Navigating the EnCase® Environment

The EnCase® program (EnCase) opens into the Home view by default when a new case is created. There are many subtabs that provide additional functionality to search, display, sort, and bookmark specific data. Other subtabs will be discussed during this lesson.

Configuring EnCase

Within the **Tools→Options** menu, the examiner may configure the administrative functions of EnCase. These are global options and may be configured without an open case.

Seven tabs appear in the resulting window.

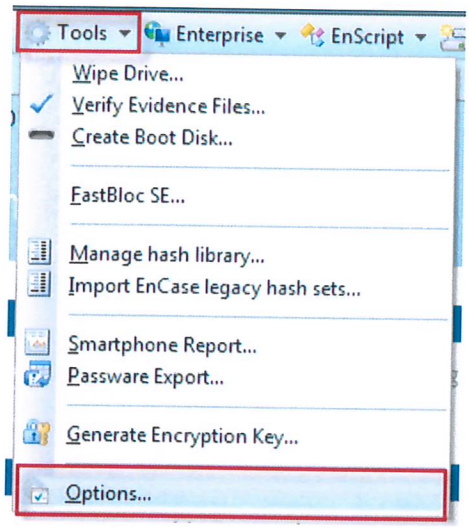

Figure 2-1 Access the Options menu to configure EnCase

- **Global** – This tab allows the user to select options that establish the global configuration settings for a case

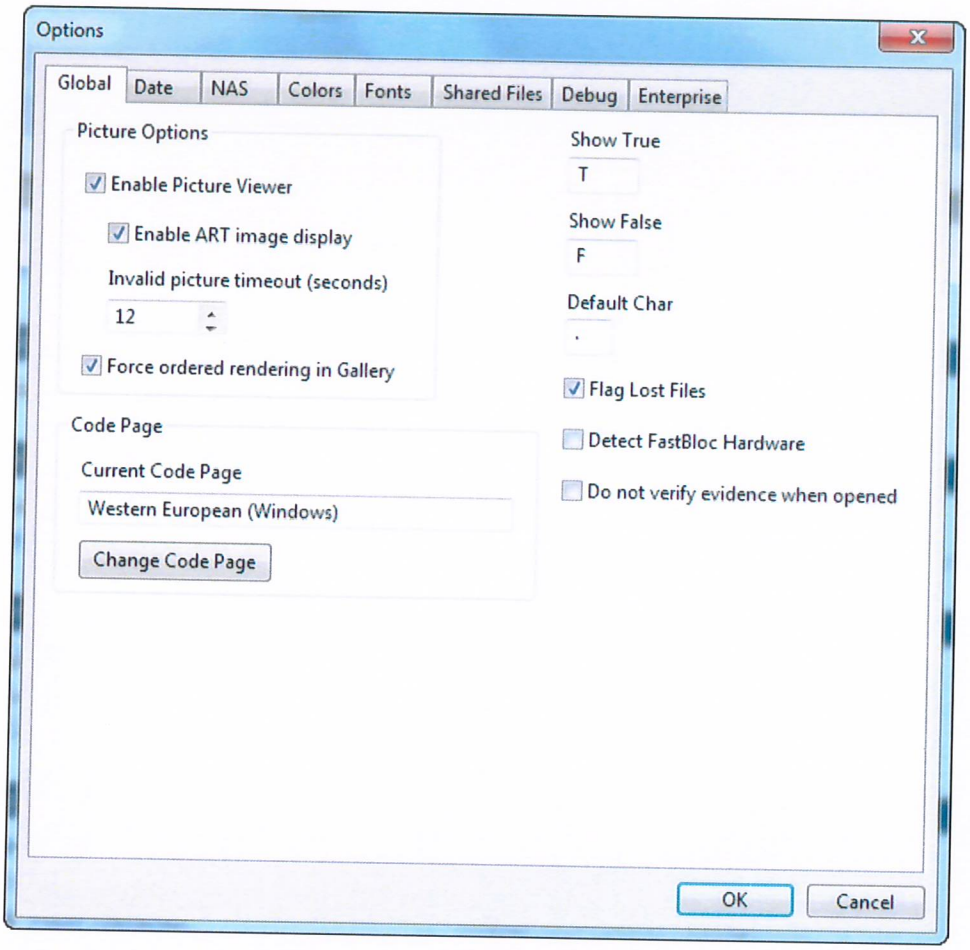

Figure 2-2 Case options – Global Options

  - **Show True / Show False** – Defines the data that will appear in a Table column indicating whether a condition is true or false. It is best to set these items to something that can be easily understood rather than the defaults of the bullet for "true" and blank for "false."
  - **Default character** – Defines a default character display within views if the byte to be displayed cannot be interpreted effectively into ASCII.
  - **Enable Picture Viewer** –Allows pictures to be displayed in various views.

- **Enable ART image display** – Provides the examiner with the ability to not display files with these characteristics, which if corrupted, may cause an Internet browser like Internet Explorer to crash.
- **Invalid picture timeout** – Enables EnCase to stop trying to read a corrupted image file. Instead the file is cached so that EnCase will not attempt to read it in the future. The default is 12 seconds.
- **Force ordered rendering in Gallery** – Allows images in the Gallery view in the Table Pane to be rendered/displayed in order from top left to bottom right. If the option is off, EnCase renders small pictures immediately and queues up the longer/bigger pictures. This option is off by default.
- **Code Page** – Enables the user to select the code page to be used as the default in EnCase.
- **Flag Lost Files** – This option is unchecked by default, which means that lost clusters are treated as unallocated space, decreasing the amount of time rquired to access the evidence file through a case file. If this option is checked, EnCase will tag all lost clusters in the Disk View (indicated by yellow blocks with a question mark). This option must be set before an evidence file is added to the case
- **Detect FastBloc Hardware** – Unchecked by default, determines if searching for the FastBloc® signature on a write-blocking device will occur.
- **Do not verify evidence when opened** – This is an internal option only and appears due to the hardware key flag used by our internal Training department; this function will not appear in consumer versions of EnCase® v7.

- **Date** – This set of options controls the date/time display format throughout EnCase.

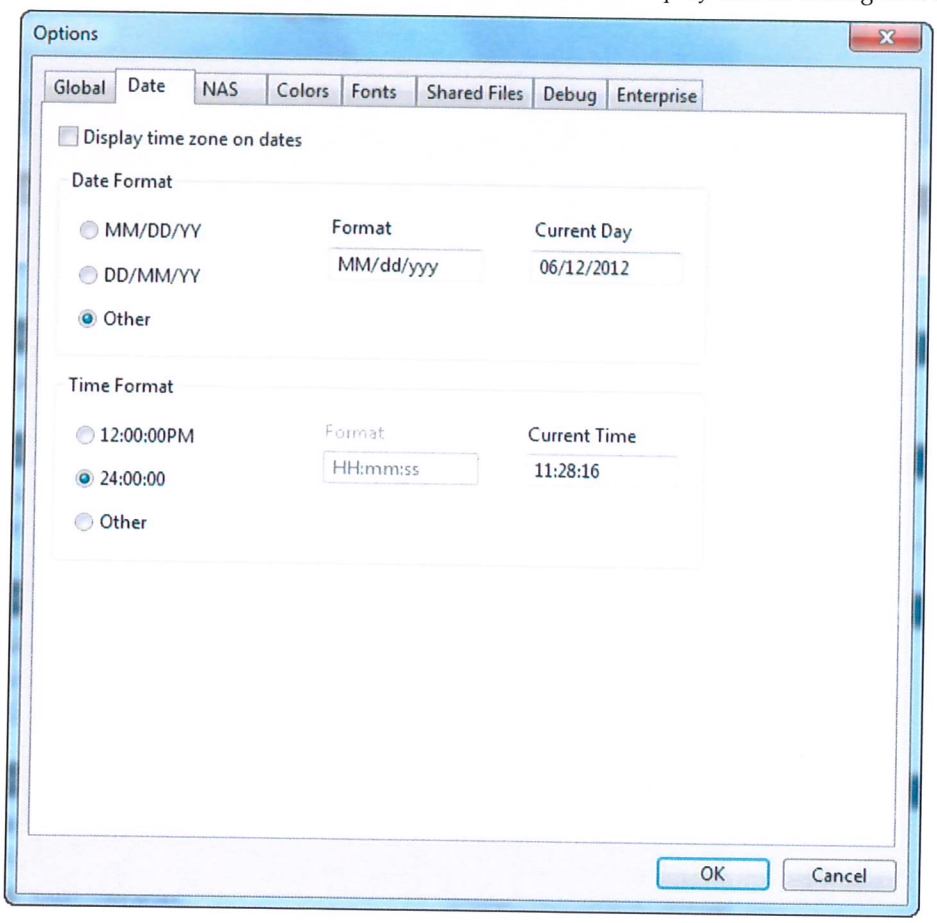

Figure 2-3 Case options – Date Options

  - **Display time zone on dates** – Unchecked by default, enables dates to be displayed with the applied time zone within EnCase or with the time zone set on the examination computer system.
  - **Date Format** – Determines the default display format for Dates interpreted and shown within EnCase.

    NOTE: To display a four-digit year, click **Other** and add a third "y" within the Format section as shown in the previous screen shot.

- **Time Format** – Determines the default display format for dates interpreted and shown within EnCase.

