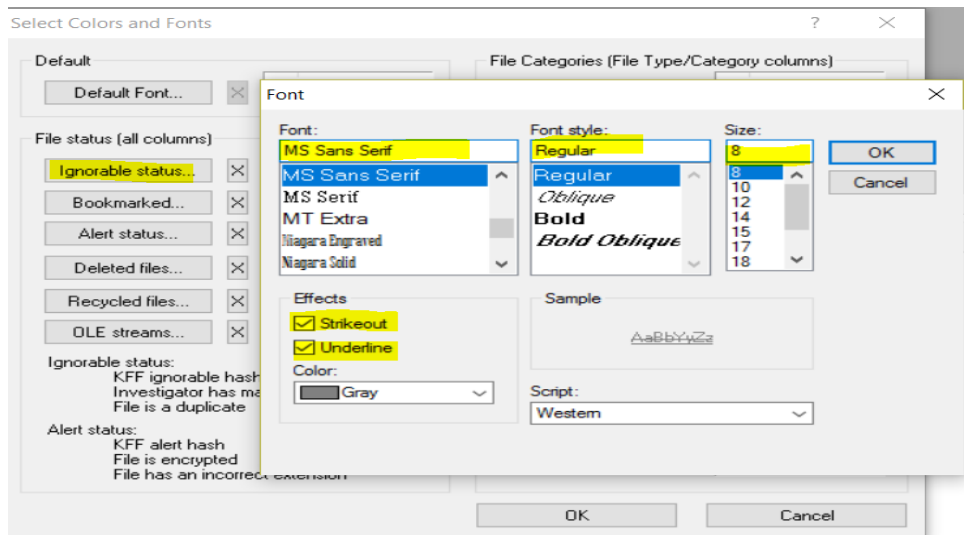
Mod Date and Acc Date and click Save as. Name the column setting Date and Time and then click OK. In the Column Settings dialog, click Save, Apply and close the window.



- Click View > Colors and Fonts.



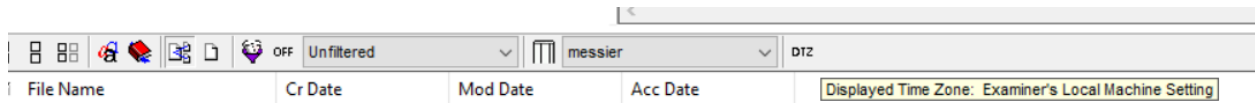
- Change the display settings for Ignorable Status.
 - In the File Status box, click Ignorable Status. In the Font menu, select a font, change the color, and mark, Strikeout or Underline. Then click OK.



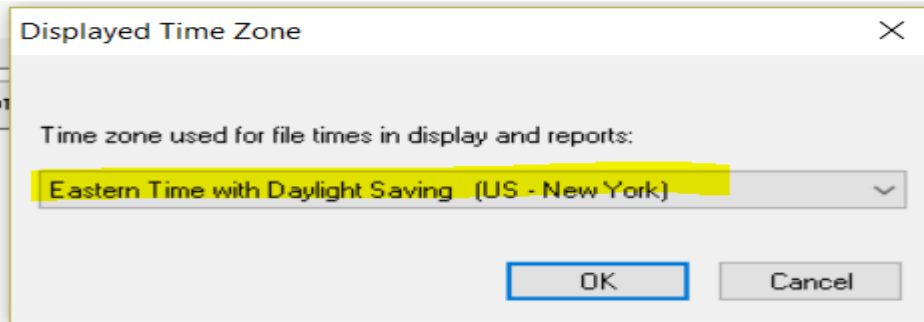
- In the Overview tab, click the KFF Ignorable container to view the appearance of Ignorable Status.

Evidence Items		File Status	File Category
Evidence Items:	4	KFF Alert Files:	0
File Items		Bookmarked Items:	0
Total File Items:	3621	Bad Extension:	7
Checked Items:	0	Encrypted Files:	8
Unchecked Items:	3621	From E-mail:	219
Flagged Thumbnails:	0	Deleted Files:	657
Other Thumbnails:	1199	From Recycle Bin:	53
Filtered In:	3621	Duplicate Items:	736
Filtered Out:	0	OLE Subitems:	423
Unfiltered	Filtered	Flagged Ignore:	0
All Items	Actual Files	KFF Ignorable:	0
		Data Carved Files:	0
		Documents:	254
		Spreadsheets:	8
		Databases:	0
		Graphics:	1199
		Multimedia:	5
		E-mail Messages:	43
		Executables:	45
		Archives:	80
		Folders:	288
		Slack/Free Space:	734
		Other Known Type:	323
		Unknown Type:	642

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.

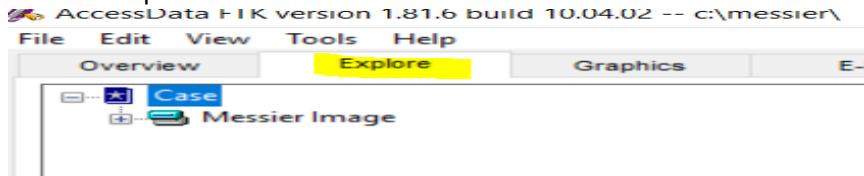


Mouse-over the DTZ symbol again and note the new settings.

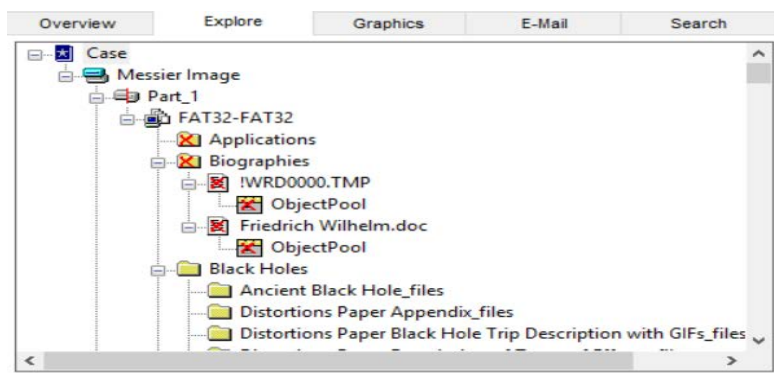


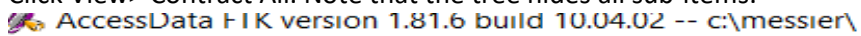
10. View Explore tab.

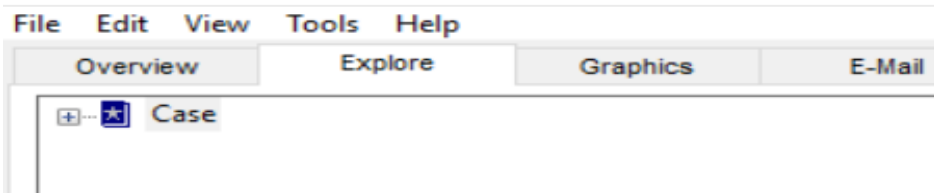
- a. Click the Explore tab.



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

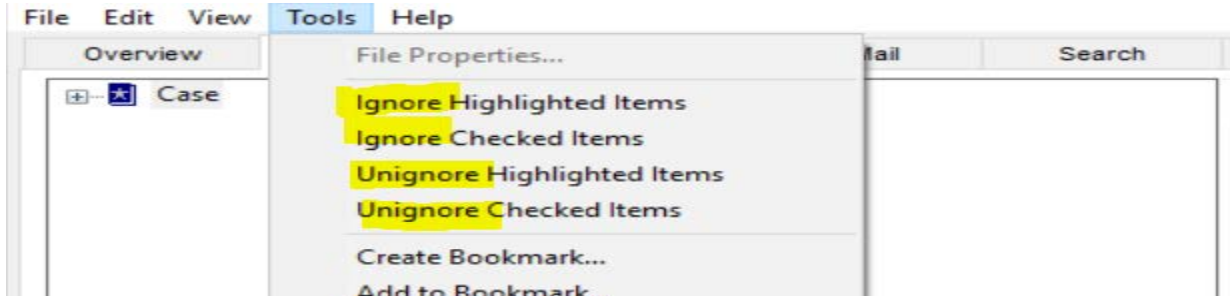


- c. Click View> Contract All. Note that the tree hides all sub-items.


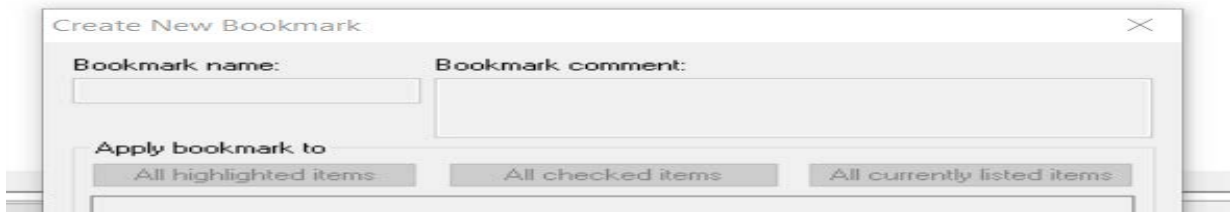


11. Exploring Tools Options

- a. On the menu bar, click Tools. Note the Ignore and Unignore options.

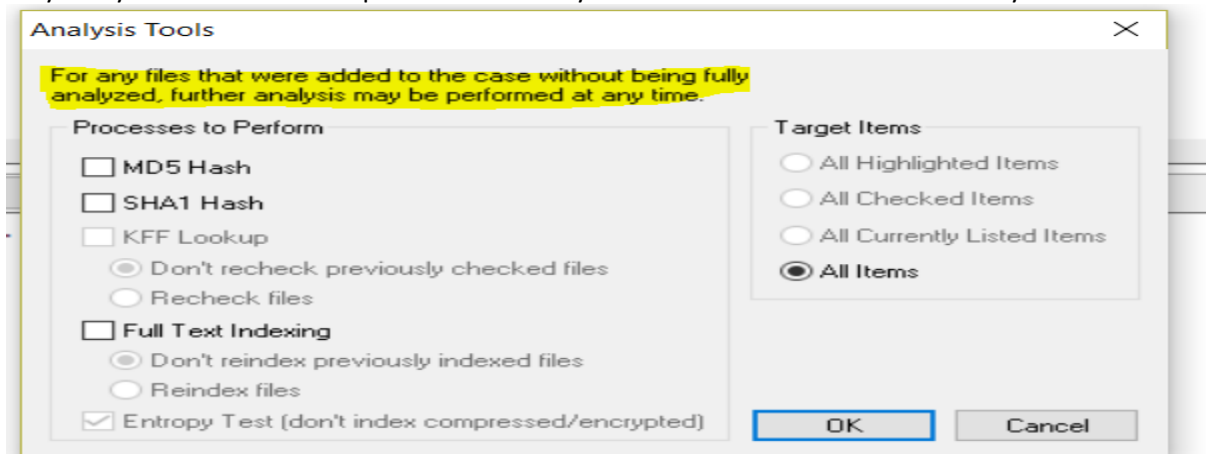


- b. Click Create Bookmark. Note the options in the Apply bookmark to box. Click Cancel to close the Create New Bookmark menu

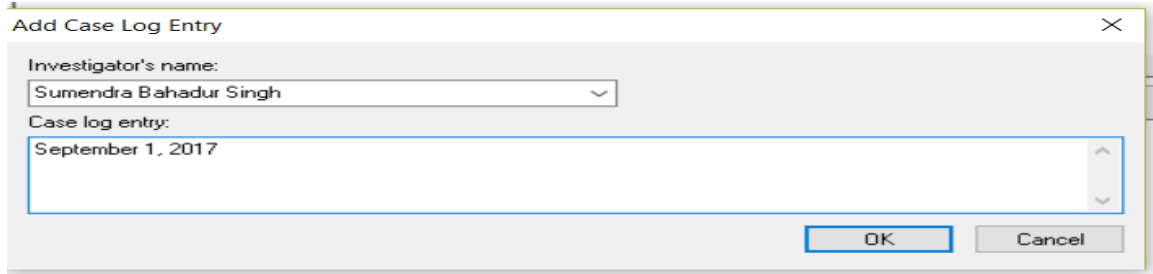


- c. Click Tools> Analysis Tools.

