How to Bookmark and Tag Your Findings

Bookmarking Data

As an examination is conducted, data is discovered that is of interest as potential evidence. This data may be in the form of document files, portions of files, images, and other objects. These items may be saved for inclusion in the examination report. These marked sections are referred to as "bookmarks." Bookmarks are saved in folders in the case file. They may be seen by selecting the **Bookmarks** link under Report on the case Home page.

Bookmarks can also contain comments and notes for tracking, accounting, and reporting purposes. Bookmarks may be placed into bookmark folders and give them names associated with meaningful aspects of the case. Case reporting templates are provided with EnCase® Forensic v7 (EnCase v7) to provide examples of how reports may be organized and customized. The Review Package function provided with EnCase v7 is used a method for exporting bookmarked data . This will be discussed later in this course.

Bookmarks are traditionally pointers to objects and/or data. For this reason, if a device or evidence file is removed from the case file, the bookmarks and search results that resolve within that device will be unavailable.

There are several different types of bookmarks. Methodologies to include these bookmarks within the case file are discussed within this lesson. These include but are not limited to:

- Notable file/single object
- File group/multiple selected/tagged objects
- Highlighted data
- Note

To access the Bookmarks tab, either select **View→Bookmarks**.

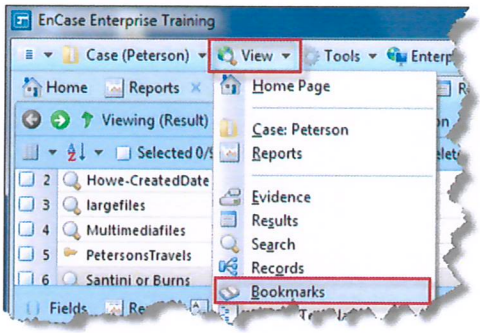

Figure 12-1 Access Bookmarks

Bookmarking a Single Item

Single-item bookmarks are used to identify individual files that contain information that is important to the current case. If the file is not an image file, the contents of the file will not be bookmarked; only the designated metadata information regarding a non-image file is displayed in the report. This type of bookmark is often used for marking non-image files that will be copied from the evidence file and placed on a CD for presentation to an attorney or case agent. It may also be used to show specific fields of important files.

Within our scenario, we have conducted keyword searches against Norm Peterson's media. Many discoveries have been made, including communication with Cliff Cavin, CEO of Bull and Finch Enterprises. Through analysis of some of this communication, it is suspected that Peterson has prepared a TrueCrypt volume with classified materials to sell to Cliff Cavin. A TrueCrypt Setup program was discovered in the root directory of Peterson's USB Flash Drive evidence file. We will bookmark this file.

Right-click on the **TrueCrypt Setup 6.3a.exe** object in the Table Pane and select **Bookmark→Single item...**

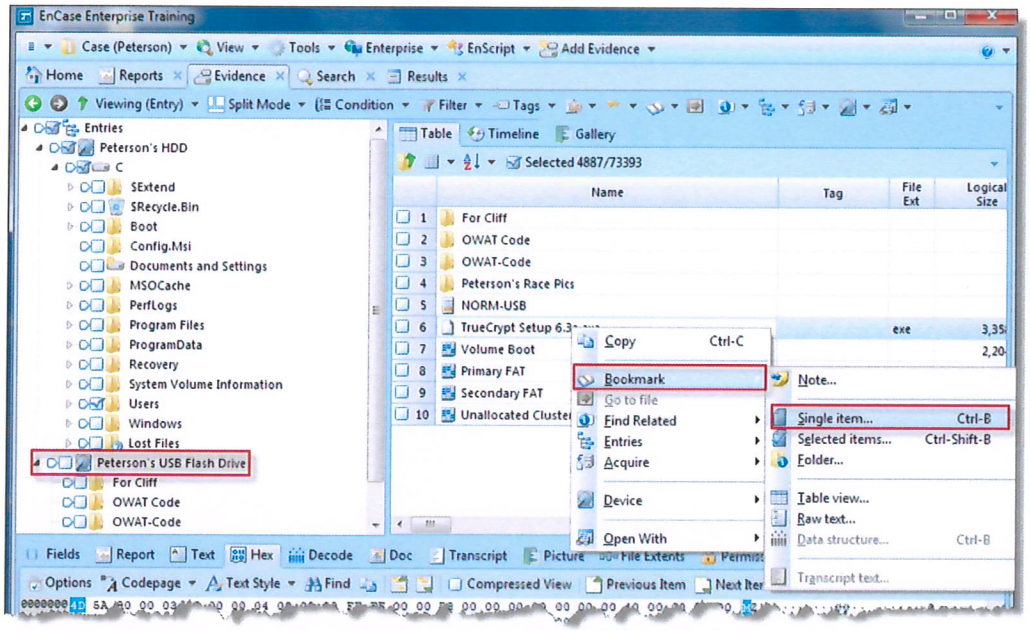

Figure 12-2 Bookmarking a Single Item...

A comment may be added to the bookmarked object(s). Previous comments may be recalled and added to bookmarked items. Add the comment "Installer for TrueCrypt Application." Click the **Destination Folder** tab after entering the comment.