- **NAS (Network Authentication Server)** – This option allows multiple copies of EnCase to authenticate to a single hardware key. This is typically used in lab environments with multiple examiners and multiple copies of EnCase. Note the message indicating that EnCase needs to be restarted if these settings change

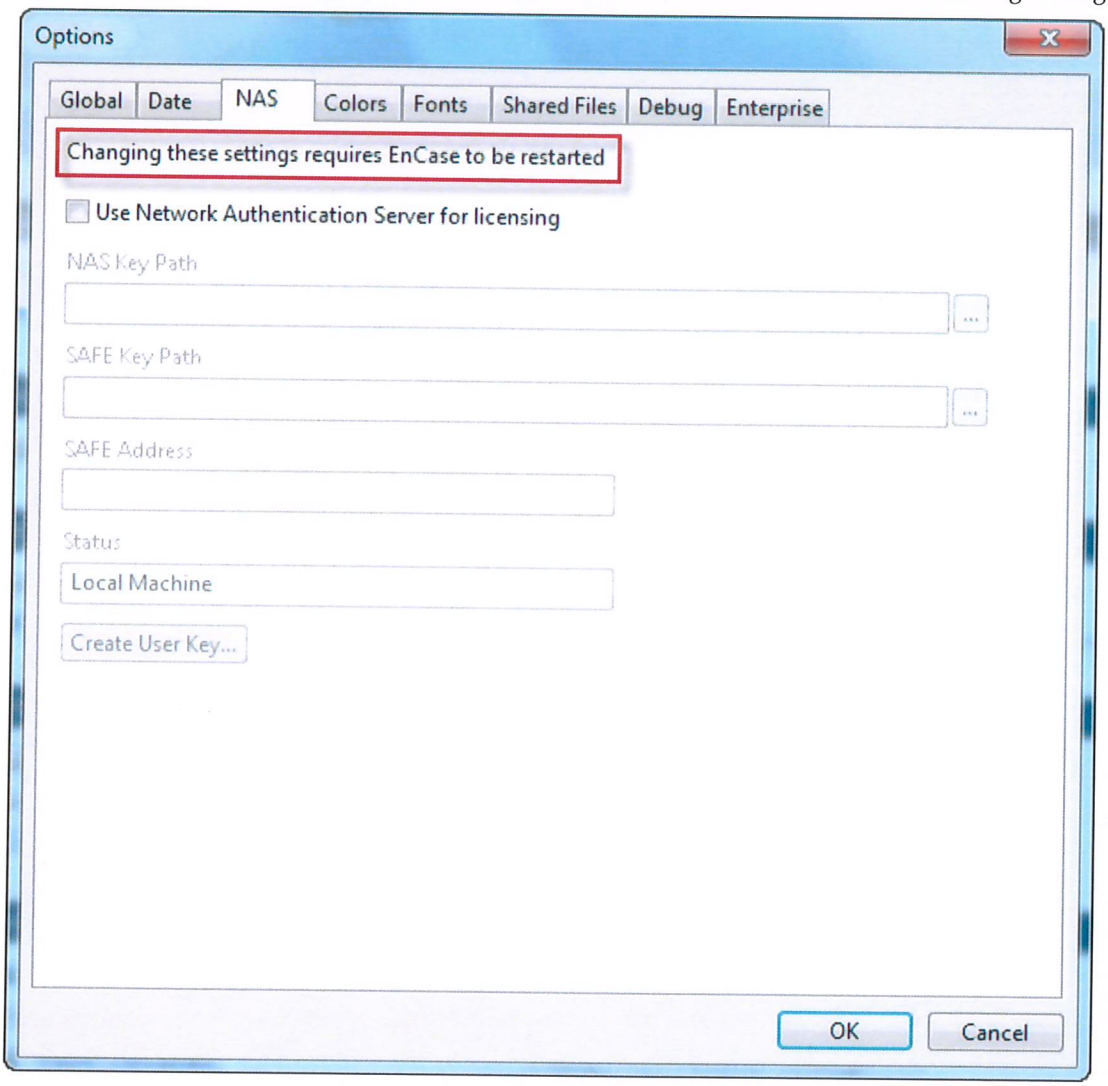

Figure 2-4 Case options – NAS options

- **Colors** – This tab allows the user to change the colors for different elements of the EnCase® interface. It is suggested that the **Background** of **Bookmark** and **Search Hit** be changed to brighter shades of their default colors.

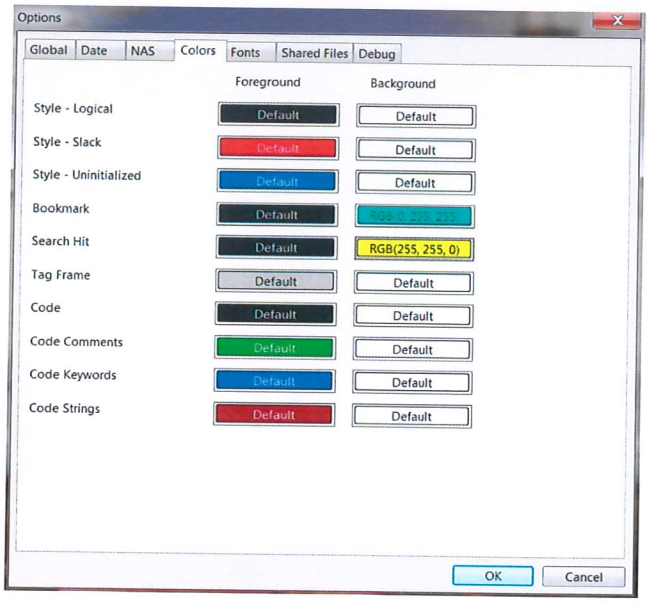

Figure 2-5 Case options – Colors options

- **Fonts** – This option allows the user to alter fonts for viewing convenience and to accommodate the special font requirements of some foreign languages to display correctly. The current font and size are displayed.

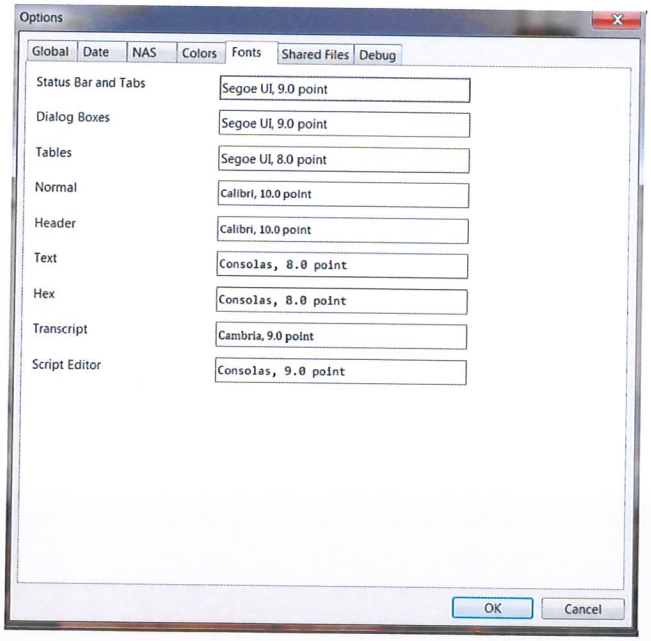

Figure 2-6 Case options – Fonts options

- **Shared Files** – This option allows the user to set shared data locations.

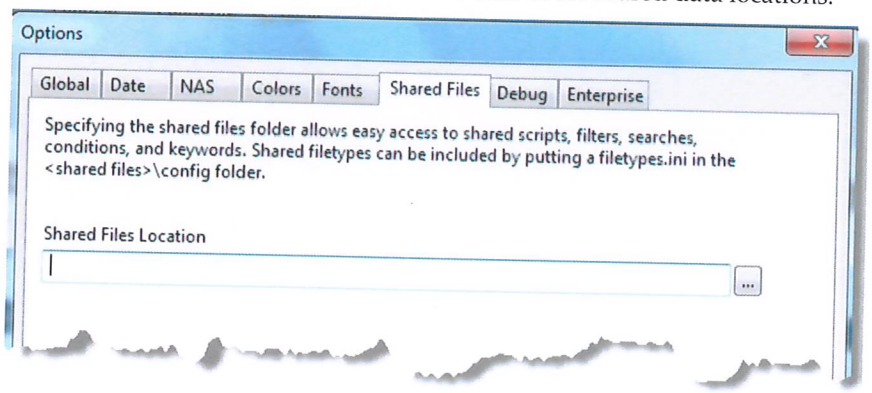

Figure 2-7 Case options – Shared Files

- **Debug** – This option is utilized by EnCase users who experience abnormal shutdowns or program lockups and by those working with customer service to determine the nature of the problem.

