

Processing Crime and Incident Scenes

4

By the end of the practical session, the students should be able to:

- ✚ Identify file metadata
- ✚ Review a case to identify requirements and plan the investigation

This lab will cover topics on understanding how to process a computer investigation scene.

4.0 Introduction

Digital evidence is anything stored or transmitted on electronic or optical media. It's extremely fragile and easily altered. Evidence rules are critical, whether on a corporate or a criminal case. Furthermore, a civil case can quickly become a criminal case, and a criminal case can have civil implications larger than the criminal case.

Lab 4.1: Identifying File Metadata

4.1.1 Task

1. Start Microsoft Word, and in a new document, type **By creating a file, you can identify the author with file metadata**. Save it in your work folder as Lab4-01.docx (or Lab4-01.doc in earlier Word versions), and then exit Microsoft Word.
2. To start FTK, click Start, point to **All Programs**, point to **AccessData**, point to **Forensic Toolkit**, and run as administrator. If you are prompted with a warning dialog box and/or notification, click OK to continue, and click OK, if necessary, in the message box thanking you for evaluating the program.

3. Click **Go directly to working in program**, and then click **OK**. Click **File, Add Evidence** from the menu.
4. In the Add Evidence dialog box, enter your name as the investigator, and then click **Next**. In the Evidence Processing Options dialog box, accept the default setting, and then click **Next**.
5. In the main Add Evidence to Case dialog box, click the **Add Evidence** button. In the next Add Evidence to Case dialog box, click the **Individual File** option button, and then click **Continue**.
6. In the Browse for Folder dialog box, navigate to your work folder, click **Lab4-01.doc**, click **Open**, and then click **OK**. Click **Next**, and then click **Finish**.
7. In the main window, click the **Overview** tab, if necessary. Under the File Category heading, click the **Documents** button. Click to select the **Lab4-01.docx** (or Lab04-doc) file in the bottom pane; its contents are then displayed in the upper-right pane. Figure 4.1 shows an example (although the filename in this figure is different).