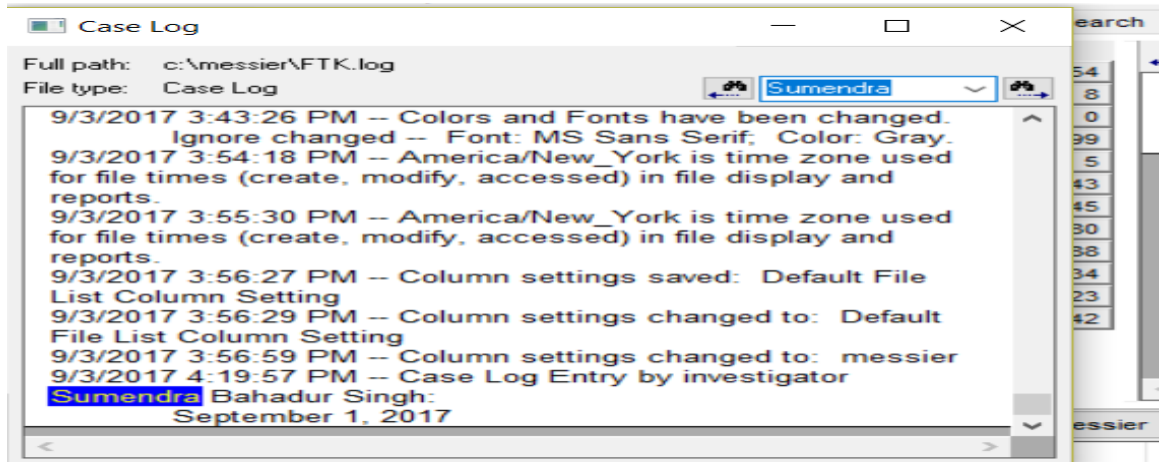
Note: The Analysis Tools menu allows you to process files that were added to the case without being fully analyzed. You can also reprocess files at any time. Click Cancel to close the Analysis Tools menu.



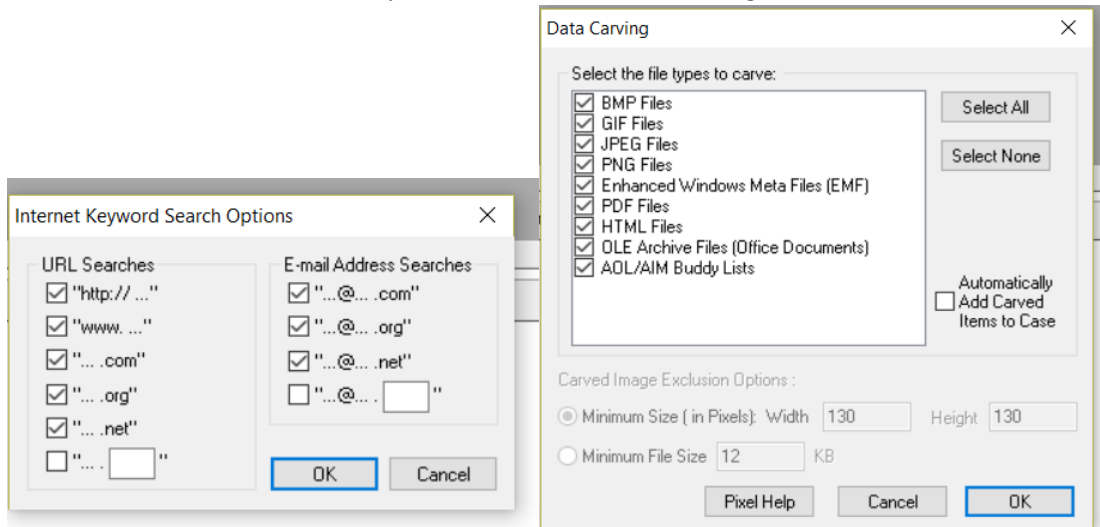
- d. Click Tools> Add Case Log Entry. Type an investigator's name and case log entry and then click OK



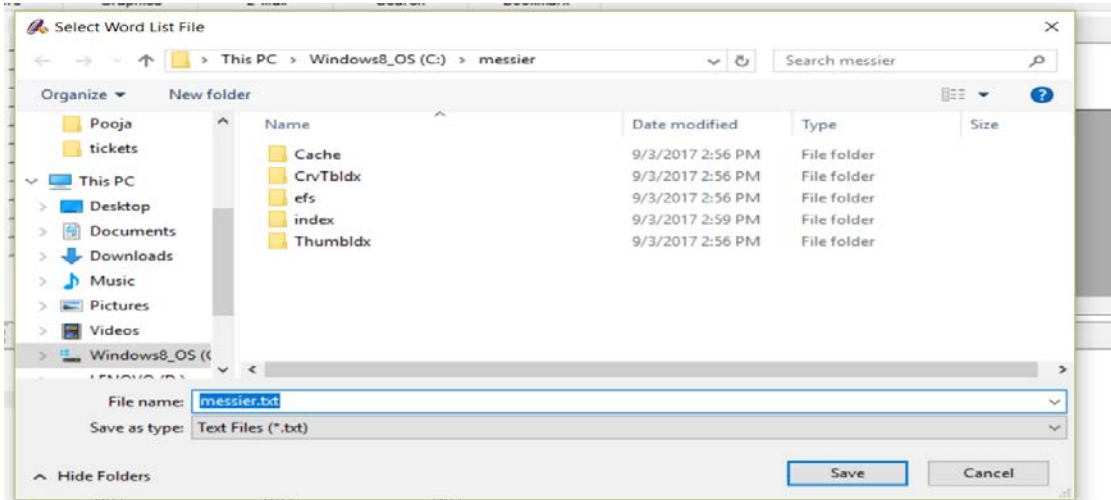
- e. To view your entry, click Tools> View Case Log. Use the Search box to find your case log entry.



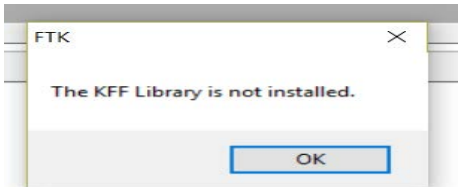
- f. Click Tools and note Internet Keyword Search and Data Carving.



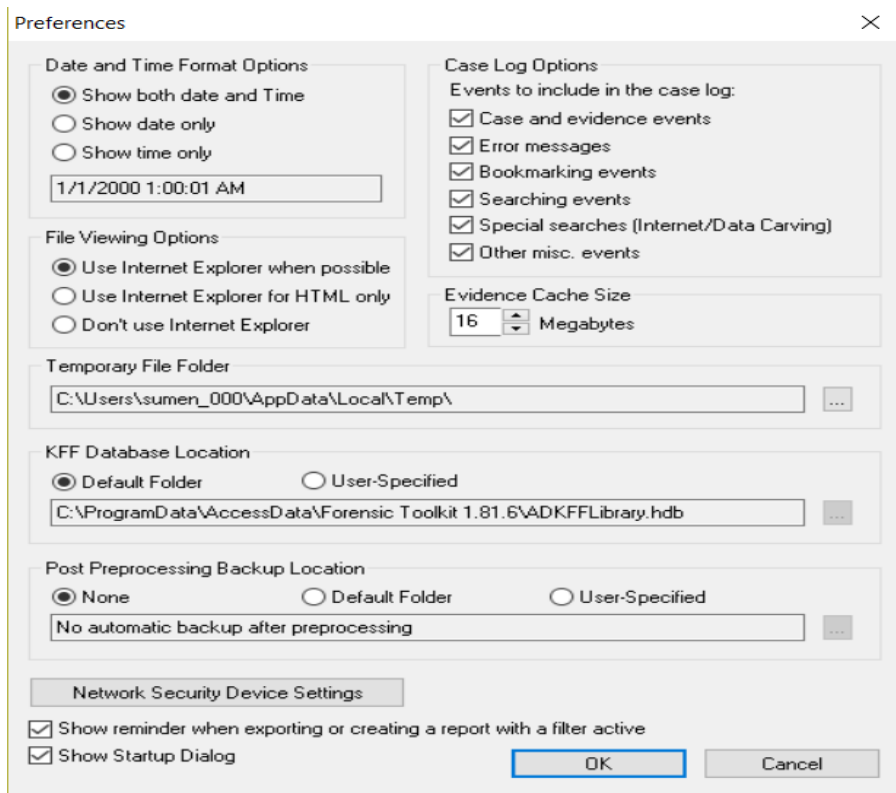
- g. Click Tools and note Export Word List.



- 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.

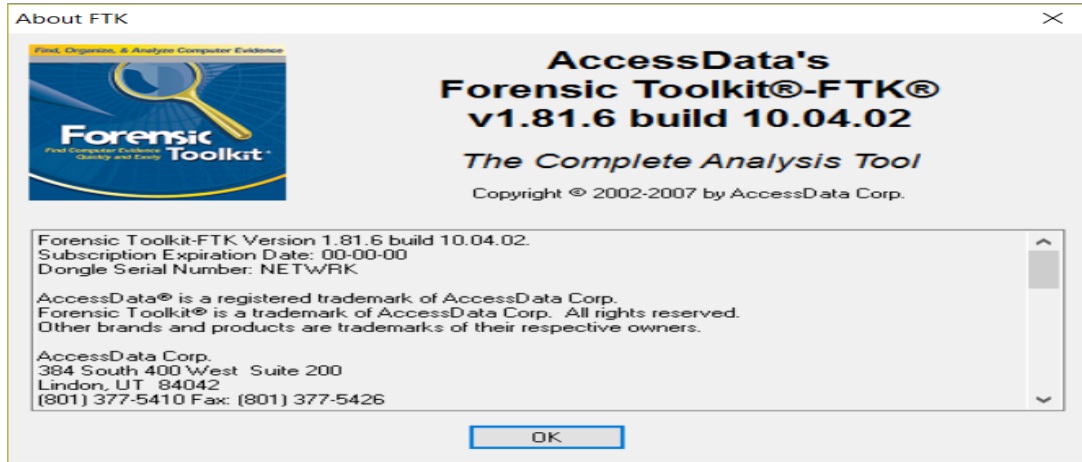


- i. Click Tools> Preferences and note the options.



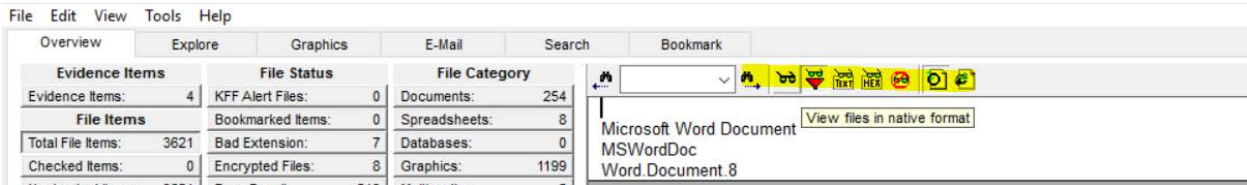
12. Exploring Help menu.