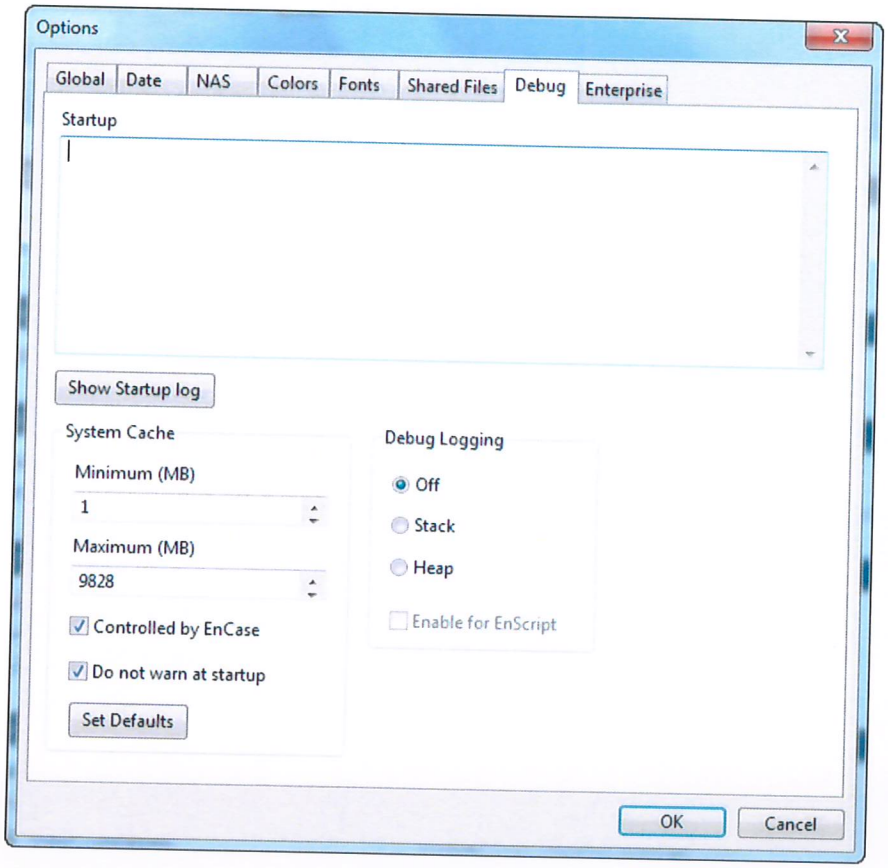

Figure 2-8 Debug tab

If changes were made within the Tools→Options menu, click **OK** to retain those changes. To save changes, click the **Application** drop-down menu to the left of **Case (LocalSystem)** and select **Save All**. This will save the case and any configuration files affected by recent operations.

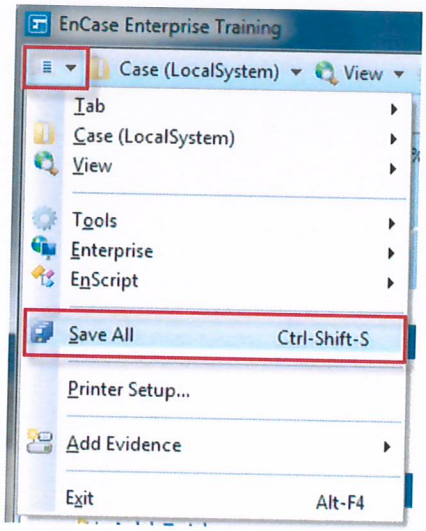

Figure 2-9 "Save All" saves case and configuration

Previewing a Local Drive

The examiner may add a preview of a local drive to the case by clicking **Add Evidence** from the Home tab and **Add Local Device** from the next screen or by selecting **Add Evidence→Add Local Device...** from either the Home or Evidence tabs (to access the Evidence tab, click **View→Evidence**).

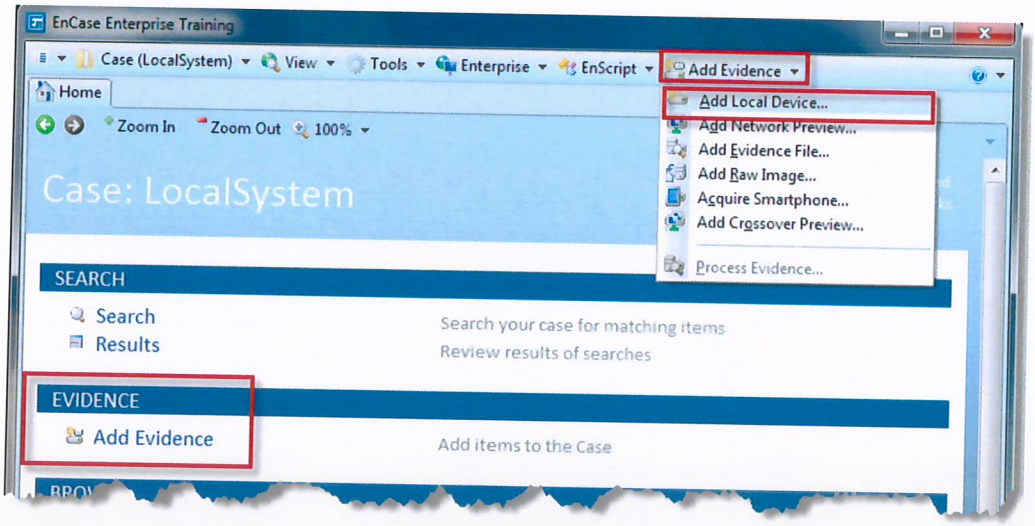

Figure 2-10 Add Evidence

The next screen is entitled "Add Local Device." Remove all blue-checks and select **Next>**.

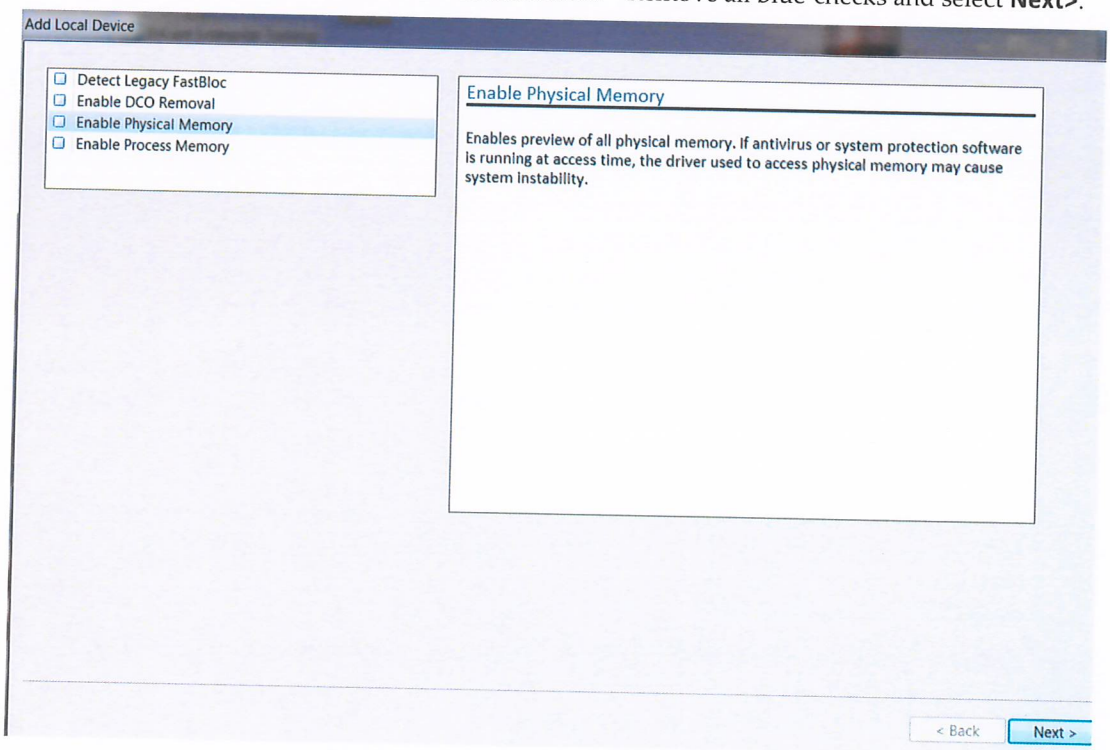

Figure 2-11 No selections necessary – click "Next>"

- **Detect Legacy FastBloc** enables the legacy FastBloc signature to be recognized as a write-protection mechanism when scanning available devices.
- **Enable DCO Removal** activates the function that causes the eventual detection and removal of Device Configuration Overlay data from a hard disk. Not a part of typical user addressable storage, one function of a DCO is to make an 80-gigabyte HDD appear as a 60-gigabyte HDD to both the BIOS and the OS.
- **Enable Physical Memory** causes the entire contents of physical memory to be accessible and imaged.
- **Enable Process Memory** causes different objects to appear, representing each currently running process within the computer system. These objects may be acquired separately.

For the purposes of this lesson, no selections are necessary – click **Next>**.

The Add Local Device window appears, displaying all drives connected to the local computer system and an object representing RAM.

