Lesson 2

Navigating EnCase® Forensic

EnCase® Forensic (EnCase) opens into the **Cases→Home** view by default when a new case is created. Because numerous cases can be open at the same time, this view is used to display the open cases.

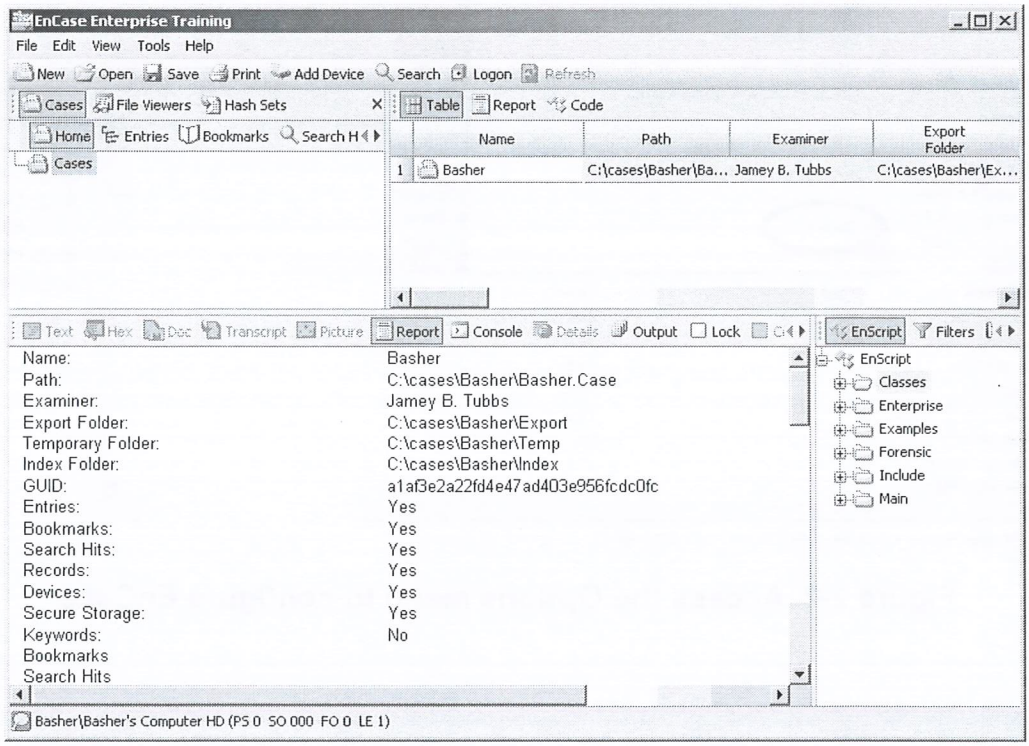


Figure 2-1 The four panes of EnCase Home view

There are many subtabs that provide additional functionality in the ability 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.

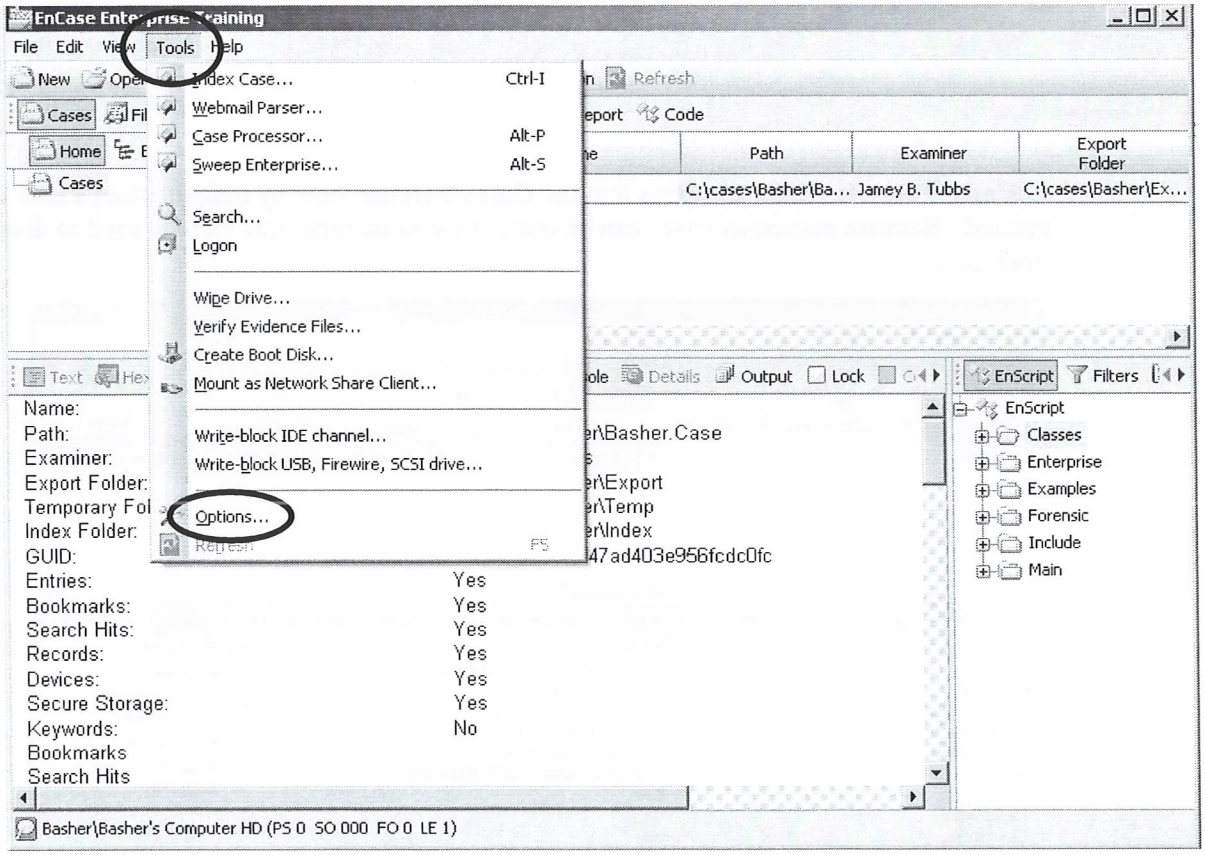


Figure 2-2 Access the Options menu to configure EnCase

Eight tabs are available: Global, Debug, NAS, Colors, Fonts, EnScript, and Storage Paths, and Enterprise. When a case is open, a ninth tab (**Case Options)** appears that allows creation/modification of default values for the case information.

