



**EnCase<sup>®</sup> Forensic Version 7  
Preview  
New Features Guide**

Copyright © 2007-2011 Guidance Software, Inc. All rights reserved.

EnCase®, EnScript®, FastBloc®, Guidance Software® and EnCE® are registered trademarks or trademarks owned by Guidance Software in the United States and other jurisdictions and may not be used without prior written permission. All other marks and brands may be claimed as the property of their respective owners. Products and corporate names appearing in this work may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation into the owners' benefit, without intent to infringe. Any use and duplication of this work is subject to the terms of the license agreement between you and Guidance Software, Inc. Except as stated in the license agreement or as otherwise permitted under Sections 107 or 108 of the 1976 United States Copyright Act, no part of this work may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise. Product manuals and documentation are specific to the software versions for which they are written. For previous or outdated versions of this work, please contact Guidance Software, Inc. at <http://www.guidancesoftware.com>. Information contained in this work is furnished for informational use only, and is subject to change at any time without notice.

# Contents

---

<b>Overview</b>	<b>3</b>
Purpose of this Guide.....	4
EnCase Forensic .....	4
New Features .....	5
<b>Installation and Configuration Changes</b>	<b>7</b>
Overview .....	8
Using an EnCase Dongle.....	8
Using the EnCase Installation Wizard .....	8
EnCase Version 7 Application Folder Locations .....	9
<b>Getting Started with EnCase Version 7</b>	<b>13</b>
Overview .....	14
Launching EnCase for the First Time.....	14
Creating a Case.....	15
Adding Evidence to a Case .....	18
Browsing Case Data.....	20
Setting Case Options .....	22
Working with Cases.....	22
<b>Evidence Processor</b>	<b>25</b>
Overview .....	26
Configuring Time Zone Settings .....	27
Preparing the Evidence to Process.....	27
Managing Evidence Processor Settings.....	29
<b>Working with Email Evidence</b>	<b>37</b>
Overview .....	38
Displaying Email Threads .....	39
Deduplicating Messages .....	42
<b>Hashing</b>	<b>43</b>
Overview .....	44
Hashing Features.....	44
Working with Hash Libraries .....	45

<b>Tagging</b>	<b>51</b>
Overview .....	52
Creating Tags .....	52
Viewing Tagged Items .....	54
Hiding a Tag .....	54
Deleting Tags.....	55
<b>Using Search Tools</b>	<b>57</b>
Overview .....	58
Search Types .....	58
Creating a Search Query .....	59
Index Query Options .....	60
Unifying Search Results.....	66
Targeted Keyword Searches .....	69
<b>Reporting</b>	<b>71</b>
Overview .....	72
Using Report Templates.....	72
Bookmarking Data for Reports .....	72
Report Template Structure .....	73
Formatting Report Templates.....	75
Report Styles .....	76
Viewing a Report.....	77
<b>Index</b>	<b>79</b>

# Overview

- Purpose of this Guide
- EnCase Forensic
- New Features

## Purpose of this Guide

This guide highlights some of the key new features of EnCase Version 7 that distinguish it from previous versions. The book is not meant to be a user's guide, but rather a view into the new look and enhanced capabilities of this potent investigative tool. Chapters are oriented toward the new capabilities of EnCase and providing users familiar with prior versions of EnCase previews and descriptions of what is to come.

## EnCase Forensic

EnCase Forensic provides investigators with a single tool for conducting large-scale and complex investigations from beginning to end. It features superior analytics, enhanced email/Internet support, and a powerful scripting engine.

With EnCase Forensic you can:

- Acquire data in a forensically sound manner using software with an unparalleled record in courts worldwide.
- Investigate and analyze data from multiple platforms—Windows, Linux, AIX, OS X, Solaris, and more—using a single tool.
- Find information despite efforts to hide, cloak, or delete.
- Easily manage large volumes of computer evidence, viewing all relevant files, including deleted files, file slack, and unallocated space.
- Transfer evidence files directly to law enforcement or legal representatives as necessary.
- Review options that allow non-investigators, such as attorneys, to review evidence with ease.
- Use reporting options for quick report preparation.

### Forensically Sound Acquisitions

EnCase Forensic produces an exact binary duplicate of the original drive or media, then verifies it by generating MD5 hash values for related image files and assigning Cyclic Redundancy Check (CRC) values to the data. These checks and balances reveal any inconsistencies with acquired data. The new version of EnCase Forensic maintains the reliability and functionality of previous versions, while simplifying usage, adding powerful new features, and significantly increasing performance.

EnCase Forensic is accessible to several types of user:

- Those responsible for collecting evidence.
- Forensic examiners and analysts.
- Forensic examiners who develop and use EnScript code to automate repetitive or complex tasks.

### Forensic Workflow

EnCase Forensic Version 7.01 facilitates the forensic workflow process through the:

1. Preview and processing of case data.
2. Analysis of evidence.
3. Reporting of findings.

## New Features

EnCase Forensic Version 7 contains a set of new features and functionality that simplify how forensics is applied to investigating digital media. Following are key features of this release:

- A new user interface that consolidates functionality and simplifies navigation.
- The ability to speed up case responsiveness and the availability of information through the new Evidence Processor. The Evidence Processor prepares a case by conducting key processing tasks like creating an index, hash analysis, signature analysis, protected file analysis, Internet and email processing, as well as keyword searching.
- EnCase now contains a high-performance indexing engine. This engine makes searching faster, and displays search results across multiple file types (for example, email messages, IM conversations, smartphones, and so forth) in one location.
- Increased scalability with efficient caching. File system, email, and other compound structures are cached to disk, reducing the time and system resources needed to review data that has already been processed. This allows EnCase to scale across large data sets.
- Email now appears as in familiar programs such as Microsoft Outlook or Lotus Notes. In addition, EnCase includes email threading and related conversations, allowing the review of conversation chains.
- More powerful and expanded capabilities for working with hashes, along with an easy to use and customizable user interface for managing hash sets and hash libraries.
- Define your own tags and associate them with files and email to keep track of important information. You can use these customized tags to filter data and generate reports.
- Completely customize your reports through a new reporting system that allows you to define all aspects of the report, including headers, footers, custom content, and formatting. You can now create reports of your evidence data with easy-to-use, supplied templates, edit those templates, or build your own custom reports.



# Installation and Configuration Changes

- Overview
- Using an EnCase Dongle
- Using the EnCase Installation Wizard
- EnCase Version 7 Application Folder Locations

## Overview

This chapter describes features associated with installing EnCase, such as using dongles, and the locations of new directories and files.

## Using an EnCase Dongle

Insert the dongle into a USB port *after* installing the software; only then can you run EnCase Forensic.

EnCase Forensic will work with either the Sentinel HASP dongle that was provided to EnCase Version 5 and Version 6 users, or the Codemeter dongle that is new to EnCase Version 7.

### *Sentinel HASP Dongle*

If you have a previous version of EnCase Forensic, you will be installing the HASP drivers along with the product.

If you are upgrading, and do not already have the HASP drivers installed, or the drivers need to be updated, make sure that the box for installing HASP drivers is checked when running EnCase Forensic.

### *Codemeter Dongle*

If you are a new user of EnCase Forensic, use the new Codemeter dongle provided with the product.

## Using the EnCase Installation Wizard

To install EnCase Forensic on your local machine:

1. Insert the application CD into your computer's CD player.
2. Wait for Autostart to begin.
3. The initial screen displays a field specifying the default install location of EnCase. You can use this default location, or enter your own installation path.
4. Click **Next** and click whether you are performing an **Install** or **Reinstall** of EnCase Forensic.
5. Click **Next**. Depending on your installation, the Installer may display **Install Help** and **Install HASP Drivers** checkboxes.
  - Guidance Software recommends that you check the box for **Install Help**.
  - You only need to install the HASP drivers if you are upgrading from a previous version of EnCase Forensic. If you are performing a reinstall and have already installed the HASP drivers and the checkbox is present, leave the box cleared. If you do *not* have a previous version of EnCase Forensic installed, the HASP drivers checkbox is not displayed.
6. Click **Next**.

When the installation wizard has finished copying and installing EnCase Forensic, reboot to complete the installation. Select whether to **Reboot Now** and complete the installation immediately, or **Reboot Later**.

7. After the computer has rebooted, insert the dongle into a USB port on your computer. You are now ready to start using the product.

## EnCase Version 7 Application Folder Locations

### *Application Folder*

This folder contains files created by the EnCase Installer that are *not* modified by EnCase.

- Windows 7 and Windows Vista default path: \Program Files\EnCase7
- Windows XP: \Program Files\EnCase7

Folder Name	Description
Certs	License certificates
Condition	Default conditions
Config	Application configuration options
Drivers	Application drivers
EnScript	Default EnScripts
Filter	Default filters
Help	Help files
Lib	Application library files
License	EnLicense files
Mobile	Mobile phone drivers
Noise	Default noise file
Template	Default case templates
ViewLib	Outside in libraries

### *User Data*

The following are user-created files that are not necessarily EnCase version or installation-specific..

- Windows 7 and Windows Vista path: \Users\\My Documents\EnCase
- Windows XP: \Documents and Settings\\My Documents\EnCase

**Backup:**

- Windows 7 and Windows Vista path: \Users\\My Documents\EnCase
- Windows XP: \Documents and Settings\\My Documents\EnCase

<b>Folder Name</b>	<b>Description</b>
Condition	User defined conditions
EnScript	User defined EnScripts
Filter	User defined filters
Keys	Encryption keys
Keyword	User defined keyword searches
Logs	Console logs
Search	User defined searches
Template	User defined case templates
Backup	Default case backup location

## *Case Folder*

This folder contains all files that make up a Version 7 case.

- Windows 7 and Windows Vista default path: \Users\\My Documents\EnCase\- Windows XP: \Documents and Settings\\My Documents\EnCase\-

<b>Item</b>	<b>Description</b>
Corrupt Pictures	Corrupt pictures
Email	Email thread database
Export	Default Case Export folder
Results	Results of search queries
Searches	Keyword search results (non-Evidence Processor)
Tags	Tag database
Temp	Default Case Temp folder

<Case Name>.Case                      EnCase Case file

## *Evidence Cache*

This folder contains the cache, index, and keywords results for a device, which are created by the Evidence Processor.

- Windows 7 and Windows Vista default path: \Users\\My Documents\EnCase\Evidence Cache\- Windows XP: \Documents and Settings\\My Documents\EnCase\Evidence Cache\-

<b>Item</b>	<b>Description</b>
Device Cache	Device caches
DeviceIndex	Device index
Searches	Keyword search results (Evidence Processor)

## *User Application Data*

This folder contains configuration files and temporary user files associated with a specific user and EnCase installation folder.

- Windows 7 and Windows Vista path: \Users\\AppData\Roaming\EnCase\EnCase7- <#>
- Windows XP: \Documents and Settings\\Application Data\EnCase\EnCase7- <#>
- 

<b>Folder</b>	<b>Description</b>
Config	User edited application configuration files

## *Global Application Data*

This folder contains files that are used to configure EnCase regardless of the user.

Windows 7 and Windows Vista path:

- \Users\All Users\AppData\EnCase
- \Users\All Users\AppData\EnCase\EnCase7- <#>

Windows XP:

- \Documents and Settings\All Users\Application Data\EnCase
- \Documents and Settings\All Users\Application Data\EnCase\EnCase7-<#>

**Note:** \Users\All Users\AppData = \ProgramData

<b>Item</b>	<b>Description</b>
Logos	Default report logo
Config	NAS and other global configuration files
ParseCache	Parse cache files
Storage	EnScript configuration files

## *Shared Files*

This is a folder location where you store shared files such as EnScripts, searches, conditions, keys, file types, text styles, and so forth.

- Windows 7 and Windows Vista path: <User Defined>
- Windows XP: <User Defined>

# Getting Started with EnCase Version 7

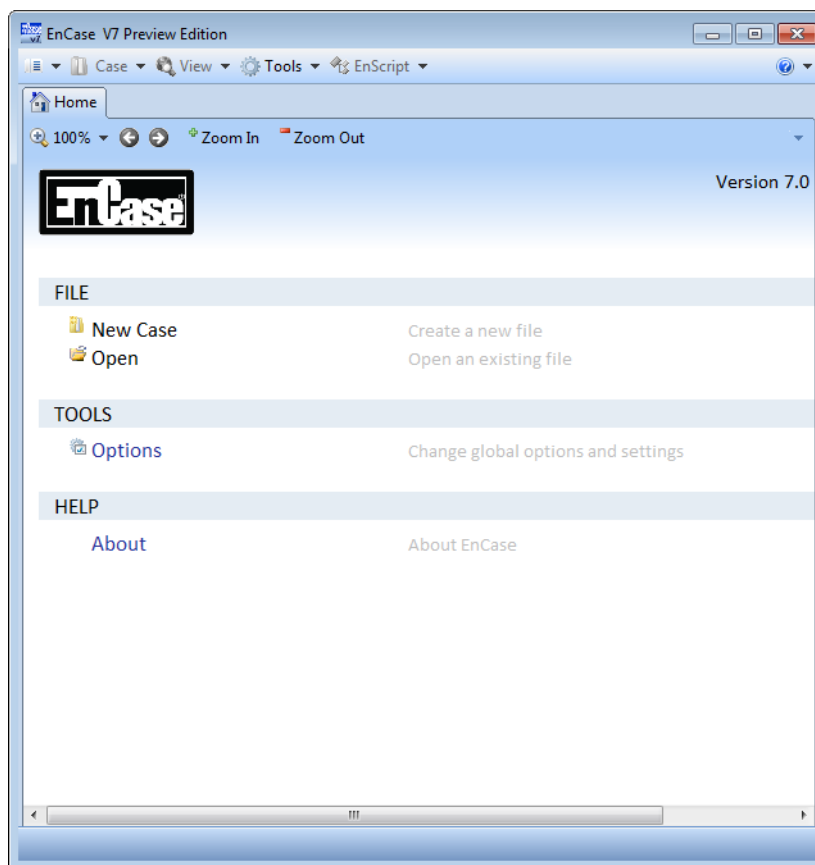
- Overview
- Launching EnCase for the First Time
- Creating a Case
- Adding Evidence to a Case
- Browsing Case Data
- Setting Case Options
- Working with Cases

## Overview

This chapter describes using EnCase to create and start work on a case, using its new user interface, explains how to navigate the interface to access EnCase features, and guides you through the initial stages of usage. Its purpose is to familiarize you with the new user interface design, and explain where the main features are located.

## Launching EnCase for the First Time

When you launch a fully licensed version of EnCase for the first time, your main screen appears as shown below:



The Home page, like all pages within EnCase, is divided into several sections, each with a specific set of functions. In descending order, they are as follows:

*Application Toolbar* Appears below the title bar, and provides drop-down menus to major functionality. The menus and their selections are primarily static throughout your investigation. The menus and their selections are discussed in more detail later in this chapter.

<i>Tabs</i>	Similar to tabs in Internet browsers, each top level tab displays a page that groups EnCase functionality. When you open EnCase for the first time, only the <b>Home</b> tab is available.
<i>Tab Toolbar</i>	These components include the back and forward arrows, which function the same as in any standard browser, and various viewing options that allow you to resize the panel dimensions to whatever best suits your needs. This toolbar also contains menus and buttons that are specific to the selected tab.
<i>Page body</i>	The Page body varies, depending on the tab that you are viewing. The Home page consists of labels that identify the product, case, the functionality available, and sections that identify categories of EnCase components and contain links to the features or actions belonging to each category.