- 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

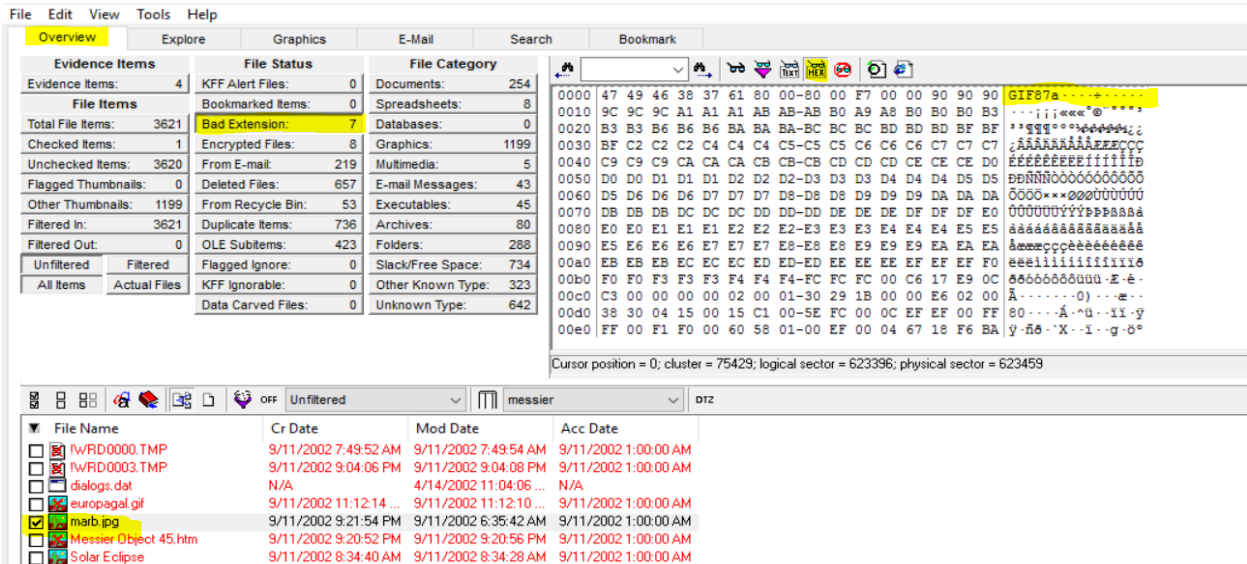
We can review the toolbar shortcut, place your pointer over each toolbar button and view the tool tip that appears. Note the relationship of buttons to menu options.



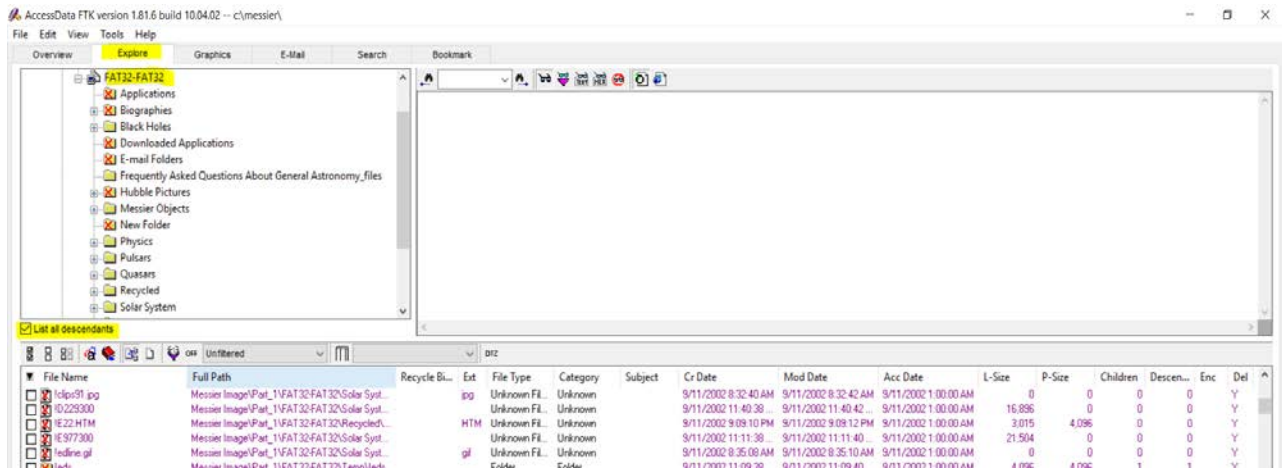
14. Reviewing FTK Tabs.

With MessierImage.E01 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.

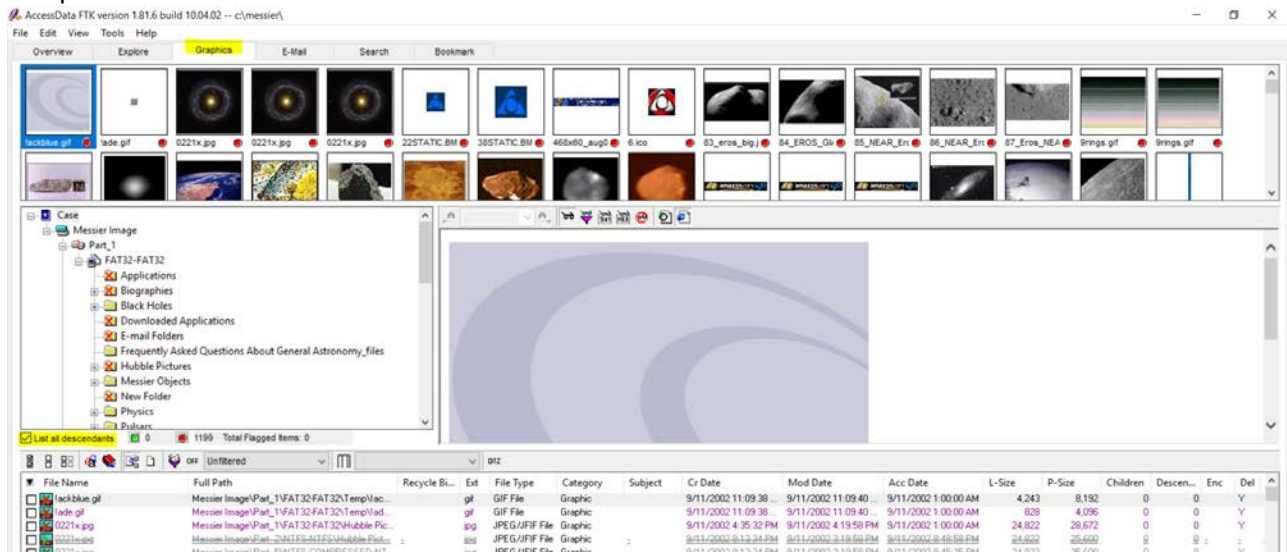
AccessData FTK version 1.81.6 build 10.04.02 -- c:\messier\



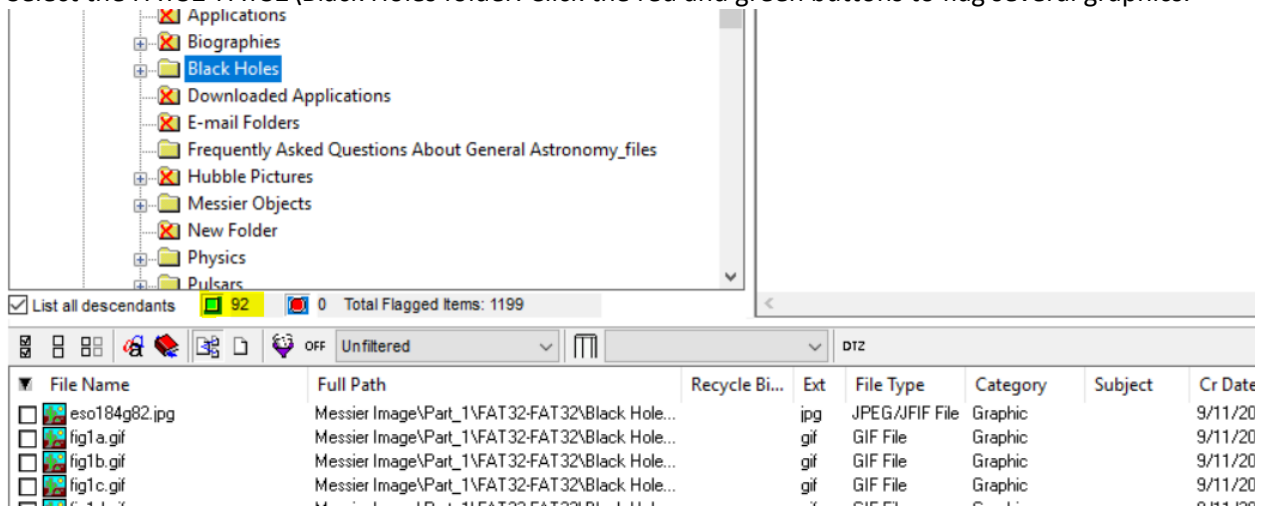
Click the Explore Tab. Select the FAT32-FAT32\Physics folder. Check List all descendants.

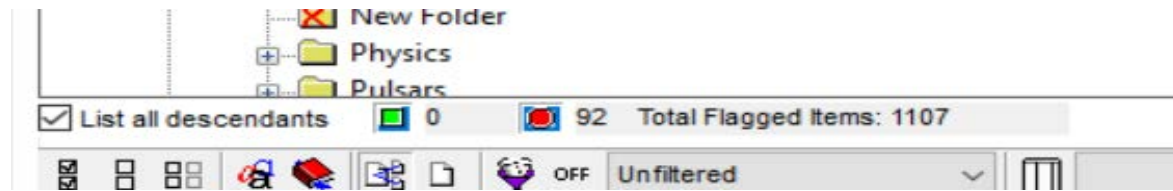


Click the Graphics Tab. Check List all descendants. Note that the List all Descendants feature is tab-independent.

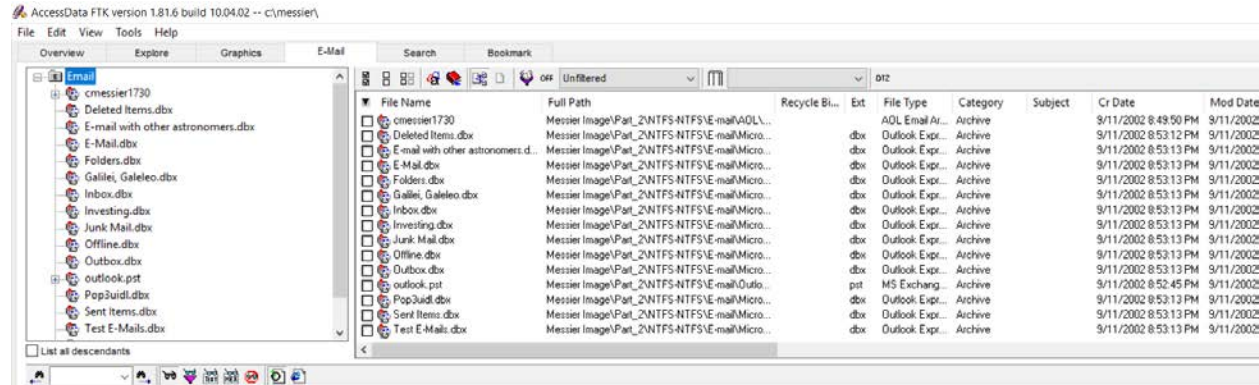


Select the FAT32-FAT32\Black Holes folder. Click the red and green buttons to flag several graphics.