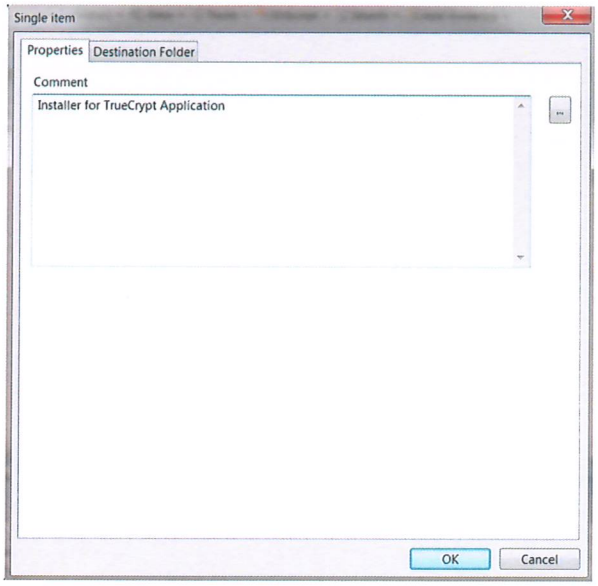

Figure 12-3 Bookmark comments

Choose the folder in the case template to add the bookmark. Add a new folder by typing the folder name. If adding a new folder, ensure the proper root folder is highlighted. In this case, we will place this application within the existing Documents folder. So, highlight the **Documents** folder and click **OK**.

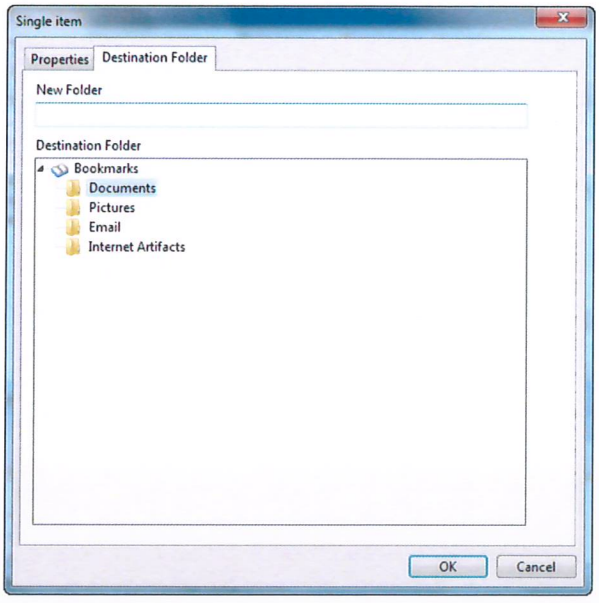

Figure 12-4 Select Bookmark Destination Folder

Verify the presence of the bookmark by accessing the Bookmarks tab (**View→Bookmarks**). Highlight the **Documents** folder in the Tree pane. The object should appear in the Table Pane. Select the **Report** view in the View Pane; the object name and the metadata the report template displays by default should appear. The contents of the single object do not appear in the Report view unless a Highlighted Data Bookmark is invoked or the object is an image file. Choose the **Evidence** tab to return to the display of the thumb drive.