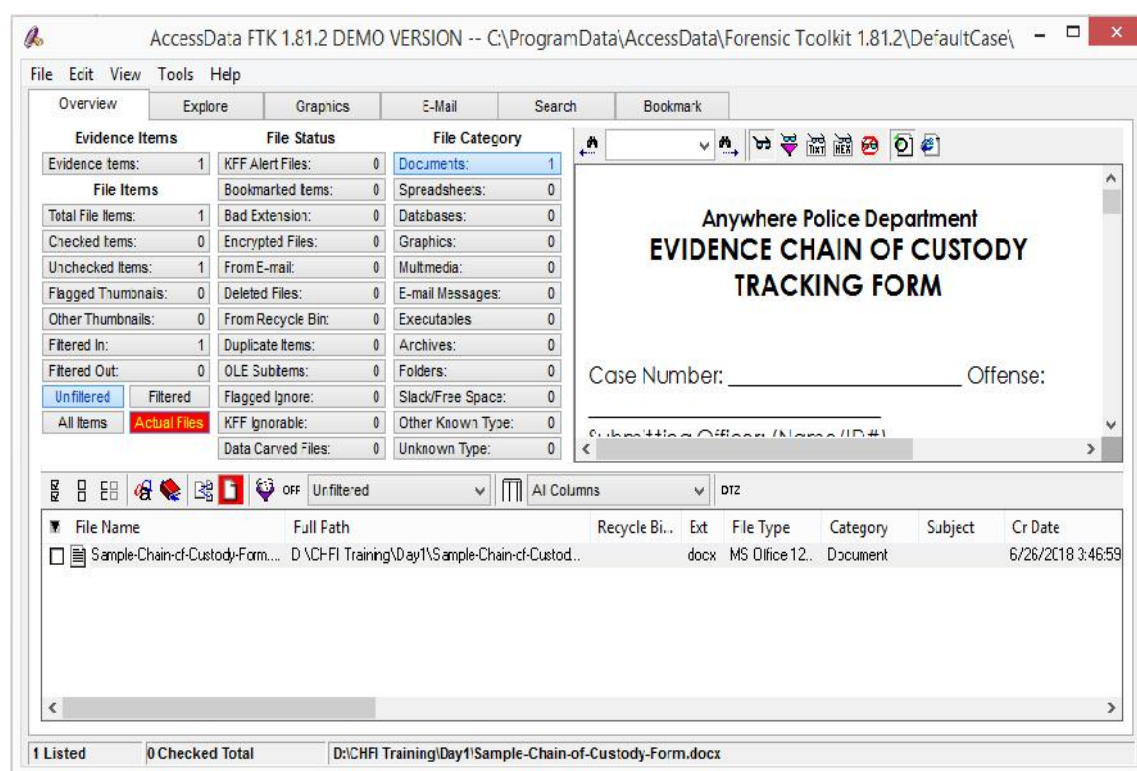


Figure 4.1 Selecting a document

8. On the File List toolbar at the upper right, click the **View files in native format** button, if the button isn't already selected. (Hint: Hover your mouse over buttons to see their names displayed.)
9. Next, click the **View files in filtered text format** button. If you entered your username and organization when you installed Word, that information is displayed as depicted in Figure 4.2.

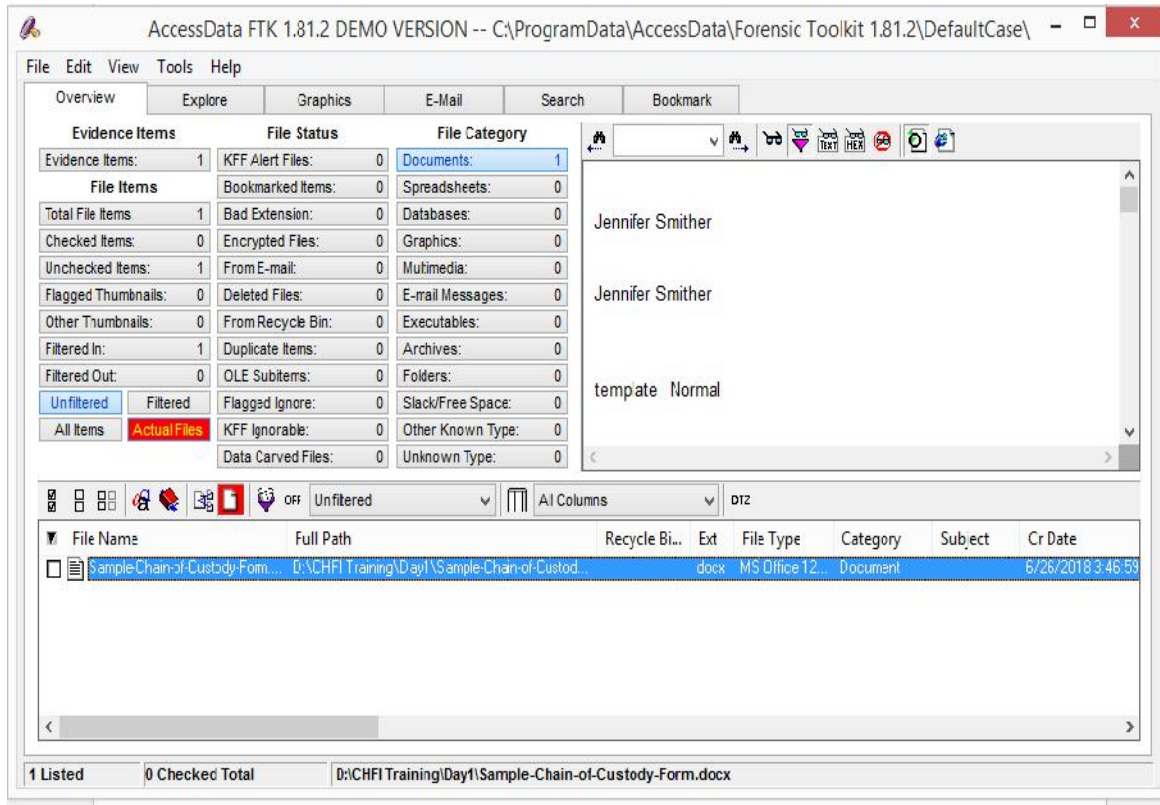


Figure 4.2 Viewing file metadata

10. Exit FTK, clicking **No** if prompted to back up your work.

Based on the task above, describe:

- a. What is metadata?
- b. The significant of identifying file metadata in forensics investigation process.