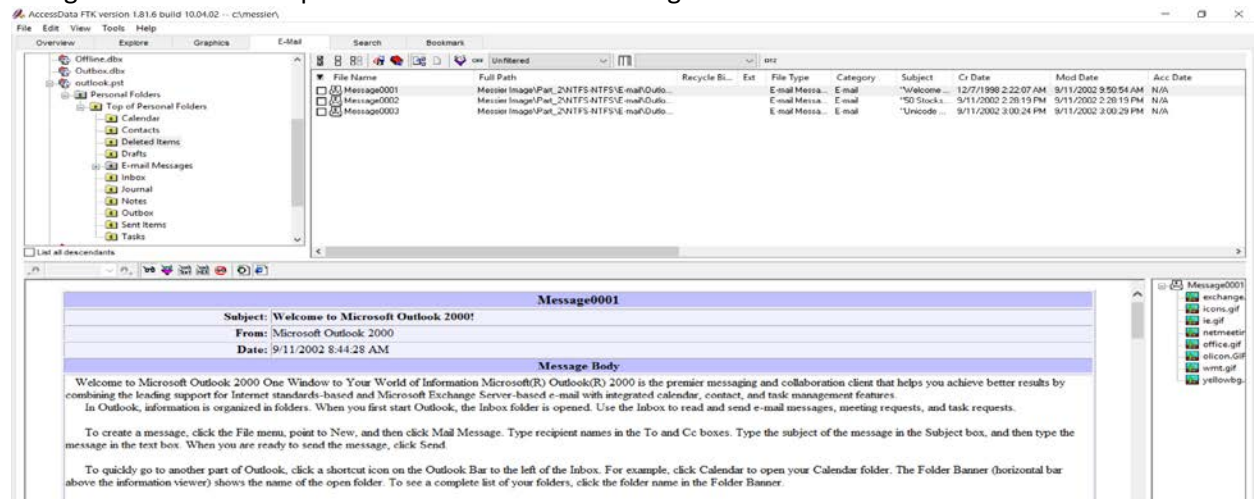




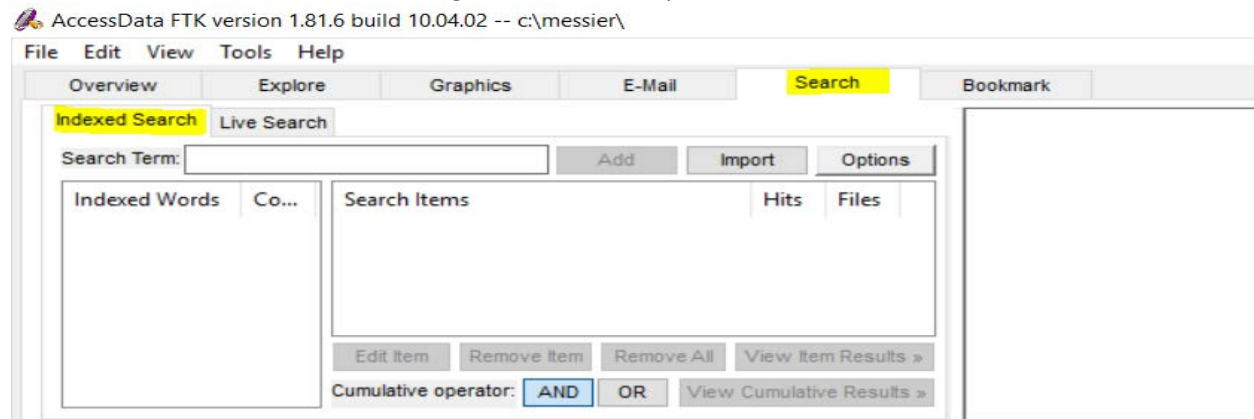
Click the E-Mail Tab. Note the different viewing panes. Several email file types are supported.



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

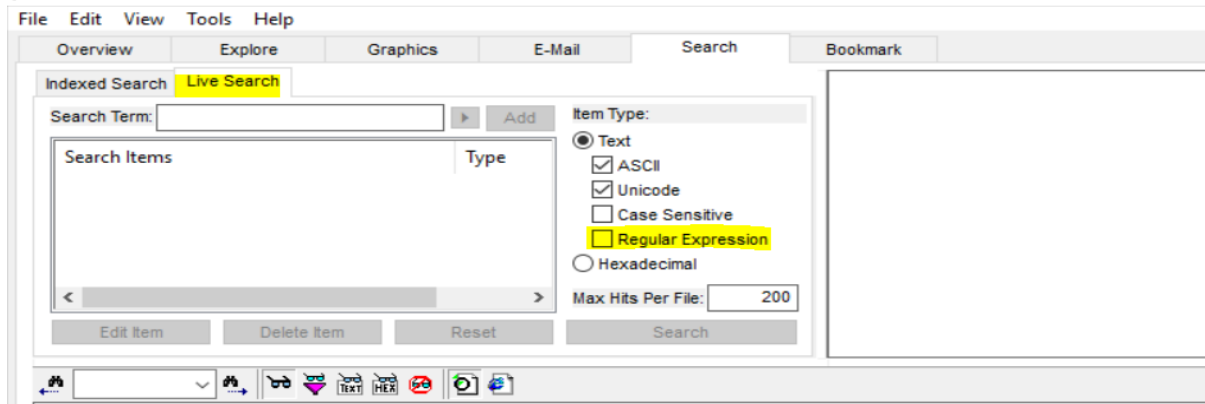


Click the Search Tab. Note the Indexed Search options. An indexed search uses the index file to find search terms. FTK uses the search engine, dtSearch, to perform indexed searches.



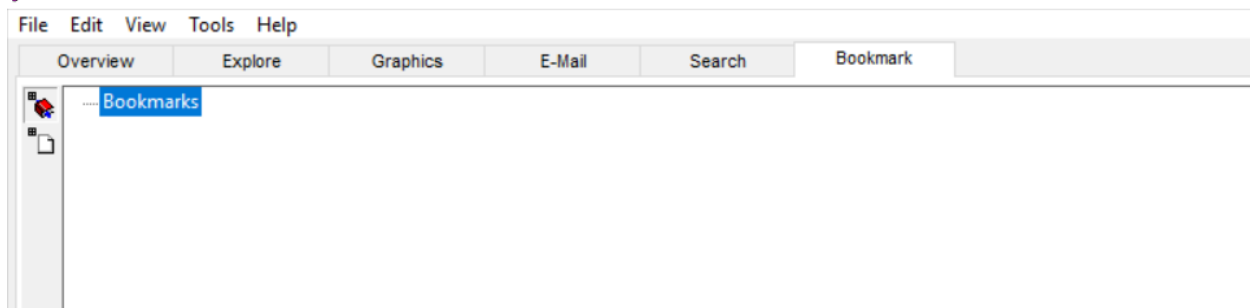
Click the Live Search Tab. Note the options. Live searches support regular expressions.

AccessData FTK version 1.81.6 build 10.04.02 -- c:\messier\



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

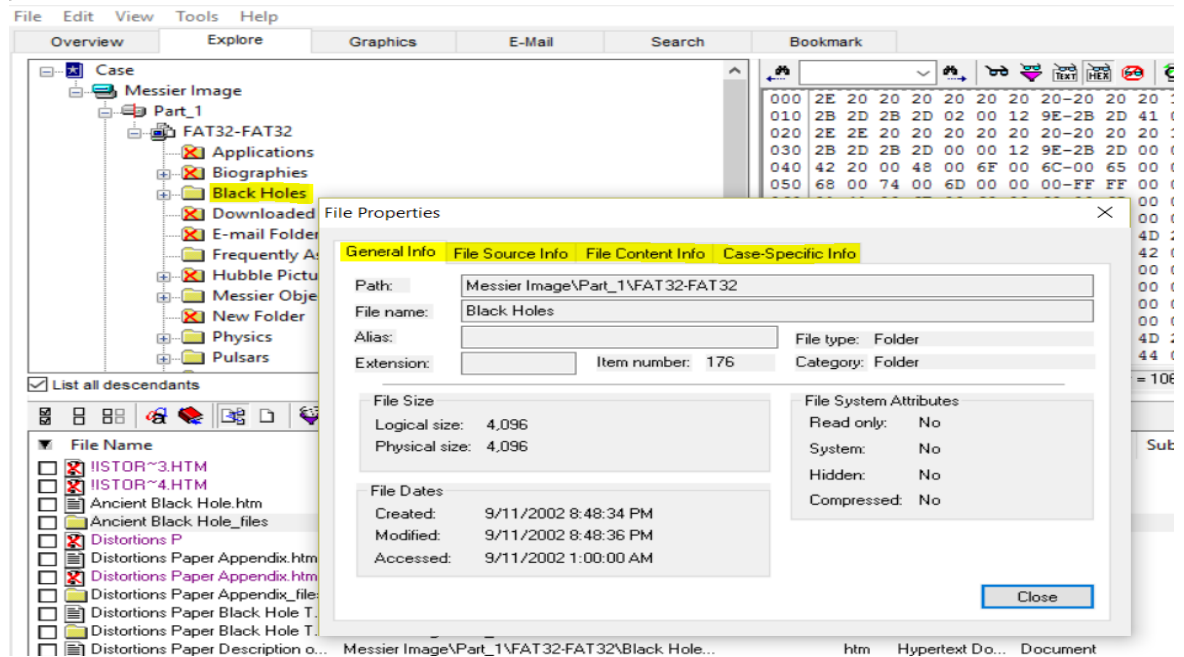
AccessData FTK version 1.81.6 build 10.04.02 -- c:\messier\



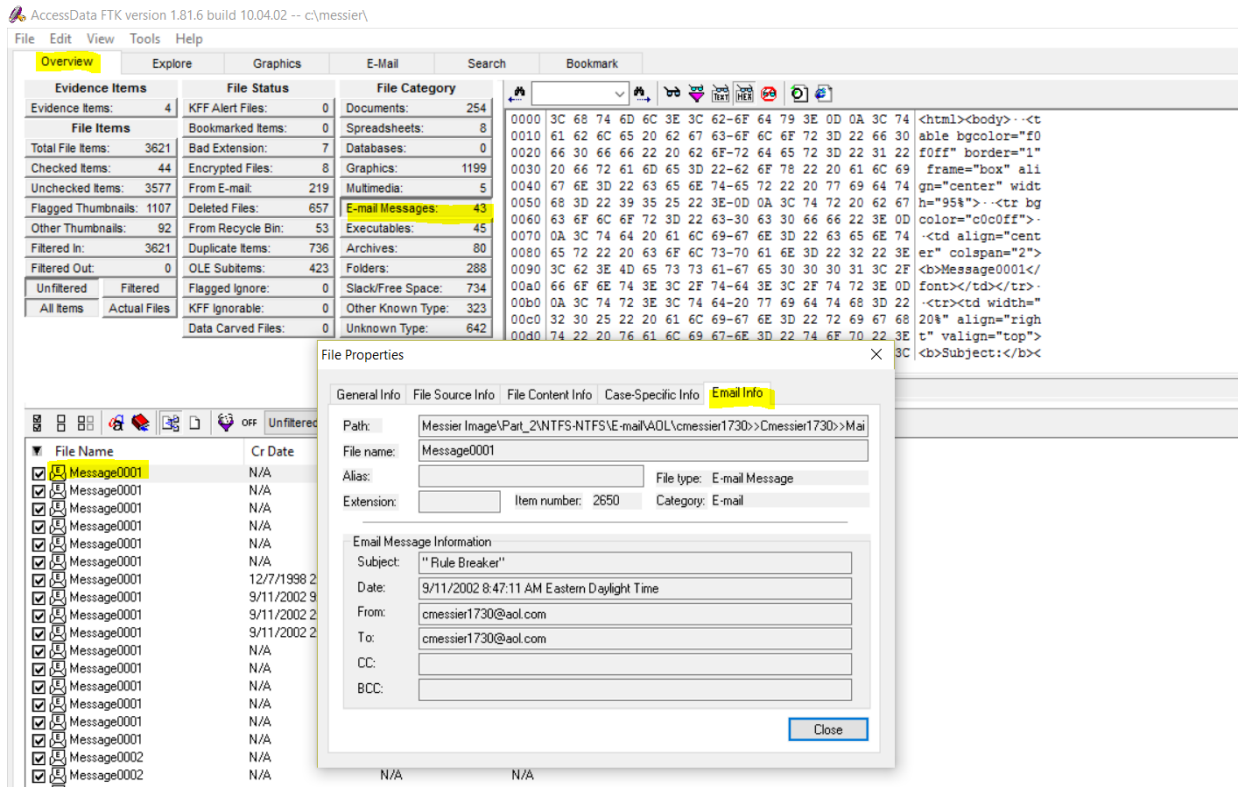
15. Viewing File and Folder Properties

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

AccessData FTK version 1.81.6 build 10.04.02 -- c:\messier\

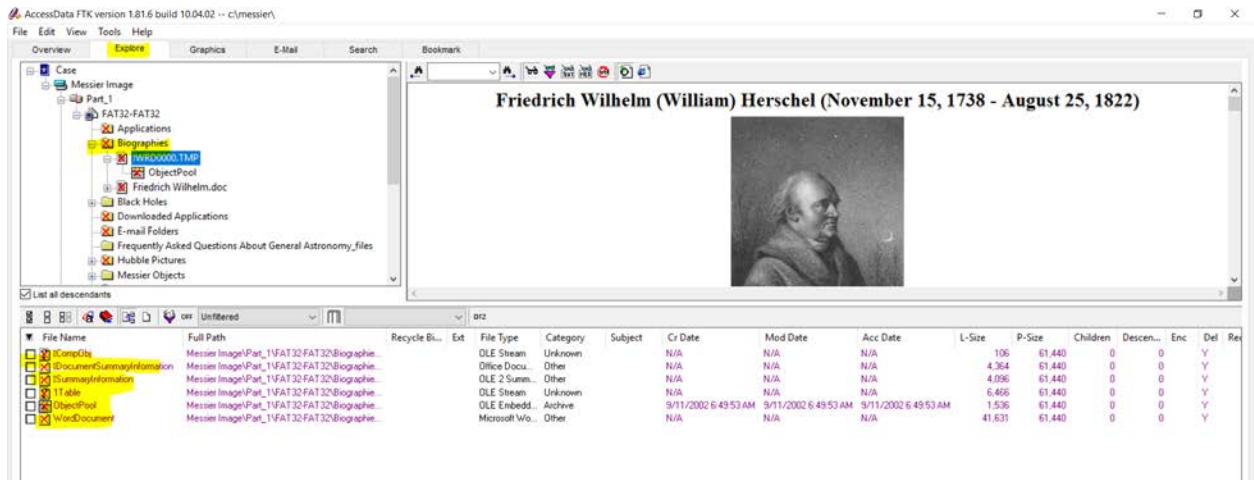


- b. Go to the E-Mail Messages container in the Overview Tab. Select All Items so you can view the items within the PST container. Right-click an email file and select File Properties. Note the options, particularly, the E-Mail Info tab.