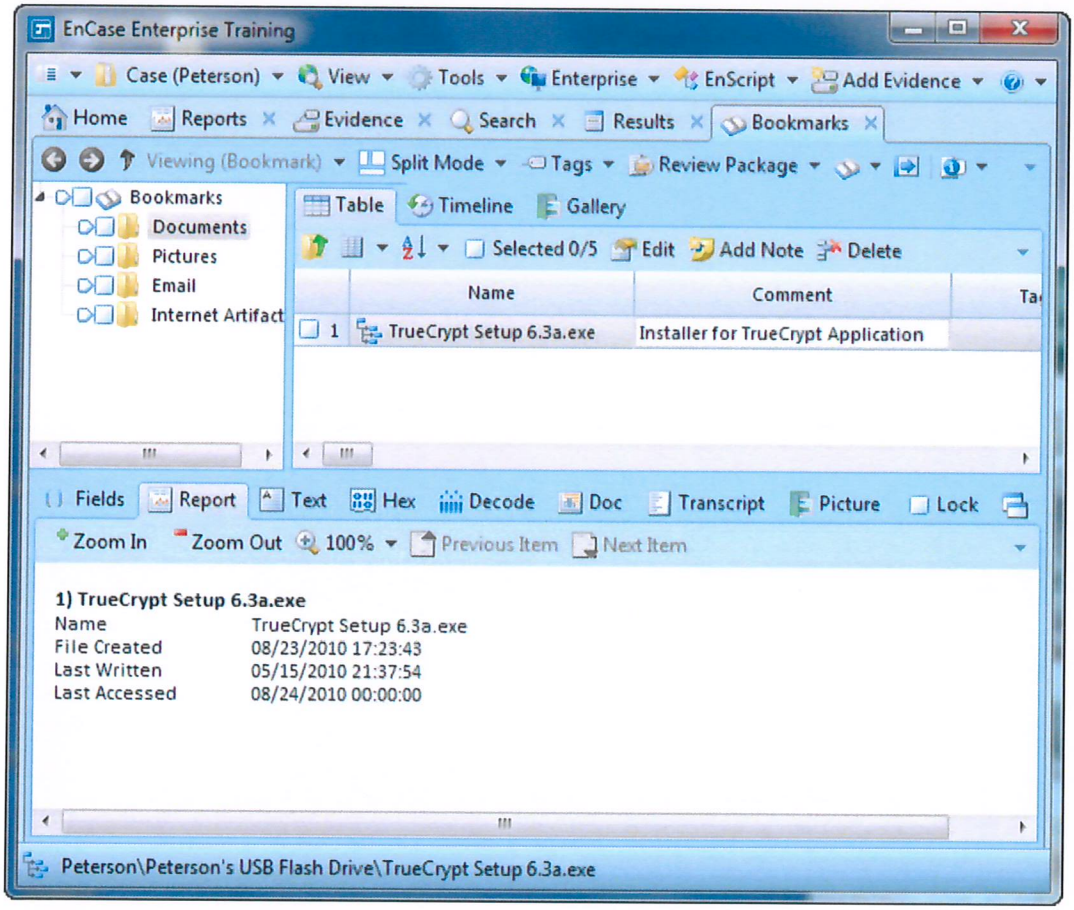

Figure 12-5 Display of Bookmark tab and Report view

Bookmark Multiple (Selected) Items

Selected items bookmarks are similar to single item bookmarks except that they are used to mark a group of files not a single, highlighted file. A group of files is normally bookmarked because of some distinct quality that exists in all the selected files. It may be that all the files are images or perhaps they were all created at the same time. Another possibility is that the files are all of the same type: accounts, checks, database files, etc.

Before beginning, ensure that no blue-check exists in the Selected or Dixon box. The first step is to select the files you wish to bookmark. From the **Evidence→Viewing (Entry)** view, blue-check several files to bookmark. The Selected/Dixon box will indicate how many files are blue-checked or selected. In this example, view Peterson's USB Drive and highlight the **Peterson's Race Pics** folder in the Tree Pane. These images may have some bearing on his using company funds for personal travel. Sort by the extension column in the Table Pane and scroll to the top of the list. There are two objects in this folder with the extension .AVI that appear to be videos; blue-check these two items and any other two images; the Dixon box should reflect four objects blue-checked. Right-click anywhere in the Table view and select **Bookmark→Selected Items...**

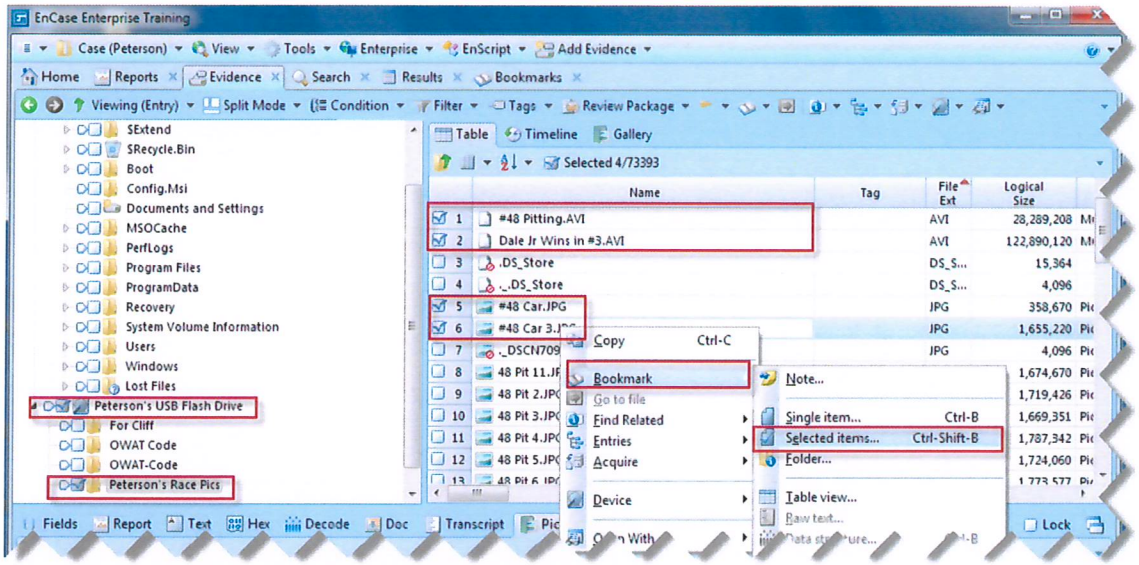

Figure 12-6 Select items; right-click; choose Bookmark→Selected Items...

Highlight the **Bookmarks** folder and enter the new folder name "Videos." Notice that no option for a comment is offered. Click **OK**.

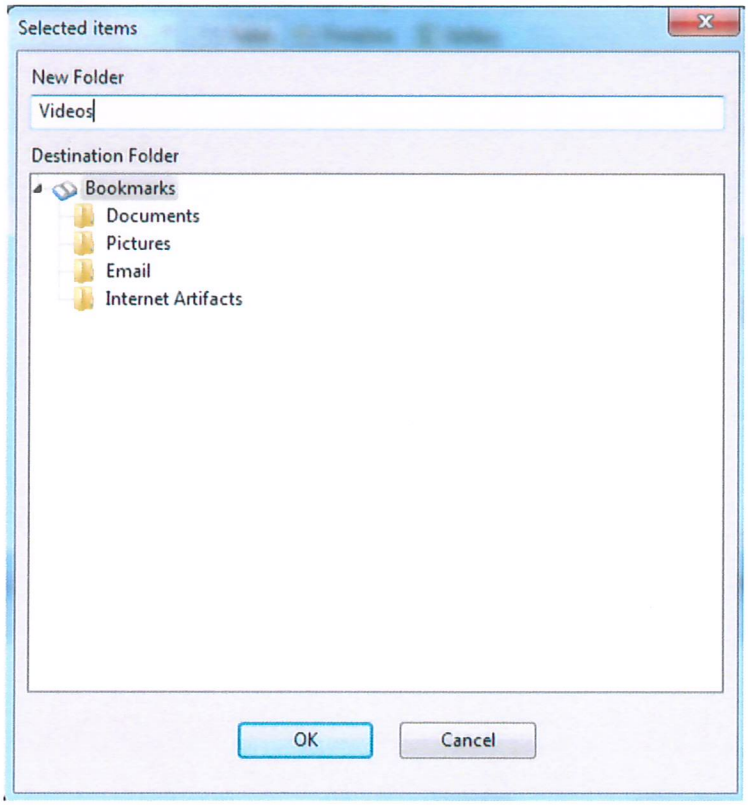

Figure 12-7 Bookmark Destination Folder

The Bookmarks tab displays the new folder and its contents. Highlight any object in the folder and the Report view in the View Pane; the object name and the default metadata should appear. Notice that the images represented by the JPG files appear in the report. Other metadata regarding bookmarked objects are included in the report by editing the report template.