Lab 4.2: Reviewing a Case

In this lab, you apply each task learn in Chapter 2 task to a hypothetical investigation to create a preparation plan for searching an incident or crime scene. The general tasks you perform in any computer forensics case are:

- Identify the case requirements
- Plan your investigation
- Conduct the investigation
- Complete the case report
- Critique the case

Case:

A company called Superior Bicycles, with a Web site at www.superiorbicycles.biz, specializes in creating new and inventive modes of human-driven transportation. Two employees, Chris Murphy and Nau Tjeriko, have been missing for several days. A USB drive has been recovered from Chris's office with evidence that he had been conducting a side business using company computers. Steve, a manager, talks to other employees, but no one knows why Chris and Nau aren't at work. To learn where Nau might be, Steve searches the surface of her desk and notices travel brochures for European tours. Steve also looks around Chris's office again and finds notes about a Swiss supplier Steve once used and another USB drive with the supplier's name on the label. Steve suspects the USB drive contains more information and calls you, the computing investigator for his company. He describes Chris and Nau's absence from the company and asks you to examine the USB drive to see whether it identifies their whereabouts.

4.2.1 Task 1: Identifying the case requirements

Before you analyze the USB drive, answer the following basic questions to start your investigation:

1. What is the nature of the case?
2. What are their names?
3. What do they do?
4. What is the OS of the suspect computer?
5. What type of media needs to be examined?
6. What is the suspect computer's configuration, such as type, CPU speed, and hard drive size?

4.2.2 Task 2: Planning the investigation

To find information about Chris and Nau's whereabouts, list what you can assume or already know about the case such as:

- Chris and Nau's absences might or might not be related.
- Chris's computer might contain information explaining their absence.
- No one else has used Chris's computer since he disappeared.

4.2.3 Task 3: Conducting the Investigation

In this task activities, use forensics tool to extract and analyze an image file. The requirements of this task is shown in Table 1.

Table 1: Requirements

Tool	Image
FTK Toolkit	Lab4-02.001

Notes: Please download the tools and images from your lecturer's PC.

Task 3.1: Acquiring Evidence with AccessData FTK

1. To start FTK, click **Start**, point to **All Programs**, point to **AccessData**, point to **Forensic Toolkit**, and click **Forensic Toolkit**. If you are prompted with a warning dialog box and/or notification, click **OK** to continue, and click **OK**, if necessary, in the message box thanking you for evaluating the program.
2. In the AccessData FTK Startup dialog box, click the **Start a new case** option button, and then click **OK**.
3. In the New Case dialog box, enter your name as the investigator, **Lab4-02** as the case number, and a suitable case name, and then click **Next**.
4. Fill out the information in the Forensic Examiner Information dialog box as you want it to appear in your final report, and then click **Next** until you reach the Evidence Processing Options dialog box. Make sure the Data Carve check box is *not* selected because this option makes processing take much longer; you can always do data carving later, if necessary. Then click **Next**.

5. In the Refine Case - Default dialog box, click the **Include All Items** button as shown in Figure 4.3, and then click **Next**.