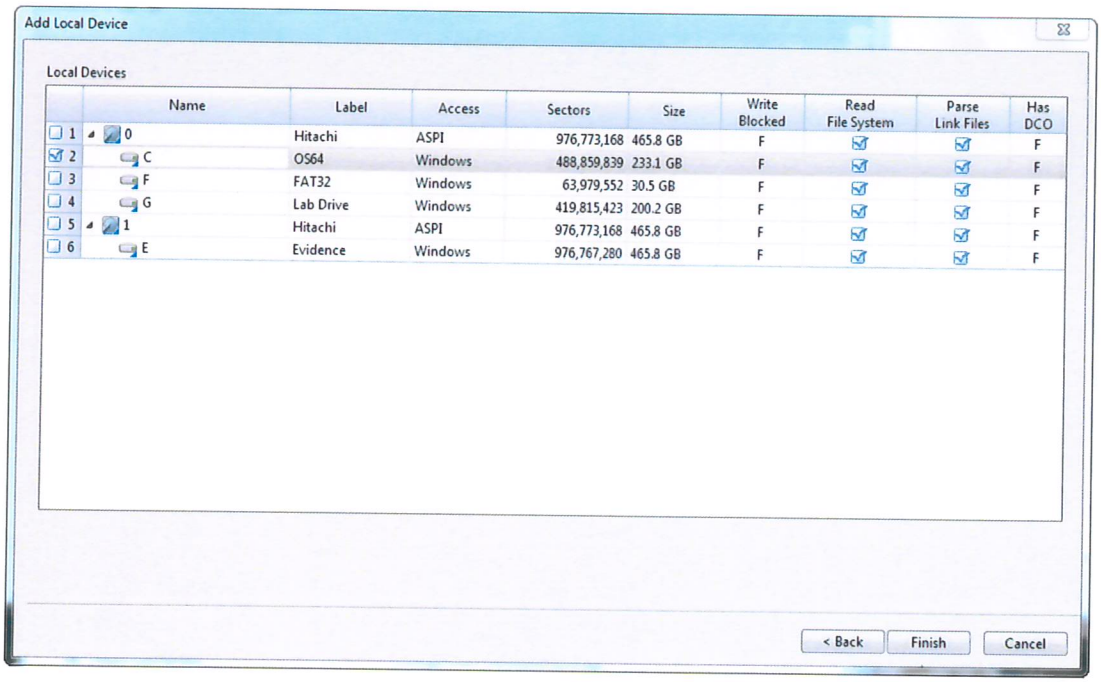

Figure 2-12 Blue-check volume "C" and click "Finish"

Notice that there is a differentiation in position and icon between the physical drive **0** and the logical volume **C**. Select the volume booted from by placing a blue-check in the box to its left and click **Finish**. To see the object representing logical volume C, ensure that the Evidence tab is displayed. If not, click **View→Evidence**.

Within the Viewing (Evidence) view, double-click within the **Name** column of the desired previewed drive to see the objects it contains.

NOTE: To browse more than one item, blue-check the items and click **Open**.

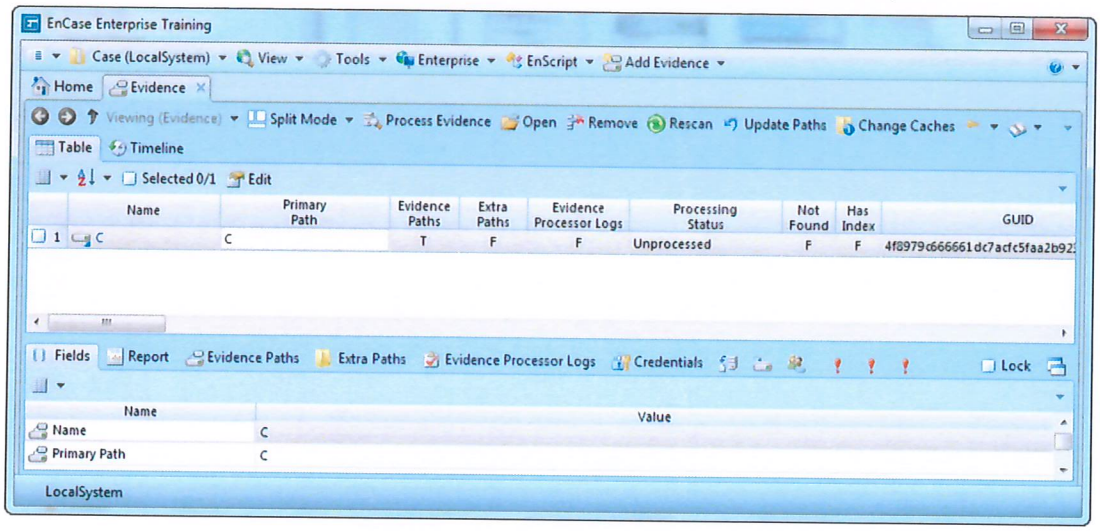

Figure 2-13 Click "C" on Evidence tab to see objects

The screen is initially divided into three sections:

- Tree Pane (left pane)
- Table Pane (right pane)
- View Pane (bottom pane)

The selections in the **Tree Pane** affect the **Table Pane** and the selections in the **Table Pane** affect the **View Pane**.

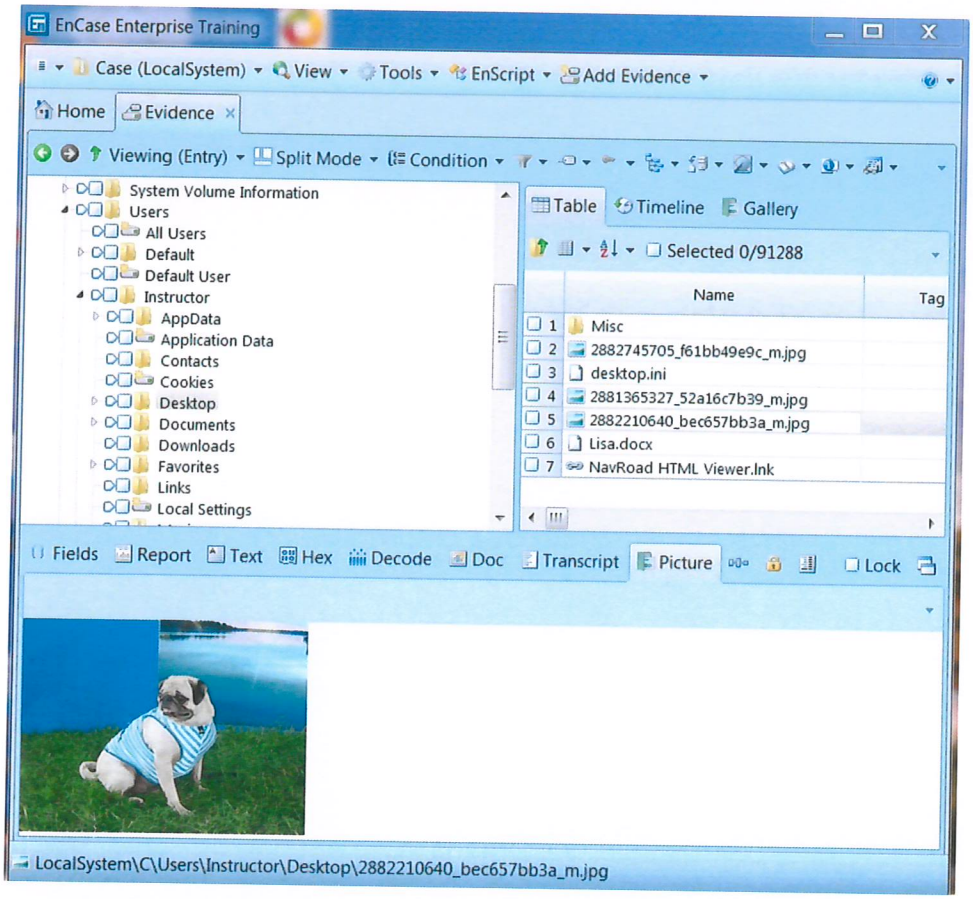

Figure 2-14 View of the three panes

Tree Pane / Evidence View

Within the Tree Pane and the Evidence tab/view, the examiner is provided with a tree-structured view of the evidence. It presents each evidence file as a folder that contains additional folders. Only evidence files and the folders contained within them are displayed in this view. Individual files are displayed in the Table Pane (discussed later). The triangles can be used to expand and contract the tree structure just as in Windows® Explorer.

Right-clicking on an object in the Tree Pane brings up a context menu with many selections, including the choice to expand or collapse from the highlighted position. Everything in the Tree will be affected by performing this operation on the Entries object in the Tree Pane.

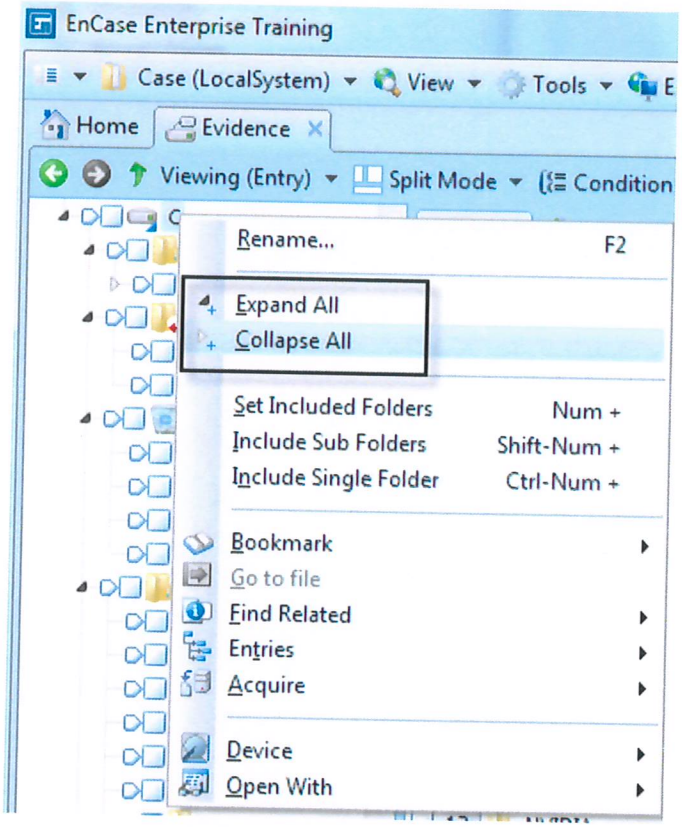

Figure 2-15 Collapsing a folder structure

Selecting **Collapse All** causes all folders to contract. The structure is different when expanded with the arrow.