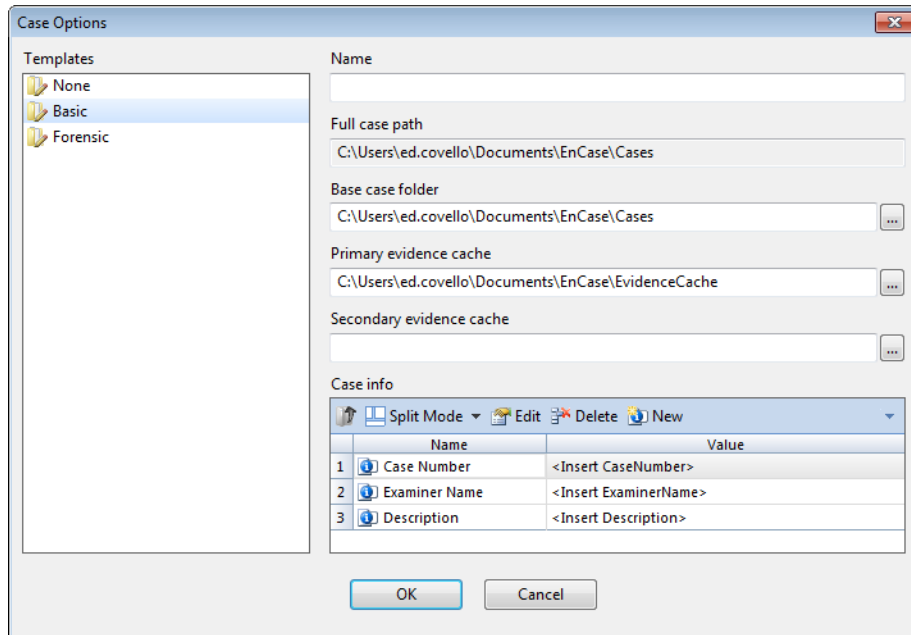
## Creating a Case

After installing and configuring EnCase, you can create a new case with an EnCase-supplied case template. Following are instructions for creating a new case with an EnCase-supplied case template. After you create a case, most of the EnCase features and their navigation paths become available. You begin creating a case from the Case pane.

To create a new case:

1. Click **New Case** beneath the FILE category on the Main panel body.
2. The Case Options dialog displays. This dialog is where you select a case template. You must also name the case.
3. In the figure below, the **Basic** template is selected.

4. You can enter a case **Name** at this point, then click **OK**.



When you create a new case, you will see a list of available templates (these are `.CaseTemplate` files). EnCase supplies several predefined templates, whose names appear in this box along with any saved templates.

To select a template:

- Click on a name from the case **Templates** list to select it. In the above figure, the **Basic** template is selected.

Although you can configure a new case completely from scratch, Guidance Software recommends using a template, as it simplifies the case creation process. Each case template contains a uniquely configured set of the following:

- Case Info items with default values
- Bookmark folders and notes
- Tag names
- Report template
- User-defined report styles

You can also create your own templates by saving any case as a template. Afterwards, the new template will appear in the **Templates** list and will be available for future use. If you intend to create a number of cases with a similar structure, it makes sense to save one of them as a template and use it to generate the other cases.

**Name:** A text string you enter to identify the Case file. In EnCase Version 7, a case is no longer contained within a single file, but is a folder containing many components. The name specified in this field will be used to name the Case folder, as well as components contained within that folder.

**Base Case folder:** The folder in which the case file is stored. This field is not writable.

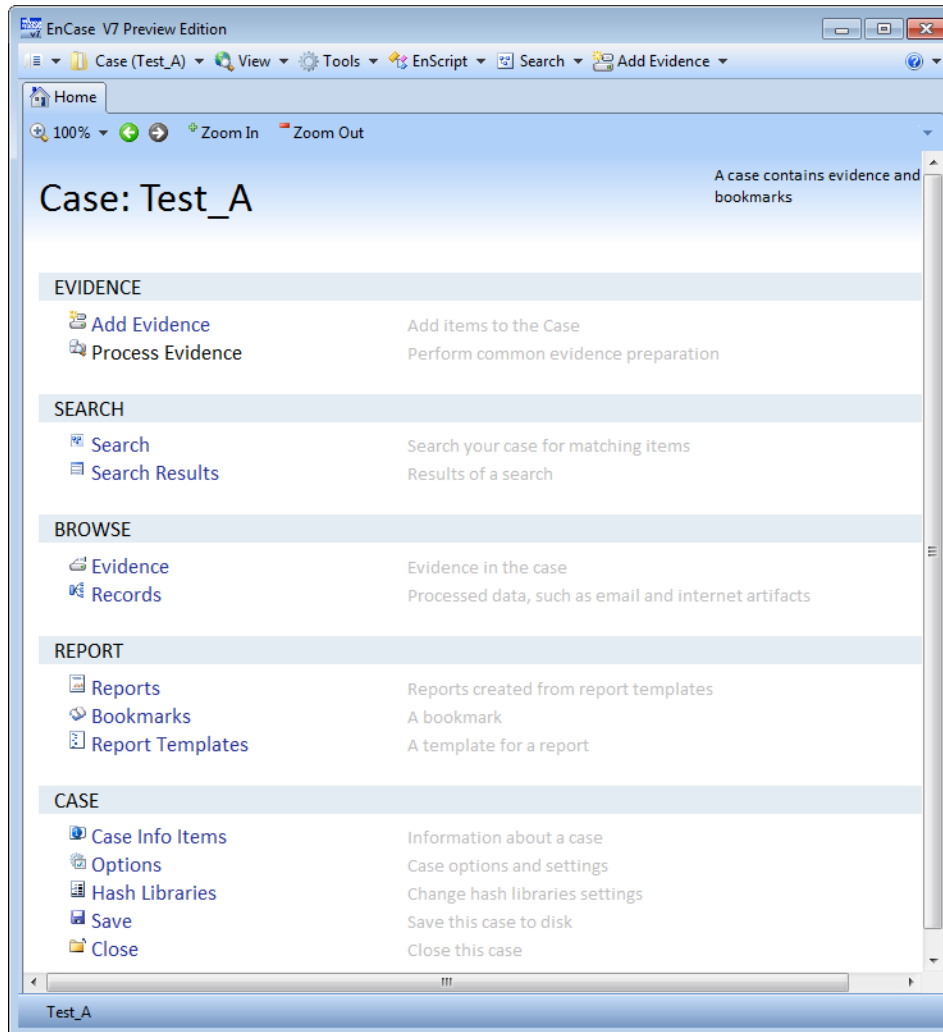
**Base Case folder:** This is the location where the above case folder will be created. By default, EnCase uses a folder under the users `My Documents` folder. This field is not writable.

**Primary evidence cache:** EnCase Version 7 uses cache files to speed up application responsiveness, enhance stability, and provide scalability across large data sets. The primary evidence cache folder is the location where EnCase will save and/or access these files. Cache files may be created in advance through the Evidence Processor and a user can simply point to a folder that contains this data. Although there is an evidence cache for each device in a case, the evidence cache does not need to be stored with the evidence files. If cache files have not been created for a device, they will be stored in this folder when the Evidence Processor is run. This field is not writable.

**Secondary evidence cache:** EnCase allows a user to specify a secondary location where a previously created evidence cache can be found. This allows users to specify a folder on a network share or other location where cache files may be stored. Unlike the primary evidence cache folder, EnCase will only read previously created files from this location. All new cache files will be stored in the Primary evidence cache folder. This field is not writable.

**Case info:** Case Info Items are user configurable name-value pairs that document information about the current case. These items are primarily used to insert user-definable information into a Report. To create Case Info Items, use the **New** button above the table to generate as many name-value pairs as you need.

Click **OK** to apply the case options. The **Home** tab will then display a page for this particular case with the case name displayed at the top. This case page lists hyperlinks to many common EnCase features and you can use it as the main landing page for this case. You are now ready to begin building your case.

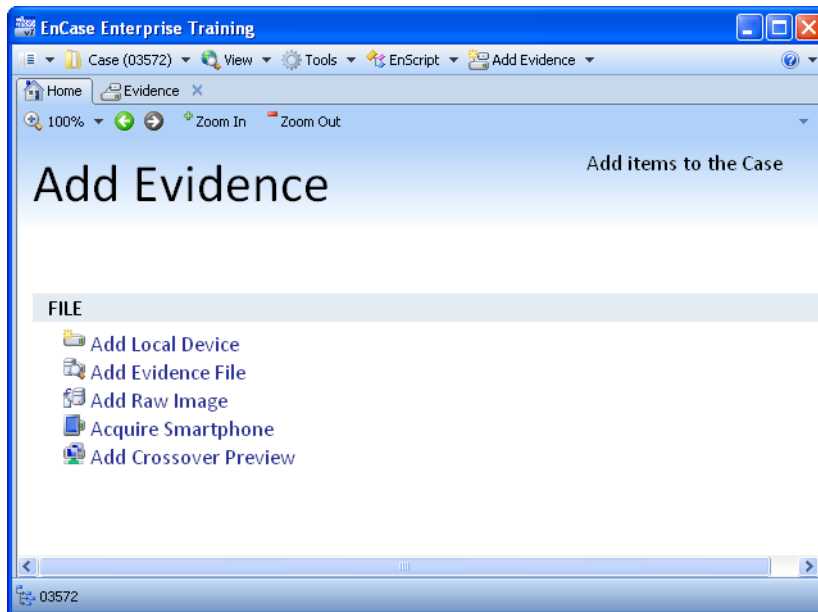


## Adding Evidence to a Case

Once a case is created, you can add evidence to your case by selecting the **Add Evidence** hyperlink on the case page or selecting the **Add Evidence** drop-down menu from the application toolbar.

Both of these methods allow you to add different types of evidence to a case.

If you click the **Add Evidence** link on the Case page, the page changes to that shown below. At any time, you can use the back or forward buttons to help navigate through the different Home tab pages.



The **Add Evidence** menu also contains these selections and, a selection to access the Evidence Processor. See the Evidence Processor *Overview* (on page 26).

The following list describes the possible evidence selections:

#### **Add Local Device**

Initiate the process of adding a local device attached directly to your local computer. This can be the main system drive, or a device attached through a Tableau write-blocker.

#### **Add Evidence File**

Specify an evidence file to add to the active case. This can be an EnCase Evidence file (E01) or Logical Evidence file (L01).

#### **Add Raw Image**

Add a raw or dd image file of a physical device to the active case.

#### **Acquire Smartphone**

Acquires a smartphone. After clicking the **Acquire Smartphone** link, the dialog allows you to specify the device type and the kinds of data that you want to collect into an evidence file.

#### **Add Crossover Preview**

Crossover cable acquisitions require both a subject and forensic machine. This type of acquisition also negates the need for a hardware write blocker. It may be desirable in situations where physical access to the subject machine's internal media is difficult or not practical. This is the recommended method for acquiring laptops and exotic RAID arrays. This option allows you to preview a machine acquired through a crossover cable acquisition.

## Process Evidence

Process the case evidence, in an automated fashion, across a wide selection of parameters. This selection includes features such as:

- Analyzing file signatures. See *File Signature Analysis* (on page 34).
- Creating an index of the case evidence data. See *Index Text* (on page 33).
- Searching for email threads and conversations. See *Find Email* (on page 30) and *Thread Email* (on page 31).
- Searching Internet artifacts. See *Find Internet Artifacts* (on page 31).

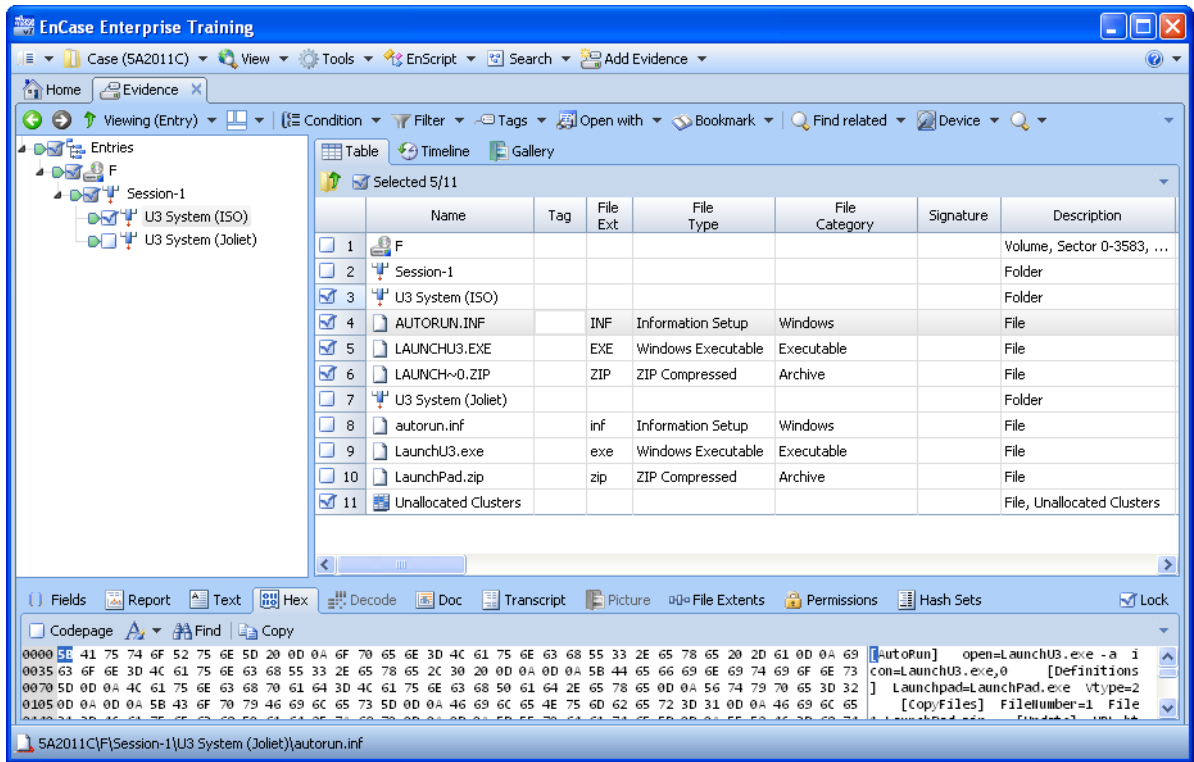
See the *Evidence Processor Overview* (see "Overview" on page 26) for more information on the processing of evidence.

## Browsing Case Data

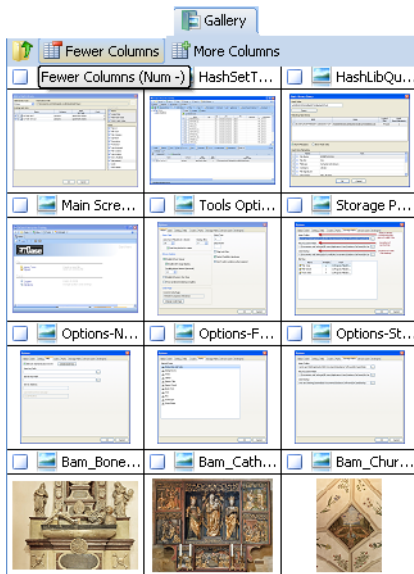
After creating a case and adding evidence, use the **Evidence** link on the case home page to view the evidence in a number of different ways.