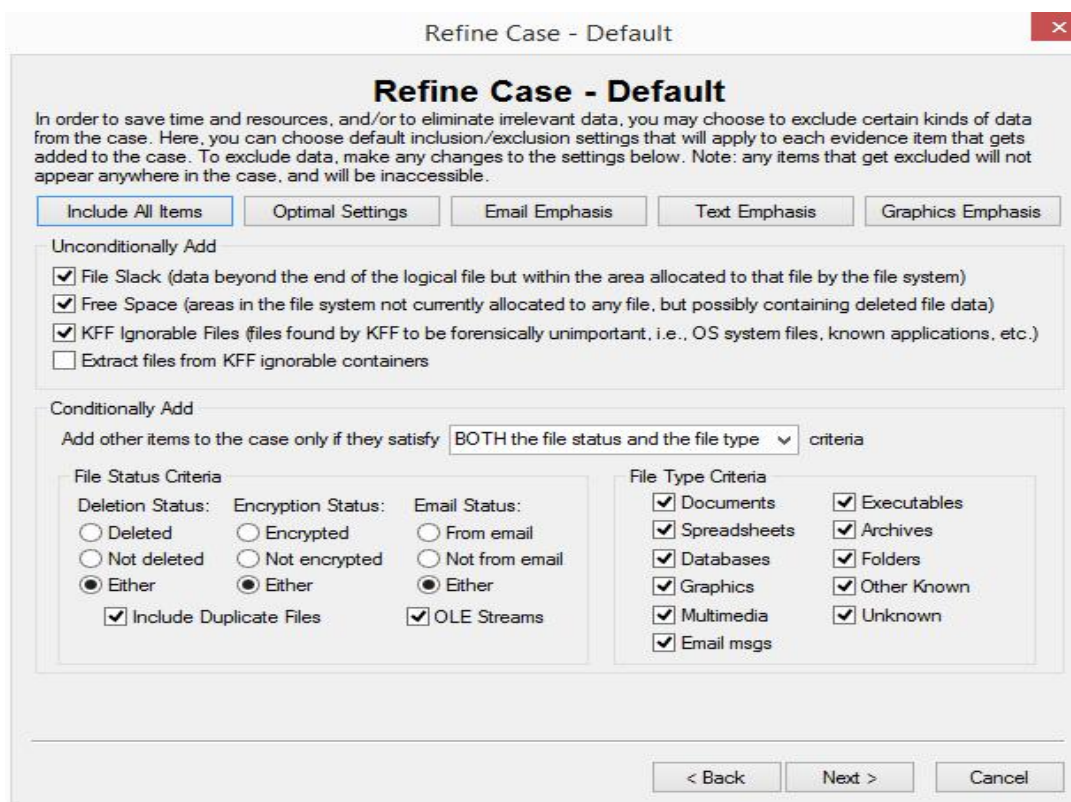
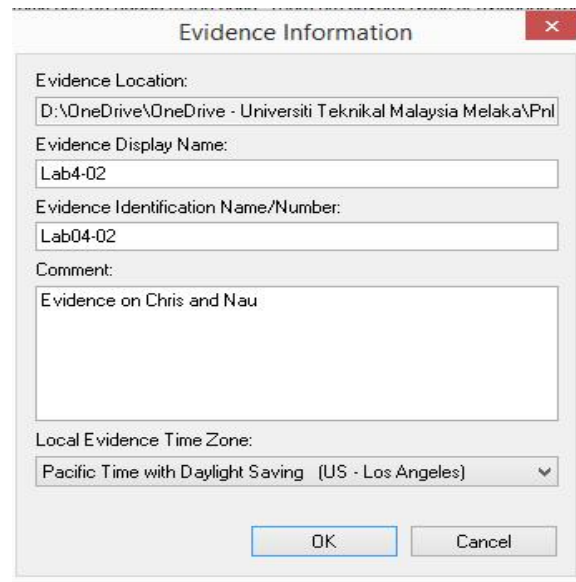


Figure 4.3 The Refine Case – Default dialog box

6. In the Refine Index - Default dialog box, accept the default settings, and then click **Next**.
7. In the main Add Evidence to Case dialog box, click the **Add Evidence** button.
8. In the second Add Evidence to Case dialog box, click the **Acquired Image of Drive** option button, and then click **Continue**.
9. In the Open dialog box, navigate to your work folder, click to select the **Lab4-02.001** file, and then click **Open**.
10. In the Evidence Information dialog box, enter the additional information, using Figure 4.4 as a guideline. Click the **Local Evidence Time Zone** list arrow at the bottom, click the suspect's time zone in the drop-down list, and then click **OK**.