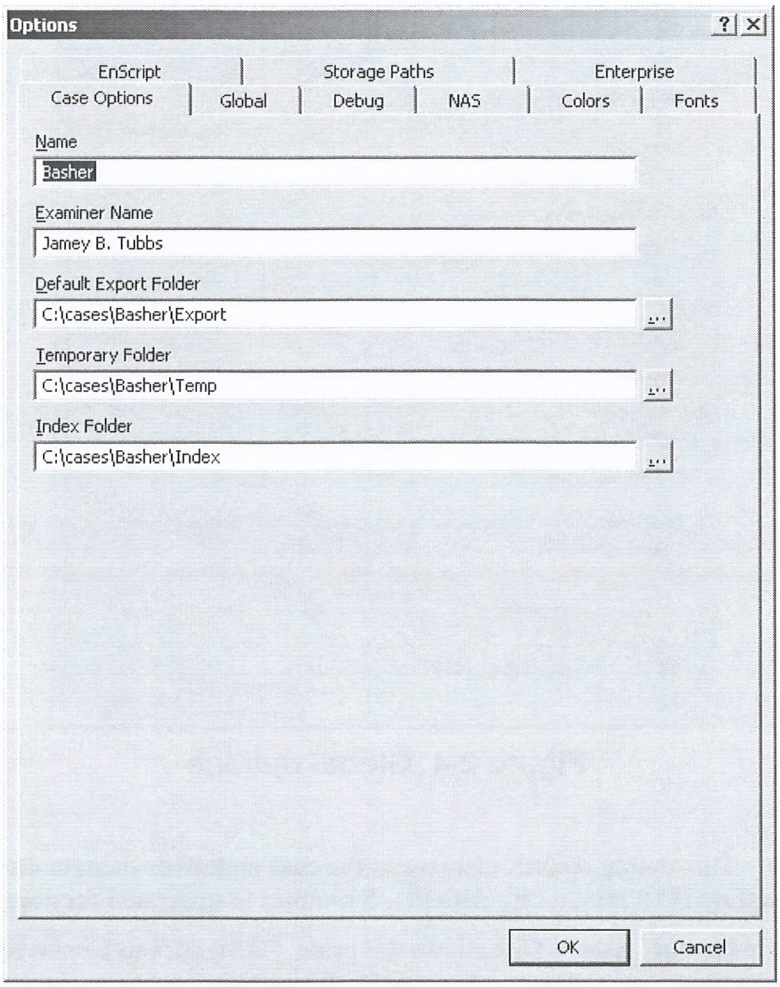


Figure 2-3 Case options – set when the case is created

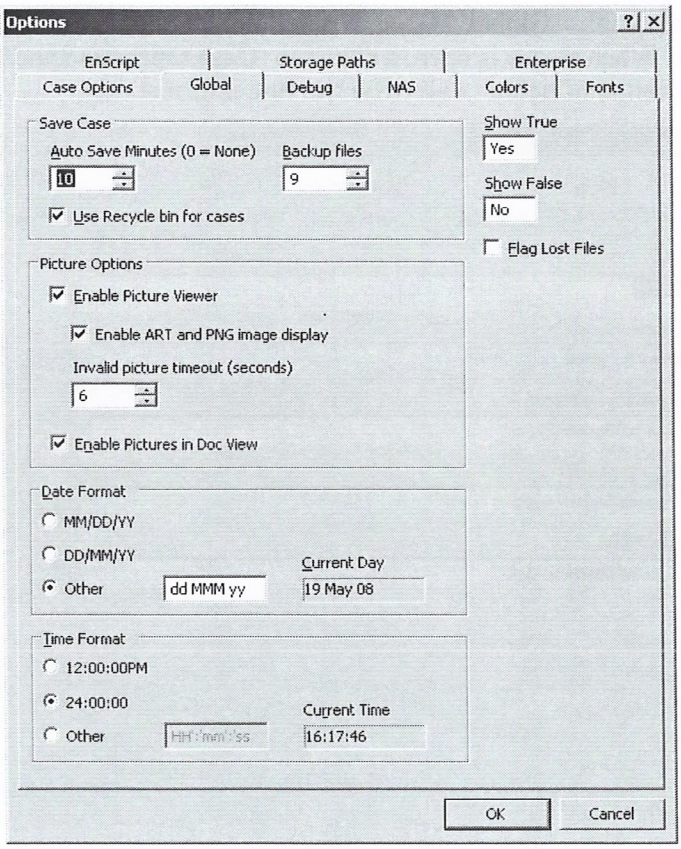


Figure 2-4 Global options

Auto Save – This option records changes to the case and saves them to the .CBAK (backup) case file. The setting is 10 minutes by default – 5 minutes is suggested for normal operations.

Use Recycle bin for cases – This allows the prior .CASE files to be moved to the Recycle Bin rather than permanently deleted. This enables for recovery in the event that the primary case file becomes corrupted. Unless an examiner experiences corruption issues, it is recommended that this option ***not*** be employed.

Show True / Show False – This option 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."

Enable Picture Viewer – This option allows pictures to be displayed in various views.

Enable ART and PNG image display – This option 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 – This option enables EnCase to stop trying to read a corrupted image file and to instead cache that file, so that EnCase will not attempt to read it in the future. The default is 12 seconds.

Enable Pictures in Doc View – This option determines whether images are displayed using Outside In technology in the Doc panel of the View Pane.

Date/Time Formats – This option configures the display of these items.

Flag Lost Files – This option is unchecked by default, which means that lost clusters are treated as unallocated space decreasing the amount of time required to access the evidence file through a case file. If this option is checked, EnCase will tag all lost clusters in Disk view (indicated by yellow blocks with a question mark). This option must be set before an evidence file is added to the case.

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

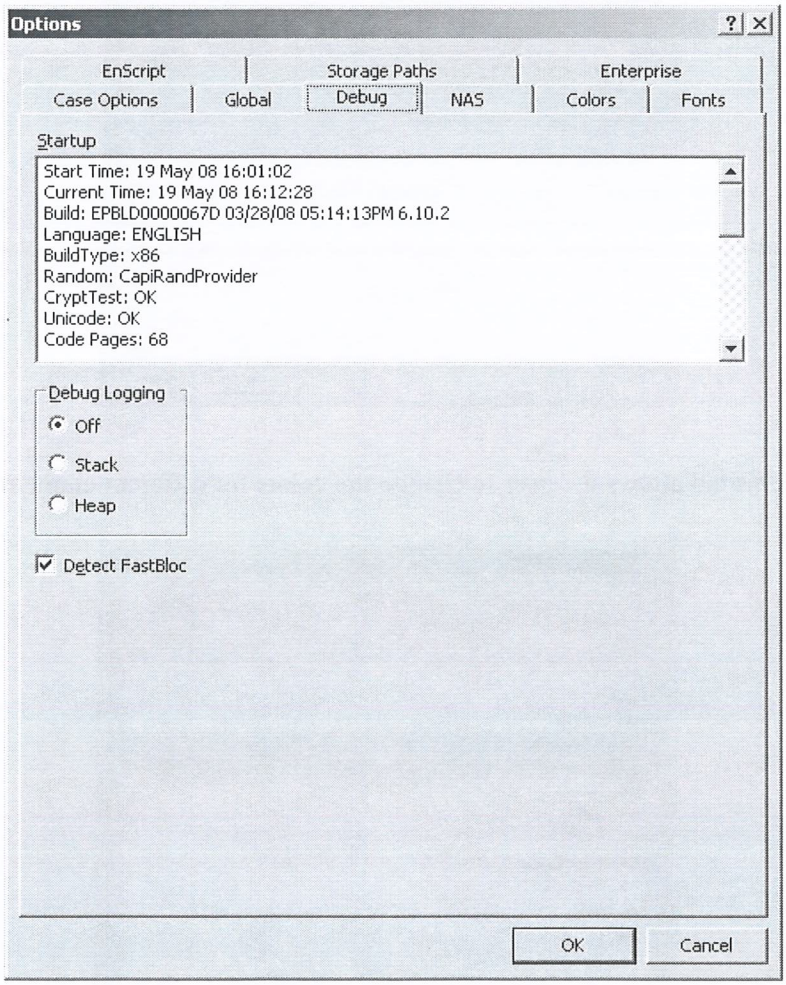
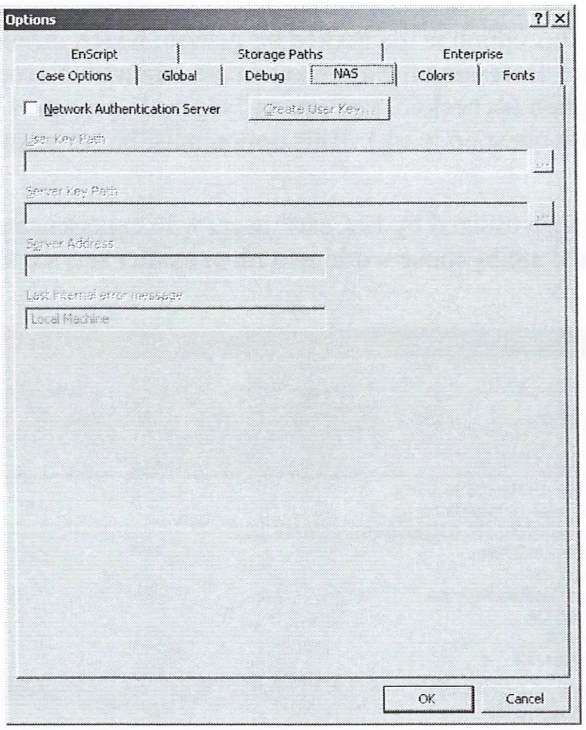