The **Evidence** tab allows you to drill into selected devices to get a Tree-Table view similar to the following:

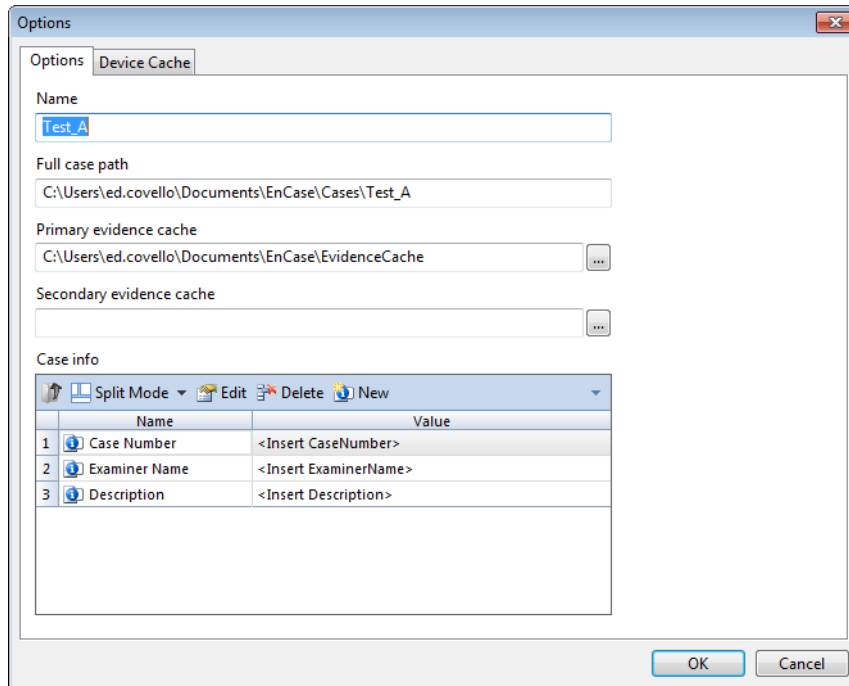


You can also browse images in Gallery view:



## Setting Case Options

Case settings are specific to individual cases. You access case options from the Case Home page by clicking **Case > Options**.



To configure case options:

1. Note that you cannot change the **Name** or the **Case folder**; they are there for informational purposes only and are read only.
2. You can change the following options:
  - **Local evidence:** Use the browse button to change this folder to use that of the Primary Evidence Cache.
  - **Global evidence:** Use the browse button to change this folder to use that of the Secondary Evidence Cache.
3. To add or edit Case Info items, click the appropriate button on the Case Info toolbar.

## Working with Cases

Use the **Case** menu and the **Case** selections on the Case Home page to work with the parameters of and perform actions on your case.

CASE	
	Case Info Items Information about a case
	Options Case options and settings
	Hash Libraries Change hash libraries settings
	Save Save this case to disk
	Close Close this case

Following are a list of basic operations for working with a case. Use the menu items on the **Case** menu, and the links beneath the Case section on the Case panel for these operations:

### Case Selections

<b>Save</b>	Saves the current case file. The default suffix for a case file is *Case; the default suffix for a backup case file is *cbak.
<b>Save As...</b>	Use to save and rename the current case file, or create a copy of the case file with a different name.
<b>Save As Template...</b>	Use to save the case as an EnCase template to use with new cases. The extension for a case template file is *.CaseTemplate.
<b>Close</b>	Closes the active case file.
<b>Open...</b>	Opens an existing case file. Note that you can have more than one case file active at a time.
<b>New Case...</b>	Opens the Case Options dialog so that you can create a new case file.
<b>Options...</b>	Allows you to edit the Case Options for the active case.
<b>Hash Libraries...</b>	Displays the Hash Libraries dialog, which provides a list of hash libraries and hash sets used in the current case, and allows you to change libraries, or enable and disable hash libraries and sets.
<b>Case Info Items</b>	Clicking this link under the Cases section takes you to the Case Info Items tab, which displays, in tree and tabular form, the name-value pairs about case information from the Case Options dialog.



# Evidence Processor

- Overview
- Configuring Time Zone Settings
- Preparing the Evidence to Process
- Managing Evidence Processor Settings

## Overview

After adding evidence to a case, the first task you undertake is running the EnCase Evidence Processor. The Evidence Processor lets you run, in a single automated session, a collection of potent analytic tools against your case data. Since you can run the Evidence Processor unattended, you can work on other aspects of the case while this tool is processing data. In short order, the case data will be processed and ready for you to begin the key analytic and reporting phases of your investigation.

Evidence Processor functions fall into two categories:

- Preparation
- Processing

You can run the Evidence Processor using a template with saved or preconfigured settings, or you can select the analytic tools to enable and customize their settings prior to running it. If additional evidence becomes available at a later date, you can always re-run the same options on that data.

A major benefit of the Evidence Processor is that its settings do not require user interaction during operation.

The following evidence processing functions are available:

- Recover folder
- Hash analysis
- Expansion of compound files
- Find email
- Find Internet artifacts
- Search for keywords
- Index text

Additionally, the following operations are always run with Evidence Processor:

- File signature analysis.
- Protected file analysis.
- Creating thumbnails from images.
- Thread email.

The EnCase Evidence Processor contains numerous useful features:

- The simultaneous processing of multiple devices.
- The convenience of acquiring devices right from the Evidence Processor.
- Saving sets of Evidence Processor options as templates to be run with little or no modification at a later date.
- The ability to be run from the command line.
- On-screen instructions that guide you through the use of each setting.
- Automatic processing of the results from any EnScript modules according to the current processor settings (Index, Keyword search, etc.).

Before using the Evidence Processor:

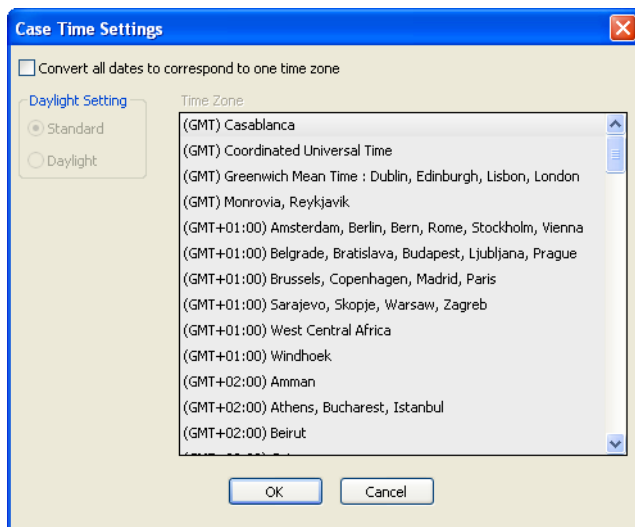
- There must be evidence in your case to process.

- If you are previewing a device, you must acquire that device prior to processing or as part of the processing..
- You should confirm that time zone settings are configured properly.

## Configuring Time Zone Settings

To configure time zone settings:

1. Click the **Evidence** tab; a list of your devices displays in the **Table** tab.
2. Select the device that you wish to modify.
3. Click the drop-down menu on the far right side of the **Evidence** tab.
4. Click **Modify time settings...** the Case Time Settings dialog appears. Select the check box, whether you want to account for daylight savings time, and a **Time Zone** if you want to **Convert all dates to correspond to one time zone**, and click **OK**.



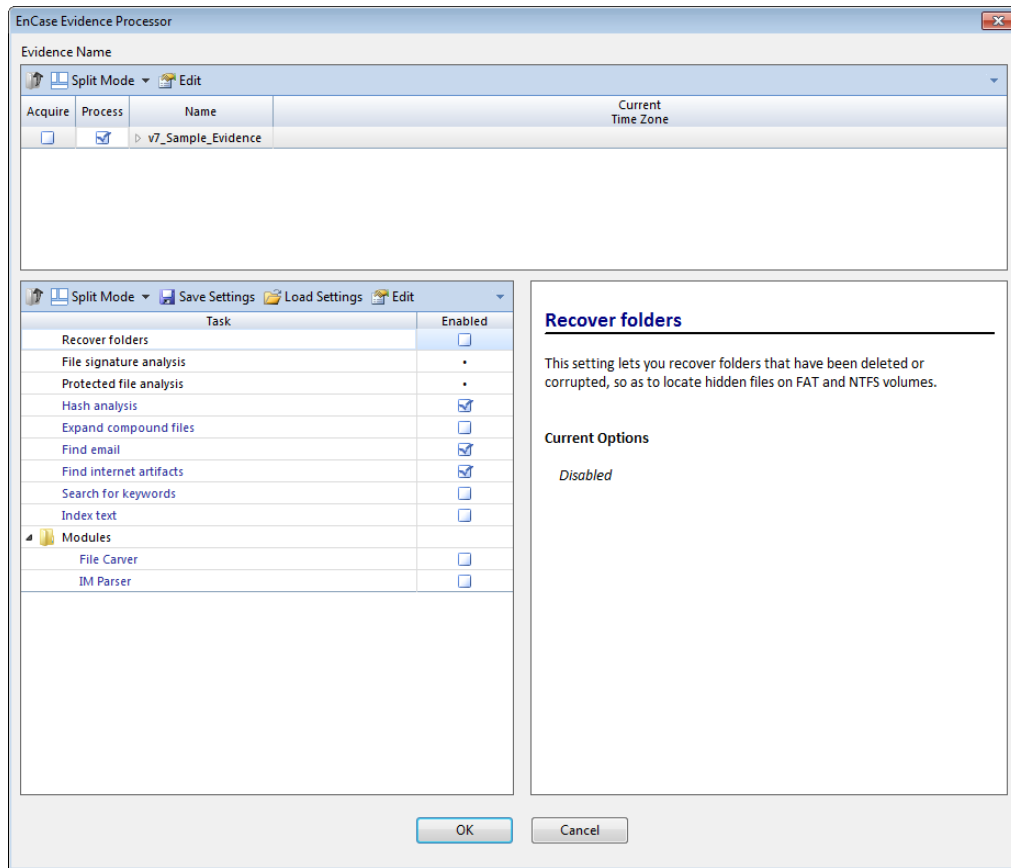
## Preparing the Evidence to Process

Once you have added evidence to your case and configured the time zone settings, you must:

- Acquire the evidence.
- Select which evidence you intend to run through the Evidence Processor.

To acquire and run select evidence through the Evidence Processor in a single operation:

1. Click **Process Evidence** beneath **Evidence** on the Case Home page to display the EnCase Evidence Processor window.



2. The Evidence Name pane contains checkboxes for acquiring and processing evidence. Note that you must acquire previewed evidence before you can process it. Initially, the checkboxes in the Evidence Name pane are cleared. Check the boxes for the evidence you want to acquire and/or process. If you have already acquired an item of evidence named in the list, you do not need to check the **Acquire** box for that item.
3. In the example below, we acquire devices "G" and "SmallDrive" by checking their boxes for **Acquire** and set them up for processing by checking their boxes for **Process**.

Evidence Name			
Acquire	Process	Name	Current Time Zone
<input type="checkbox"/>	<input type="checkbox"/>	D	(GMT-08:00) Pacific Time (US & Canada)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	G	(GMT-08:00) Pacific Time (US & Canada)
<input type="checkbox"/>	<input type="checkbox"/>	F	(GMT-08:00) Pacific Time (US & Canada)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SmallDrive	(GMT-08:00) Pacific Time (US & Canada)

## Managing Evidence Processor Settings

The lower left pane of the Evidence Processor dialog contains a table with the following elements:

- A toolbar.
- A list of the Evidence Processor **Tasks**.
- A checkbox that allows you to **Enable** (or disable) each task.

Use this pane to choose which processor settings to run and to configure their settings.

### *Using the Processor Settings Toolbar*

File and edit settings for the Evidence Processor selections pane are located in its toolbar.



Setting	Description
Split Mode	Change the display format of the options pane.
Save Settings	Save the current selection of settings as an Evidence Processor template.
Load Settings	Load a saved template to run against the current data.
Edit	Edit the options for a selected task in the window.
Drop-down side menu	Allows you to perform actions such as printing the results, and changing the layout of the Evidence Processor panels.

### *Evidence Processing Tasks*

Use this pane to select which processing tasks to configure and run.

To select an option, click its **Enable** checkbox.

- If a task name is listed in a *blue* font, click on its task name to configure it.
- If a task name is listed in a *black* font, no further configuration is necessary.

▪

Task	Enabled
Recover folders	<input type="checkbox"/>
File signature analysis	•
Protected file analysis	•
Hash analysis	<input checked="" type="checkbox"/>
Expand compound files	<input type="checkbox"/>
Find email	<input checked="" type="checkbox"/>
Find internet artifacts	<input checked="" type="checkbox"/>
Search for keywords	<input type="checkbox"/>
Index text	<input type="checkbox"/>
Modules	
File Carver	<input type="checkbox"/>
IM Parser	<input type="checkbox"/>

## Recover Folders

Running the Recover Folders task on FAT partitions searches through the unallocated clusters of a specific FAT partition for the “dot, double-dot” signature of a deleted folder. When the signature matches, EnCase can rebuild files and folders that were within the deleted folder.

This task can recover NTFS files and folders from Unallocated Clusters and continue to parse through the current Master File Table (MFT) records for files without parent folders. This operation is particularly useful when a drive has been reformatted or the MFT is corrupted. Recovered files are placed in the gray Recovered Folders virtual folder in the root of the NTFS partition.

## Hash Analysis

A hash is a digital fingerprint of a file or collection of data, commonly represented as a string of binary data written in hexadecimal notation. In EnCase, it is the result of a hash function run against any mounted drive, partition, file, or chunk of data. The most common uses for hashes are to:

- Identify when a chunk of data changes, which frequently indicates evidence tampering.
- Verify that data has not changed, in which case the hash should be the same both before and after the verification.
- Compare a hash value against a library of known good and bad hashes, seeking a match.

The Evidence Processor's hash analysis setting allows you to create MD5 and SHA-1 hash values for files, so that you can later use them for the reasons specified above. When you click the **Hash Analysis** hyperlinked name, the Edit Settings dialog appears, allowing you to check whether to run either or both of these hashing algorithms.

## Find Email

Select this setting to extract individual messages from email archives.

To select which email archive types to search for messages:

1. Click **Find Email**.
2. Click the email archive file types whose messages you want to examine, and click **OK**.
3. Check the **Find Email** box.

After processing is completed, EnCase can analyze the component files extracted from the archives, according to the other Evidence Processor settings you selected.

## Thread Email

By default, the Evidence Processor performs a thread analysis on email messages that it processes.

Once your evidence has been processed, you can track the different email threads and communication patterns among senders and receivers of the messages with the Show Conversation and Show Related email features.

## Find Internet Artifacts

Choose this Evidence Processor setting to find Internet-related artifacts, such as browser histories and cached Web pages. You can also use this setting to search for Internet artifacts of various types within unallocated space.

## Search for Keywords

Use this option to run a raw keyword search during the processing. Once you enable **Search for Keywords** by checking its box, the keyword list for the current case is displayed in the right panel.