Evidence Information

Evidence Location:
D:\OneDrive\OneDrive - Universiti Teknikal Malaysia Melaka\Ph

Evidence Display Name:
Lab4-02

Evidence Identification Name/Number:
Lab04-02

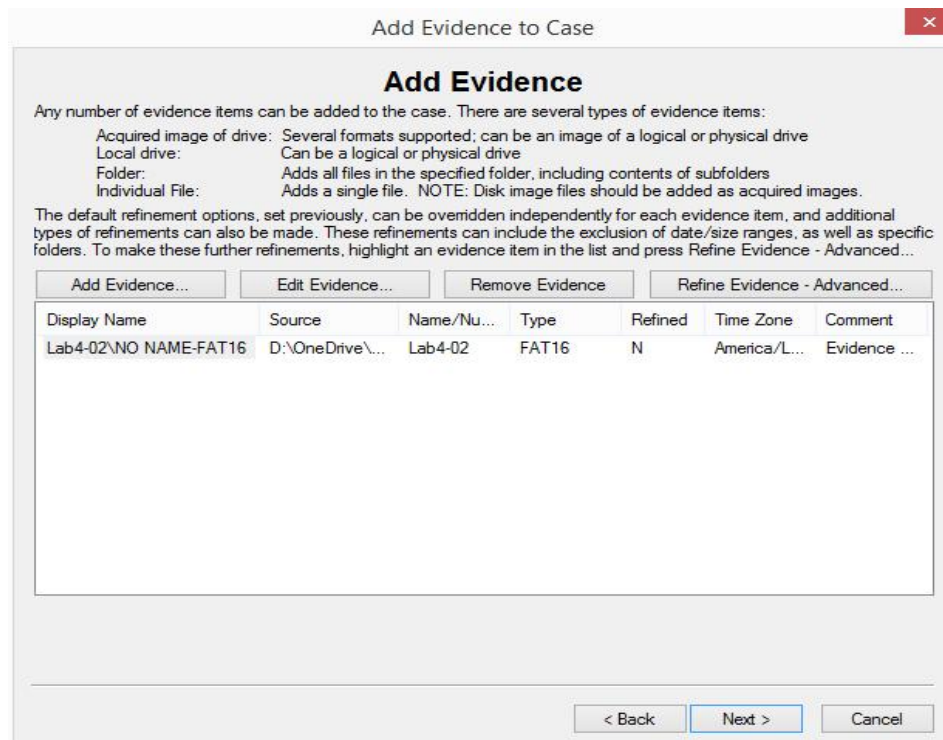
Comment:
Evidence on Chris and Nau

Local Evidence Time Zone:
Pacific Time with Daylight Saving (US - Los Angeles)

OK Cancel

Figure 4.4 The Evidence Information dialog box

11. In the main Add Evidence to Case dialog box, shown in Figure 4.5, accept the default settings, and then click **Next**.



Add Evidence to Case

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
Lab4-02\NO NAME-FAT16	D:\OneDrive\...	Lab4-02	FAT16	N	America/L...	Evidence ...

< Back Next > Cancel

Figure 4.5 The Add Evidence to Case Dialog box with image file listed

12. In the Case Summary dialog box depicted in Figure 4.6, click **Finish** to initiate the analysis. FTK then performs several steps of cataloging data and indexing every word in the Lab4-02.001 image file.