Figure 2-5 Debug tab

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.



Colors – This tab allows the user to change the colors for different elements of the EnCase® interface.

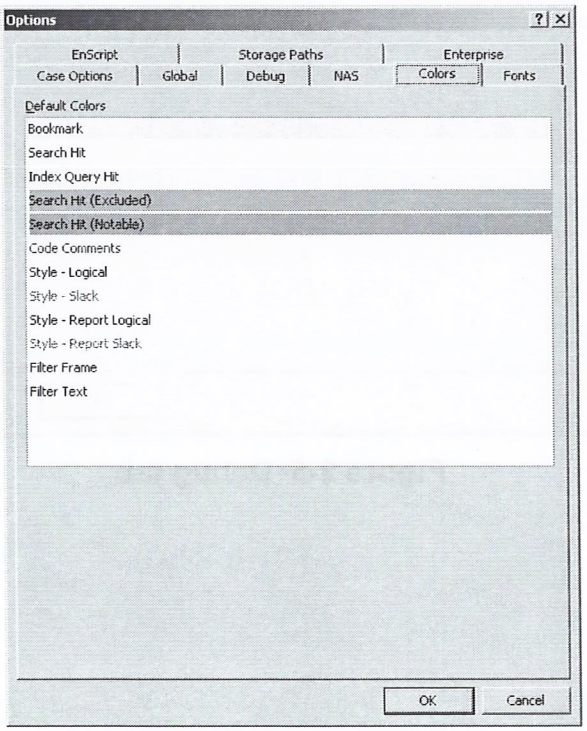


Figure 2-6 Color options

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.

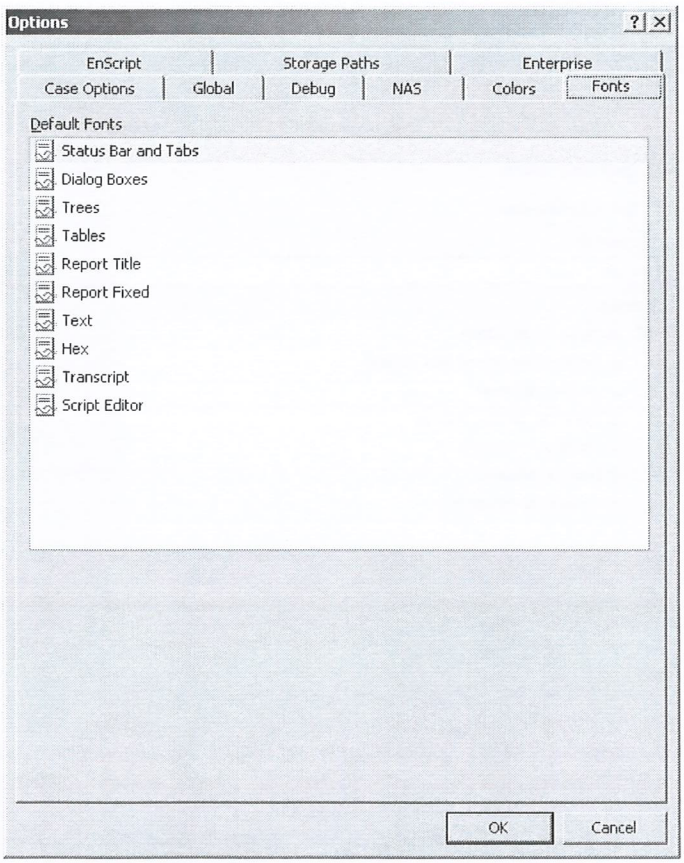


Figure 2-7 Fonts options

EnScript – These are small programs that automate examination processes. This option specifies the location of the EnScript® libraries folder, which contains programming modules used by multiple EnScript® programs.

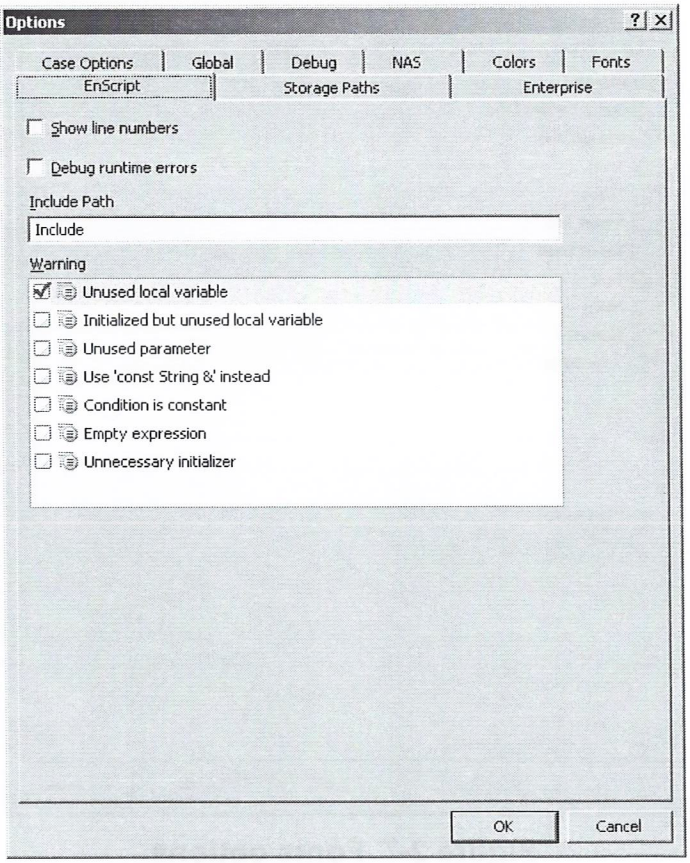


Figure 2-8 EnScript options

Storage Paths– This option allows an examiner to configure the location of .INI files used by EnCase to establish global settings. By default these files are stored in C:\Program Files\EnCase6\Config. These files may be placed on a networked drive that is accessed by multiple examiners. In this situation the files should be writable only for the examiner maintaining the configuration files. If the .INI files are stored on the local machine, examiners have the ability to modify them at any time. The examiner can also select the locations for the Index folder, record cache folder, as well as the case backup file folder location.