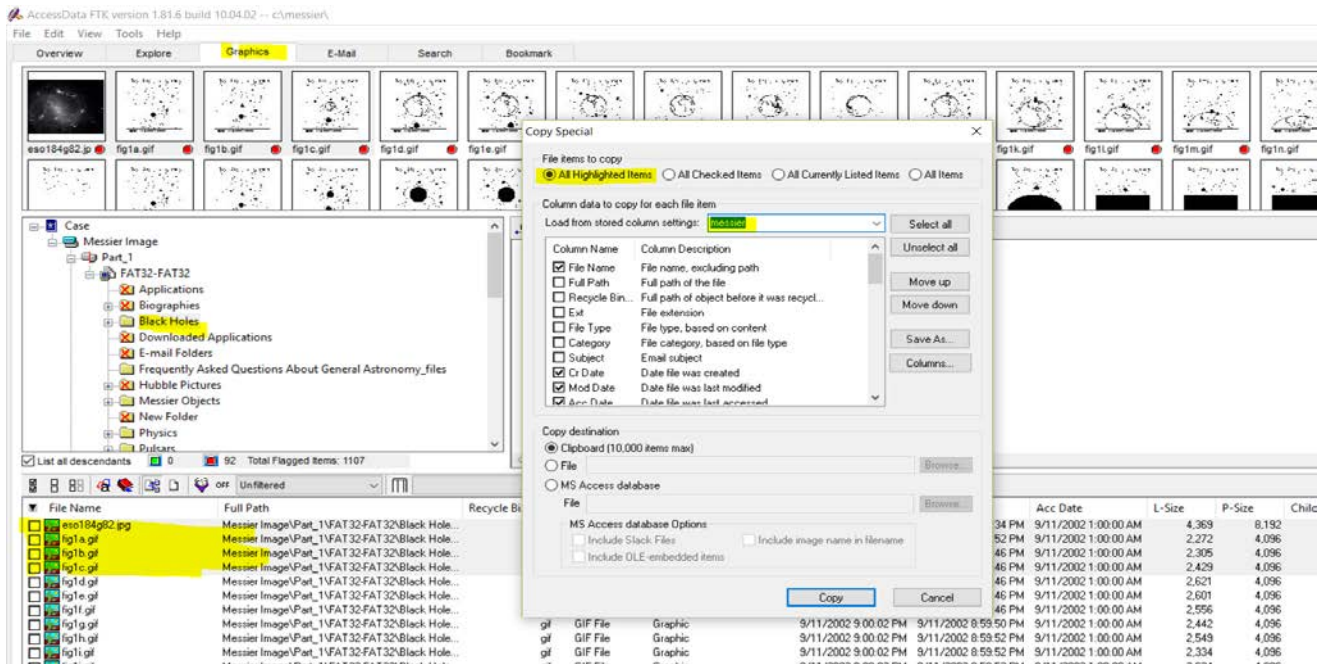
16. Viewing Metadata

- 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

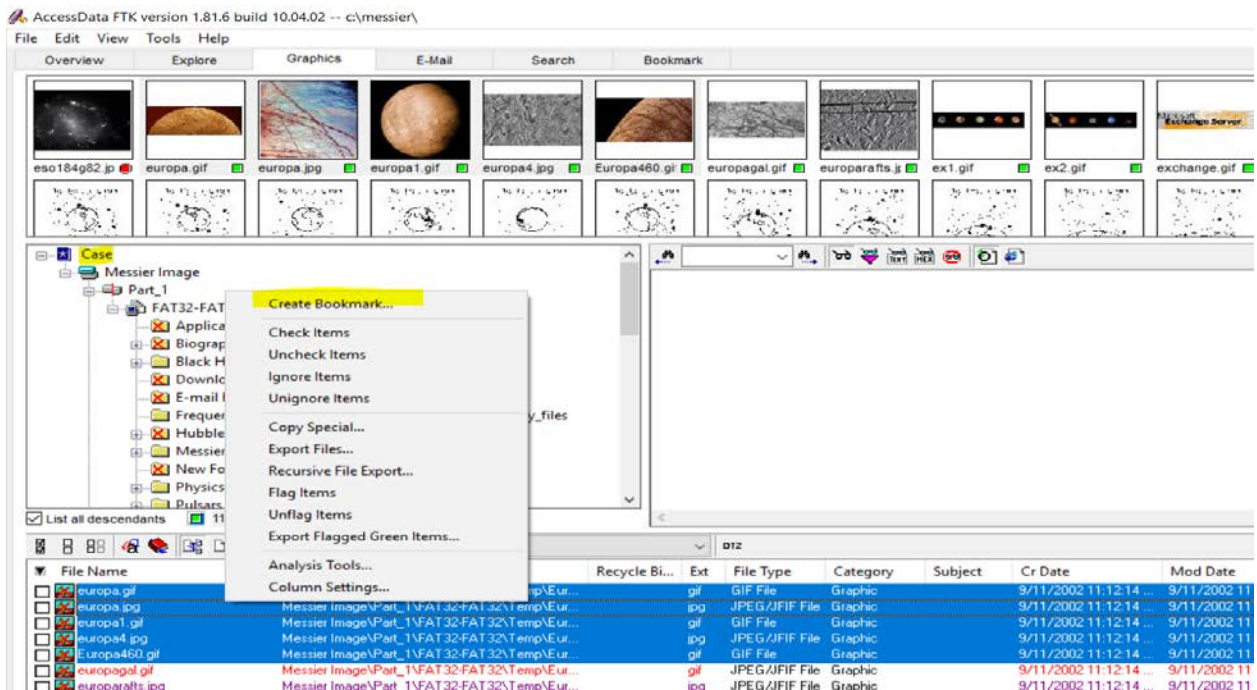
- a. Click the Graphics Tab. Select a folder, Highlight several files. Right-click the files and select Copy Special. Under File Items to Copy, select All Highlighted Items. Select the Date and Time column setting you created earlier.

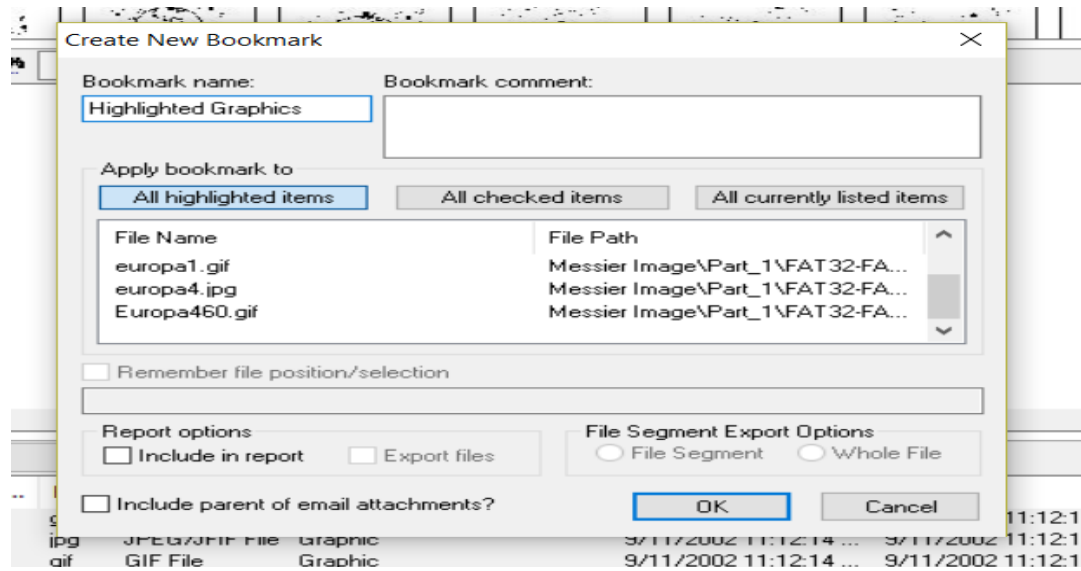


18. Working with Graphics.

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.





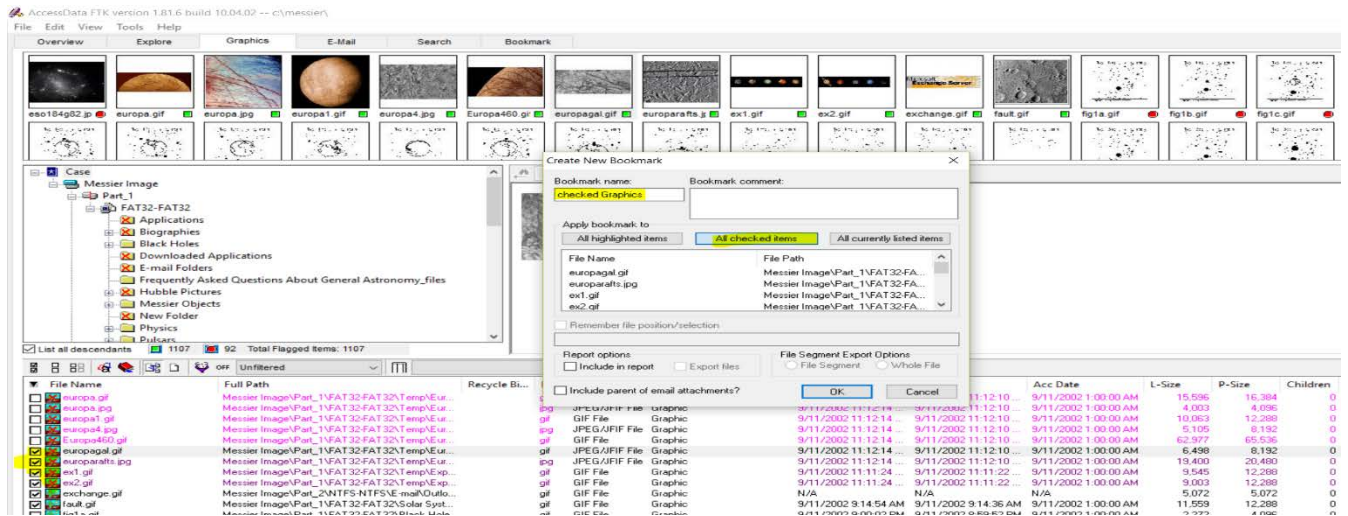
b. Adding comment on Bookmark.