The screenshot shows the Evidence Processor settings window. On the left, a table lists various tasks with checkboxes for enabling them. The 'Search for keywords' task is checked. On the right, the 'Search for keywords' panel is active, displaying instructions and a list of current options.

Task	Enabled
Recover folders	<input type="checkbox"/>
File signature analysis	<input type="checkbox"/>
Protected file analysis	<input type="checkbox"/>
Hash analysis	<input type="checkbox"/>
Create image thumbnails	<input type="checkbox"/>
Expand compound files	<input type="checkbox"/>
Find email	<input type="checkbox"/>
Thread email	<input type="checkbox"/>
Find internet artifacts	<input type="checkbox"/>
Search for keywords	<input checked="" type="checkbox"/>
Index text	<input type="checkbox"/>
Modules	

**Search for keywords**

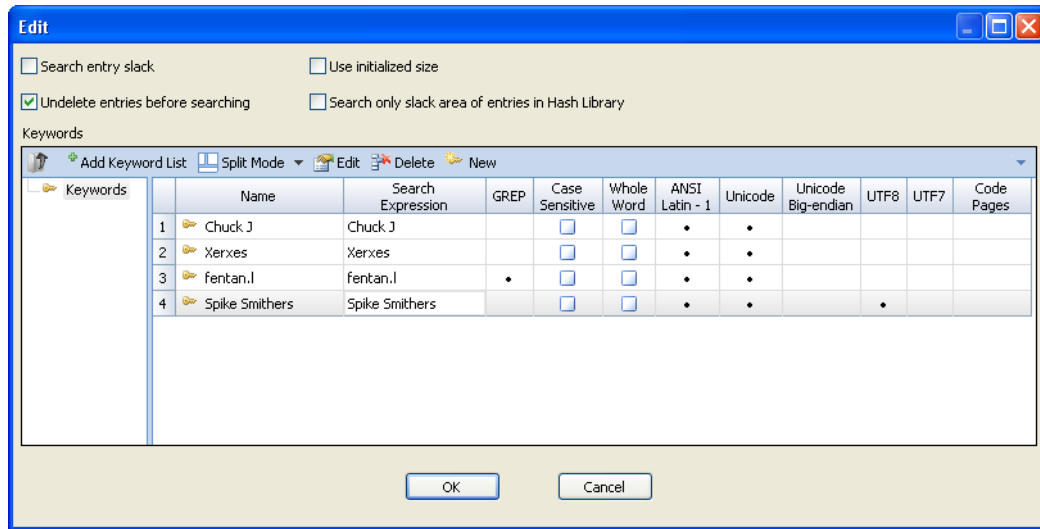
Use this facility to search raw text for specific keywords. The keywords and their settings are specified below.

**Current Options**

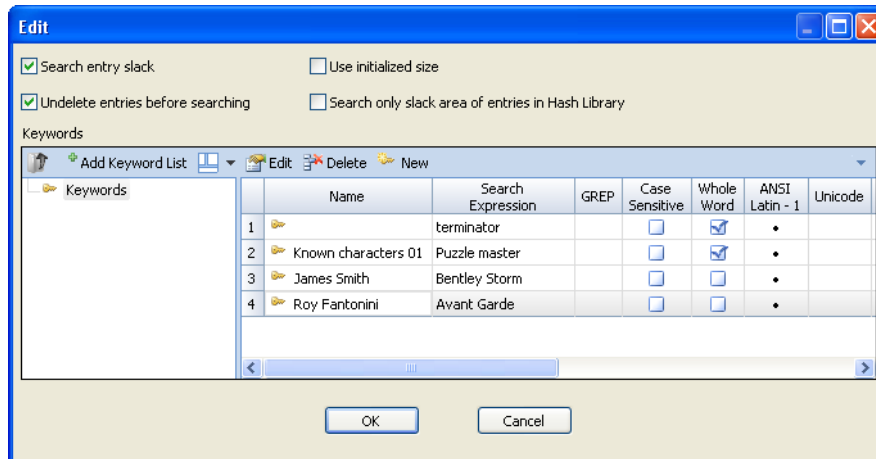
terminator
foreign
basic
contain

To edit the keyword settings:

1. Click **Search for Keywords**. The Edit Keyword List dialog appears.

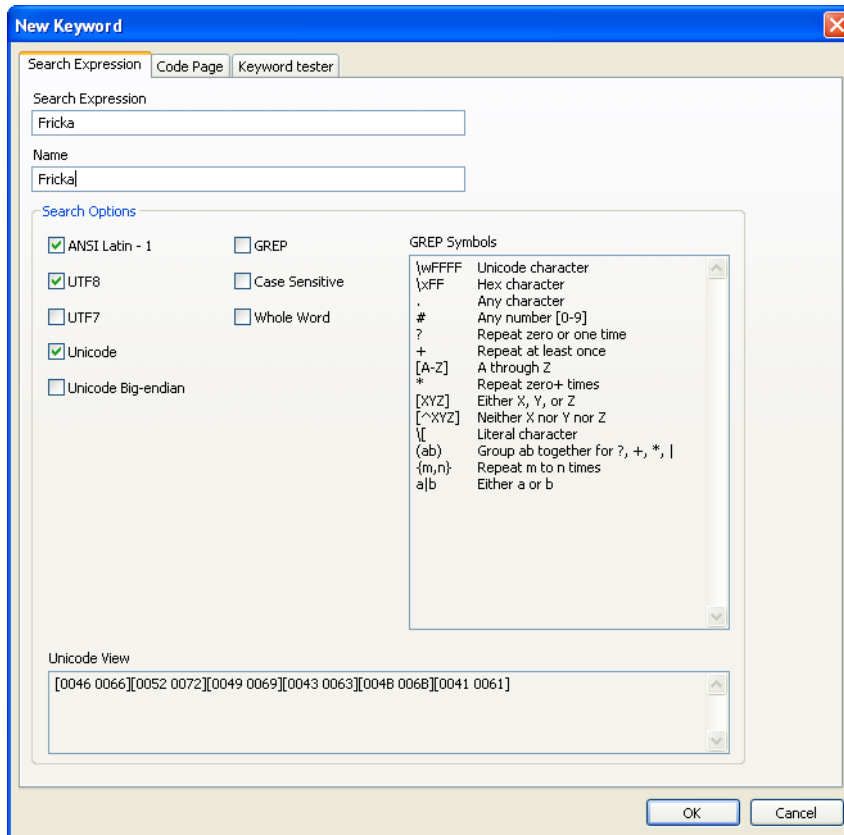


2. In the dialog, use the checkboxes and toolbar items to:
  - add a keywords list to a file
  - add new keywords
  - edit keywords
  - delete keywords
  - specify where and how to search
  - change the layout of the keyword table



To add a new keyword:

1. In the Edit Keyword dialog, click **New**. The New Keyword dialog appears.



2. Enter a new keyword in the **Search Expression** box.
3. If you intend to search for keywords using a different character set, you may need to change the code page. In that case, click the **Code Page** tab, scroll through the list, and check the code page **Name** you want.

## Index Text

Choose this selection to create a searchable index of the data in the case. Creating an index will allow users to instantly search for terms in a variety of ways. You can adjust parameters for index creation such as the minimum word length to index, or whether to use a noise file (a file containing specific words to ignore).

Compared to keyword searches, which search on the raw text, index searches search on the transcript output of the file.

Generating an index can take time; however, the trade-off in time spent creating the index yields a greater payoff with near instantaneous search times. Guidance Software recommends always indexing your case data.

## Create Image Thumbnails

By default, the Evidence Processor generates thumbnails for all image files and stores them as part of the cache.

Because thumbnails are smaller and load faster, generating thumbnails significantly improves the speed with which you can work with pictures in EnCase.

### **Expand Compound Files**

Use this setting to expand archive files, including .zip and .rar files, and/or registry archives.

For archive files, EnCase will extract the compressed or archived files and process them, according to the other Evidence Processor settings that you have chosen. This includes nested archive files, or zip files within a zip file.

### **File Signature Analysis**

A common technique used to hide data and disguise the true nature of a file is to rename the file and change its extension; for example, renaming an image file with a .jpg extension to a file with a .dll extension, which is not associated with a graphics file.

This process will determine whether the extension of a file has been modified, and whether it matches the type of file that is specified by the file's header bytes. The process is not user configurable and is always enabled, because it is necessary to support other operations within EnCase.

### **Protected File Analysis**

Encrypted and password protected files are frequently good ways to hide data. The Evidence Processor's protected file analysis process identifies these types of files, and information about the application used to protect them. This process is not user configurable and is always enabled because it takes no additional time.

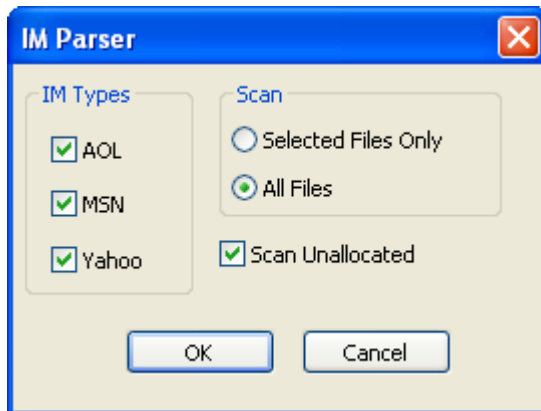
### **Modules**

The EnCase Evidence Processor has the ability to run add-in modules during processing. Some modules will ship as part of EnCase, and customers can add their own modules also. Click on the **Modules Folder** to open it and access additional evidence processing features.

### **IM Parser**

The IM Parser allows you to search for Instant Messenger artifacts from MSN , Yahoo and AOL Instant messenger clients. These artifacts include messages and buddy list contents. It also allows you to select where to search from several general location categories.

When you enable IM Parser processing and click the module name, the following dialog appears that allows you to configure its options:



### File Carver

This **File Carver** module allows you to search evidence for file fragments based on a specific set of parameters, such as known file size and file signature, and can examine unallocated space.



# Working with Email Evidence

- Overview
- Displaying Email Threads
- Deduplicating Messages

## Overview

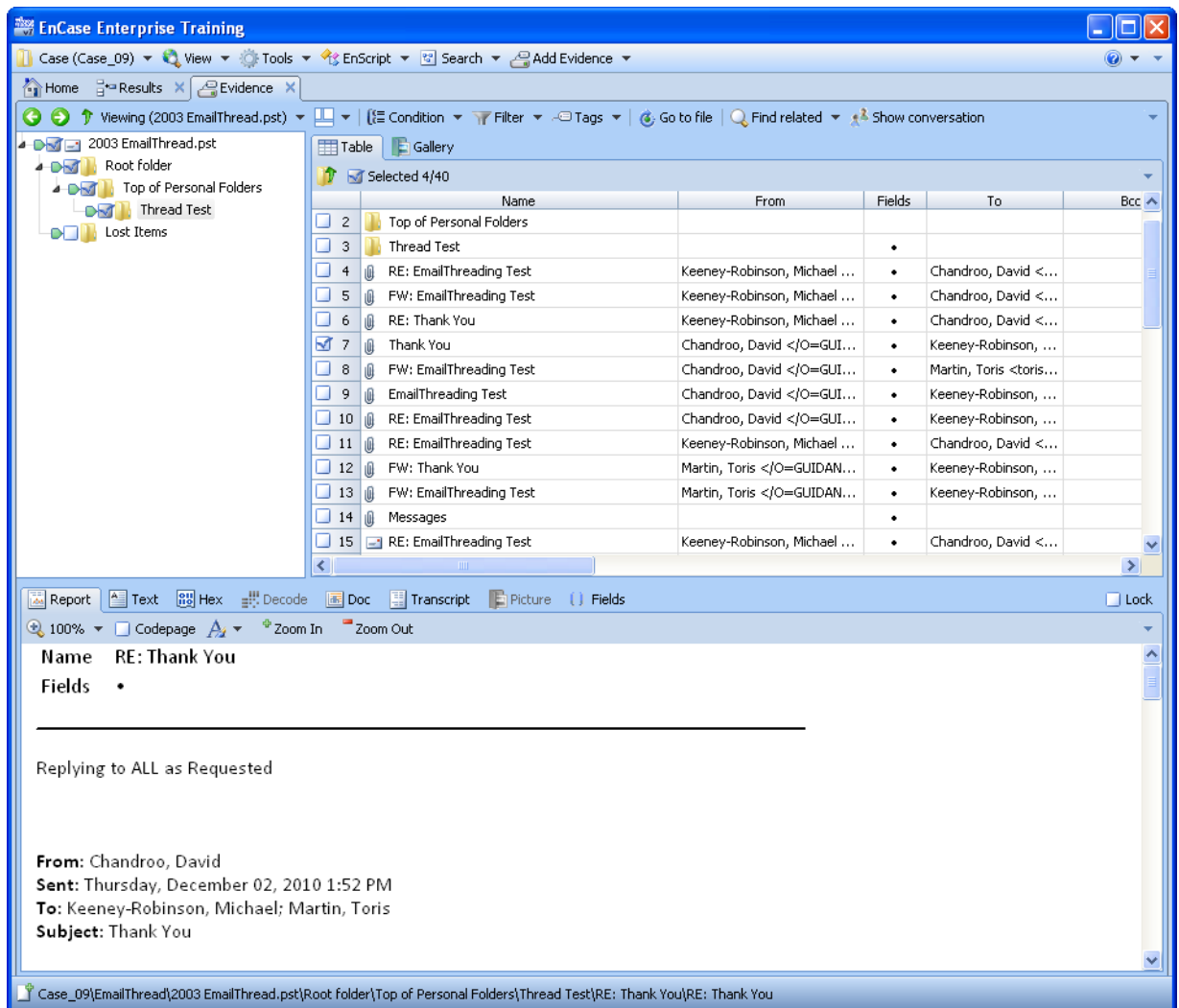
Email is a key area for forensic investigation, as it not only maintains a record of individual and corporate communications, but also contains date stamps, provides additional names or corporate entities, and may contain attachments, all of which can add to an investigation and supply further leads.

When email is viewed in a case, EnCase can search for specific kinds of mail and parse its contents. EnCase lets you view email in a format that is similar to common email programs (for example, the Microsoft Office Outlook client). The views are customizable (you can view the data in tree, table, and composite views), allowing you to see only the data you want in the format you find most convenient.

EnCase also allows you to track email threads. In most situations, thread tracking can span multiple email repositories, simplifying investigations that were previously complex and time-consuming. You use the **Search Results** tab and **Email Threading** to view data across multiple repositories.

Before conducting your email analysis, make sure that you have already processed your case data with the Evidence Processor **Find email** selection checked.

The following figure shows an example of an Outlook PST file being examined in EnCase.



In the above screen, an expanded tree view of an Outlook PST file and its folders is shown in the left pane, while the messages belonging to the PST file are shown in the right pane, and the contents of a selected message are shown in the bottom pane.

## Displaying Email Threads

EnCase analyzes two forms of email threading:

- Conversations
- Related messages

**Important:** Before you can analyze email threading, you must have already run the Evidence Processor against your case evidence with the **Find email** option selected.

To choose which form of threading to examine:

1. Click on the **Entries** tab and click to select an email in the Table pane.

2. On the **Entries** toolbar, click either the **Viewing (Show Conversation)** or **Show Related** button.

## *Show Conversation*

Email threading is based on conversation-thread related information found in the email message headers.