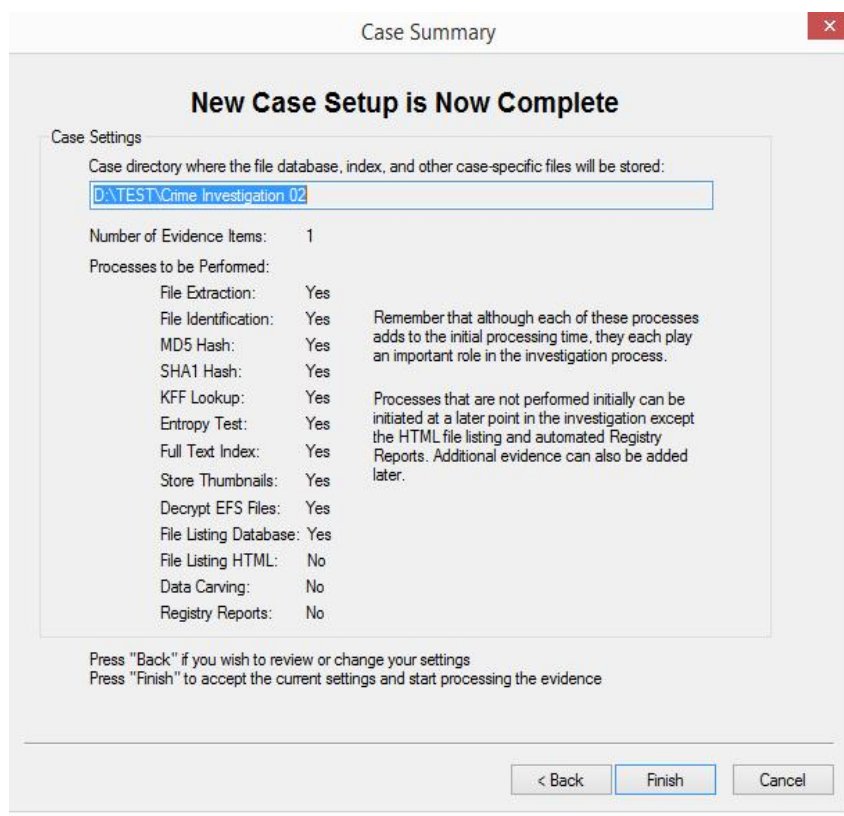


Figure 4.6 The Case Summary dialog box

13. The cataloging process organizes and lists each file in its own section for follow-up analysis as shown in Figure 4.7. The indexing feature creates a database of every word in the image file with its exact location so that you can easily look up keywords of interest to the investigation.
14. When FTK finishes cataloging and indexing, the FTK window opens to the Overview tab. To analyze an image with FTK, click the **Explore** tab. In the upper-left pane (the tree view), click to expand a folder, if needed, and then click the **List all descendants** check box.
- What happen if you are navigating between the Explore, Graphics and E-mail tabs in the FTK Window?