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

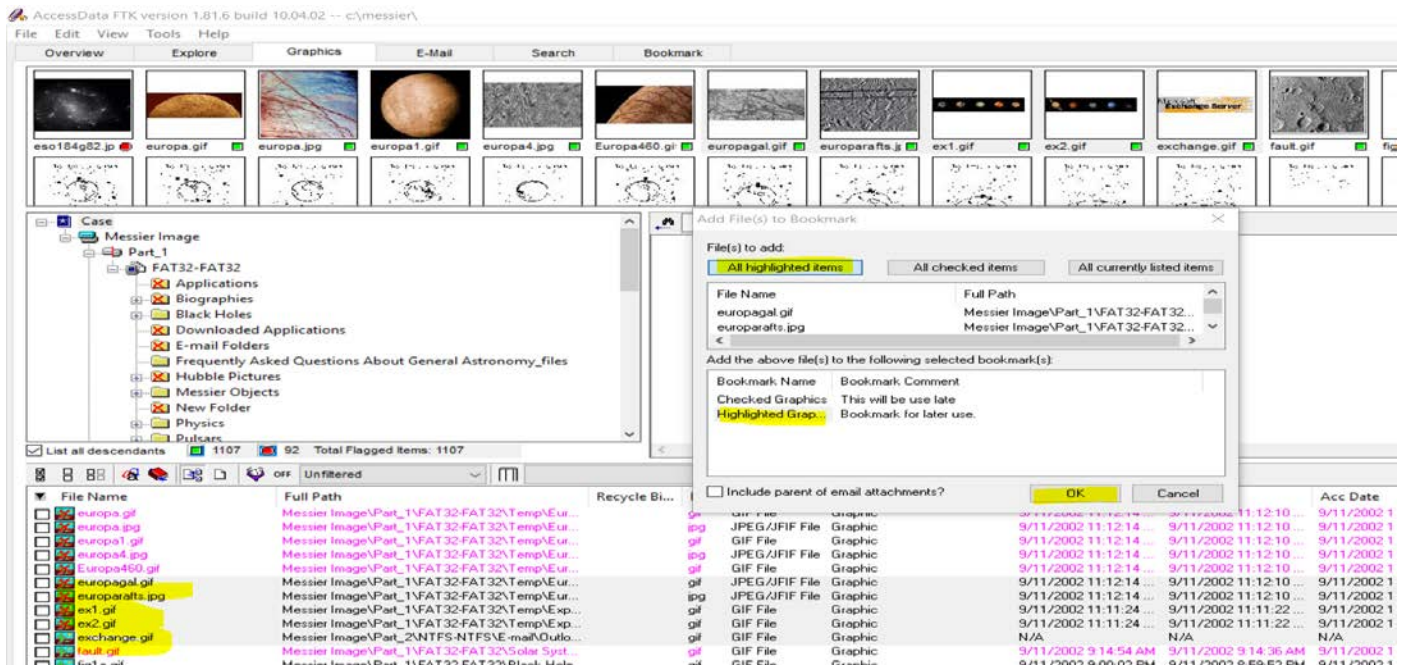


graphics and create Bookmarks. In the Create New Bookmark menu, name the bookmark Checked Graphics. Then select All highlighted items and click okay. Add the comment on the bookmarked file from Bookmark tab, add comment and save.

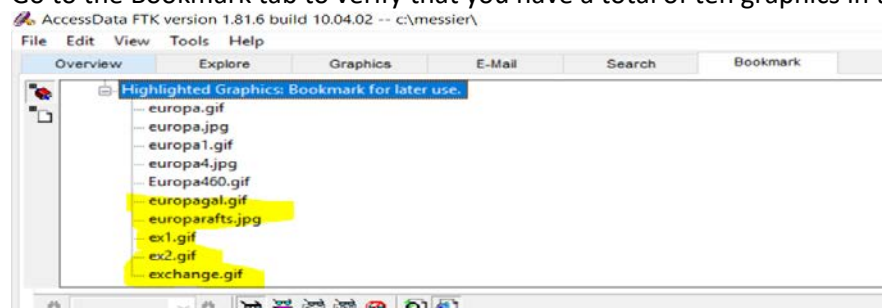


d. Adding file to existing bookmark.

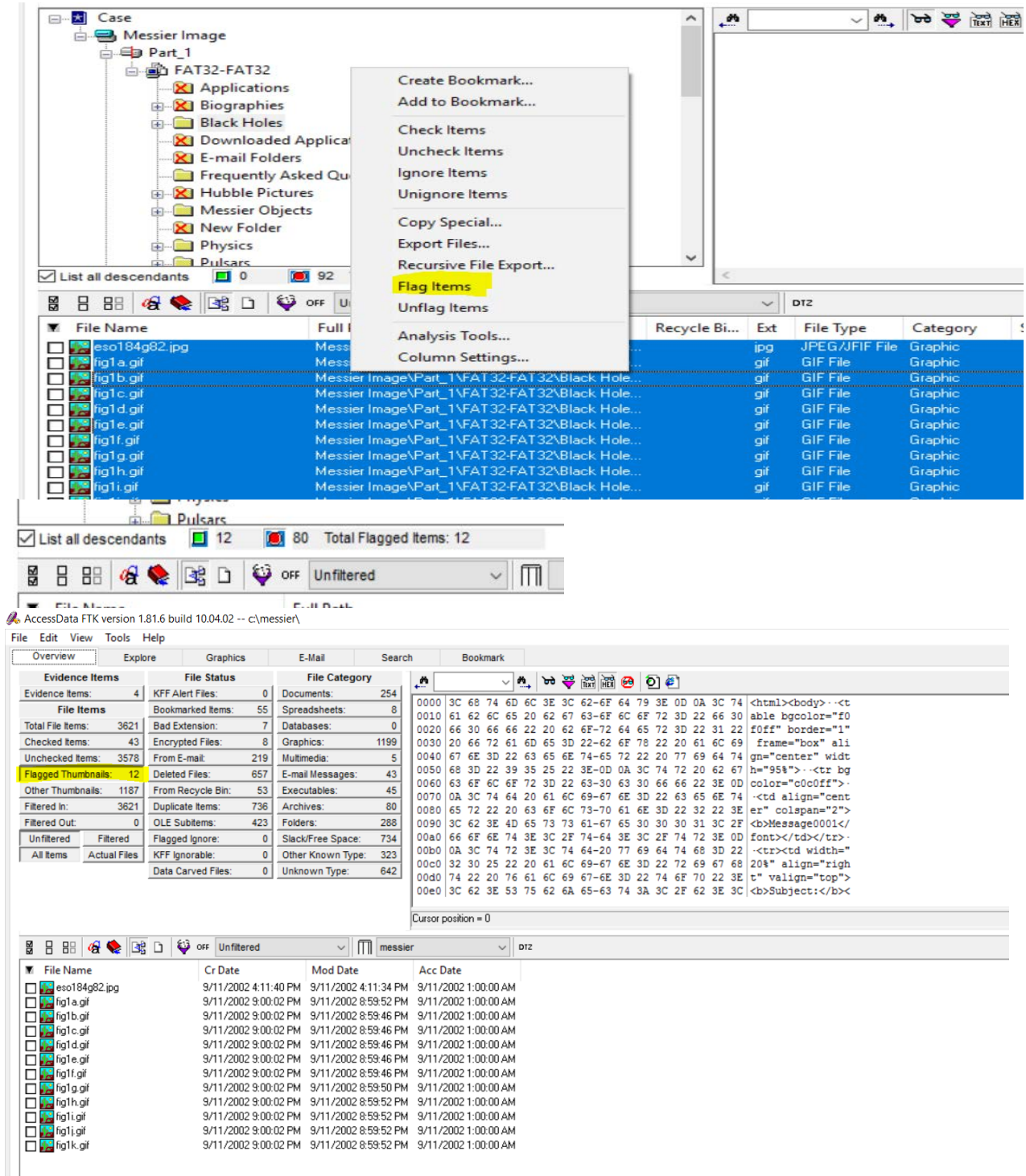
Click the Graphics Tab. Highlight five more graphics. Right-click the graphics and select Add to Bookmark. In the Add Files to Bookmark menu, select Highlighted Graphics. Then click OK.



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

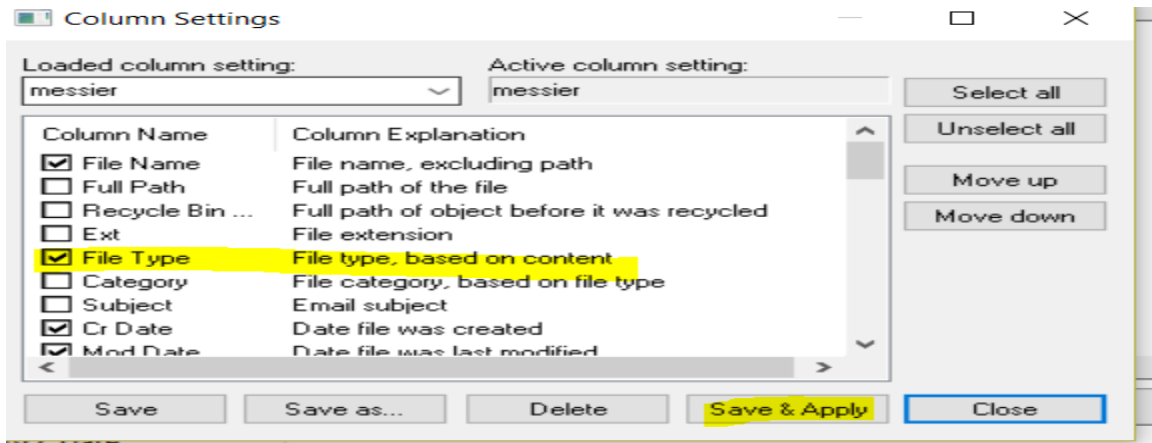
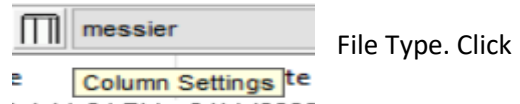


- e. Flag the files on graphics. Click the Graphics Tab. Flag twelve graphics green (click the red circles), these will be used later. Go to the Overview tab and select the Flagged Thumbnails container to verify that the graphics you just flagged are included.

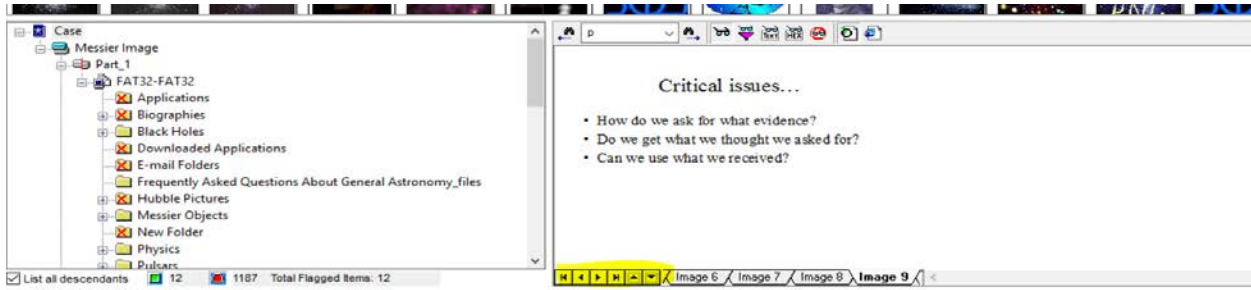


19. Add File Type to the Date and Time column settings.

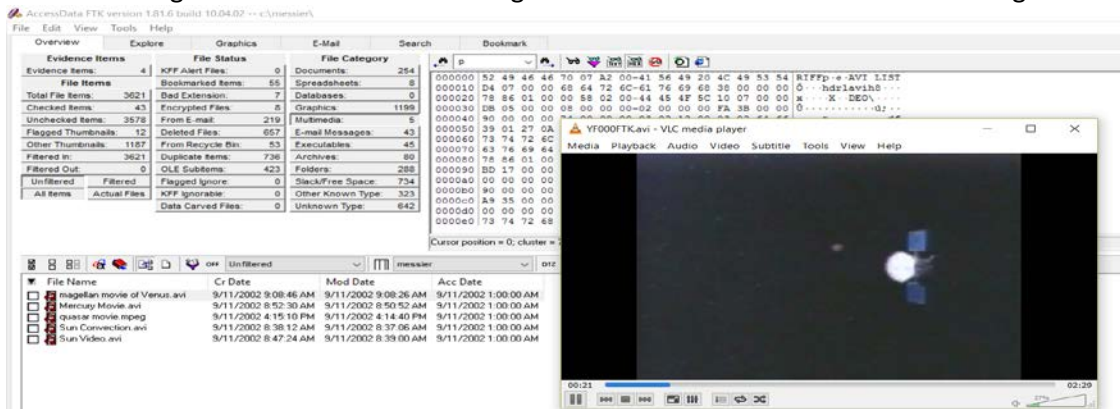
Note: The column settings are tab-independent.
 Click the Column Settings button on the toolbar Mark
 Save and Apply.