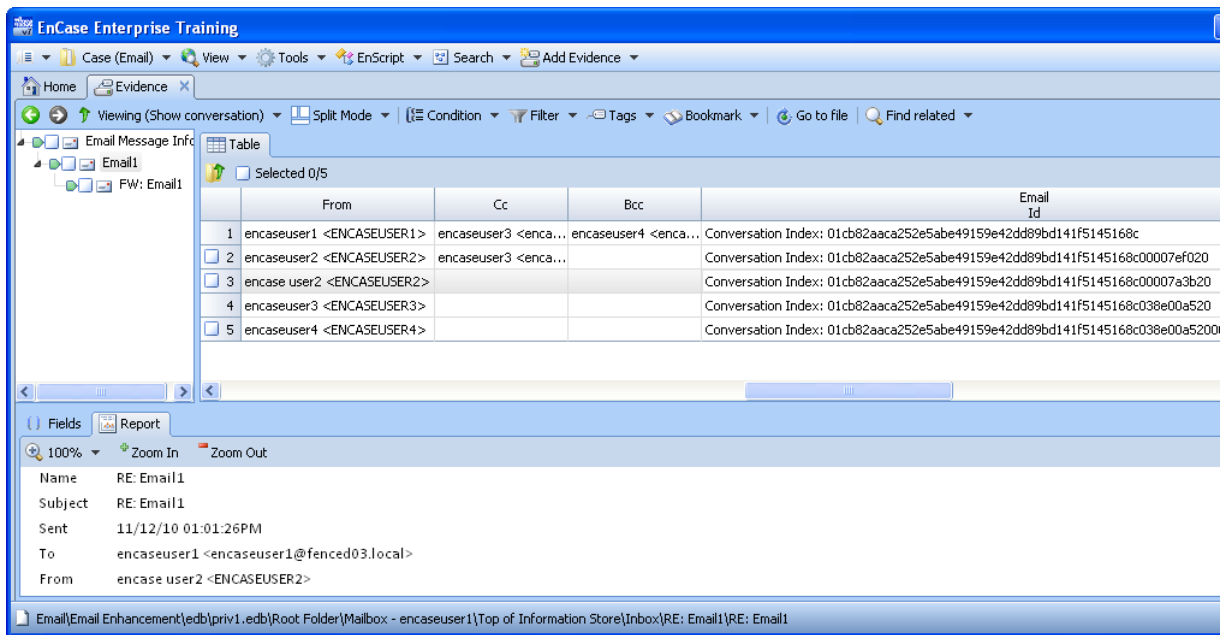
Different email systems use different methods of identifying conversations; for example:

- The header fields *Message-ID*, *Reply-To-ID*, and *References*.
- The header field *Conversation Index*.
- The header field *Thread-Index*.
- *Multiple mechanisms*, because the messages of interest cross email system boundaries. In these cases, EnCase builds a separate conversation tree for each type of data found in the header (for example, one using *Message-ID/References* and another using *Conversation Indexes*) and displays the conversation tree containing the most email.

EnCase can display conversations for all supported email types except AOL, because AOL messages do not store thread-related information. However, the feature cannot always reconstruct *complete* conversations when the conversations include messages from multiple email systems. For example, EnCase cannot fully recreate a conversation where some users are using Outlook, some are using Lotus Notes, and others Thunderbird.

If an email does not have any of the message header fields specified above, EnCase cannot construct a conversation thread for it. Selecting such an email and clicking **Show Conversation** results in a tree containing only the selected email.

The following figure shows a conversation list for a selected email (from inside the **Records** tab for the email you want to view, go to **Evidence > Viewing (Show Conversation) > Table**). Note how the emails contained within the conversation list are identified by their conversation index ID.



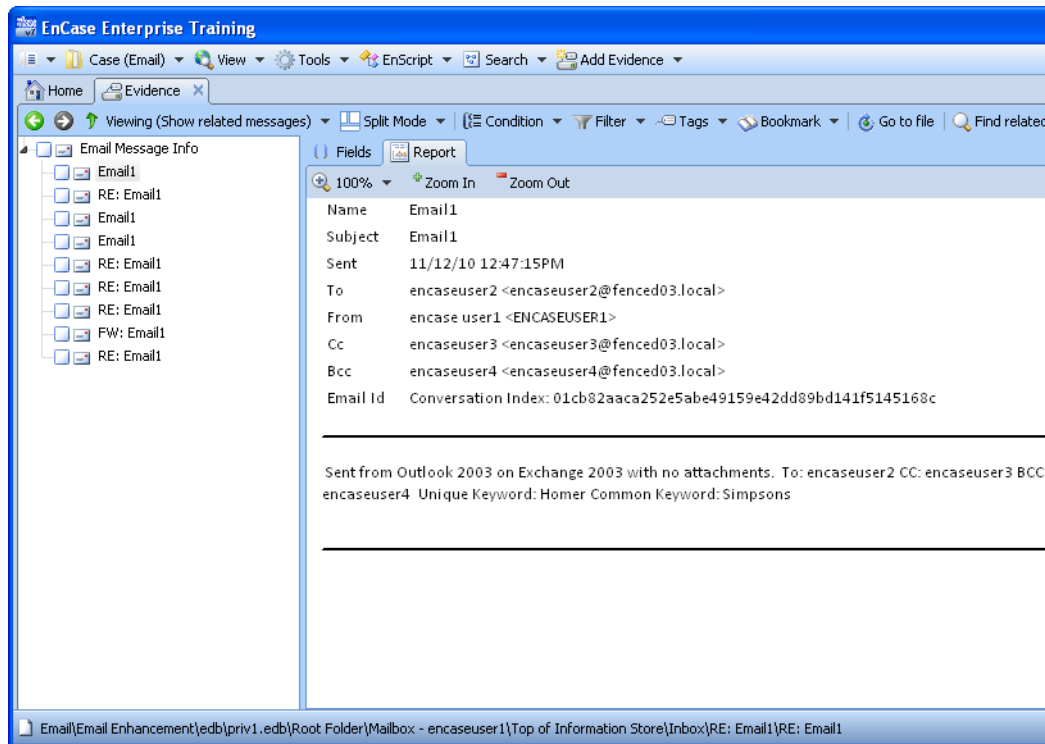
## Displaying Related Messages

The Related Messages feature is based solely on the email's subject line. The feature is useful when an examiner suspects that Show Conversation is not displaying a complete conversation thread.

All emails with identical subject lines are considered related and displayed together.

EnCase can show related emails for all supported email types. There are no limitations caused by emails originating from different email systems. Since Show Related only looks at the subject line of a message, the emails displayed may not all be related, depending upon the uniqueness of the subject line.

Following is an example of a list of related emails. The list is displayed in the left pane; the content of the first email in the list is displayed in Report view (from inside the **Records** tab for the email you want to view, go to **Evidence > Find Related > Report**).



## Deduplicating Messages

Multiple copies of an email often exist because:

- An email was sent to multiple email aliases.
- The sender's Sent Items and the recipient's Inbox are located in a single case multiple times in different email archives.

To avoid displaying the same message multiple times, EnCase deduplicates (or removes duplicate) messages in both the Show Conversation and Show Related email views.

# Hashing

- Overview
- Hashing Features
- Working with Hash Libraries

## Overview

Analyzing a large set of files by identifying and matching the unique hash value of each file is an important part of the computer forensics process. Using the hash library feature of EnCase, you can import or custom build a library of hash sets, allowing you to identify file matches in the examined evidence.

Computer forensics analysts often create different hash sets of known illicit images, hacker tools, or non-compliant software to quickly isolate known "bad" files in evidence. Hash sets are distributed and shared among users and agencies in multiple formats. These formats include NSRL, EnCase hash sets, Bit9, and others.

Until recently, the hash set standard to identify a file was the MD5 hash calculation. Large hash distribution sets, such as the NSRL set, are now distributed using the SHA-1 hash calculation. EnCase will offer continued support for MD5 hash sets, from old versions of EnCase and other products, as well as the new SHA-1 hash format sets.

EnCase uses an extensible format for hash sets that allows:

- Storing metadata along with the hash value in field form.
- Support of MD5, SHA-1, and additional hash formats within the same file structure.
- Users to associate tags with items in the hash set.

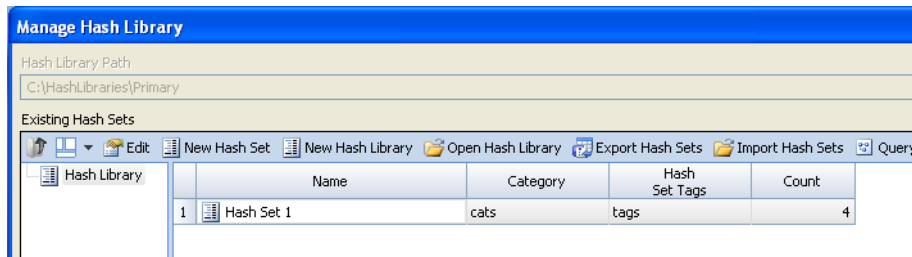
## Hashing Features

EnCase Version 7 contains several new and expanded hashing features:

- A versatile user interface for hash library management: you can create hash sets and libraries, import and export hash libraries, query hash sets, and view hash sets or individual hash items.
- Hash libraries can contain multiple hash sets, and each set can be enabled or disabled.
- You can create as many hash libraries or hash sets as you want.
- If a hash belongs to multiple sets, every match will be reported.
- Each case can use up to two different hash libraries at the same time.
- You can save individual hashes in a separate folder without placing them in a specific hash set or hash library (for example, you may want to retain a hash of an item for later use without committing it to a particular hash set or library).

## Working with Hash Libraries

A hash library is a folder containing the file-based, database-like structure in which EnCase stores hash sets. To work with hash libraries, click **Tools > Manage Hash Library** on the Application Toolbar. The following dialog displays:



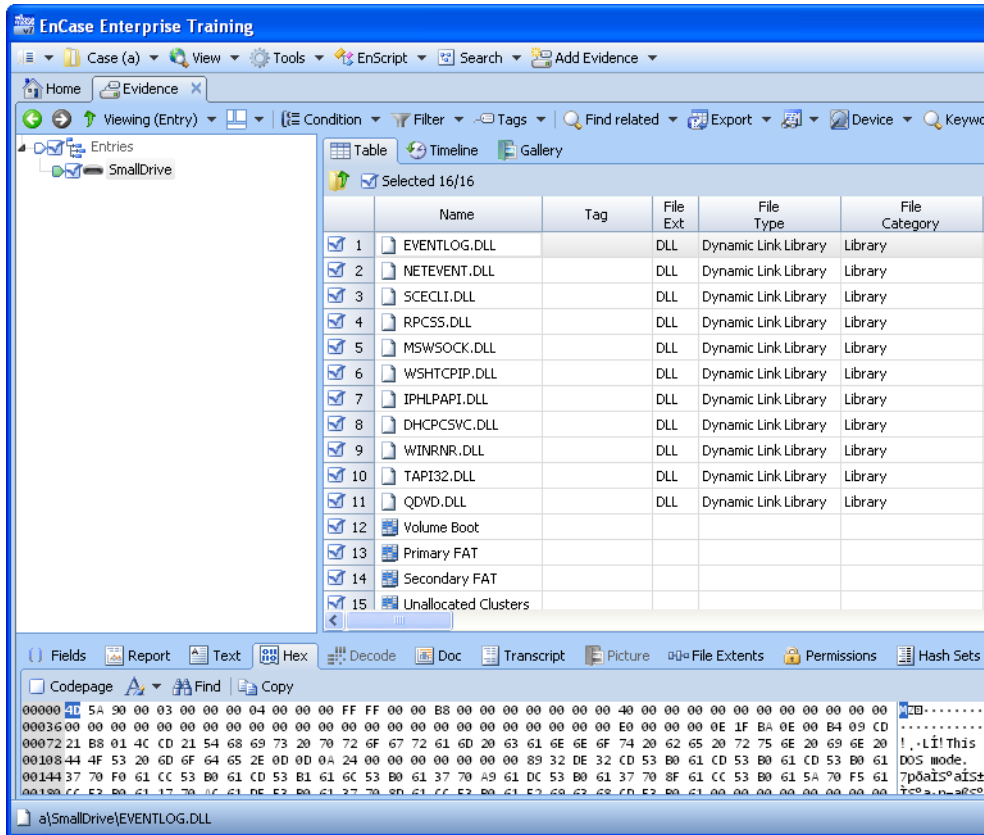
From the Manage Hash Library dialog you can manage any existing hash libraries or create a new one. You use its toolbar:

- Create a new hash library or edit an existing library.
- Create new hash sets within a library or edit an existing hash set within a library.
- Import and export hash sets from one library to another.
- Query a hash library for a particular value.

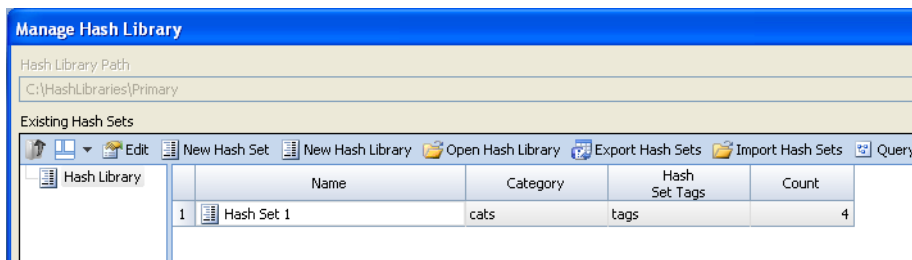
### *Creating a Hash Library*

To create a hash library, you perform the steps described below:

- Click **Tools > Manage Hash Library**.



- On the Manage Hash Library panel toolbar, click **New Hash Library**.

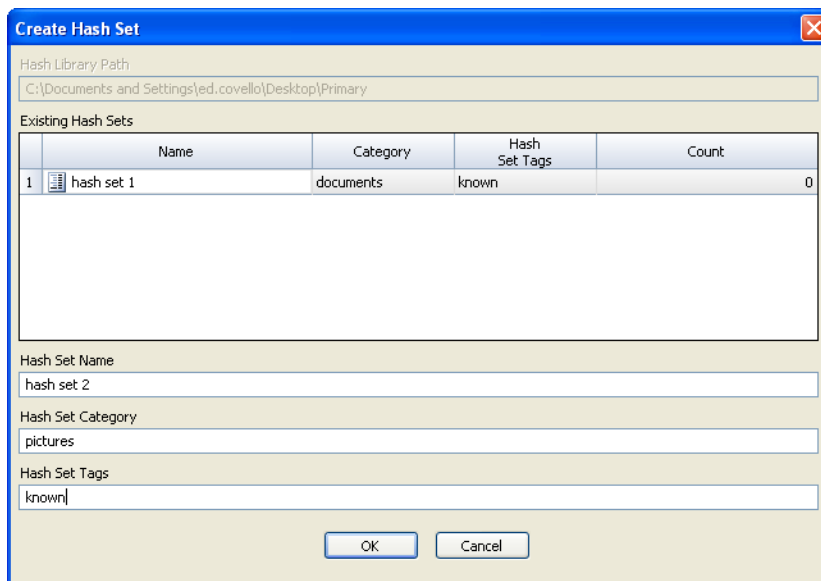


- Browse for a folder to hold the hash library. If you use an existing folder, it must be empty (otherwise, the contents of the folder will be deleted).
- Provide a name for the hash library (for example, Windows 7 Files, Company Secrets, or Hash Library #1).
- If you wish to import hash sets from another library, select **Import Hash Sets** from the toolbar. You can then browse to a library and select individual sets to import. If you wish to create new hash sets for this library, proceed to the next section.