Selecting **Expand All** expands all folders from the highlighted folder.

There are three methods used within EnCase to focus on specific files or folders. These methods have different purposes:

- **Highlighting** a folder displays the entries within that folder in the Table Pane. This is used for viewing information only. Clicking on the triangle to the left of folder names in the Tree pane also highlights that folder as well as expands the folder. When the folder is expanded to reveal its folder children, the triangle becomes darker and changes orientation.
- The **Set Include Option** method (sometimes called "home plate" or "show all") displays all the entries, files, and folders for that folder and all subfolders in the Table Pane. It overrides the highlighting option. It is activated by clicking on the polygon next to the tree of the folder name in the Tree Pane in the Evidence view and in any other view displaying a similar folder structure. This is used for viewing information only. When a folder is *included*, the other folders are *grayed out*. All files and folders within the folder and subfolders are displayed in the Table Pane. To deactivate this function, click on the **Set Include Option** icon again or click twice on another include icon.

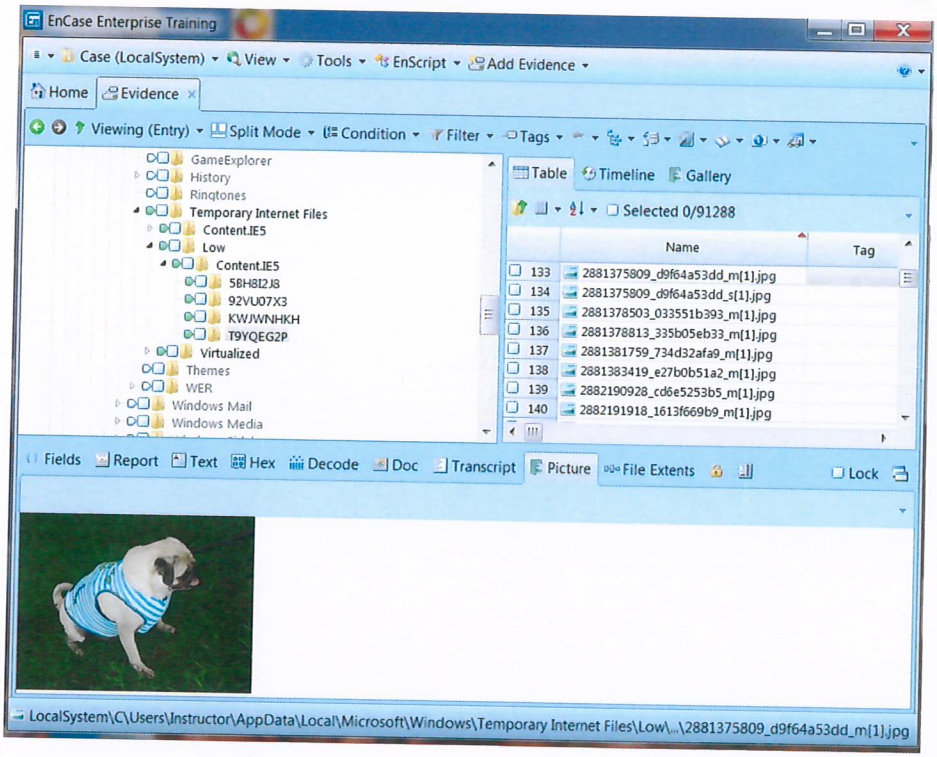

Figure 2-16 "Set including" a folder structure

- The **blue-check** or **select for future action** method is used for designating files or folders on which to perform an analysis operation such as a keyword search. This can be implemented from a variety of views. It is activated by clicking on the square next to the tree of the entry name in any view.

In the following example, one folder has been selected. This folder (Desktop) has a *white background* within the *blue-checked* square (☑), indicating all entries within the folder have been selected. The recommended method for selecting all objects within a folder is to select or blue-check the folder in the Tree Pane.

The Instructor folder has a *gray background* within the blue-checked square (☑), indicating not all entries within the folder have been selected.

The Dixon Box above the objects in the Table Pane indicates how many entries have been selected. In this example, 9 entries have been selected; 8 file objects and 1 folder object.

To deselect all entries, click within this Dixon Box to remove the blue-check and to remove blue-checks from elements of the Evidence view and the Table Pane.

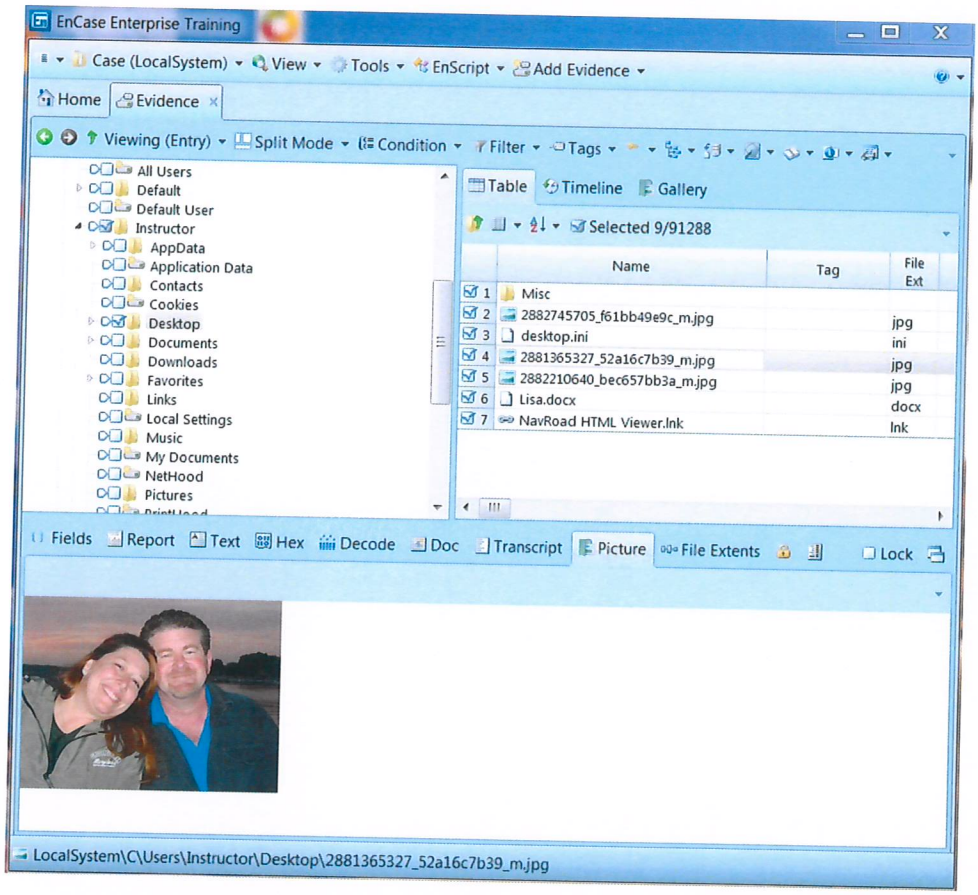

Figure 2-17 "Blue-checking" entries and the Dixon Box

Within the Tree Pane there are many views that can be accessed for different purposes. All of these views may be accessed through the tabs available above the Tree Pane or through the View menu. Any tabs not displayed above the Tree Pane will be displayed by selecting them through the View menu.

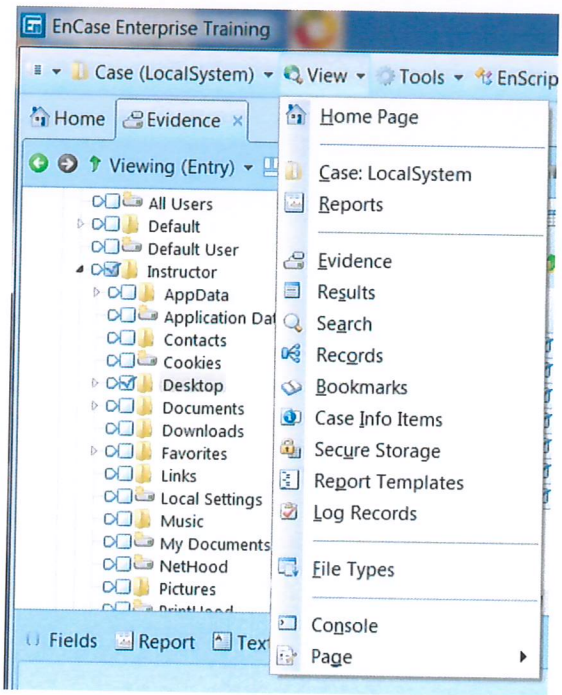

Figure 2-18 View menu

Table Pane – Table View

By default the Table Pane is in the Table view. Within this view are the subfolders and file objects that are contained within the folder(s) and are highlighted or included (Set Include Option) in the Tree Pane. Highlighting or including (Set Include Option) a folder affects the display in the Table Pane as previously explained.