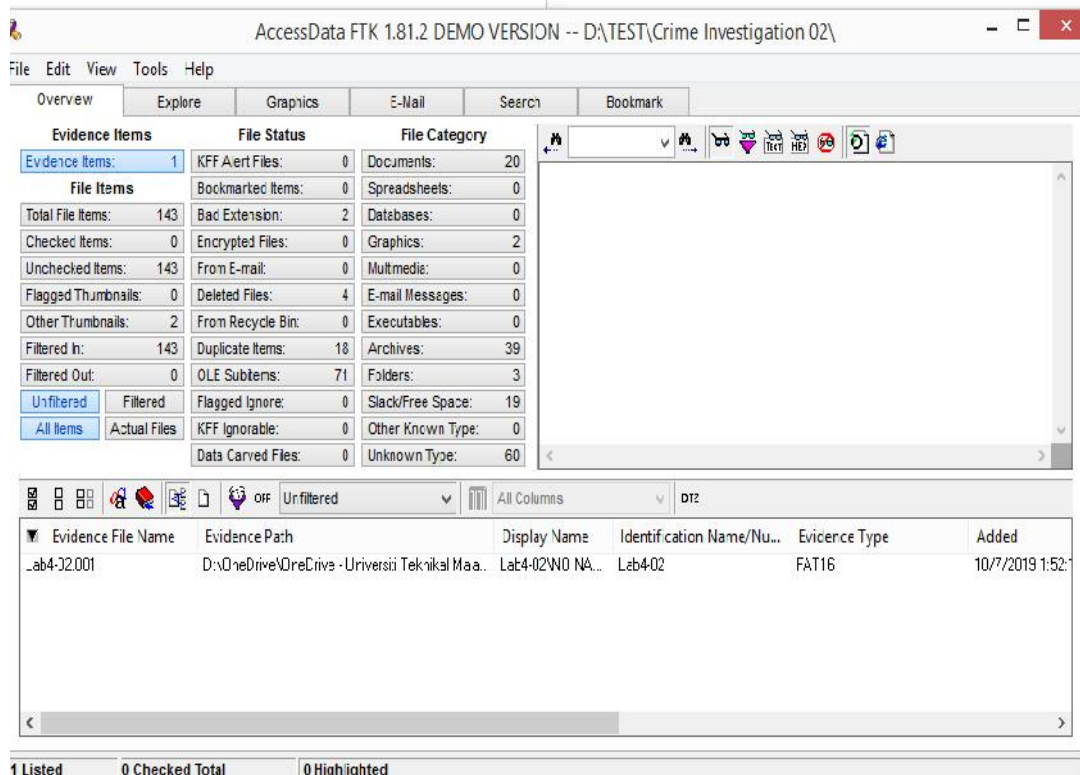


Figure 4.7 After cataloging process

15. Navigate through each file in the lower pane by clicking the filenames one at a time. The upper-right pane displays any data in the files. For example, Figure 4.8 shows the data for the PICT0059.jpg file selected in the lower pane. For this task, please select PICT0032.jpg. Review this data to see what information can be retrieved from this image.
16. When you have located a file containing information you think is important, click the check box next to the filename in the lower pane. Continue searching for more information, and select any additional files of interest.
17. After you have selected all files of interest, click **Tools, Create Bookmark** from the menu. In the Create New Bookmark dialog box, type a bookmark name and any comments. Then click the **All checked items** button, click the **Include in report** and **Export files** check boxes as illustrated in Figure 4.9, and click **OK**. (Please describe the purpose of bookmarks in FTK.)