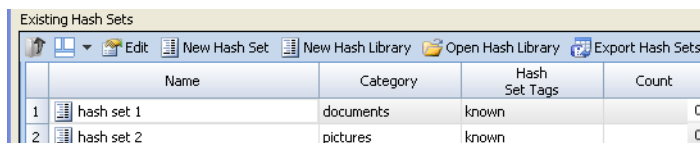
## Creating a Hash Set

Hash sets (which contain the individual hash entries) are located within hash libraries. There are two steps to creating a hash set. The first step is to create an empty hash set within a library, and the second is to add information to it. To create a hash, you perform the steps described below:

1. Click **Tools > Manage Hash Library**.
2. Make sure that you either browse and point to an existing hash library or create a new one. This is the hash library to which you will add the hash set.
3. On the Manage Hash Library panel toolbar, click **Create New Hash Set**.
4. Enter a **Hash Set Name**, and enter information for **Hash Set Category** and **Hash Set Tags**.



5. Click **OK** and click **OK** again when you are prompted to add the new hash set. The new hash set is listed under **Existing Hash Sets** in the Manage Hash Library panel.



## Adding Hash Values to a Hash Set

Once you have created a hash set within a library, you can add information to it. The steps for adding hash values to a hash set are as follows:

1. Add the device or evidence from which you want to generate a hash value to a case.
2. Hash the files on the device by using the hashing feature of the Evidence Processor.
3. Go to the table of evidence files or images whose hashes you want to add to the hash set.
4. On the **Evidence** tab, under the **Entries** table, expand the Entries view.
5. In the **Table** tab, check those entries whose hash values you want to add to the hash set.

6. In the Tab toolbar, click the **Entries** drop-down menu (indicated by the red arrow, below), and select **Add to Hash Library...** The **Add to Hash Library Panel** displays.
7. Choose the Hash Library to which to add the hash items by using the **Hash Library Type** drop down menu. Select the Primary or Secondary hash library if they are defined, or you can select Other and browse to a library.
8. Once you have selected a library, select one or more previously created hash sets from the **Existing Hash Sets** window.
9. On the Add to Hash Library panel, **Fields** list, select the fields you want to add to the hash library for the selected items. Some fields are added by default, however, you can add other optional fields, depending on your needs. All fields that are added to the set will be reported when a hash comparison matches a particular hash set. The more fields that you add to a set, the larger the set becomes.
10. Click **OK**.
11. If the hash values were added to a library that was set as the Primary or Secondary hash library, you can check whether the item was successfully added to the hash set as follows:
  - On the **Table** tab, highlight the row containing the item.
  - In the bottom pane, click **Hash Sets**. The hash set name, hash library, and other hashing information about the item should appear.

	Name	Category	Hash Set Tags	Hash Items	Hash Library Path
1	hash set 2	pictures	known	•	C:\Documents and Settings\jed.covello\Desktop\Primary

## Querying a Hash Library

At times, a user might want to query a hash library for a particular hash value to see if it exists and to see what metadata exists with that value.

To conduct a query of a known hash value:

1. On the Home panel, click **Tools > Manage Hash Library > Open Hash Library**.
2. On the Browse for Folder dialog, browse to the folder containing the hash library to run the query against and click **OK**. The Manage Hash Library dialog now lists the hash sets belonging to the hash library you opened.
3. Click **Query**.

- Paste the value into the **Hash Value** field on the Hash Library Query panel and click **Query**.

**Hash Library Query**

Hash Value  
a510b91253544d56b5712d66be8371e9




Query

Matching Hash Items

	MD5	SHA1	Logical Size
1	a510b91253544d56b5712d66be8371e9	cf620087b36ecb566201e62d012726b08cbccdc	47,616

Show Metadata    Show Hash Sets

Hash Item Metadata

	Name	Text
1	 File Name	EVENTLOG.DLL
2	 File Ext	DLL
3	 Filetype	Dynamic Link Library

- In the above example, the **Matching Hash Items** table shows that a match occurred against an MD5 hash in the selected hash library.
- You can obtain more detailed information about the matched hash item by clicking either **Show Metadata** (shown in above panel) or **Show Hash Sets**.



# Tagging

- Overview
- Creating Tags
- Viewing Tagged Items
- Hiding a Tag
- Deleting Tags

## Overview

The EnCase tagging feature allows you to mark evidence items for review. You define tags on a per case basis and default tags can be part of a Case Template.

Any item that you can currently bookmark can also be tagged. You can search for tagged items, view them on the **Search Results** tab, and view the tags associated with a particular item in an Evidence or Records table.

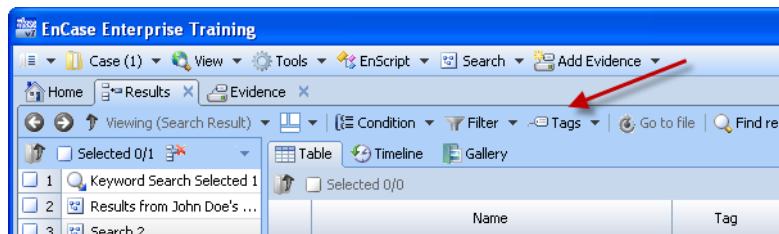
Following is a list of tag features and characteristics:

- You can create tags as part of a case or add them to a Case Template. You can customize each of the tags with specific colors and display text.
- You can edit saved tags: change their colors and text, hide specific tags from viewing, and delete a tag.
- Tags are local to a specific case (that is, you cannot create global tags), and the maximum number of tags that you can use for a case is 63.
- You can directly manipulate tags on the EnCase user interface: change their order, delete them, and so forth.
- You can modify the order in which tags are displayed in the Tag column.
- Once you have created a tag, you can build searches based on tags and also tag search results. You can also combine tags with index and keyword search queries.
- You can create tags using EnScript.

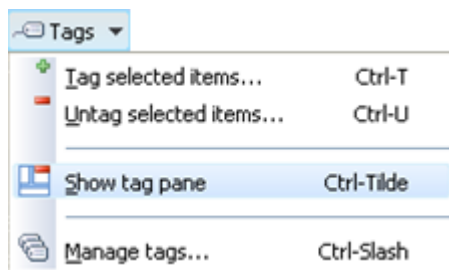
## Creating Tags

To create a tag:

1. On the **Records**, **Evidence**, or **Bookmark** tab, click **Tags** on the toolbar.

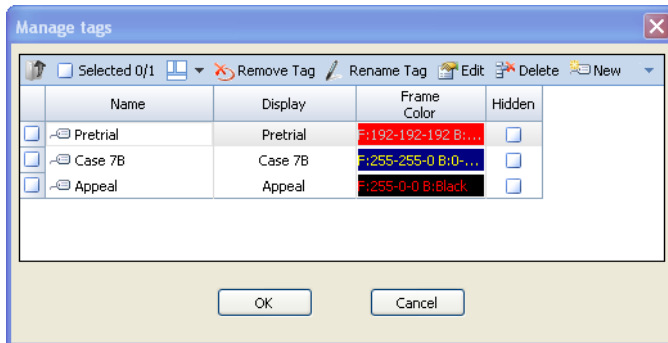


2. On the **Tags** dropdown menu, click **Manage Tags**.



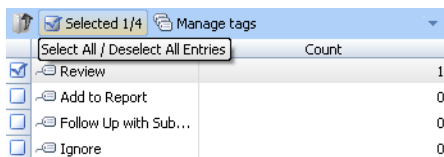
3. On the Manage Tags toolbar, click **New**.

- On the New Tag Item panel, enter a **Name**, the **Display Text** that you want to appear in the tag column (use short display names to conserve space in the column), and the Frame Color (foreground and background colors) for the tag. You can also hide or disable the tag by checking its **Hide** box.
- Repeat steps two through four until you have created the tags you want. You can always add, remove, and rename tags later.

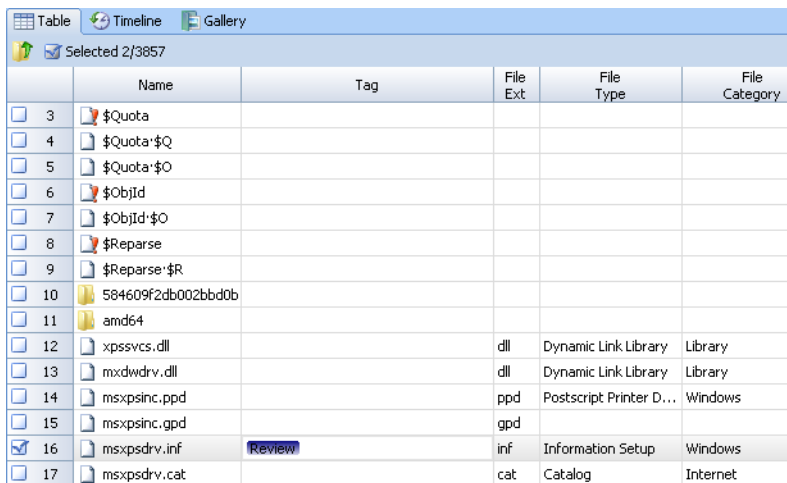


To tag an evidence item, do the following:

- On the **Evidence** tab, display your evidence items. (You can also assign tags to **Records** and **Bookmarks**.)
- Select the evidence item to assign a tag by highlighting or checking it.
- Display a list of available tags by clicking **Tags > Show Tag Pane**. A pane appears in the lower right corner of the EnCase user interface containing a list of default and custom tags.



- Check the tag that you want to assign to an evidence item (this example uses the Review tag).
- The tag you selected appears in the Tag column of the selected evidence item.

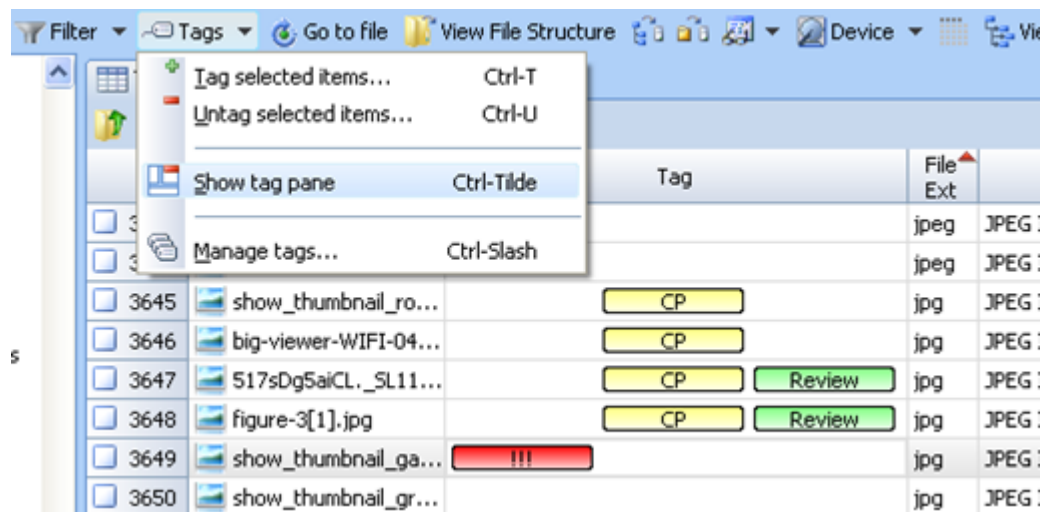


You can also set a tag by clicking on its position in the Tag column.

- Display a list of available tags by clicking Tags > Show Tag Pane. The order that the tags are shown in the table (top to bottom) corresponds to the order that they are displayed in the Tag column (left to right).
- To set a tag using the Tag column, click the space in the Tag column where the tag would be displayed, and it will then appear. As an example, if you have two tags configured, half of the column will be used to display the first tag, and the second half of the column will be used to display the second tag. If you click in the first half of the tag cell for the item you wish to tag, that will apply the first tag to that item and it will now appear in the column. To remove a tag, simply click the tag in the column.

## Viewing Tagged Items

The following figure shows the EnCase Tag menu and a portion of a results table with some of the tagged items. Note how the Tag column can display multiple tags, customized with different text and in different colors. You can change the order of the tags on a row by clicking on a tag and dragging it in the Tag pane.



## Hiding a Tag

If you have configured a tag that you do not currently want to show in the Tag column or the Tag pane, you can hide the tag from the Manage tags window. This will not delete a tag, but simply hide it from view.

To hide a tag, follow these steps:

1. On the **Evidence** tab, click the **Tags** button.
2. On the Manage Tags dialog, check the box in the **Hidden** column for the cell corresponding to the tag you want to hide.

## Deleting Tags

Tags that you do not want to use can be deleted from the Manage tags window. Deleting a tag removes the tag name from the case and deletes all references to the tag in the tag database. This action cannot be undone. When deleting a tag, if that tag has been assigned to an item in the case, a warning dialog will indicate the number of tags to be deleted. If no items are tagged with that tag name, then no warning will be displayed.

To delete a tag, follow these steps:

1. On the **Evidence** tab, click the **Tags** button.
2. On the Manage Tags dialog, check the row containing the tag that you want to delete.
3. On the Manage Tags toolbar, click **Delete**.



# Using Search Tools

- Overview
- Search Types
- Creating a Search Query
- Index Query Options
- Unifying Search Results
- Targeted Keyword Searches

## Overview

This chapter describes the enhancements made to searching in EnCase search, including:

- The ability to search across multiple types of data, including files, email, and Internet history, and view the results on a single screen.
- A powerful index search capability
- The ability to search based on user-customized tags.

## Search Types

There are three principal methods of searching through evidence in EnCase:

- Index searches. Evidence data is indexed through the Evidence Processor prior to searching; see *Index Text* (on page 33).
- Raw searches (searches based on non-indexed, raw data)
- Tag searches. Searches based on user-defined tags; see *Tagging* (on page 51).

### *Index Searches*

Creating an index builds a list of words from the contents of a device. The index entries contain pointers to the occurrences of the specific word on the device.

There are two steps to using indexes:

- Generating an index
- Searching an index

Generating an index creates index files associated with devices. Creating an index can be time consuming, depending on the amount of evidence you are indexing as well as the capabilities of your computer hardware. Evidence file size, and thus, the resultant index size is an important consideration when building an index. Attempts to index extremely large evidence files can tax a computer's resources.

You generate a search index *early* in the EnCase workflow sequence, as follows:

1. Make sure that your case contains the device you want to index.
2. From the Evidence menu, click **Process Evidence**. The Evidence Processor displays. This dialog contains the selection for indexing text.
3. Follow the instructions in the Evidence Processor chapter. See *Index Text* (on page 33) for information.

During the creation of an index, the transcript text of the file is extracted using Outside In technology, and then the text is broken into words which are added to the index. Unlike raw keyword searches, indexing is done against the transcript content of the file so that text contained in compound files such as Microsoft Office files can be properly identified. Although we cannot obtain a transcript of slack space and unallocated space, they are also processed and broken into words in the best manner possible so that we can find hits in those areas also.