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."

AccessData FTK version 1.81.6 build 10.04.02 -- c:\messier\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	4	KFF Alert Files:	0	Documents:	254
File Items		Bookmarked Items:	55	Spreadsheets:	8
Total File Items:	3621	Bad Extension:	7	Databases:	0
Checked Items:	43	Encrypted Files:	8	Graphics:	1199
Unchecked Items:	3578	From E-mail:	219	Multimedia:	5
Flagged Thumbnails:	12	Deleted Files:	657	E-mail Messages:	43
Other Thumbnails:	1187	From Recycle Bin:	53	Executables:	45
Filtered In:	3621	Duplicate Items:	736	Archives:	80
Filtered Out:	0	OLE Subitems:	423	Folders:	288
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	734
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	323
		Data Carved Files:	0	Unknown Type:	642

Error
View window could not view this file.

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

AccessData FTK version 1.81.6 build 10.04.02 -- c:\messier\

File Edit View Tools Help

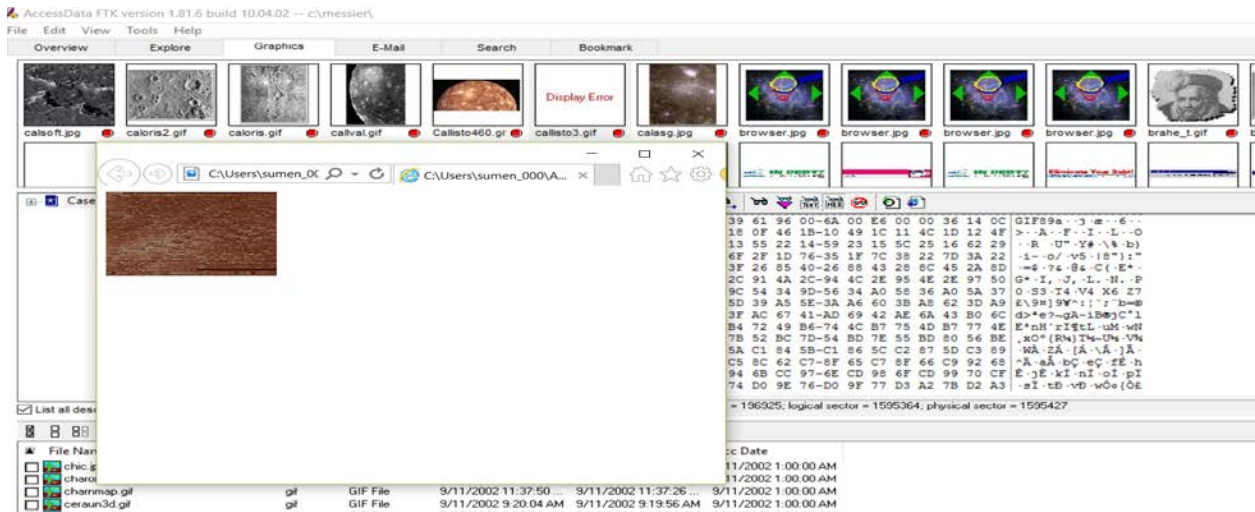
Overview Explore Graphics E-Mail Search Bookmark

File Name	File Type	Cr Date	Mod Date	Acc Date
callisto3.gif	GIF File	9/11/2002 11:12:30 ...	9/11/2002 11:12:28 ...	9/11/2002 1:00:00 AM
Callisto460.gif	GIF File	9/11/2002 11:12:30 ...	9/11/2002 11:12:28 ...	9/11/2002 1:00:00 AM
Callisto_files	Folder	9/11/2002 11:12:30 ...	9/11/2002 11:12:32 ...	9/11/2002 1:00:00 AM

calsoft.jpg caloris2.gif caloris.gif callval.gif Callisto460.gif **callisto3.gif** calas.jpg browser.jpg brows

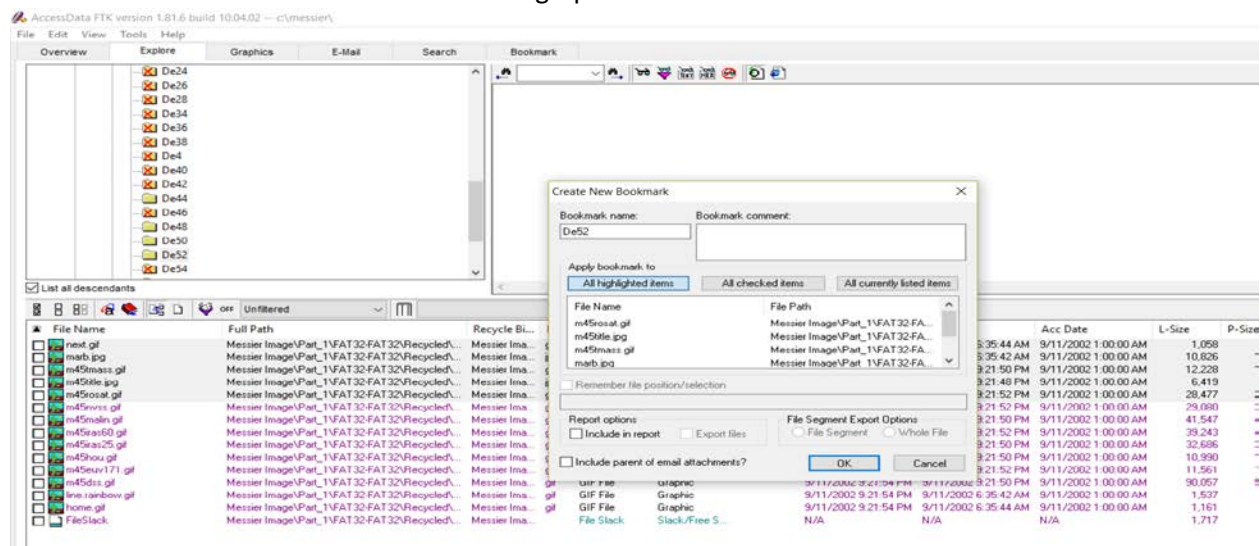
Case

Right-click the thumbnail and view with your browser.

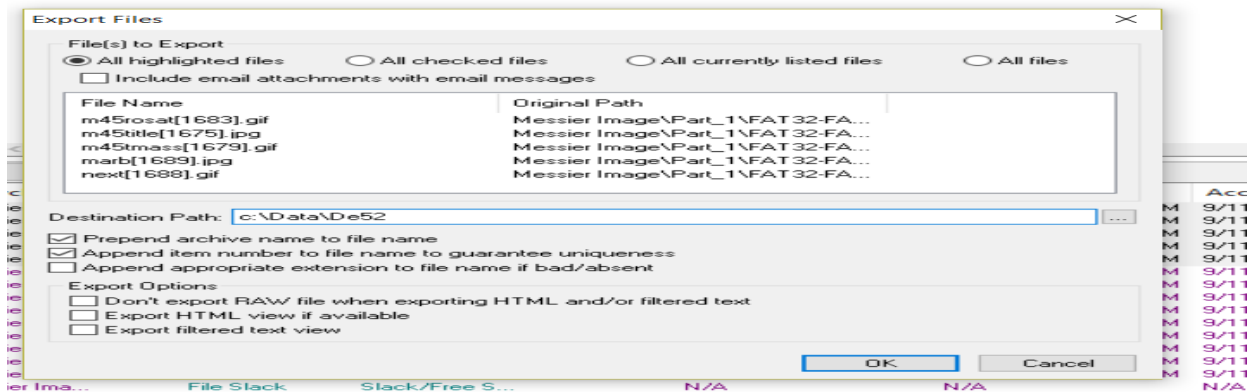


PRACTICAL: IDENTIFYING, BOOKMARKING, AND EXPORTING GRAPHICS FILES

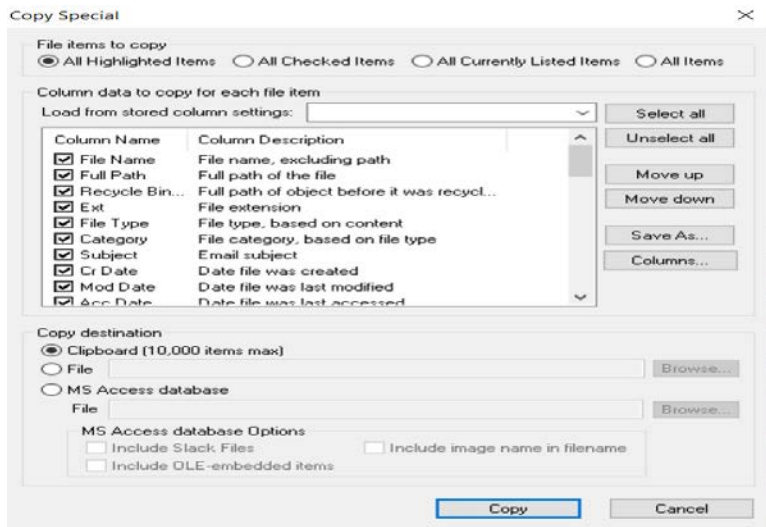
1. Navigate to \Recyclef\J)e52 on FAT32-FAT32. Select at least five graphics. Create a bookmark name De52 add those graphics to the bookmark.



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.



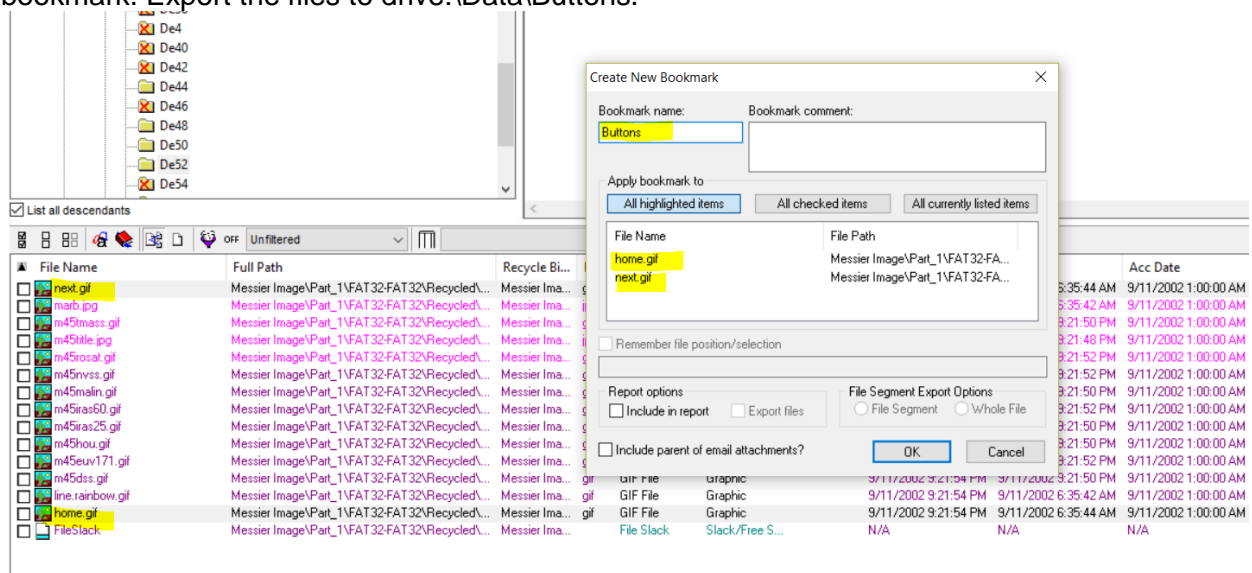
Book1 - Excel

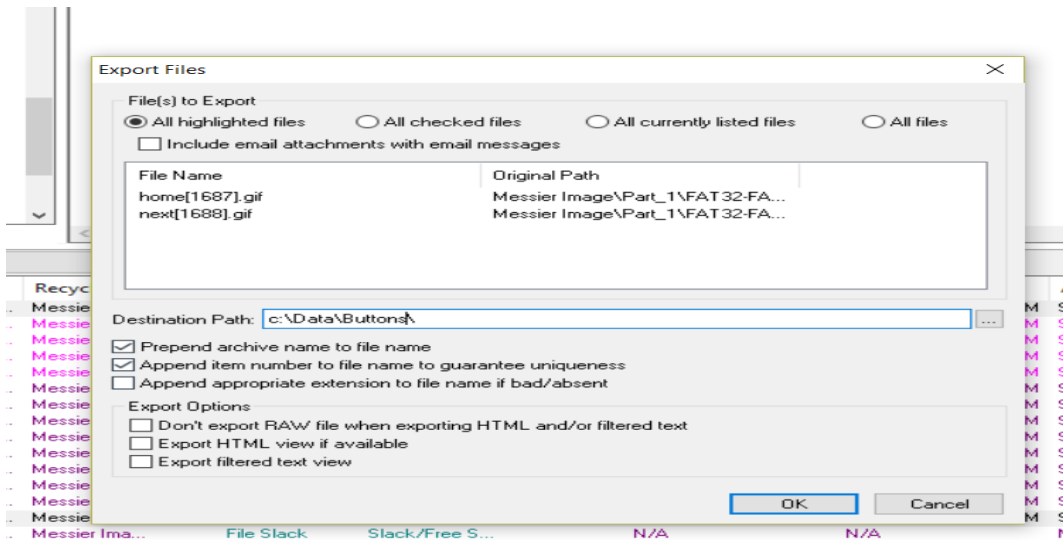
File Home Insert Page Layout Formulas Data Review View Tell me what you want to do