Note Bookmark

From the Bookmarks view, the note bookmark provides more formatting flexibility than the other comment methods discussed thus far. This bookmark is designed for text data – up to one-thousand characters.

Highlight the **Videos** folder in the Tree Pane and highlight the first object in the Table Pane. Click on **Add Note** above the Table Pane.

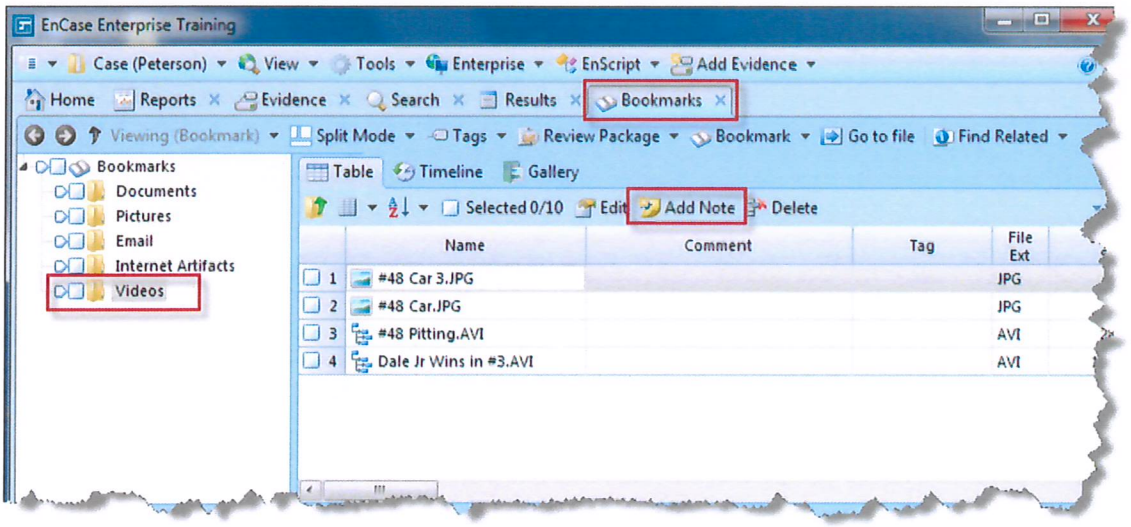

Figure 12-8 Add a Note Bookmark

Add the desired text and click **OK**. The Name field will identify the note bookmark so that it may be used for other items. The Comment field contains the actual notes made by the examiner. Enter any name and comment or enter the data below and click **OK**.