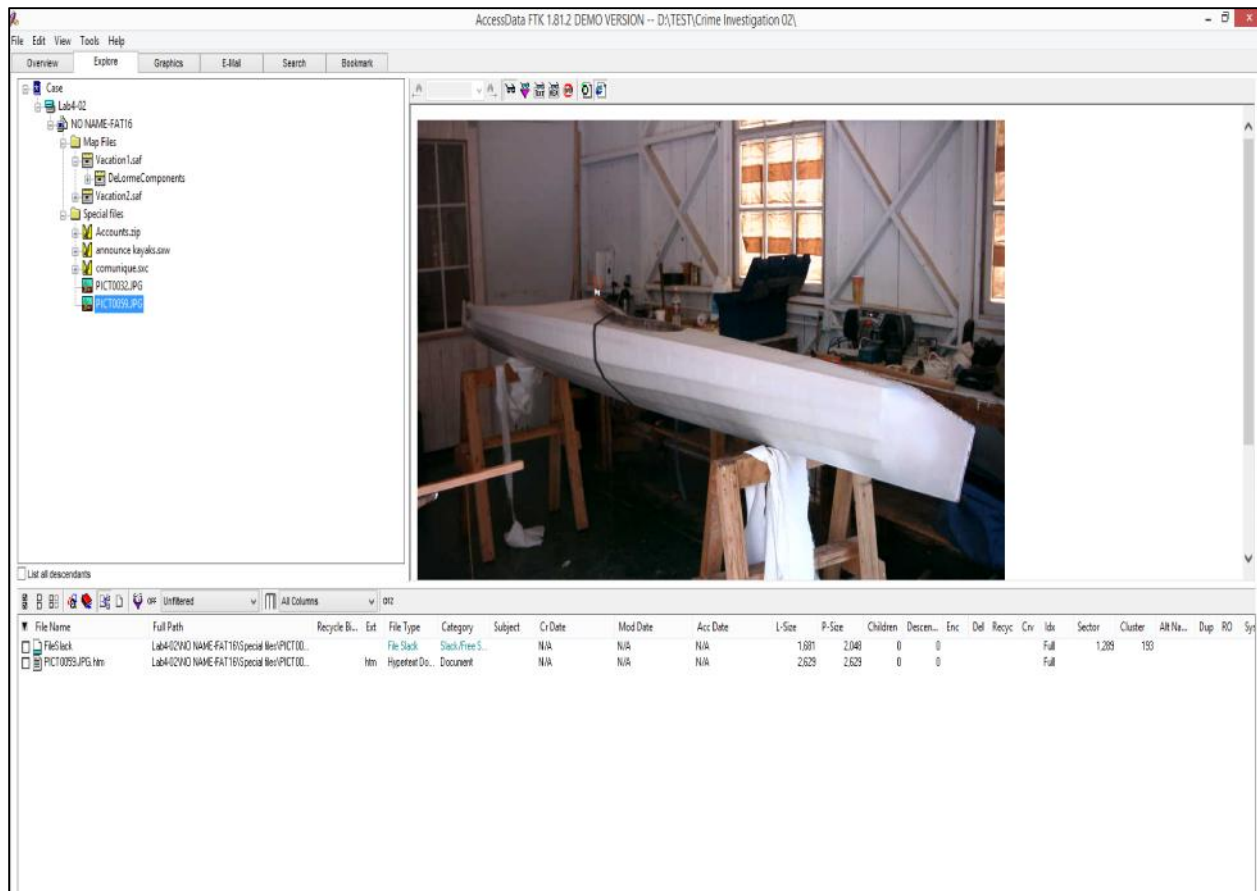


Figure 4.8 Selecting files of interests

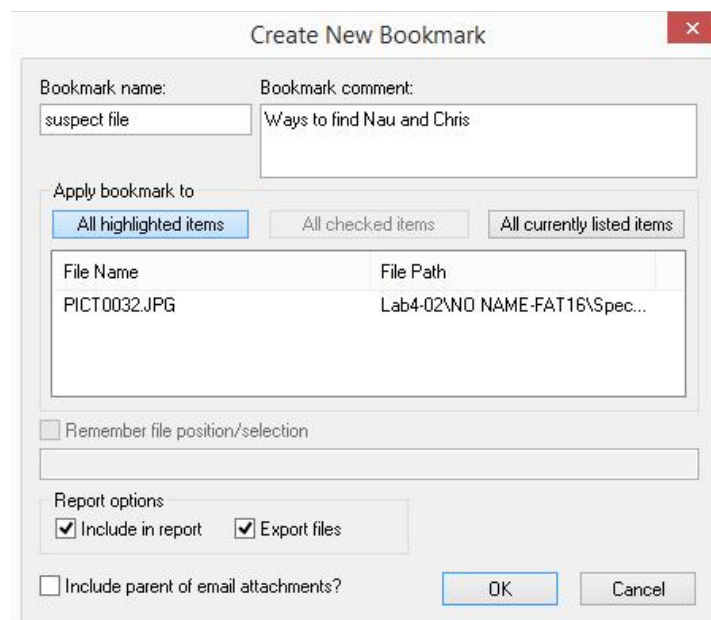


Figure 4.9 The Create New Bookmark dialog box

18. After you have bookmarked key files containing possible evidence, click **File, Report Wizard** from the menu. In the Case Information dialog box, click to select the **Include Investigator Information** in report check box (if necessary), click to select the investigator's name in the drop-down list box, and then click **Next**.
19. In the Bookmarks - A window, click **Next**. Continue clicking **Next** through the remaining report wizard windows until you reach the Report Location window, and then click **Finish**.
20. When the Report Wizard displays a prompt asking whether you want to view the report, click **Yes** to see the report in your default Web browser. Click the links to view the report's contents, and then close your browser. When you're done, exit FTK by clicking **File, Exit** from the menu. If prompted to back up your case, click **No**.