Highlighting an object in the Table Pane displays the object's location in the **Status Bar** (under the image in this example).

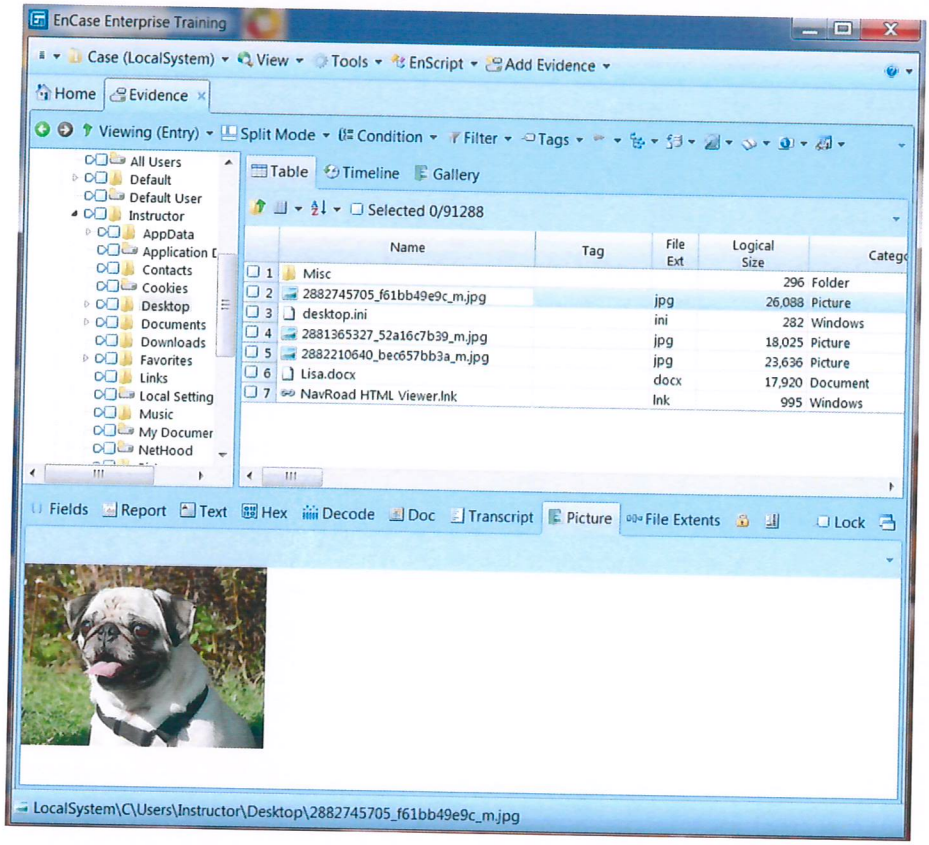

Figure 2-19 Status Bar

The **highlighting** and **Set Include Option** features are intended to view desired files and folders in the Table Pane. If there are one or more folders designated with the set include feature, the highlighting feature will not change the number of files/folders displayed in the Table Pane.

This differs from the **Select** box located to the right of the pointed box. This is intended to *select* with *a blue check* the files and folders on which to perform certain operations, including but not limited to searching and exporting. With the **Set Include Option** feature activated, the select operation will not alter the number of files/folders displayed in the Table Pane.

Within the Table Pane above the actual table, which contains metadata about the objects being displayed, is:

- the **Go To Parent** button,
- the column options,
- the sort options, and
- Selected 3/174319 the **Dixon Box**.

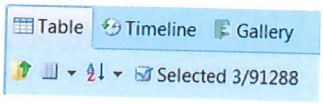

Figure 2-20 Above Table Pane

The Go To Parent button focuses on the parent folder of the highlighted object in the Table Pane.

The Dixon Box displays the number of objects selected or blue-checked (i.e., Dixon box) to the left of the forward slash and the total number of objects in the device to the right of the forward slash.

The relevant column and sort options will be discussed later.

The Table view in the Table Pane displays many columns of information about the displayed entries:

1. **Name** identifies the file/folder/volume, etc., in the evidence file
2. **Tag** specifies a tagged or marked object; this tagging feature is most commonly used within Reporting

- **File Ext** displays the entry's extension, which initially determines whether this entry is displayed in the Gallery view
- **File Type** identifies the type of file; after a Signature Analysis is run, this data is generated from the results
- **File Category** indicates the category of the file from the File Types table
- **Signature Analysis** displays the results of a file signature analysis operation
- **Description** describes the *condition* of the entry – whether it is a file or folder, deleted, or deleted/overwritten
- **Protected** indicates whether the object is password protected or encrypted
- **Protection Complexity** identifies the severity of the protection or encryption
- **Is Picture** indicates whether the object is an image (T) or not (F)
- **Is Deleted** displays *T* if the entry is in a deleted state; *F* if it is not

NOTE: The display depends on how the Show True/False options were set in the Tools→Options→Global menu.

- **Last Accessed** displays the last-accessed date/time. This typically reflects the last time the operating system or any compliant application touched the file (such as viewing, dragging, or right-clicking). Entries on FAT volumes do not have a last-accessed time.
- **File Created** typically reflects the date/time the file/folder was created at that location. A notable exception to this is the extraction of files/folders from a ZIP archive. Those objects will carry the created date/time as they existed when the objects were placed in the archive.
- **Last Written** reflects the date/time the file was last opened and saved
- **Entry Modified** indicates when the administrative data for the file was last altered for NTFS and Linux
- **File Deleted** displays the deleted date/time if the file is documented in the Recycle Bin's Info2 file
- **File Acquired** identifies the date/time the evidence file in which this entry resides was acquired
- **Logical Size** specifies the file size as the operating system addresses the file
- **Initialized Size** displays the size of the file when it is opened (applies only to NTFS file systems)
- **Physical Size** specifies the size of the storage areas allocated to the file
- **Starting Extent** identifies the starting cluster of the entry
- **File Extents** displays the number of cluster fragments allocated to the file
- **Permissions** shows security settings of a file or folder
- **Physical Location** displays the number of bytes into the device at which the data for an entry begins
- **Physical Sector** lists the sector number into the device at which the data for an entry begins
- **Evidence File** indicates the name of the evidence file where the entry resides
- **File Identifier** displays an index number for a Master File Table (NTFS) or an Inode Table (Linux/UNIX)
- **Code Page** is the character encoding table upon which the file is based
- **MD5 Hash Value** is a 128-bit value for a file entry, generated by a hash analysis process
- **SHA-1 Hash Value** is a 160-bit value for a file entry generated by a hash analysis process
- **GUID** is a unique value representing an object
- **Hash Set** displays a Boolean value, indicating whether there is a Hash Set tab in the View Pane for a particular object (this column will always display *T*)
- **Short Name** displays the name that Windows gives the entry using the DOS 8.3 naming convention
- **VFS Name** is used to display the name for files mounted with the EnCase® Virtual File System (VFS) Module in Windows Explorer

- **Original Path** displays information derived from data in the Recycle Bin. For files within the Recycle Bin, this column shows where they originated when they were deleted; for deleted/overwritten files, this column shows the file that has overwritten the original.
- **Symbolic Link** is data pertaining to the equivalent of a Windows Shortcut in Linux and UNIX
- **Is Duplicate** displays TRUE (Yes) if the displayed file is a duplicate of another
- **Is Internal** indicates whether the file is an internal system file, such as the $MFT on an NTFS volume
- **Is Overwritten** indicates if the entry has been overwritten by another object

Organizing Columns

Table columns may be rearranged in any order as in Microsoft® Excel. Click on the column heading and drag the column, dropping it into its new location.

The examiner may choose the Table columns to display in the Table view. Click the **Column** button above the Table Pane and choose **Show Columns...** All columns are displayed by default. Remove the blue-check beside the columns not to be displayed.

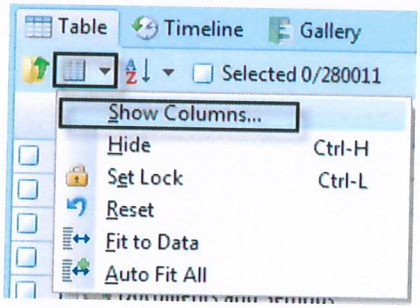

Figure 2-21 Column→Show Columns...

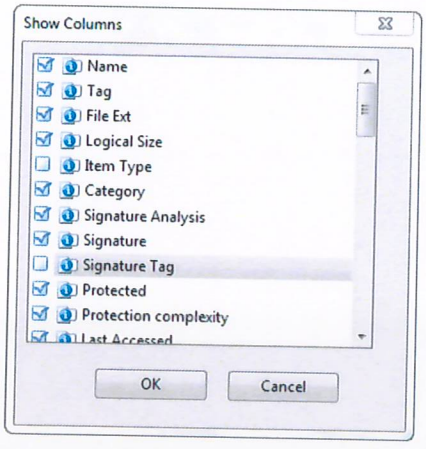

Figure 2-22 Remove blue-checks from undesired columns

Columns may be sorted by up to six layers deep. To sort by a column, double-click on the column heading. A red triangle will appear in the column heading, indicating whether the sort is ascending or descending. Double-click on the column again to reverse the primary sort. To institute a subsort or secondary sort, hold down **Shift** and double-click on the column heading. If the subsort is to be the opposite order of its parent sort, hold down **Ctrl** and **Shift** and double-click on the column heading. Initiate a primary sort on **File Ext** and a secondary sort on **Name**.