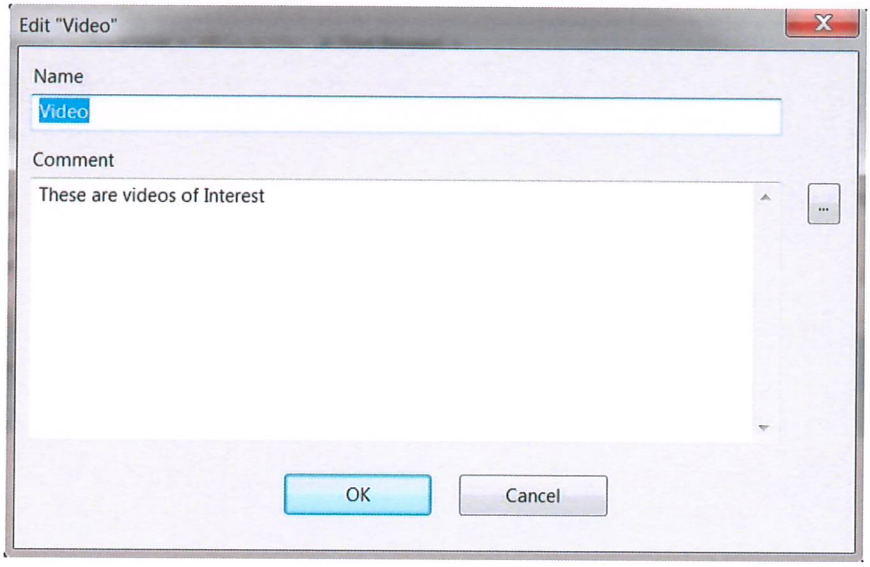

Figure 12-9 Note Bookmark

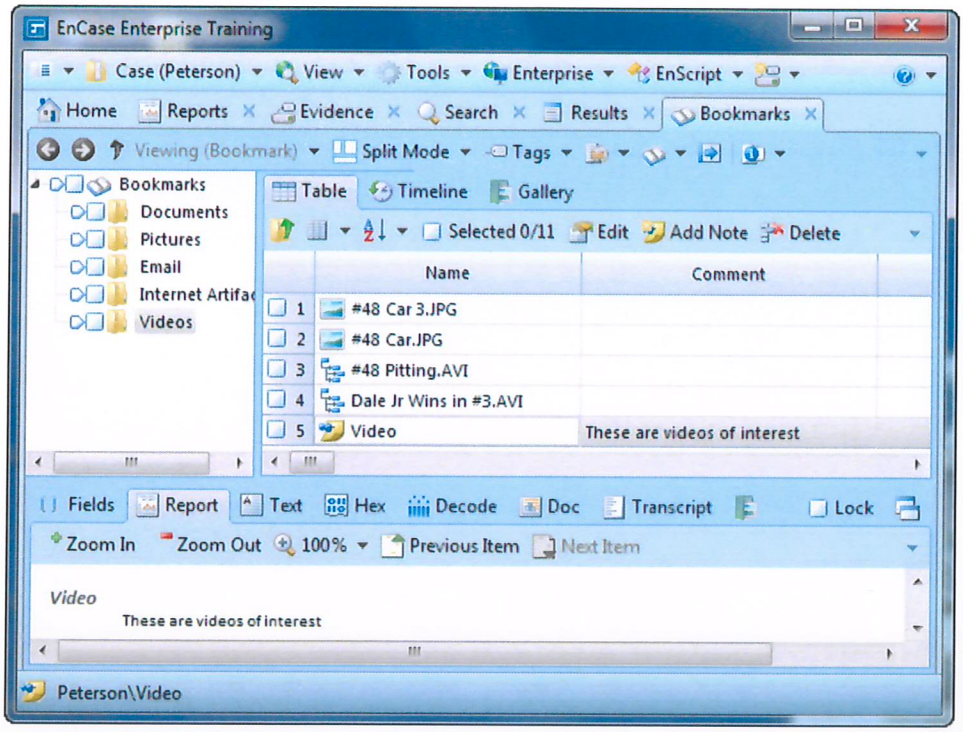

Figure 12-10 After adding note bookmark

The examiner may change the order of the bookmarks in a folder. Left-click on the previously created note bookmark (In between the blue-check box and the Name field of the object being moved) and drag-and-drop it so it is the first item in the Videos folder.

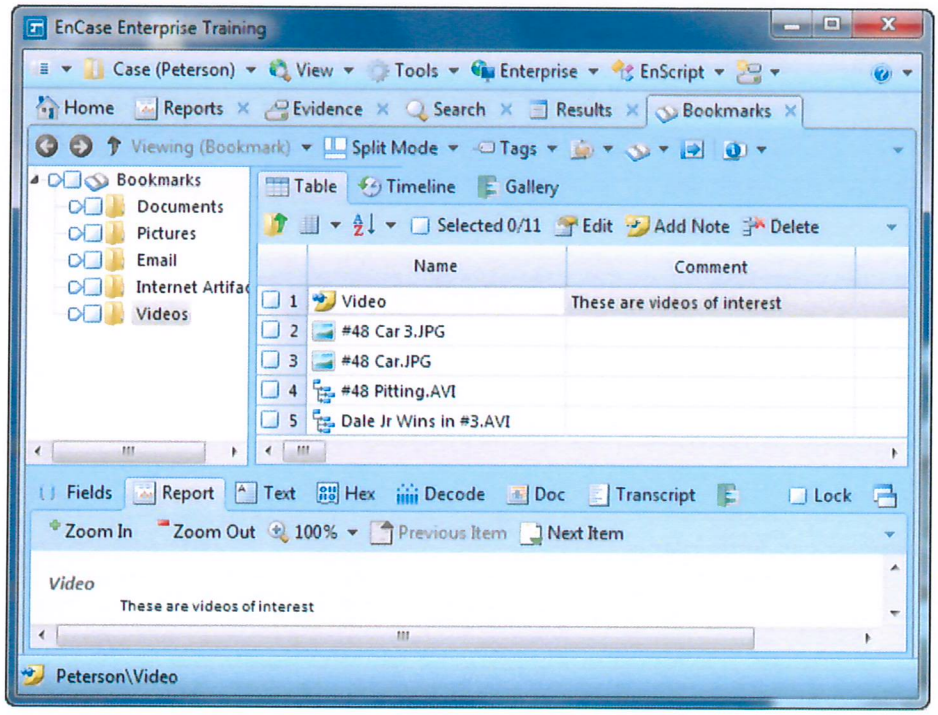

Figure 12-11 New order of bookmarks

The examiner may move or copy multiple bookmark objects at the same time. In this example, highlight the **Videos** folder in the Tree Pane of View→Bookmarks. The objects within the folder should be displayed in the Table Pane. Ensure the Selected/Dixon Box is unchecked. Blue-check the two images in the Videos folder to be moved to the Pictures folder.