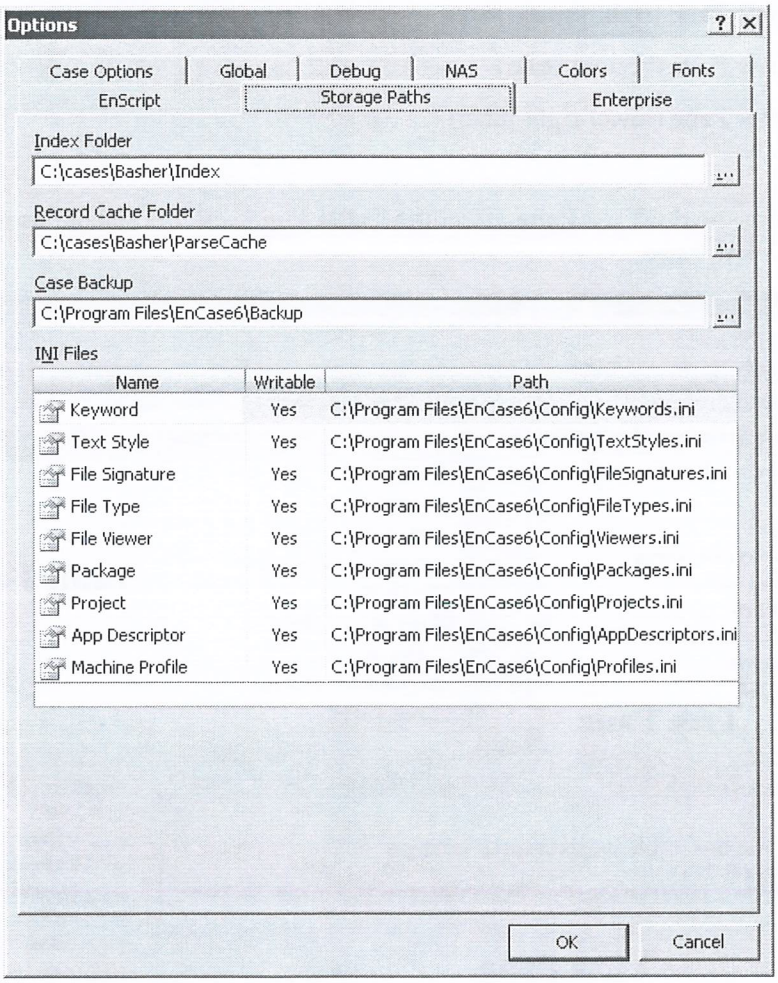


Figure 2-9 Storage path options

BASIC LAYOUT

To see the file structure of a particular evidence file linked to a case file, select the **Cases→Entries→Home** view.

The screen is initially divided into four sections:

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

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

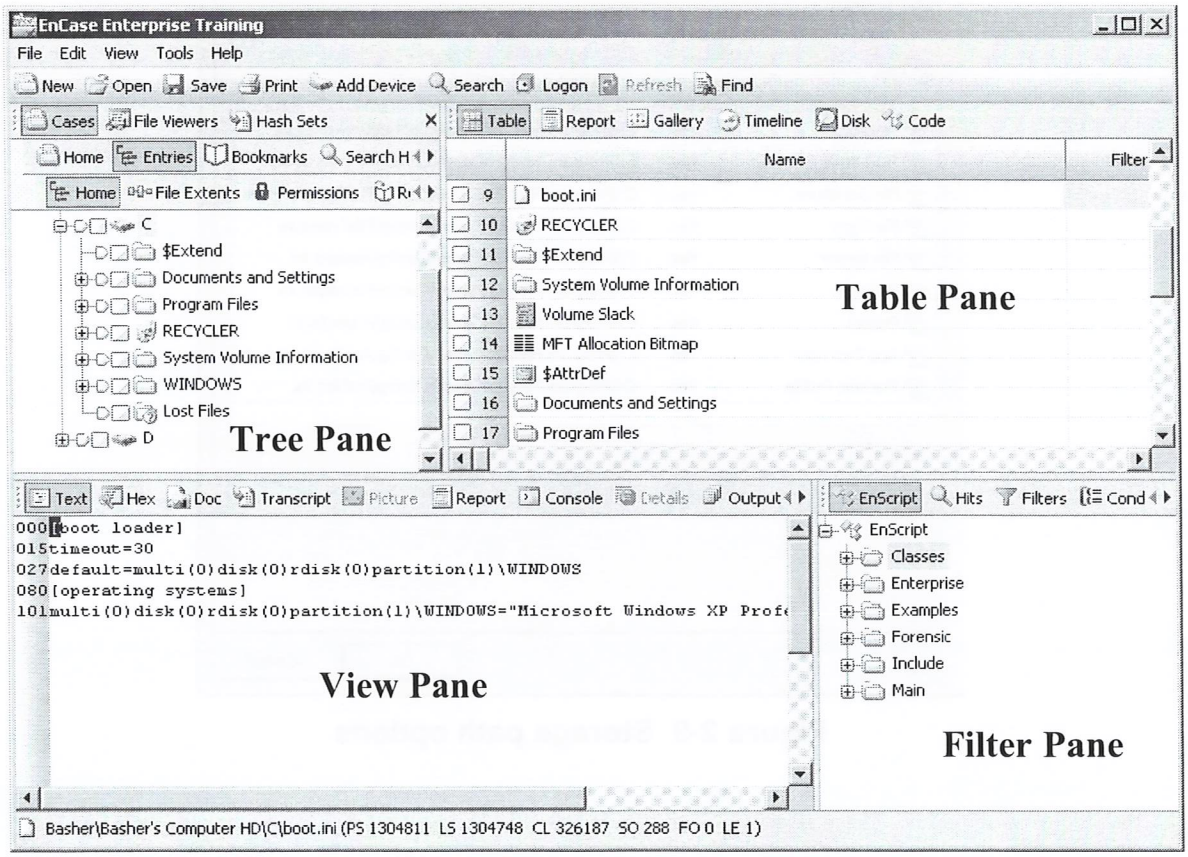


Figure 2-10 View of the four panes

Tree Pane / Cases View

Within the Tree Pane and the Cases→Entries→Home 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 plus and minus signs can be used to expand and contract the tree structure just as they are used in Windows® Explorer.

Right-clicking on an *object* in the Tree Pane will bring up a context menu with many selections, including the choice to expand or contract everything from the selected position. Everything in the case will be affected by right-clicking on the Entries folder.