H12

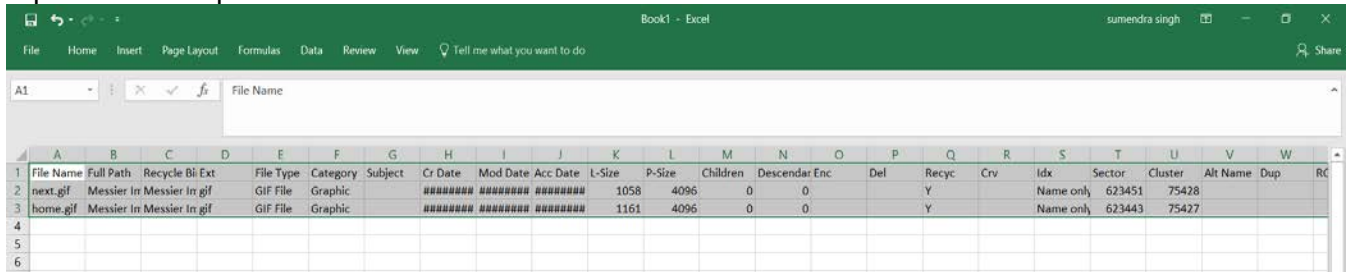
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	File Name	Full Path	Recycle Bin	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Children	Descendar	Enc	Del	Recyc	Crv	Idx	Sector	Cluster	Alt Name	Dup	RC
2	next.gif	Messier Im	Messier In	gif	GIF File	Graphic		#####	#####	#####	1058	4096	0	0			Y		Name only	623451	75428			
3	marb.jpg	Messier Im	Messier In	jpg	GIF File	Graphic		#####	#####	#####	10826	12288	0	0			Y		Name only	623459	75429			
4	m45tmas	Messier Im	Messier In	gif	GIF File	Graphic		#####	#####	#####	12228	12288	0	0			Y		Name only	623123	75387			
5	m45title.j	Messier Im	Messier In	jpg	JPEG/JFIF	Graphic		#####	#####	#####	6419	8192	0	0			Y		Full	622819	75349			
6	m45rosat	Messier Im	Messier In	gif	GIF File	Graphic		#####	#####	#####	28477	28672	0	0			Y		Name only	623291	75408			
7																								
8																								

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.

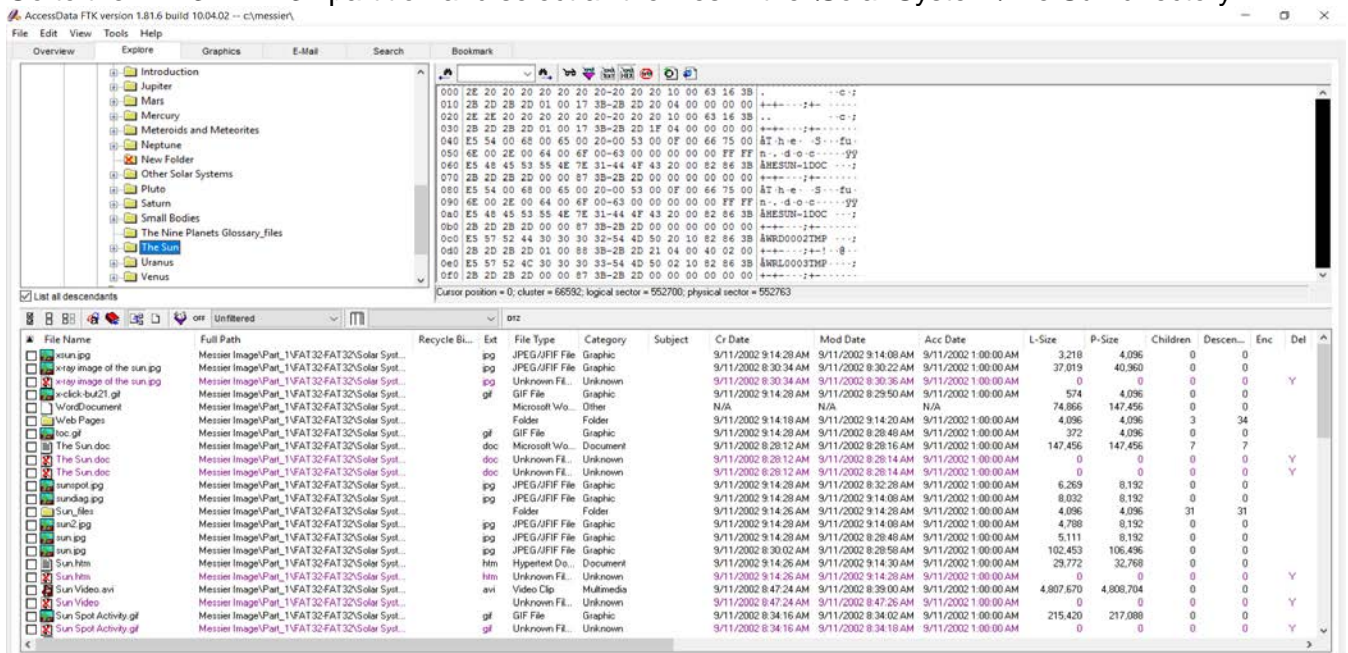




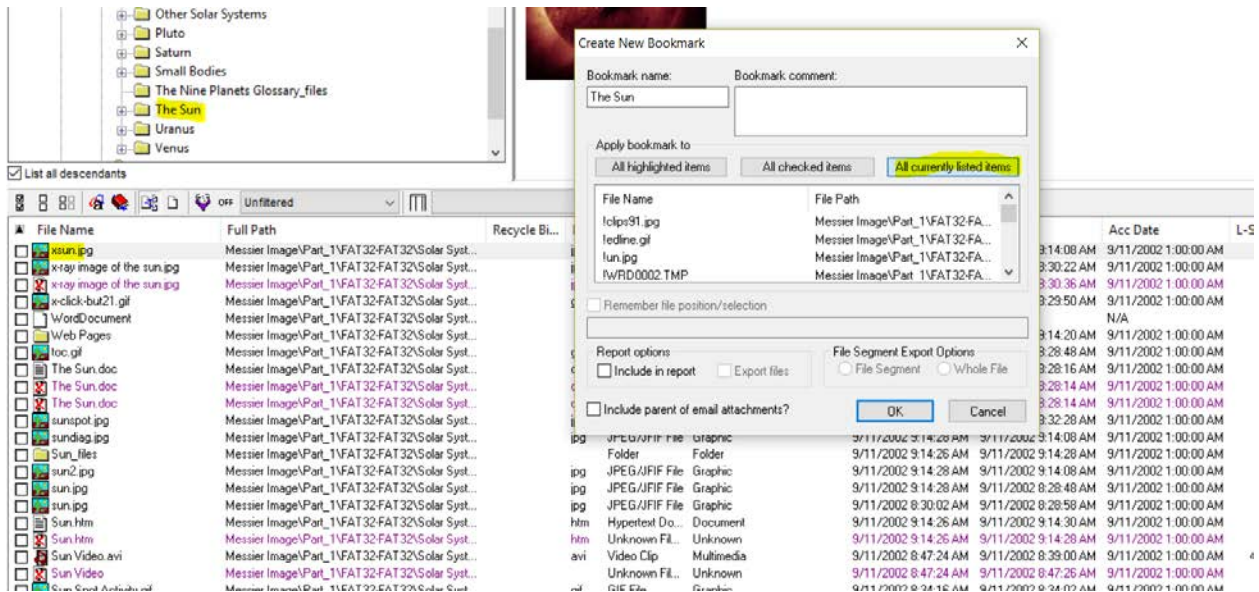
Use Copy Special to copy a list of the dates and times associated with the exported files to the clipboard. Then paste this data into Microsoft Excel.



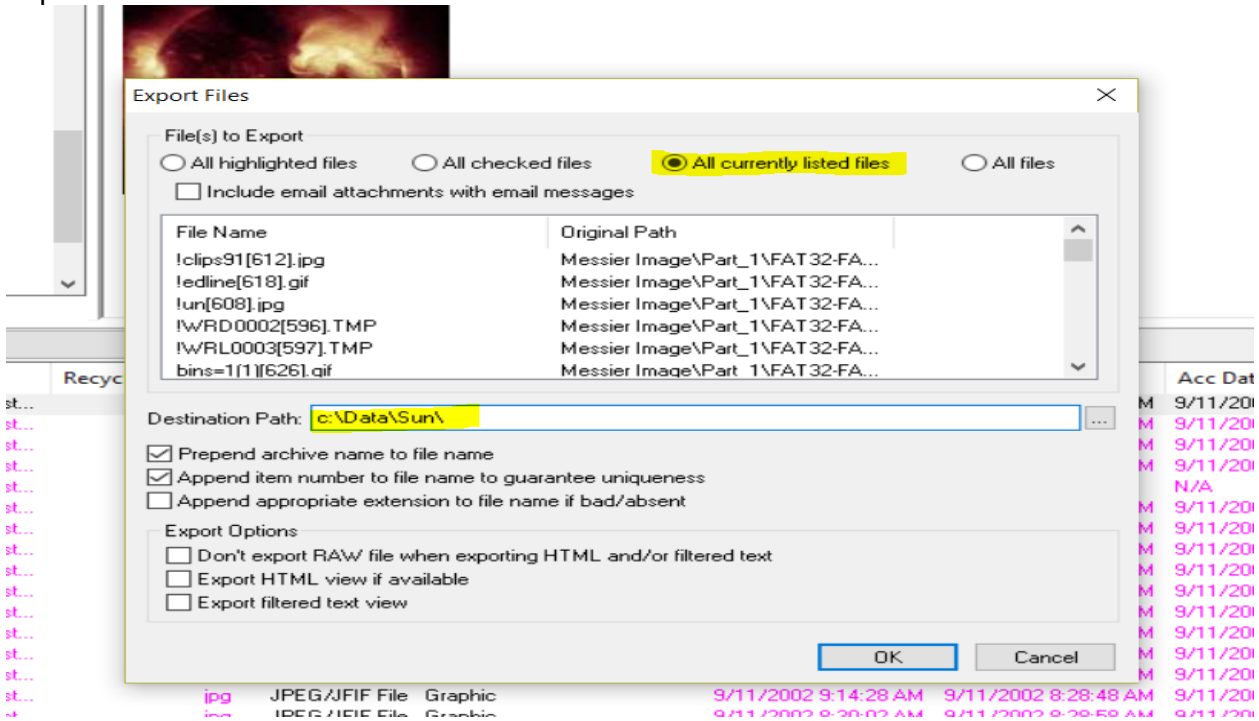
Go to the FAT32-FAT32 partition and select all the files in the \Solar System\The Sun directory.



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.