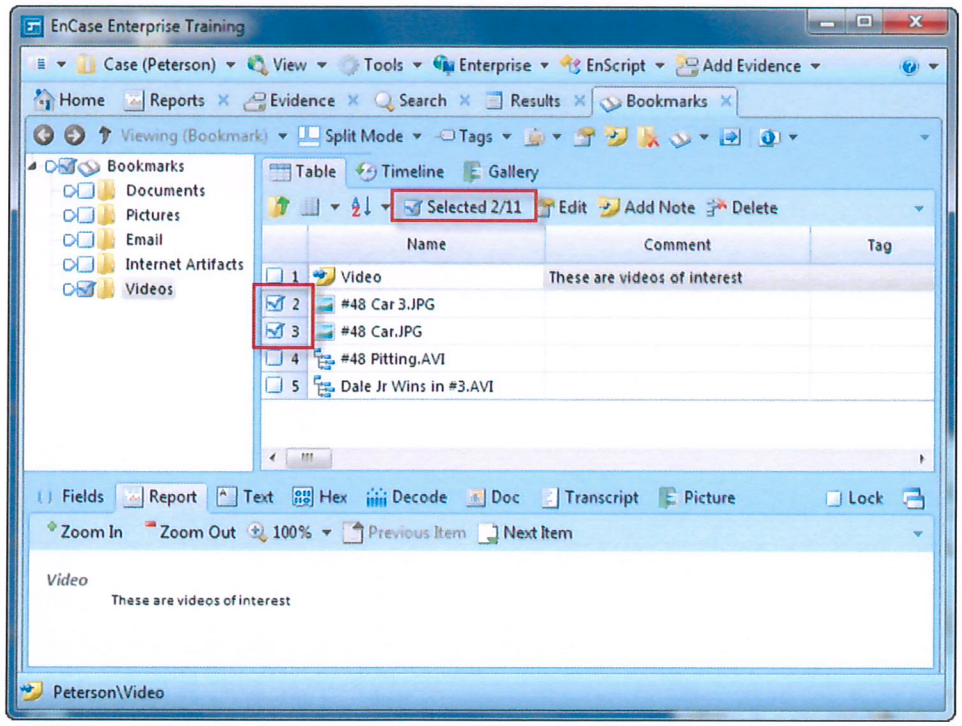

Figure 12-12 Blue-check images to copy/move

Right click in the Table Pane, in-between the blue-check box and the Name field of one of the objects being moved, and drag-and-drop to the Pictures folder in the Tree Pane. To copy the two blue-checked images to the Pictures folder, choose the option **Copy Selected Items Here**; to move the two blue-checked images to the Pictures folder, choose the option **Move Selected Items Here**.

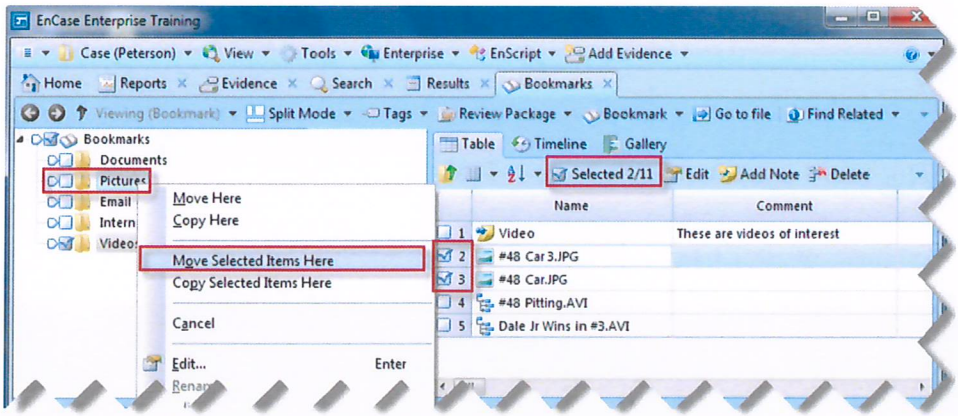

Figure 12-13 Copy and move selected items

The examiner may rename the folder (F2), reorder folders, add new folders, delete folders, and arrange the examination report as appropriate.

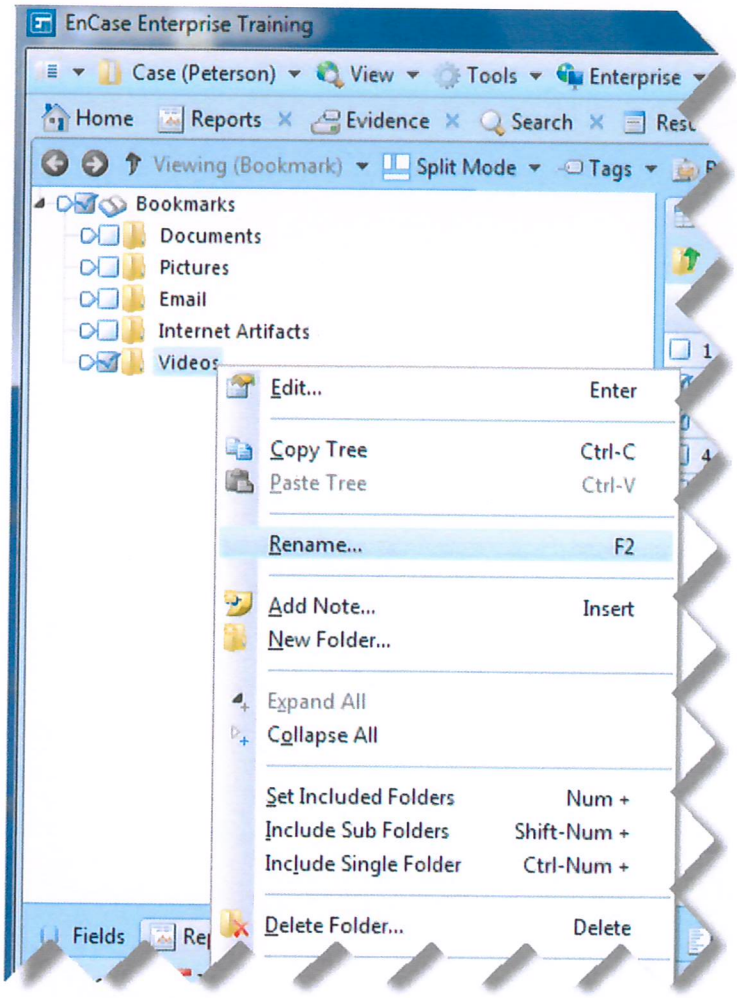

Figure 12-14 Rename, delete, and manage the Bookmark folders

Bookmarking Highlighted Data

Within the Evidence or Results tabs, a portion of the contents of an object may be bookmarked. In this example, access the **Peterson's USB Flash Drive** within the Evidence→Viewing (Entry) tab. Remove any blue checks by clicking in the Selected/Dixon Box above the Table Pane. Highlight the **Peterson's Race Pics** folder in the Tree Pane.