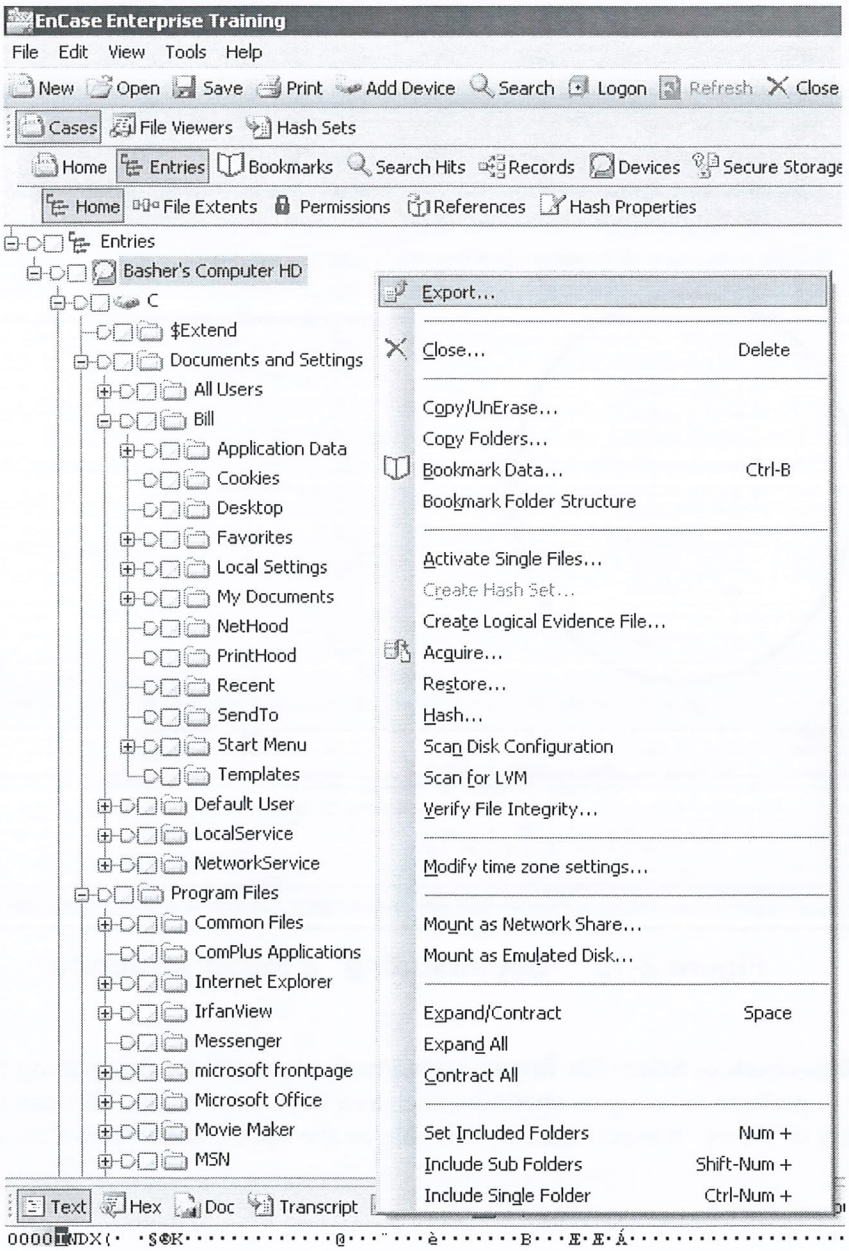


Figure 2-11 Contracting a folder structure

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.

The **Set Include Option** (sometimes called "home plate") method 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 to the tree of the folder name in the Tree Pane in the Cases→Entries→Home 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.

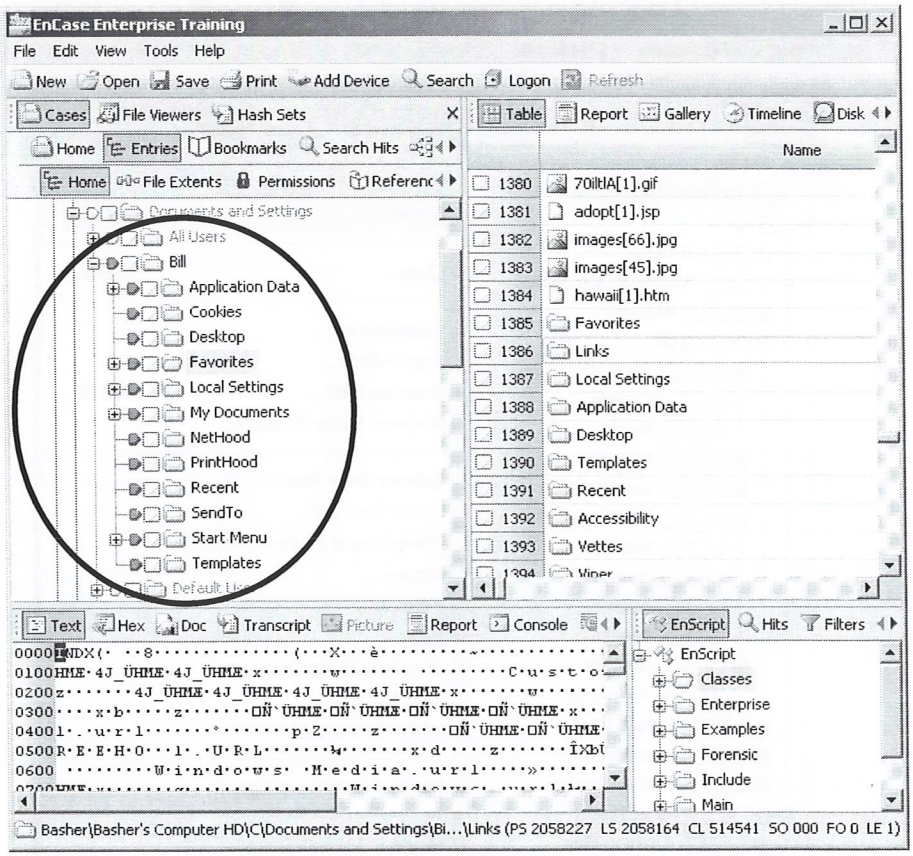


Figure 2-12 "Set including" a folder structure

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 to the tree of the entry name in any view.

In the example below, seven folders have been **selected**. These folders have a **white background** within the *blue-checked* square indicating all entries within the folder have been selected. The Documents and Settings folder has a **gray background** within the blue-checked square indicating not all entries within the folder have been selected. The **Dixon Box** between the Table and View Panes indicates how many **entries** have been **selected.** To deselect all entries, click within this Dixon Box to remove the blue check, and to remove blue checks from elements of the Cases→Entries→Home view and the Table Pane.