Index searching allows you to rapidly searches for terms in the generated index, and is the recommended type of search in EnCase. Querying an evidence file's index locates terms much more quickly than using non-indexed queries.

## Raw Searches

Although index searching is the recommended type of search, there may be times when you want to perform a search across the raw contents of a device. In those cases, you can perform a keyword or non-indexed search on your case data. Because keyword searching only searches the raw binary form of a file, some content may not be discovered if it is compressed or obfuscated.

To perform a raw keyword search on your data:

- Make sure that your case contains the device that you want to search.

For information, see the *Search for Keywords* (on page 31) option of the Evidence Processor. In addition to keyword searching using the Evidence Processor, you can also initiate a raw keyword search of one or more devices from the **Evidence** tab. To initiate a search in this manner, follow these steps:

1. Navigate to the Evidence tab and then navigate to the top level of the tab (using the **View** dropdown menu on the tab toolbar).
2. Select the device or devices that you wish to search using the checkboxes on the left side of the table.
3. Select **Keyword Search All Entries** from the tab toolbar.
4. Select a previously run search or create a New search.
5. Select the keywords and options that you wish to use (see the *Search for Keywords* (on page 31) option of the Evidence Processor) and select **OK**.

**Note:** Keyword searches that are not initiated from the Evidence Processor are stored with the case and are case specific. Keyword searches that are conducted with the Evidence Processor are stored with the device's cache files and can be used with any number of cases.

## Tag Searches

EnCase also provides the capability to search for instances of particular tag that you have created. Suppose you create a collection of 20 tags associated with pieces of evidence, one of which is named "Fraud." You can search through your evidence for all instances of that tag, and the result set that displays will consist only of evidence with that tag. For more information, see the *Tagging Overview* (on page 52).

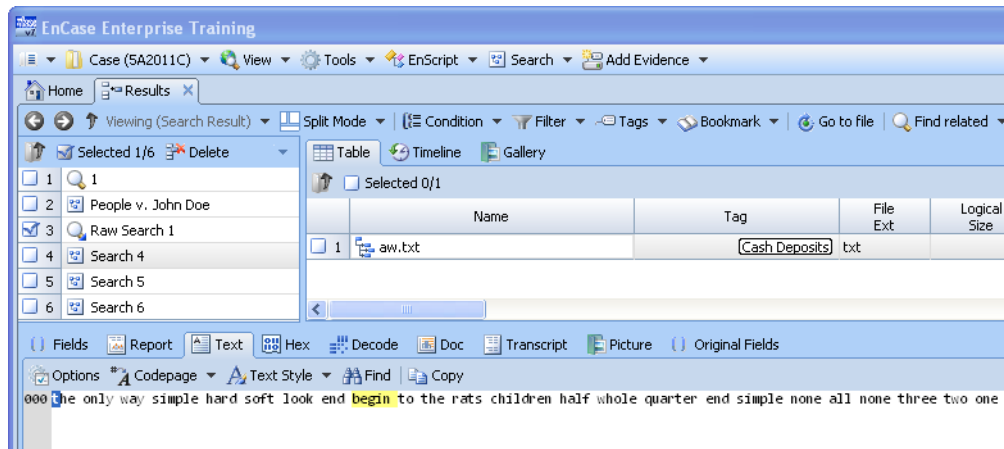
## Creating a Search Query

Once your case has been indexed, keyword searched, tagged or any combination of the three, you can then search for desired information. To create a unified search, do the following:

1. Click the Search menu on the application toolbar and select New Search...
2. Enter a Name for the search. This name will be used to save the search criteria and must use filename compliant characters.
3. Enter a Result Name. This name will appear on the search results page.

4. In the Criteria panel, click the checkboxes to select the combination of **Index**, **Tags** and **Keyword** searches that you would like to add to your query.
5. For each item that you selected, click the hyperlinked name of the item to set its options. See below for information on setting options.
6. Click **Save & Run**.

The following figure shows a simple raw search run from the **Results** tab. The raw search is conducted against the file `aw.txt`, shown on the **Table** tab, and the results of the search are shown in the view window, with a single hit, the word *begin*.



## Index Query Options

When you click Index to set the query options, a new window is displayed with three tabs. These tabs are:

- Text. The tab where you enter text base queries.
- Terms. A hierarchical view of the query terms and logic.
- Report. A "plain English" representation of the query terms and logic.

On the right side of the window is a dynamic list that shows the terms in the index and the number of occurrence of a term. This is extremely helpful when crafting a query so that you can immediately see if the term exists in the index. EnCase will show you all words in the index that start with the term that you have typed, and will dynamically update the list as you type additional letters. At any time, you can double click on a query term, and it will show the show the information about that term.

## Search New

By default, EnCase searches for items containing all the keywords in the search term. For instance, the search term George Washington searches for all items that contain both the word George and the word Washington.

- You can search for documents containing either keywords by using the OR operator: George OR Washington

- You can use the AND operator for clarity: George AND Washington

However, the latter term produces exactly the same results as the original search term.

### Proximity

To search for two keywords within a specified number of words from each other, use the w/ operator:

- George w/3 Washington
- Abraham w/5 Lincoln

### One word before another

You can also search for documents where the first keyword precedes the second by no more than a specified number of words:

- George pre/3 Washington
- Abraham pre/3 Lincoln

### Keywords apart from each other

To search for documents where the keywords are *not* within a certain number of words of each other, use the nw/ or the npre/ operators:

- George nw/3 Washington
- Abraham npre/3 Lincoln

### Exact phrases

You can search for exact phrases using quotation marks (""), which is the same as using the pre/1 operator:

- "George Washington" is the same as George pre/1 Washington

### Near the front or end of the document

You can use the reserved words firstword and lastword with the proximity operators to refer to the beginning or end of the document. For example,

- George w/3 firstword  
finds documents where George is one of the first three words in the document, and
- Washington nw/20 lastword  
finds documents where Washington is not any of the last twenty words in the document.

### With two variables

Use parentheses to group multiple words within a search term. For example, in the following search term:

- Bill w/5 (Clinton or Gates)

the index marks as responsive all items containing the word Bill within five words of either Clinton or Gates.

### With multiple variables

You can also construct a complex proximity search that includes Boolean operators on both sides. For example, in the following search expression:

- (Bill and William) w/5 (Clinton and Gates)

the index marks as responsive all items containing both the words Bill and William within five words of both Clinton and Gates.

### Grouping Search Queries Together

You can group search queries together using parentheses to form logical expressions. How you use parentheses indicates to the search engine the order in which it should look for the search terms. For instance:

- (George and Washington) or (Abraham and Lincoln)

finds all items with either both the words George and Washington or both the words Abraham and Lincoln

You can nest parenthetical expressions; for example:

- (George and (Washington or Bush))

finds all items that contain the word George and either the words Washington or Bush.

Alternatively,

- (George and Washington) or Bush

finds all items that contain the words George and Washington, or Bush.

You can use parentheses to join proximity queries (pre/, w/) to Boolean logic queries (AND, OR). For example,

- Delaware and (George pre/3 Washington)

finds all items that contain the word Delaware and that also contain the word George no more than three words before Washington.

You cannot use parentheses to put a Boolean term into a proximity term:

- DISALLOWED: George pre/3 (Washington and State)

Instead, express this term as follows:

- (George pre/3 Washington) and (George pre/3 State)

### Searching for Keywords in Document or Email Fields

By default, EnCase searches for keywords in every indexed text field of the document or email. You can restrict the fields that you search using the bracket ([ ]) field specifier. For instance, to search only for keywords in the subject line, use:

- [Subject]George

You can use parentheses to group keywords together within a field:

- [Subject](George Washington)
- [Subject](George pre/2 Washington)

You can use aliases to group together a section of fields:

- [Address] searches the [To], [From], [CC] and [BCC] fields
- [Date] searches the [Accessed], [Created], [Modified], [Written], [Sent] and [Received] fields

Common fields for all items are:

- [Name]Name of file.File extension (the file will not be found unless it contains the extension)
- [Extension]File extension
- [Category]Category of file, such as Picture

### Searching for Date Fields or Date Properties

You can search for items by date or date range using field syntax. Dates are entered in ISO 8601 syntax between # marks, and can be general, such as:

- [Created]#2004#

Or very specific:

- [Created]#2004-11-19T11:54:03#

You can also search for date ranges using an ellipsis (...):

- [Created]#2004-02-03...2004-02-17#

The above term searches for any item with a creation date between Feb. 03, 2004 and Feb. 17, 2004. You can search for items before or after a particular date by leaving off one end of the range:

- [Created]#2004-02-03...#
- [Created]#...2004-02-17#

File date fields are:

- Accessed
- Created
- Modified
- Written

Email date fields are:

- Sent
- Received
- Created

### Searching for Numeric Properties

You can search for items by number range using field syntax. Numbers are entered between # marks and can be specific, such as:

- [Size]#1034# Analyzing Collected Data 355

Or a range, using ellipses, such as:

- [Size]#1000...3000#

The above term searches for any item with a size between 1000 bytes and 3000 bytes. You can search for numbers above or below a particular point by leaving one end of the range off:

- [Size]#...3000#
- [Size]#1000...#

### Searching for Case Sensitive Terms

By default, all index queries are case-insensitive. You can make queries case-sensitive by using the <c> operator:

- <c>George
- <c>(George and Washington)

You can specify case-sensitive queries for fields:

- <c>[subject](George pre/3 Washington)

### Using Wildcards to Search for Patterns

You can search for incomplete words or word prefixes using the ? and \* operators.

#### *Wildcard for single characters*

The ? operator stands as a placeholder for any single characters. For instance,

- c?t

results in hits for documents containing cat, cot, and cut, but not caught.

#### *Wildcard for multiple characters*

The \* operator stands as a placeholder for any number of characters. For instance,

- ind\*

results in hits for documents containing indecisive, indignant, and Indiana.

#### *Multiple wildcards*

A keyword may contain multiple wildcards (either \* or ?), but may not contain wildcards at both the beginning and end of the word. For instance,

- ind\*ia\*a
- c?t?
- \*fi?y

are valid keywords. However,

- \*india\*
- ?cat?
- \*fish?

are not valid keywords.

#### *Using wildcards with punctuation*

The wildcards ? and \* only work for the following punctuation types:

- Dash (-)
- Underscore (\_)
- Period (.)
- Comma (,)
- At symbol (@)
- Apostrophe (')

**Note:** Punctuation characters will not be found using wildcards if they are at the beginning or end of words.

### Using Stemming Lists to Search for Similar Words

You can use the stemming operator ~ to search for similar words. By default, the stemming operator replaces your word with all words similar to it in the English language. For instance,

- swim~

results in hits for documents containing swim, swim's, swimming, swam, swum, etc. Stemming uses the language packs on the server to find words similar to your original term.

When you test your term, a stemming list is added to the term. Stemming lists are contained within the <> characters and clearly display the stems for the keyword. For instance, the default stemming list for swim is:

- <s:swim swim's swims swims' swimming swam swum swim>

You can override the default stemming behavior by modifying the stemming list. For instance,

- <s:swim swam swum>

would result in hits for documents containing swam and swum, but not swimming, swim's, etc. You can incorporate stemming into any location you could use the OR operator. For instance,

- run~ and [Created]#2002#
- <s:run ran running runner>

results in hits for documents created in 2002 and contain at least one of run, ran, running, or runner.

### Fields in Index Queries

Index queries can be created that target data in specific data fields. By selecting the **Fields** button on the toolbar, you can double click on a Field name and add it to your query. After adding the Field name, type the value that you wish to query for. The available fields are:

#### General Fields

- Any Field
- Content – body of document or Email (transcript)
- Category
- Description
- Extension
- File Type

- Path
- Hash Value
- Logical Size
- Dates
- Accessed Date
- Created Date
- Modified Date
- Written Date

#### Email Fields

- To
- From
- Subject
- Sent Date
- Attachment Size
- BCC
- CC

### *Index Query Logic*

In addition to adding Fields into your query, you can also add additional types of logic to customize the result set. The available options are:

- *Case Sensitivity*
- *Stemming*
- *Terms w/ combining logic*
- *Preview dictionary w/ hit count*
- *Can Combine w/ Keyword Searches and Tags*
- *Can Filter or Condition on Search Results*
- *Can combine multiple search results w/ AND/OR logic*
- *Can view previously run searches*

## Unifying Search Results

EnCase allows you to view search results from a variety of sources, using the single **Search Results** tab. The results can span numerous types of data (for example, files on the **Entry** tab, email information, and Internet artifacts), and contain the results of a filter, condition, or search (including Index, Keyword, and/or Tags).

All of the operations above produce distinct result sets. The queries that are used to display the result sets are stored as files in the users EnCase directory.

Search Result sets can display quickly because they show a subset of available metadata for each item. To view additional information about an item, simply select the item and click **Go to file** in the tab toolbar. The unified metadata available in the Search Results table is:

#### *Name*

- For an Entry Item: Entry Name
- For an Email Record: Email Subject
- For an Internet History Record: URL

#### *Logical Size*

- Entry: Logical Size
- Record: Logical Size (PR\_LOGICAL\_SIZE)

#### *Last Accessed Date*

- Entry: Accessed
- Record: Accessed (PR\_ACCESSED)

#### *File Created Date*

- Entry: Created
- Record: Created (PR\_CREATION\_TIME)

#### *Last Written Date*

#### *From*

- Email Record: From field
- Internet History Record: User

#### *Recipients*

- Email Record: Aggregation of To\Cc\Bcc fields

#### *Comment*

#### *Item Type*

#### *Category*

#### *Primary Device*

#### *Item Path*

The Search Result table displays two additional columns that are dynamically generated based on the items in the table:

#### *Extension*

- Generated from the Search Result Name at display time

#### *Tags*

- Generated from the current case at display time

### Queries available on the **Search** Tab

- *Search index options*
  - Fields
  - Any Field
  - Content – body of document or Email (transcript)
  - Category
  - Description
  - Extension
  - File Type
  - Path
  - Hash Value
  - Logical Size
  - Dates
    - Accessed Date
    - Created Date
    - Modified Date
    - Written Date
- *Email*
  - To
  - From
  - Subject
  - Sent Date
  - Attachment Size
  - BCC
  - CC
- *Case Sensitivity*
- *Stemming*
- *Terms w/ combining logic*
- *Preview dictionary w/ hit count*
  
- *Can Combine w/ Keyword Searches and Tags*
- *Can Filter or Condition on Search Results*
- *Can combine multiple search results w/ AND/OR logic*
- *Can view previously run searches*

## Targeted Keyword Searches

In EnCase Version 7, comprehensive keyword searching is done using the Evidence Processor. In addition to this functionality, EnCase also has the ability to run a targeted keyword search against selected data

1. From the **Evidence** tab, check specific items that you want to keyword search.
2. From the Tab toolbar, select **Raw Search** and **New Raw Search**, and a new window will display.
3. Select the keywords and options that you wish to use (see the *Search for Keywords* (on page 31) option of the Evidence Processor) and select **OK**.
4. When the search has completed, you will be taken to the **Search Results** tab to view the results of your targeted search.

The targeted search will only act on items selected in the current view. If you have multiple devices in your case, but are currently viewing only one of them, the search will only run on that device, regardless of whether you checked items in another device. If you wish to run a target search against two or more devices in your case, you must **Load Selected Evidence** into one window. The targeted search cannot run on a physical device and a mounted device at the same time.