In our scenario, a camera and other photographic equipment were reported as missing from the media center in June of 2010. The camera was a Nikon Coolpix 80.

In the Table Pane, highlight any image (for example **#48 Car.JPG**) in the Tree Pane and view the image in the Text view in the View Pane. Data referencing the camera make and model as well as a date/time when the picture was taken is displayed. The camera that took this photo was a Nikon Coolpix 80. This data must be documented.

Highlight beginning with the "**N**" in **Nikon** through the date/time as shown as follows. Right-click within the highlighted data and select **Bookmark→Raw Text...**

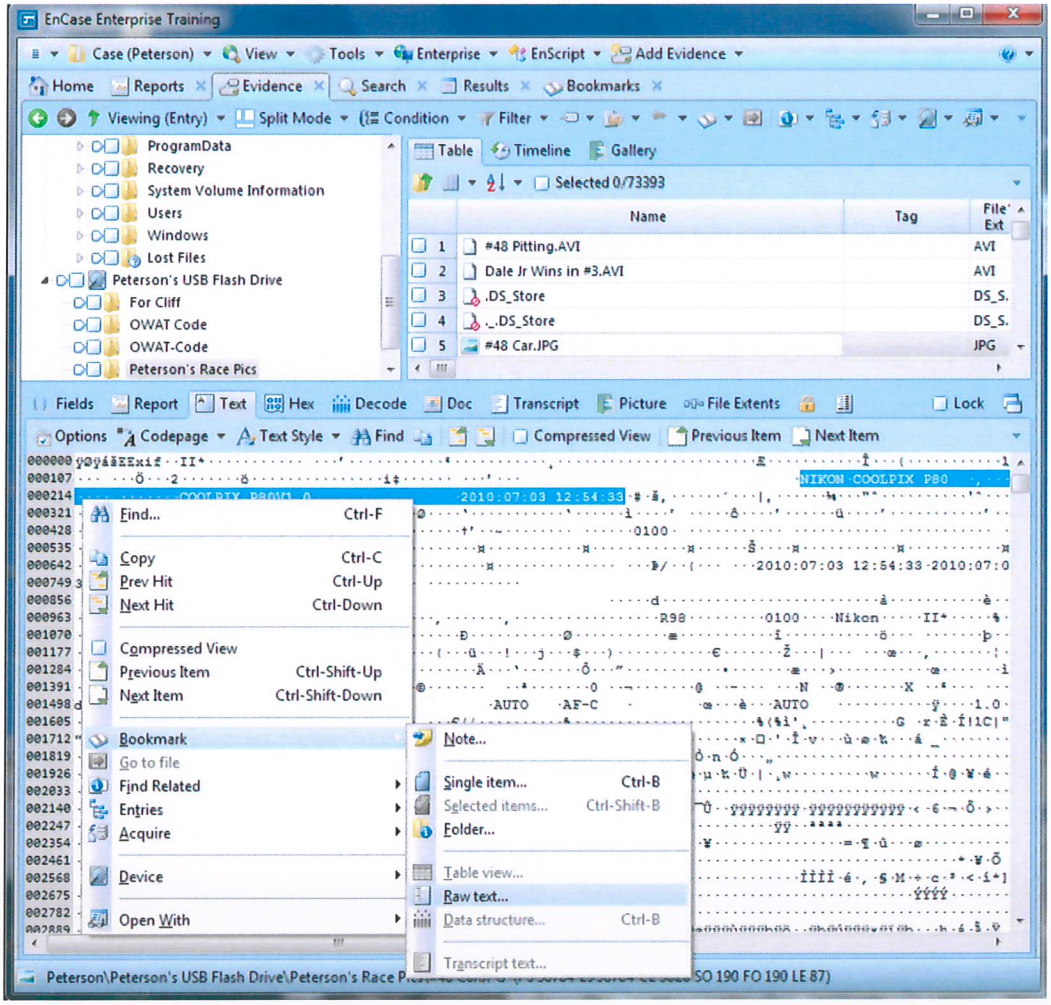

Figure 12-15 Bookmark raw text within JPG image file

Within the Properties tab, type "Within JPG images, camera make, model, text date/time" and click on the **Destination Folder** tab.