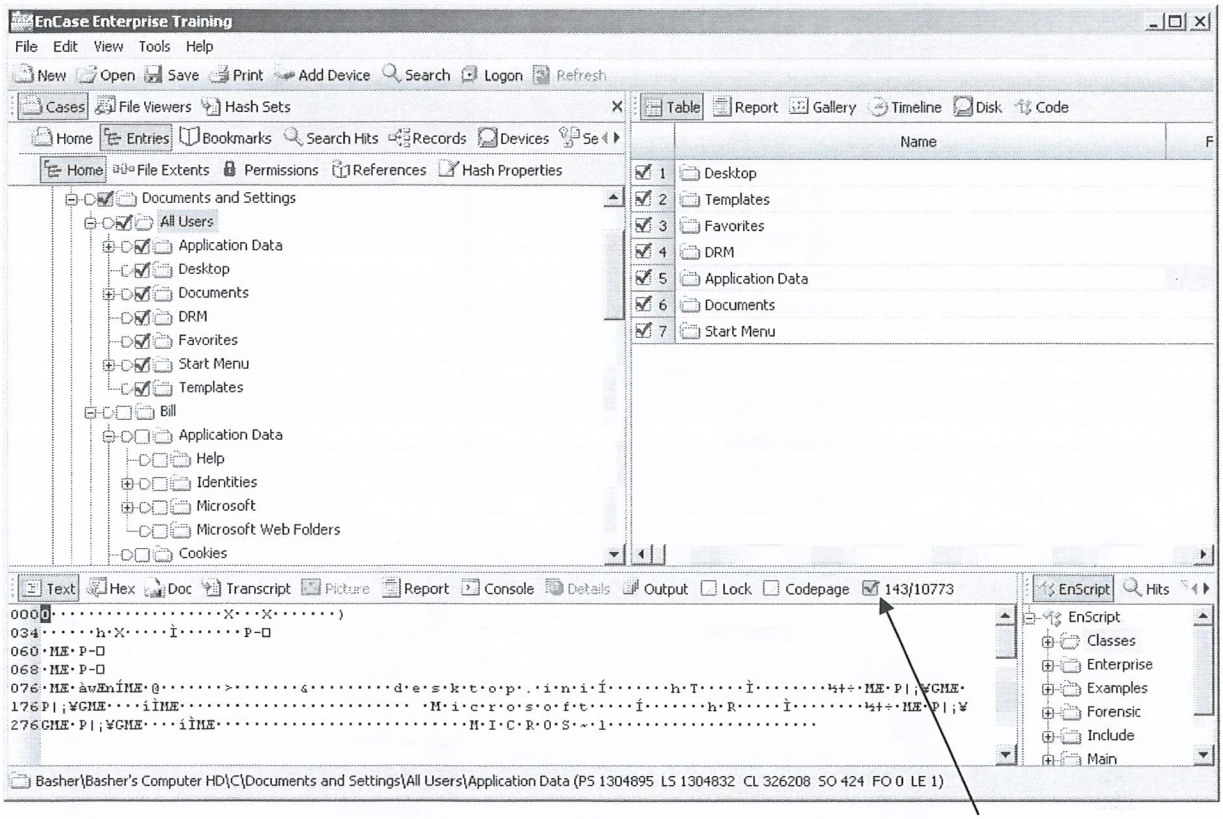


Figure 2-13 "Blue-checking" entries and the Dixon Box

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→Cases menu. Any tabs not displayed above the Tree Pane will be displayed by selecting them through the View→Cases menu.

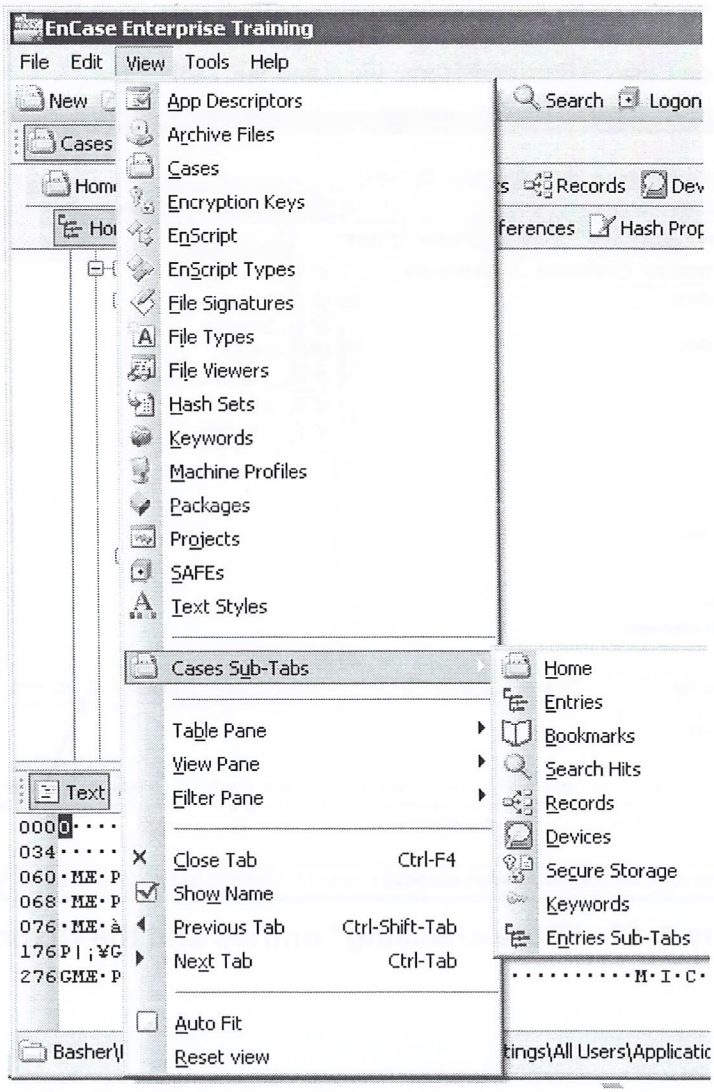


Figure 2-14 View→Cases menu

Table Pane

By default the Table Pane is in the Table view. Within this view are the subfolders and files that are contained within the folder(s) that 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.

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 *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, signature analysis, copying, exporting. With the Set Include Option feature activated, the select operation will not alter the number of files/folders displayed in the Table Pane.

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

- **Name** identifies the file/folder/volume, etc., in the evidence file
- **Filter** specifies the name of the filter run to display this entry
- **In Report** indicates whether or not the item will appear in the Report view
- **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 Type** table
- **Signature** displays the results of a file signature analysis
- **Description** describes the *condition* of the entry – whether it is a file or folder, deleted, or deleted/overwritten
- **Is Deleted** displays "Yes" if the entry is in a deleted state; "No" 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, edited, and then saved
- **Entry Modified** indicates for NTFS and Linux when the administrative data for the file was last altered

- **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
- **Physical Size** specifies the size of the storage areas allocated to the file
- **Initialized Size** is the size of the file when it is opened. Applies only to NTFS file systems.
- **Starting Extent** identifies the starting cluster of the entry
- **File Extents** displays the cluster fragments allocated to the file. Click within this column for an entry, and then click on the Details tab in the View Pane to see the cluster fragments.
- **Permissions** shows security settings of a file or folder
- **References** lists the number of times the selected entry is bookmarked
- **Physical Location** is 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** is where the entry resides
- **File Identifier** is 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
- **Hash Value** is a 128-bit value for a file entry generated by a hash analysis process
- **Hash Set** displays the hash set to which a file belongs generated by including hash sets in a hash library in a hash analysis process
- **Hash Category** displays the hash category to which a file belongs generated by including hash sets in a hash library in a hash analysis process
- **Hash Properties** displays whether or not the individual object is part of a hash set and whether or not that file is notable or Known
- **Full Path** identifies the location the file is located within the evidence file, including the evidence file name and a volume identifier
- **Short Name** is the name Windows gives the entry using the DOS 8.3 naming convention
- **Unique 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, and 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 a subsequent object

Organizing Columns

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

Columns may be sorted by up to five layers deep. To sort by a column, double-click on the column heading. To institute a subsort, hold down **Shift** and double-click on the column heading.

Columns may be *locked* on the left side of the Table view, so that when the examiner scrolls to the right of the Table view, the initial columns are still visible. To lock a column, right-click on the column heading, select **Columns** and select **Set Lock**. The lock is instituted on the position of the column. If other columns are moved into that position, they are locked. To release the lock, right-click on the column, select **Columns** and then **Unlock**.

Other Table Pane Views

Report – Generates a quick report for indicated files in the Table Pane. Used most often with graphics. To include entries in the Report view, right-click on the **In Report** column for the desired entry, and select **In Report**. The column for that entry should change to **Yes** (whatever representation you have for "yes" in the Show True/False options in the Tools→Options→Global menu). To change multiple entries, select them with a blue-check, right-click in the **In Report** column, and select **In Report – Invert Selected Items**.

Gallery – 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 the increase of the number of images displayed at any one file, right-click in the Gallery and select **Fewer/More Columns/Rows**. AOL .ART files may be displayed (in Windows 2000) if the Internet Explorer AOL support module is installed, which can be retrieved from:

www.microsoft.com/windows2000/downloads/recommended/aolfix/default.asp.

Timeline 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.

Disk View – Allows viewing of files and folders in terms of where the data appeared on the media. Placement of clusters and/or sectors and fragmentation of files may be observed.