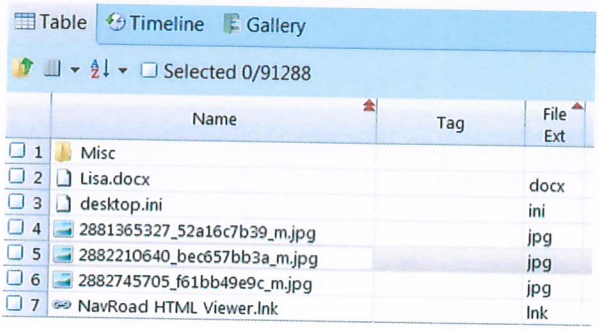

Figure 2-23 Primary sort Name; Secondary sort File Ext

To remove all sorting or to utilize the menu for sorting, click on the **Sort** button above the Table Pane and click **Remove Sort**.

Columns may be *anchored* or *locked* on the left side of the Table view, so that when the examiner scrolls to the right in the Table view, the initial columns are still visible. To lock a column, click on any cell within the column to be locked, click the **Column** button above the Table Pane and select **Set Lock**. The lock is instituted on the position of the column and a bold vertical line will be seen to the right of the locked column. If other columns are moved into that position, they are locked.

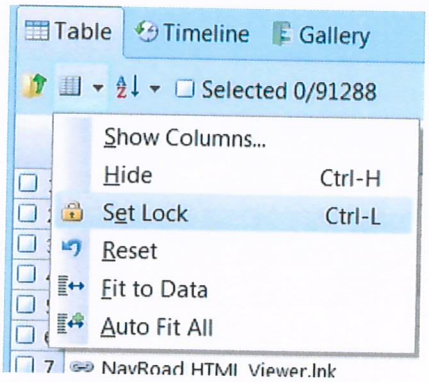

Figure 2-24 Lock second column

To release the lock, click within the last column locked, click the **Column** button above the Table Pane, and select **UnLock**.

Table Pane – Gallery View

This view displays images in a thumbnail view. These images are displayed (by default) based on their extension. The Signature Analysis function enables files to be analyzed to see if they were renamed to disguise their existence on the media.

To reduce or increase the number of images displayed at any one time, click the buttons above the Gallery that indicate **Fewer Columns** or **More Columns**.

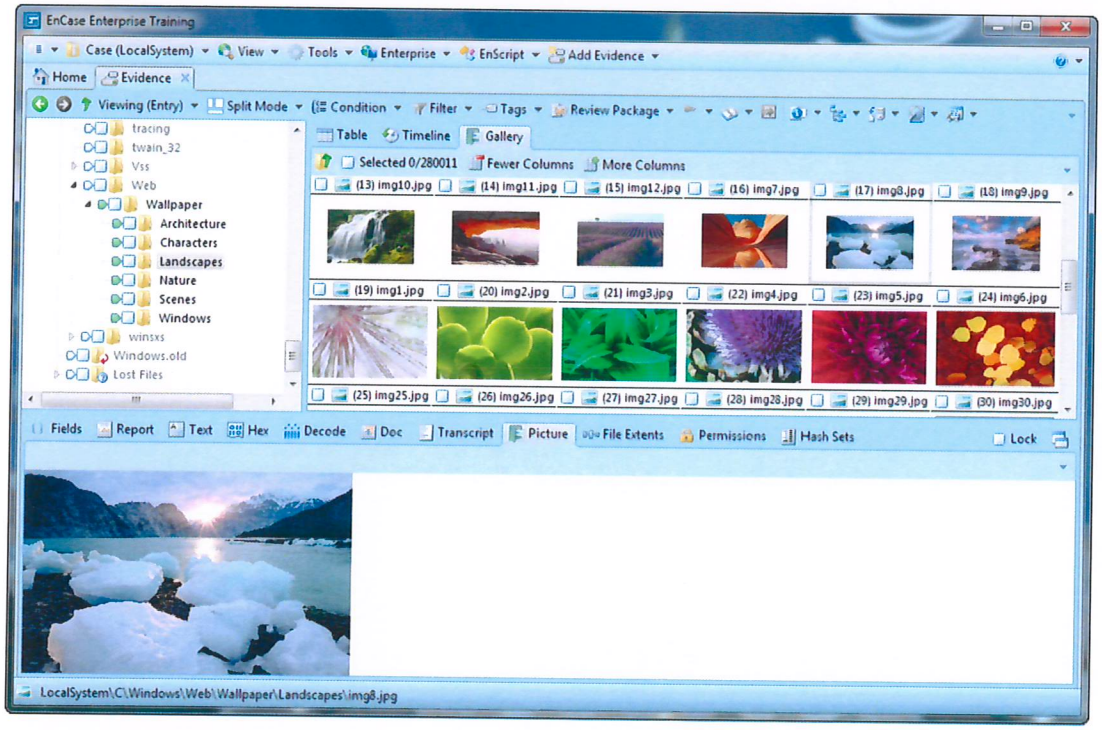

Figure 2-25 Gallery view

Images may be blue-checked and/or tagged from the Gallery view or from the Table view.

Table Pane – Timeline View

This view shows patterns of different types of dates and times. You can zoom in (higher resolution) to a second-by-second timeline and zoom out (lower resolution) to a year-by-year timeline. This will be discussed in more detail in a separate lesson.

View Pane

The View Pane displays the contents of the item highlighted in the Table Pane. It contains several tabs that customize the view of the object:

- **Fields** – Displays every possible property or column in the Table Pane and any metadata that exists for the highlighted object
- **Report** – Shows properties for the highlighted object that contains metadata
- **Text** – Reveals the ASCII view for the highlighted object
- **Hex** – Displays the Hexadecimal view and ASCII view for the highlighted object
- **Decode** – Interprets highlighted data within the contents of a highlighted object
- **Doc** – Using the Stellent Outside-In Viewer, reveals the contents of the highlighted object based on the interpretation of a file header or file signature
- **Transcript** – Filters out high-ASCII characters of the highlighted object and shows only user-readable characters, numbers, and symbols
- **Picture** – Displays the EnCase Internal Viewer's interpretation of an image based on the extension of the highlighted object
- **File Extents** – Reveals physical and logical specifications of data within highlighted object related to the media imaged
- **Permissions** – Displays SIDs (Security Identifiers) associated with the highlighted object
- **Hash Sets** – Shows any hash sets associated with the highlighted object as a result or running the Hash Analysis through the Processor

EnCase checks the contents of the file highlighted in the Table Pane to see if it is an object that can be decoded internally, like an image. If so EnCase will provide the ability for the user to view the object using the Picture view in the View Pane and the image is displayed. As previously mentioned, the location of the object will be displayed in the Status Bar and the folder containing the object will be highlighted indirectly in the Tree Pane.

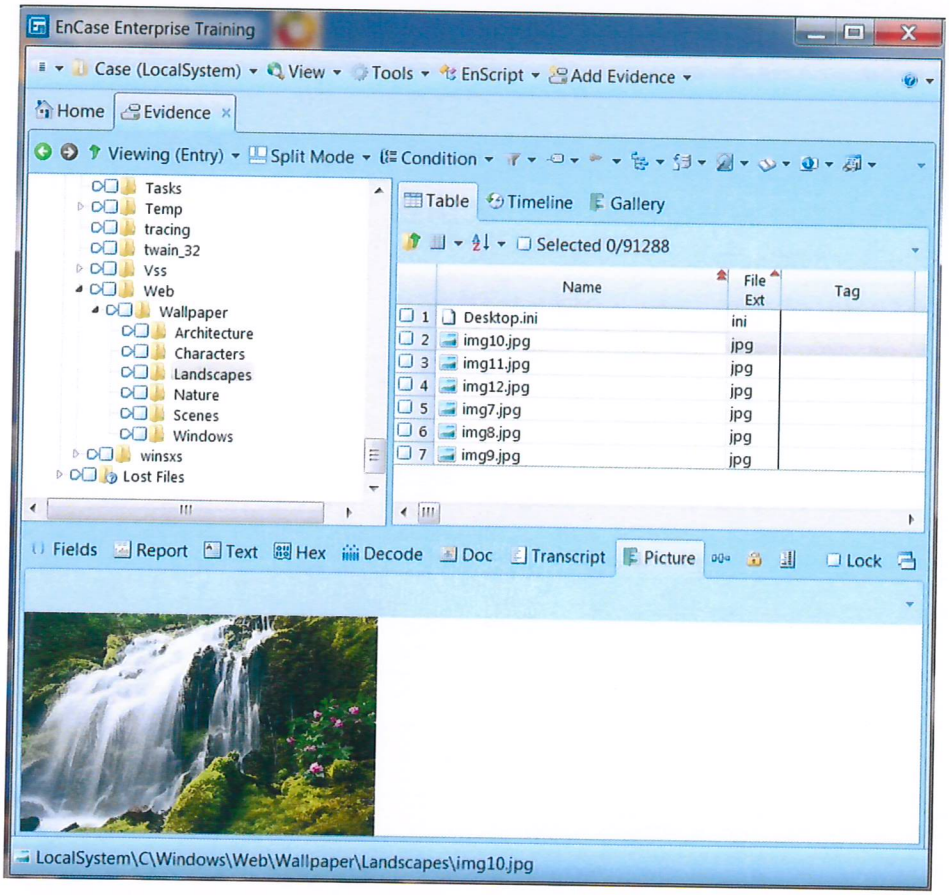

Figure 2-26 Picture view in View Pane

If numerous files highlighted in the Table Pane are images, EnCase will default to the Picture view for subsequent images. If a Microsoft® Word document is then highlighted, EnCase will change the default view in the View Pane to text. If the examiner wishes to have every highlighted item displayed in Hex or Text view, they need only click on the square beside **Lock** to lock that view. To unlock the view, remove the blue-check from the box.