# Reporting

- Overview
- Using Report Templates
- Bookmarking Data for Reports
- Report Template Structure
- Formatting Report Templates
- Report Styles
- Viewing a Report

## Overview

The final phase of a forensic examination is reporting the findings, which must be well-organized and presented in a format that the target audience will understand. EnCase Version 7 has added several enhancements to its reporting capabilities that strengthen this phase of the process. These include:

- The inclusion of reporting templates that you can use as is or adjust to suit your needs.
- The capability to control a report's format, layout, and style.
- The ability to add notes and tags to a report.

Reports in EnCase Version 7 consist of two parts:

1. Report templates that hold the formatting, layout, and style of the report.
2. Bookmark folders where reference to specific items and notes are stored. The Report template links to bookmark folders to populate content into the report.

## Using Report Templates

A report template is one component of a case template. Each of the default case templates has a customizable report template included. Different case templates may contain different report templates, and each of these templates is completely customizable. In addition to the report template, each case template also includes bookmark folders that are referenced in the report.

Besides the default templates, users can define their own custom reports and save them as part of a case template. For more information, see *Using a Case Template to Create a Case* (see "Creating a Case" on page 15).

## Bookmarking Data for Reports

In EnCase, as you work on a case, you typically discover files, portions of files, and other objects that are of interest as potential evidence and save these items for reference. These marked sections are referred to as *bookmarks*. Bookmarks are saved in folders in the case file. You can view them 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. You place bookmarks into bookmark folders and give them names associated with meaningful aspects of the case.

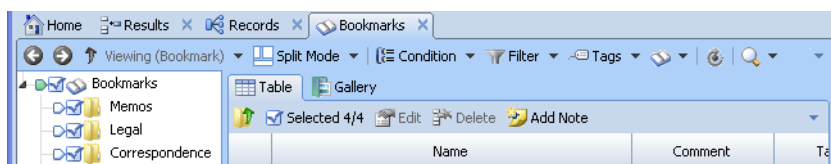
The bookmark folders and their bookmarked data are referenced by the elements of the report structure. The bookmark references constitute a major portion of the report structure, and the bookmark content lying within the bookmark folders appear as formatted report data.

To bookmark data into a folder:

1. Click the **Bookmarks** link on the Case home page in the Reports section.



2. The **Bookmarks** tab and its options display.



3. Create appropriate folders to hold your bookmarks and add any desired notes to the folders.
4. To bookmark data, select content from almost any tab and click the **Bookmark** drop down menu on the **Tab** toolbar. Select the appropriate bookmark type, add a name, and comment as desired, and click **OK**.
5. View your bookmarks in the **Bookmarks** tab.

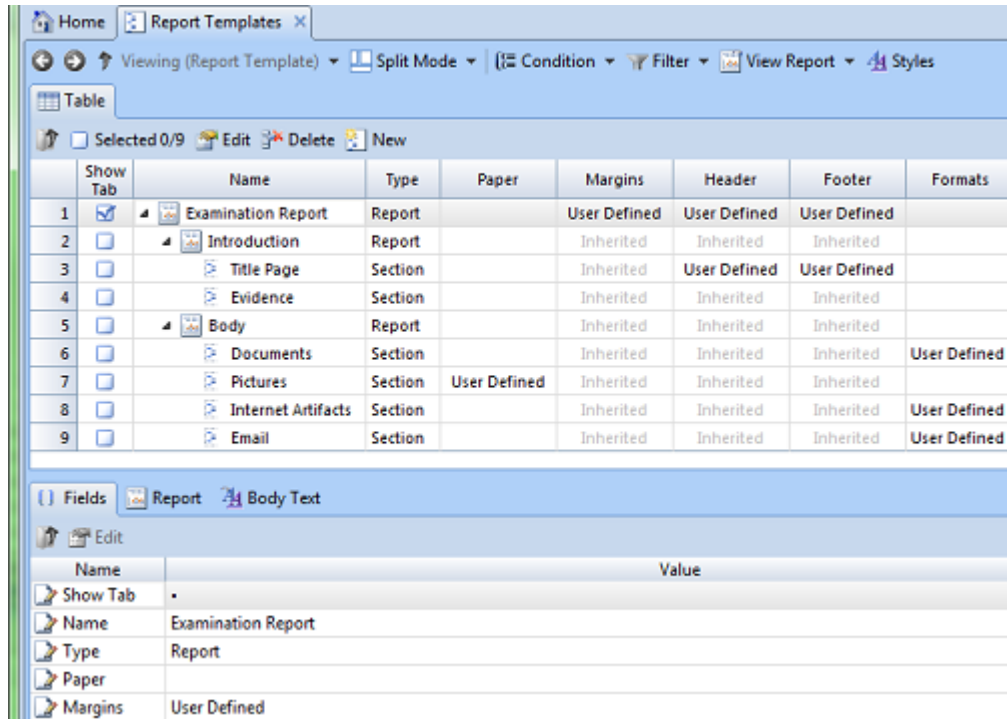
## Report Template Structure

Before viewing a report, you need a report template, or outline of what the report will look like. The report template also defines how your case data is formatted and styled. This structure consists of:

- Report Sections. Sections contain groups of like information and formatting, and provide the ability to organize your report.
- Report Formatting. This includes page layout, section design, and text styles.

- Report elements, which are collections of bookmarks. Bookmarks are a key element of the report structure. You do not embed bookmarks into a report template, but embed a *reference* to the contents of a bookmark folder.

Following is an example of a report template (**Report Templates > Table**). For organization and flexibility in reporting, a report component can be designated as either a Report or Section, as shown in the Type column of each Table row. Report components typically only contain formatting information for components beneath them, while Section components contain formatting information and Report elements. The columns to right of Type indicate whether a particular formatting option is user-defined or inherited from the report or section above it in the hierarchy of rows.



The screenshot shows the 'Report Templates' window in EnCase Forensic. The main area displays a table with the following data:

	Show Tab	Name	Type	Paper	Margins	Header	Footer	Formats
1	<input checked="" type="checkbox"/>	Examination Report	Report		User Defined	User Defined	User Defined	
2	<input type="checkbox"/>	Introduction	Report		Inherited	Inherited	Inherited	
3	<input type="checkbox"/>	Title Page	Section		Inherited	User Defined	User Defined	
4	<input type="checkbox"/>	Evidence	Section		Inherited	Inherited	Inherited	
5	<input type="checkbox"/>	Body	Report		Inherited	Inherited	Inherited	
6	<input type="checkbox"/>	Documents	Section		Inherited	Inherited	Inherited	User Defined
7	<input type="checkbox"/>	Pictures	Section	User Defined	Inherited	Inherited	Inherited	
8	<input type="checkbox"/>	Internet Artifacts	Section		Inherited	Inherited	Inherited	User Defined
9	<input type="checkbox"/>	Email	Section		Inherited	Inherited	Inherited	User Defined

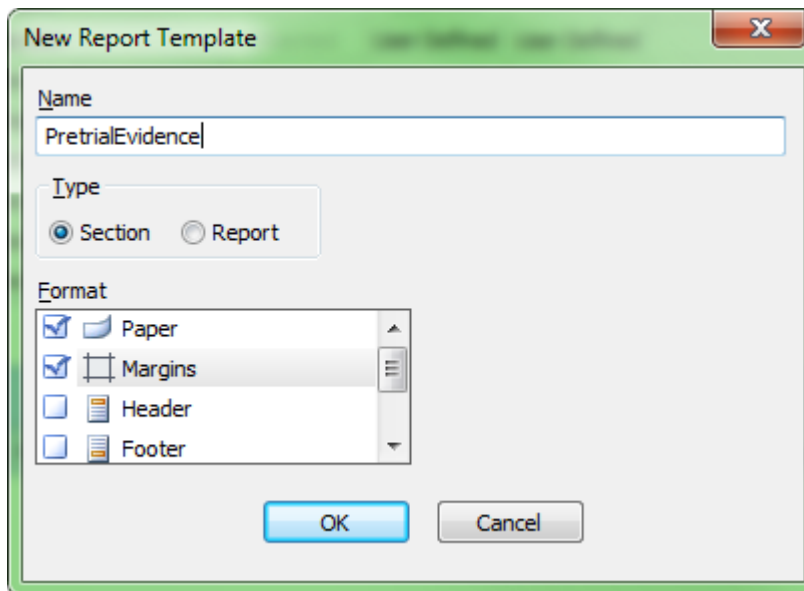
Below the table, the 'Fields' section is expanded to show the properties of the selected 'Examination Report' component:

Name	Value
Show Tab	<input checked="" type="checkbox"/>
Name	Examination Report
Type	Report
Paper	
Margins	User Defined

To add new reports or sections to the template:

- Highlight the row above the new element you want to add.

- Click **New** on the **Table** tab. The New Report Template dialog appears.



- Type a **Name** for the new Report Template component.
- Select a **Type** (Section or Report) for the new template component.
- Select whether you want to customize a **Format** style by checking its box, or use the default format style by leaving the box clear.
- Click **OK**. The new template component will appear below the row that you highlighted.

## Formatting Report Templates

There is a wide range of formatting options available for customizing EnCase reports. Guidance Software recommends using the default case templates as a starting point and customizing them as necessary. These templates provide examples of most reporting options.

As demonstrated in the above picture, report templates can and should be designed as a hierarchal tree to simplify formatting. If properly designed, report sections will inherit formatting options from above and therefore changes to the formatting will only have to be made in one location.

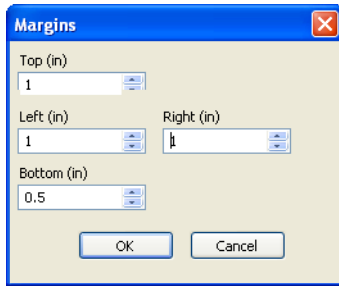
The following is a list of items that can be customized:

- Section Name. This name is for organizational reference in the template only and does not populate into the report.
- Paper. This includes orientation and size.
- Margins. Values can be set for top, bottom, left and right margins.
- Header/Footer. Users can design a completely customized header or footer that contains Case Info Items and other various data.
- Data Formats. The display characteristics of each bookmark type can be customized. This includes data style and content.
- Section Body Text. The layout and content of each section is specified in the Body Text.
- Show Tab. This options determines if this report or section is displayed as a tab in the Reports tab.

- Excluded. Provides the ability to quickly exclude a section from a report if it is not applicable.

To edit a formatting option:

1. Right click a cell that represents the report element and the formatting component you want to edit.
2. Click **Edit...** on the cell's context menu.
3. Change the default values for the formatting option to the values you want. In the example shown below, the Margins cell for the Body element is selected, and the left and right margins are changed from the default values to one inch. Click **OK** when you are finished.



**Note:** Remember formatting options, from beginning to end, are inherited by default. Therefore, in this example, the margins for the report components that follow the one you customized will inherit those margin settings, unless you edit them.

## Report Styles

As in Microsoft Word, Styles are used to set text formatting options. EnCase comes with many default styles that can be used in report templates, and users can create their own styles. Users can override a default style by creating a user style with the same name.

Options that can be designated in a Style include:

- Font type and font size
- Alignment (left, center, right, justified)
- Indenting (left, right, first line)
- Space before/after
- Borders
- Tabs
- Text color
- Background color

To create a user defined style:

From the **Report Template** tab, select **Styles** from the **Tab** toolbar.

1. A new window appears that contains a tab for **Default Styles** and a tab for **User Styles**. Users can examine the available Default Styles by looking in that tab.
2. Switch to the **User Styles** tab.
3. Select **New** from the toolbar. The ability to Edit or Delete an existing User Style can also be found in the toolbar.

4. Provide a name for the Style and desired configuration options. Font, Text Foreground and Text Background can all be set by double clicking on the appropriate field.

## Viewing a Report

Once you have configured your Report Template and added Bookmarks to the appropriate folders, there are two ways to view a report:

- From the **Report Templates** tab, select **View Report** from the tab toolbar. This will list all reports that have the **Show Tab** option set. Selecting a report from the menu takes you to the Reports tab to view the selected report.
- Select the **Reports** tab from the Case Home page or the View menu. In the **Reports** tab you will see a tab for each report that has the **Show Tab** option set.

Reports are dynamically generated every time that you switch to a specific report in the **Reports** tab. To save a report, right-click on the report and select **Save As**. The following output formats are available:

- TEXT
- RTF
- HTML
- XML
- PDF

Once you select the output format, specify a **Path** and optionally set the **Open file** option if you want the file to open in the default application after saving.

**Note:** It is recommended that users wishing to edit their report in Microsoft Word save the report in RTF format. The EnCase RTF report is completely compatible with Microsoft Word.



# Index

## A

Adding Evidence to a Case • 18  
Adding Hash Values to a Hash Set • 47  
Application Folder • 9

## B

Bookmarking Data for Reports • 72  
Browsing Case Data • 20

## C

Case Folder • 10  
Codemeter Dongle • 8  
Configuring Time Zone Settings • 27  
Create Image Thumbnails • 33  
Creating a Case • 15  
Creating a Hash Library • 45  
Creating a Hash Set • 47  
Creating a Search Query • 59  
Creating Tags • 52

## D

Deduplicating Messages • 42  
Deleting Tags • 55  
Displaying Email Threads • 39  
Displaying Related Messages • 41

## E

EnCase Forensic • 4  
EnCase Version 7 Application Folder Locations • 9  
Evidence Cache • 11  
Evidence Processing Tasks • 29  
Evidence Processor • 25  
Expand Compound Files • 34

## F

Fields in Index Queries • 65  
File Carver • 35  
File Signature Analysis • 34  
Find Email • 30  
Find Internet Artifacts • 31  
Formatting Report Templates • 75

## G

Getting Started with EnCase Version 7 • 13  
Global Application Data • 11

## H

Hash Analysis • 30  
Hashing • 43  
Hashing Features • 44  
Hiding a Tag • 54

## I

IM Parser • 34  
Index Query Logic • 66  
Index Query Options • 60  
Index Searches • 58  
Index Text • 33  
Installation and Configuration Changes • 7

## L

Launching EnCase for the First Time • 14

## M

Managing Evidence Processor Settings • 29  
Modules • 34

## N

New Features • 5

## O

Overview • 3, 8, 14, 26, 38, 44, 52, 58, 72

## P

Preparing the Evidence to Process • 27  
Protected File Analysis • 34  
Purpose of this Guide • 4

## Q

Querying a Hash Library • 48

## R

Raw Searches • 59  
Recover Folders • 30  
Report Styles • 76  
Report Template Structure • 73  
Reporting • 71

## S

Search for Keywords • 31

- Search New • 60
- Search Types • 58
- Sentinel HASP Dongle • 8
- Setting Case Options • 22
- Shared Files • 12
- Show Conversation • 40

## **T**

- Tag Searches • 59
- Tagging • 51
- Targeted Keyword Searches • 69
- Thread Email • 31

## **U**

- Unifying Search Results • 66
- User Application Data • 11
- User Data • 9
- Using an EnCase Dongle • 8
- Using Report Templates • 72
- Using Search Tools • 57
- Using the EnCase Installation Wizard • 8
- Using the Processor Settings Toolbar • 29

## **V**

- Viewing a Report • 77
- Viewing Tagged Items • 54

## **W**

- Working with Cases • 22
- Working with Email Evidence • 37
- Working with Hash Libraries • 45