Code View – Displays an EnScript tab in the Filter Pane.

View Pane

The View Pane displays the contents of the item highlighted in the Table Pane. The Console view is an option to copy data from *status* screen displays showing the results of an analysis process.

The View Pane has default settings that should be understood. Initially the View Pane defaults to the Report view. EnCase checks the contents of the file highlighted in the Table Pane to see if it is an image that can be decoded internally. If so EnCase will provide the ability for the user to select the Picture view in the View Pane and display the image.

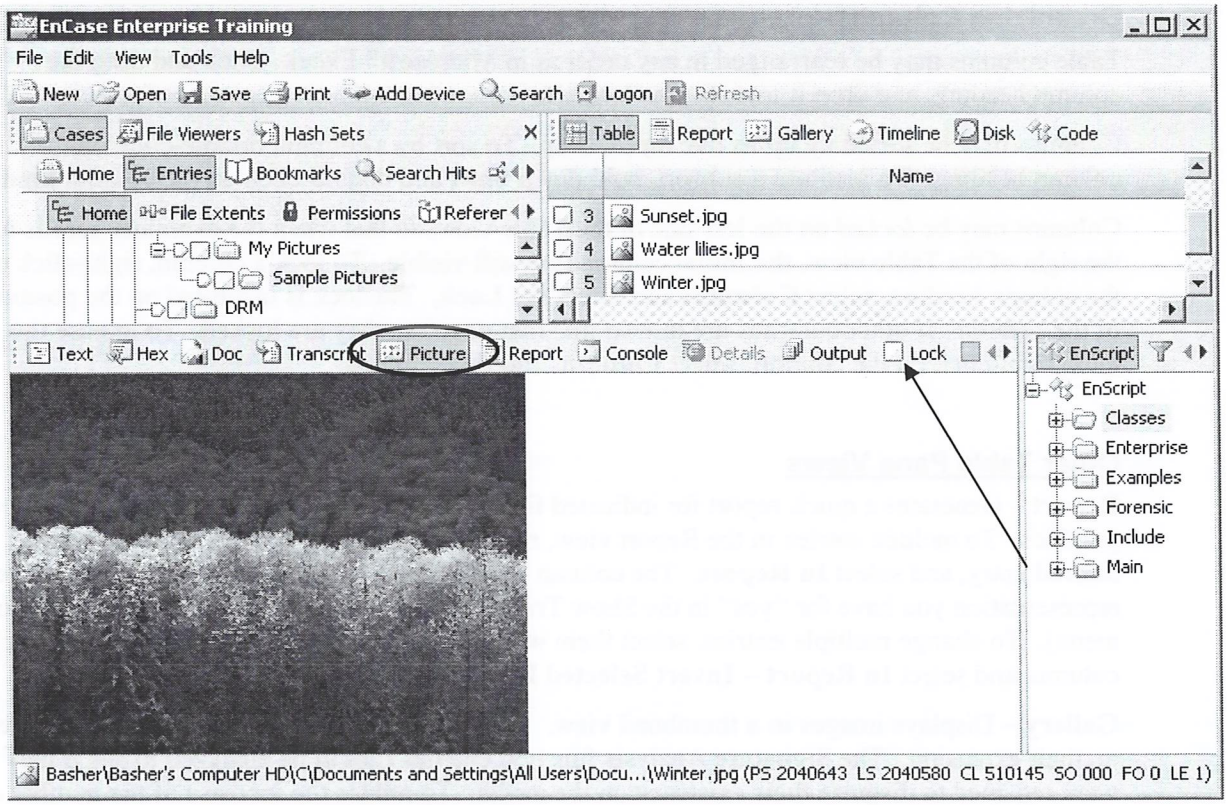


Figure 2-15 Picture view in View Pane

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 the Hex or Text view, he 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 is viewed in Hexadecimal.

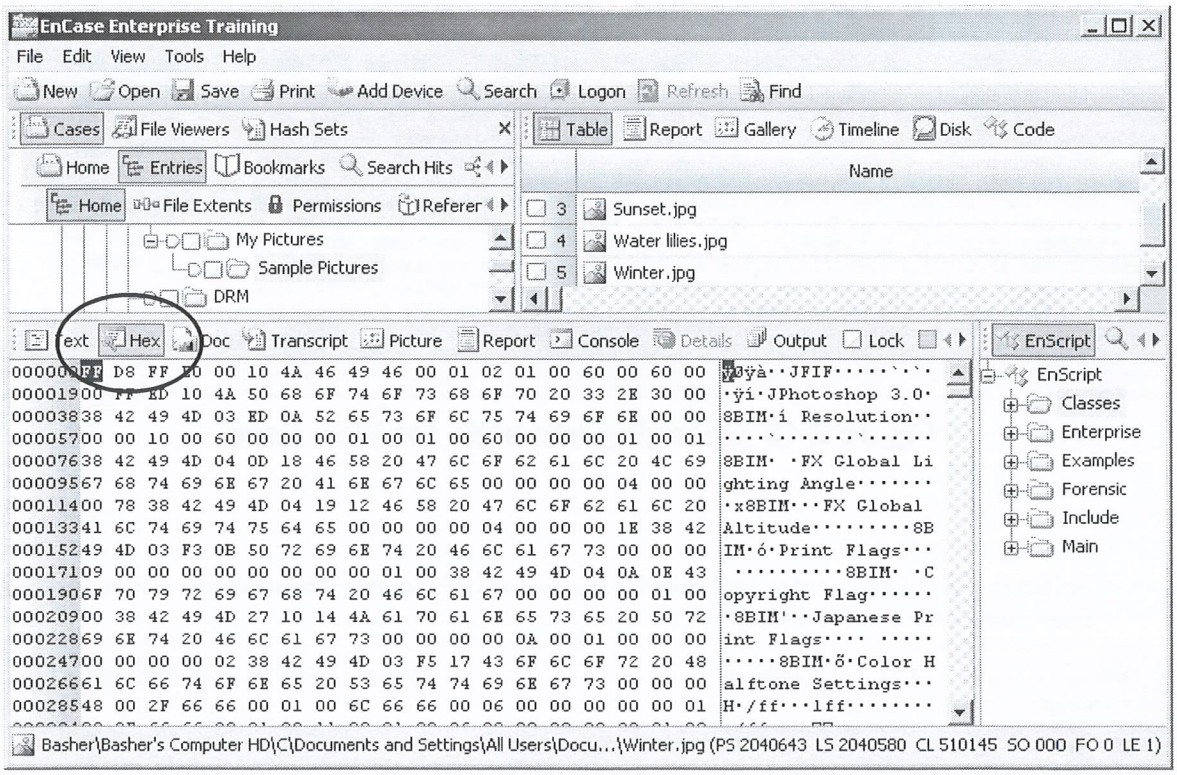


Figure 2-16 Viewing a picture in the View Pane as hex

Here is a text file displayed in Text view.

