Searching the Case

Overview

EnCase® Forensic (EnCase) provides a powerful search engine to locate information anywhere on the physical or logical media. After creating a case file, a keyword search operation may be conducted.

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

- **Tag searches** – Searches based on user-defined tags
- **Index searches** – Evidence data is indexed through the EnCase® Evidence Processor prior to searching
- **Raw searches** – Searches based on non-indexed, raw data

Tag Searches

EnCase also provides the capability to search for instances of a particular tag or identifying term 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. More information is provided within a future lesson.

Index Searches

Using the Evidence Processor, you create an index, consisting of 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 (covered in a previous lesson)
- Searching an index

Generating an index creates index files associated with devices and 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 should generate an index on your evidence ***early*** in your analysis process. This is done through the Evidence Processor. It is suggested that acquired evidence files be indexed.

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 that 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 2007 and 2010 files, can be properly identified. Although EnCase® v7 does not create a transcript of slack space and unallocated space, they are also processed and broken into words in the best manner possible, so EnCase can find hits in those areas also.

Index searching allows you to rapidly search for terms in the generated index and it is the recommended type of search in EnCase. Index searching enables you to search through the indexed content of the drive as well as the metadata of file and folder objects. Because EnCase v7 conducts indexing at the logical level, EnCase v7 will find fragmented keywords. Index search expressions be saved within a folder and filename specific by the user. The file is created with the extension .EnSearch. Saved Search Expressions may be recalled and the search run again.

Raw Searches

Raw Searches may be conducted on evidence files, live devices, or selected objects. Searching with one or more raw keywords performs a logical search through the selected active file structure, and performs a physical search though unallocated and unused disk area. Raw keyword search expressions must be saved prior to running the search and may be saved within the folder and filename designated by the user. Saved Search Expressions may be recalled and the search run again.

Overview of Index Search Options

Searching for All or Any Keywords

By default, EnCase searches for items containing all query keywords:

"George Washington" searches for "George" and "Washington"

For either keyword, use the **OR** operator:

George OR Washington

You can also use the **AND** operator:

George AND Washington

Searching for Keywords Near Each Other

For two keywords within a certain number of words of each other, use the **w/** operator:

George w/3 Washington

Where the first keyword precedes the second keyword by no more than a certain number of words, use the **pre/** operator:

George pre/3 Washington

You can also search for exact phrases using quotation marks (""), which is identical to using the **pre/1** operator:

"George Washington" or George pre/1 Washington

Grouping Search Queries Together

You can group search queries together to form logical expressions by using parentheses. This indicates to the search engine the order in which it should look for the search terms:

(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 as much as you want:

(George and (Washington or Bush)) finds all items that contain the word "George" and either the words "Washington" or "Bush"

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

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 the word "Washington"

Searching for Keywords in Document Fields

By default, EnCase searches for your keywords in every indexed text field of the document

You can restrict the fields that you search using the [] field specifier.

Document fields include:

- [Name]*Name*
- [TruePath]*Original location of the file, including the workstation or server name*
- [Category]*Category of document* (document, database, picture, etc.)
- [Extension]*File extension*
- [FileType]*Type of file*
- [Description]*Description*

Searching for Date Fields or Date Properties

You can search for items by date or date range using field syntax. Dates include Created, Accessed, Modified, and Written. Use the **Fields** button to select the desired field to include in the index search.

Dates may just include the year:

[created]#2004#

Or be very specific:

[created]#2004-11-19#

Dates may be within a range:

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

Search for items before or after a particular date by leaving one end of the range off:

[created]#2004-02-03...# or

[created]#...2004-02-17#

Searching for Numeric Properties

Use the **Fields** button to select the LogicalSize field to include in the index search.

Numbers are entered between **#** marks and can be specific:

[Logicalsize]#1034#

Or a range:

[Logicalsize]#1000...3000#

The previous query searches for any item with a size between 1000 and 3000 bytes.

You can search for numbers above or below a particular point by leaving one end of the range off:

[Logicalsize]#...3000# or

[Logicalsize]#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)

Using Wildcards to Search for Patterns

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

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"

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

*ind** results in hits for documents, containing "indecisive," "indignant," and "Indiana"

Stemming

To apply stemming to your keyword searches, use the ~ operator:

Sail~

To stem words within a specific list, use **~<s**: keyword, keyword, keyword>:

Sail~<s:sail, sails, sailing, sailed>

SCENARIO

In this lesson, we will conduct searches based on an investigative scenario.

Norm Peterson is an employee of ZeroBit Incorporated. Zerobit is a government and military contractor that manufactures devices and software code to drive these devices. Norm Peterson has recently come under suspicion of improper and illegal activities. Dominic Santini, Peterson's supervisor, suspects that Peterson has used ZeroBit funds to further personal endeavors. Santini also has discovered that Peterson lied to Nick Burns, lead programmer on the classified OWAT project, in an effort to acquire the computer code associated with this project.

Our task is to determine if Peterson has, in fact, used Zerobit funds personally and if he has possession of the OWAT code.

Using the processed Peterson case, blue-check the evidence files and select **Open** from the button bar to see the objects in both evidence files.

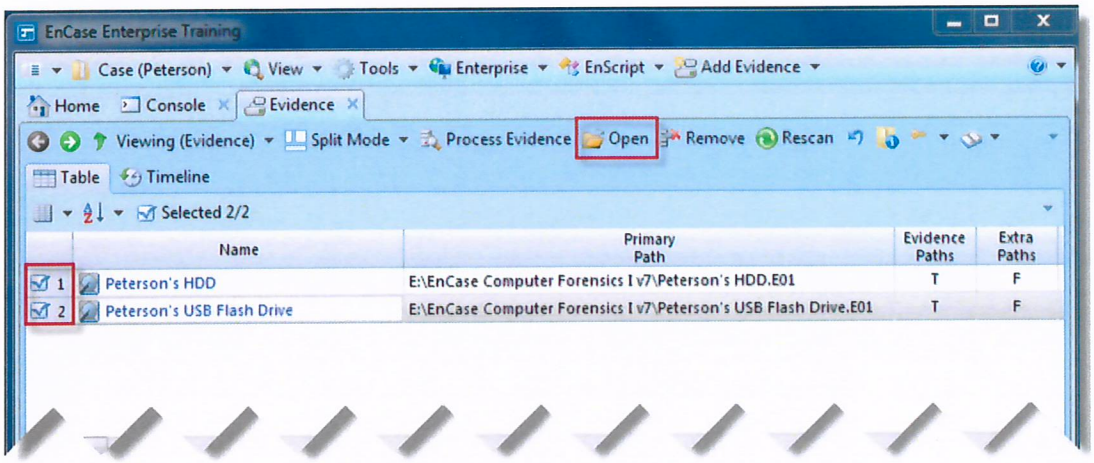

Figure 10-1 View Objects in both evidence files in case