Here is the same picture viewed in hexadecimal.

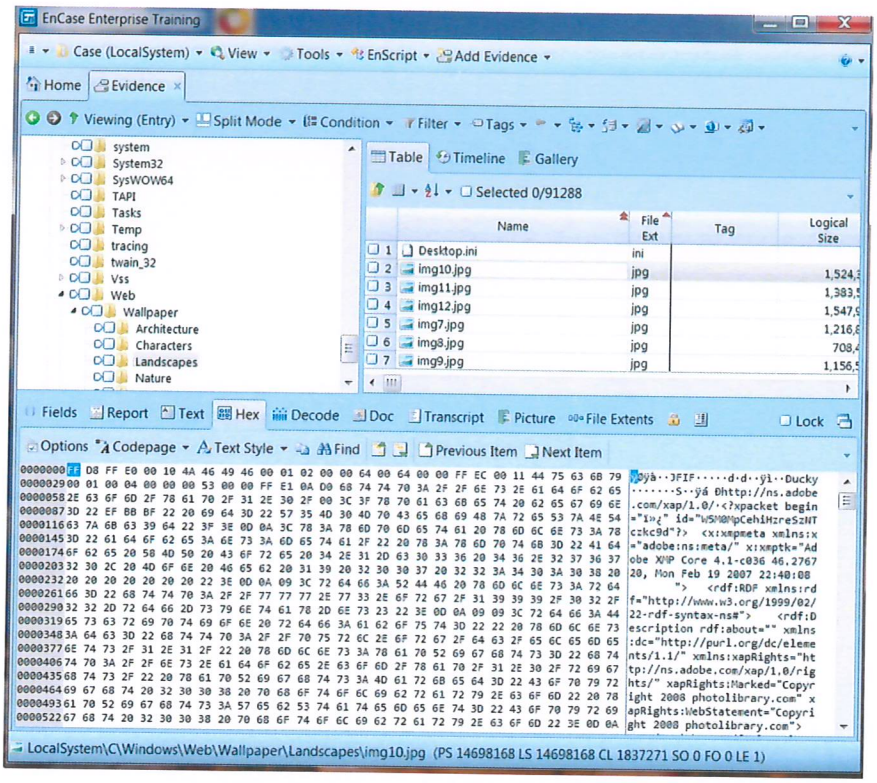

Figure 2-27 Viewing a picture in the View Pane as hex

When the EnCase window is not maximized or is reduced in size, the buttons change. The icons are still displayed but the corresponding descriptive text is not displayed. Compare the following screenshot to the previous figure. *Mouse over* the buttons to reveal their identity.

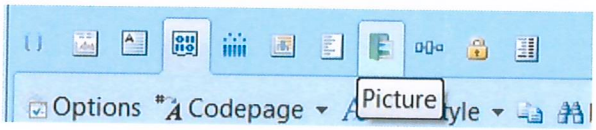

Figure 2-28 Viewing a picture as hex – see buttons above View Pane

Here is a text file (a cookie) displayed in Text view. The default viewing option is designed to fit to the width of the window pane (FTP).

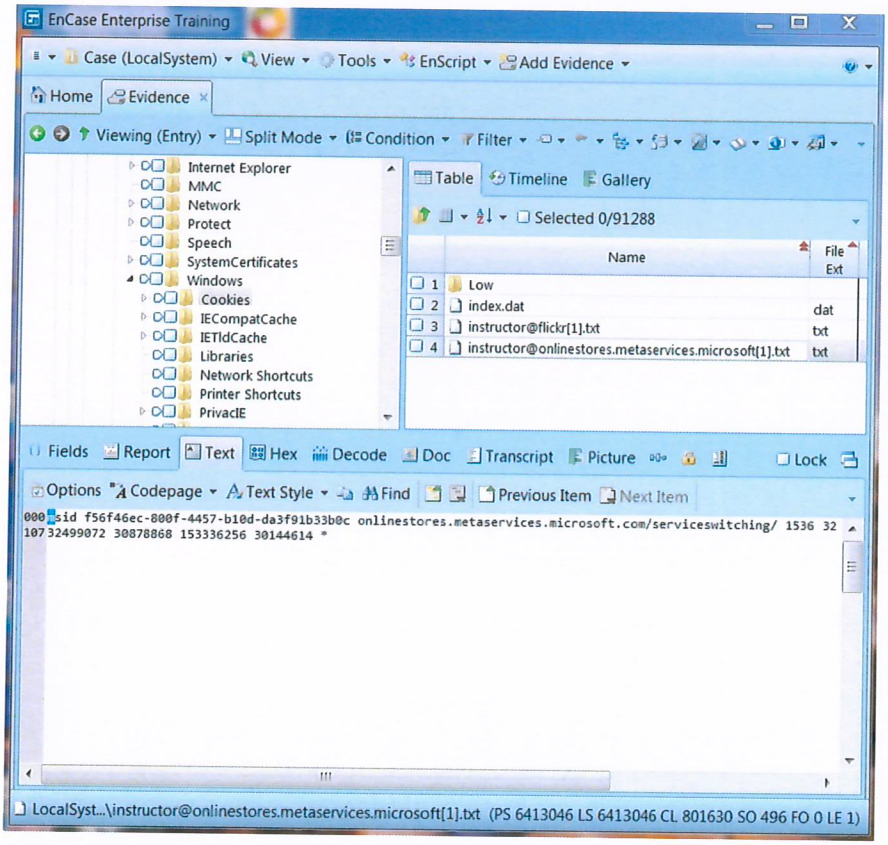

Figure 2-29 Text file in the View Pane

Here is the same text file displayed with a viewing option designed to obey soft or hard returns, and if none exist, to begin on the next line after 80 characters. The Options button above the View Pane is used to adjust settings within the Text view.

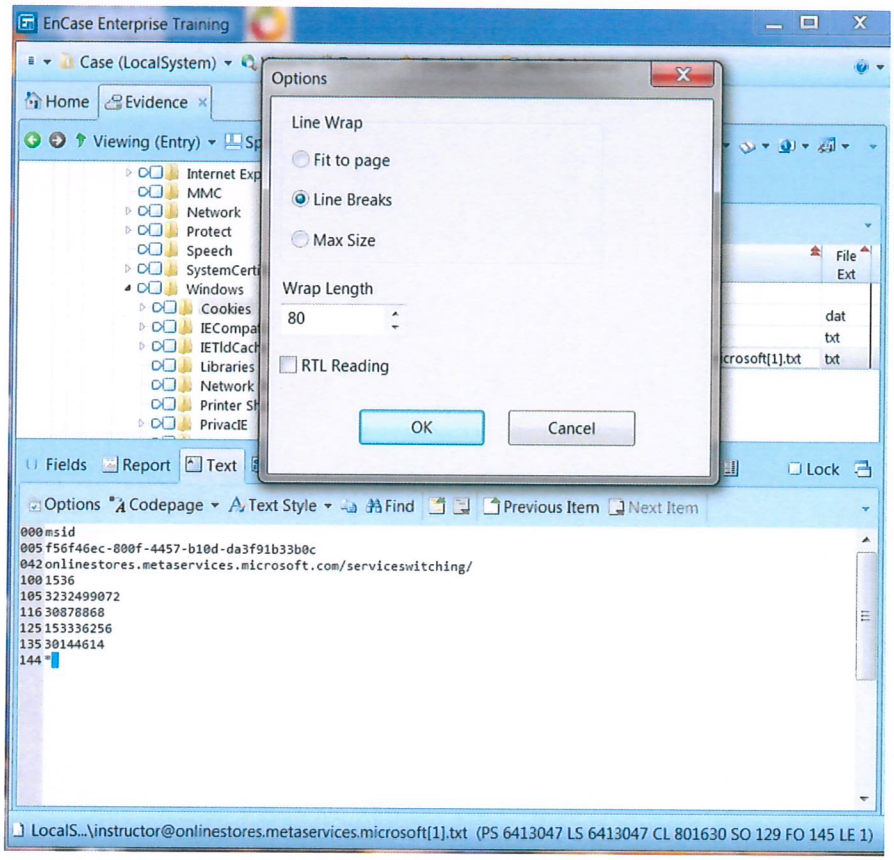

Figure 2-30 Text file in the View Pane