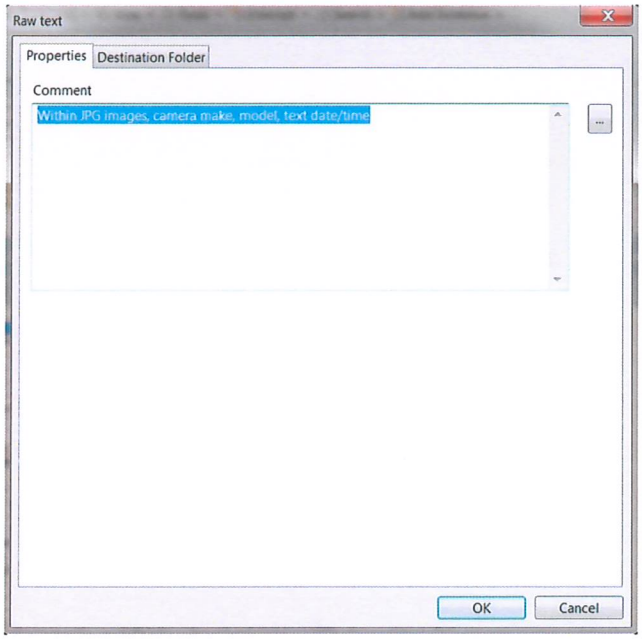

Figure 12-16 Enter comment in Properties tab

Within the Destination folder tab, place this bookmark in the Pictures folder. Highlight the **Pictures** folder and click **OK**.

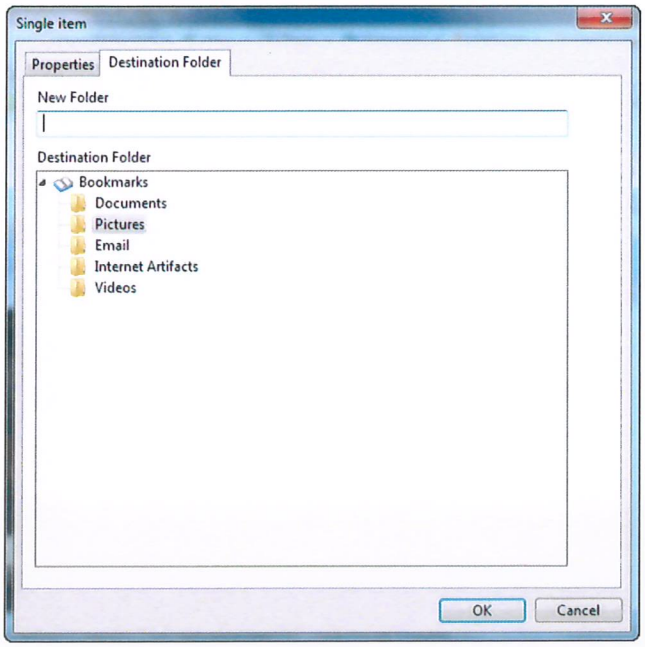

Figure 12-17 Highlight the Pictures folder – click "OK"

The raw data for the bookmarked information is displayed in the Bookmarks tab. Highlight the **Pictures** tab in the Tree Pane, highlight the object recently bookmarked in the Table Pane, and select the **Report** view in the View Pane.

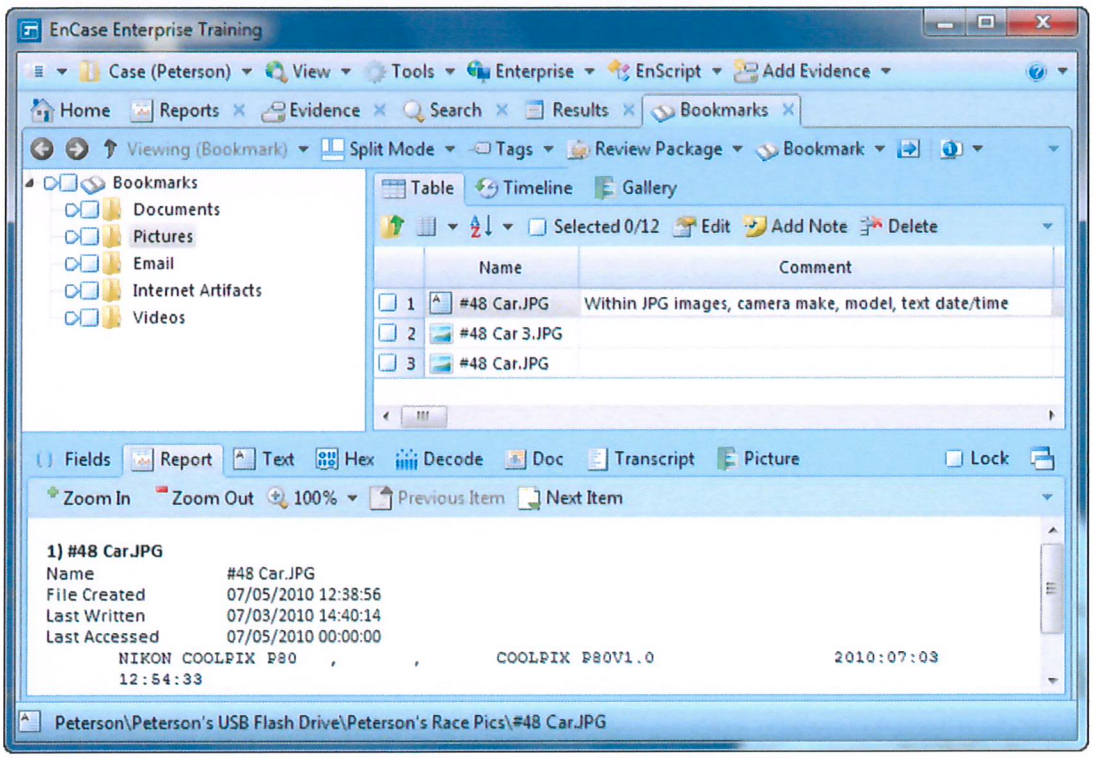

Figure 12-18 Raw data bookmark displayed