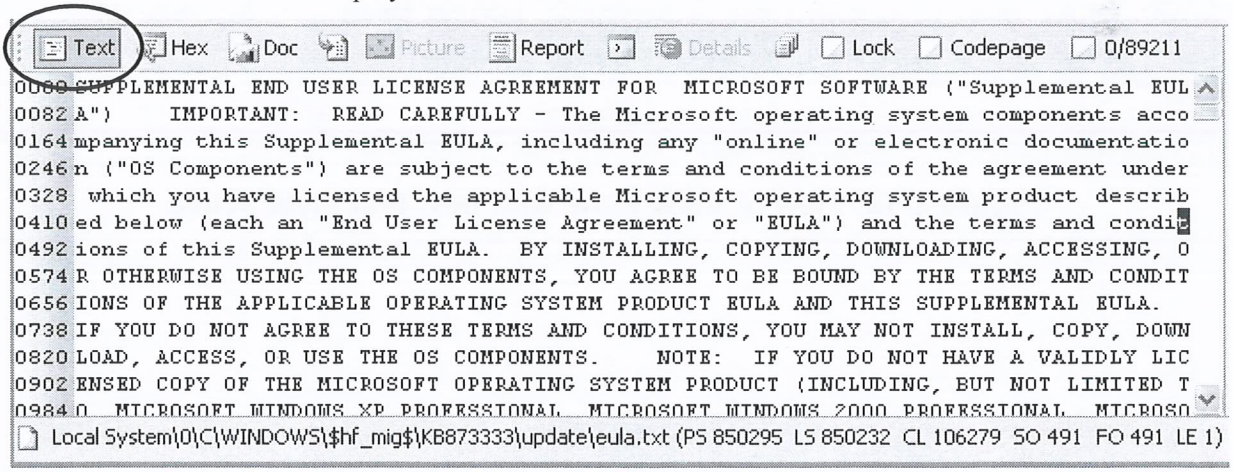


Figure 2-17 Text file in the View Pane

Although the text is readable, its format can be improved by altering the text style from the **Text Styles** tab in the Filter Pane.

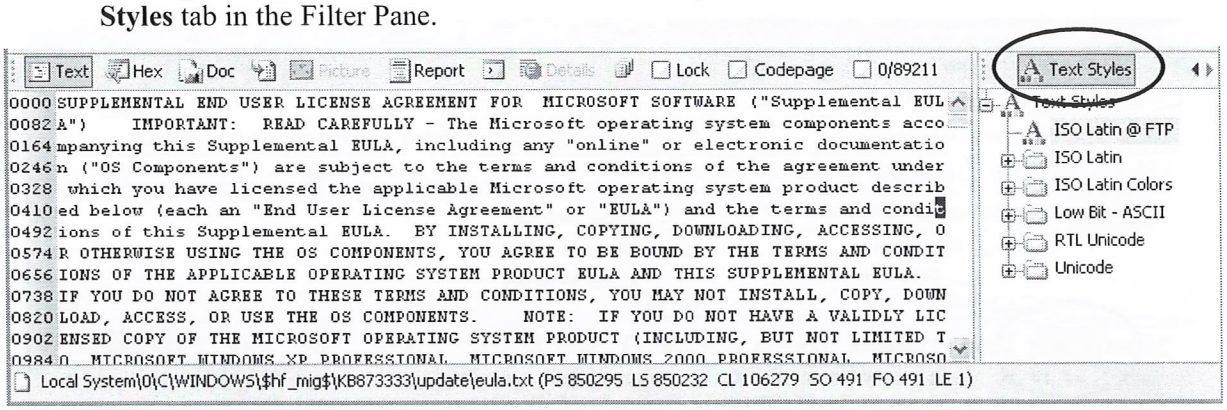


Figure 2-18 Changing text style for View Pane

Select the ISO Latin folder, and then ISO Latin @ 100 within. The changes will be displayed immediately in the View Pane.

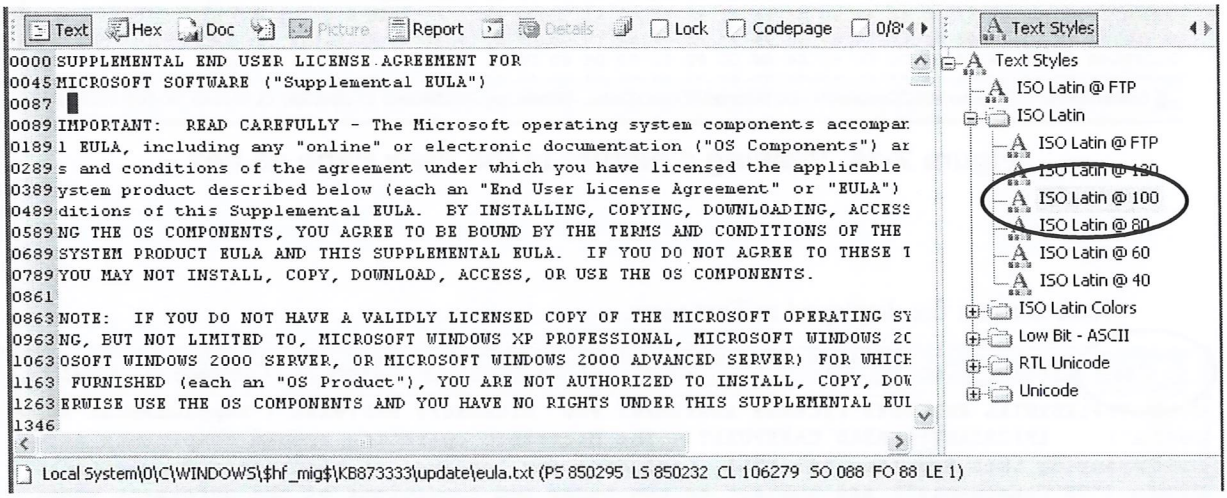


Figure 2-19 View of View Pane with new text style active

It is important to be aware of one's current positioning within the case especially when documenting the location of evidence found in unallocated space. The status bar found at the bottom of the screen will provide that information.

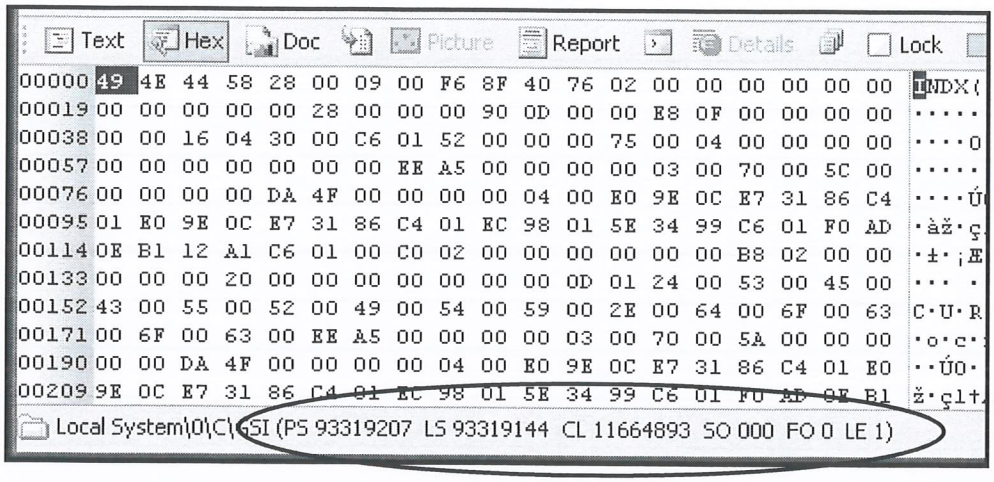


Figure 2-20 Location of status bar

The codes are translated as follows:

PS Physical sector number

LS Logical sector number

CL Cluster number

SO Sector Offset – The distance in bytes from the beginning of the sector

FO File Offset – The distance in bytes from the beginning of the file

LE Length – The number in bytes of the selected area

The status bar also shows the full path of the item highlighted, and if a deleted/overwritten file is highlighted, it indicates the overwriting file.

Notes