Task

Using the Large Files and Multimedia Files results sets previously created, combine them so that only the objects that have a multimedia category ***and*** a logical file size greater than 4,000,000 are displayed. Name this combined result "LargeMultimediafiles."

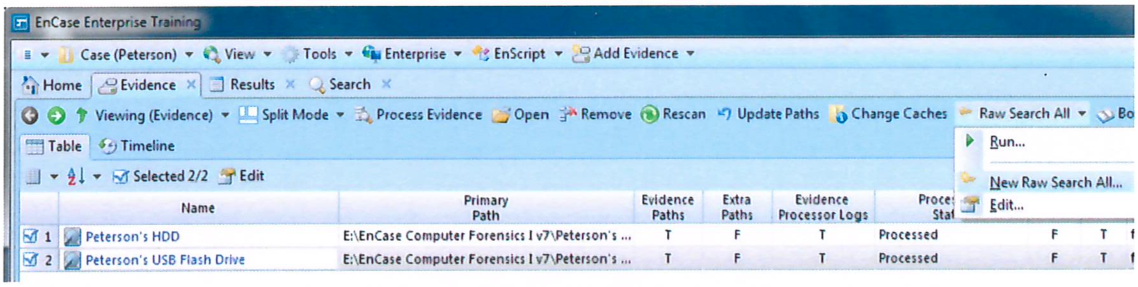
How many hits are displayed?

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. This device may be indexed or not indexed. A raw search searches the physical disk in unallocated clusters, unused disk areas, logical files, and file slack. Because keyword searching only searches the raw binary form of a file, some content may not be discovered if it is compressed or obfuscated. If an allocated file contains a keyword that is fragmented between two clusters, a raw keyword search will result in a hit, whereas a file that becomes unallocated will not. Raw keyword searches do not search the metadata of objects in the case. Raw search keywords must be saved and are saved within a folder and file designated by the user.

A raw keyword search may be initiated from several different tabs within EnCase:

- **Evidence Processor** – will run against every blue-checked evidence file
- **Evidence tab**, **Viewing (Evidence) View**, **Raw Search All** button – Runs against all evidence files and previewed devices within the case



	Name	Primary Path	Evidence Paths	Extra Paths	Evidence Processor Logs	Proce Stat			
☑ 1	Peterson's HDD	E:\EnCase Computer Forensics I v7\Peterson's ...	T	F	T	Processed	F	T	f
☑ 2	Peterson's USB Flash Drive	E:\EnCase Computer Forensics I v7\Peterson's ...	T	F	T	Processed	F	T	f

Figure 10-23 Raw Search All from main Evidence tab

- **Evidence tab**, **Viewing (Entry) View**, **Raw Search Selected** – Runs against all selected or Blue-checked objects – example used within this lesson.

Raw searches provide significant functionality when examining a live device through a preview mode. Use a raw search if the purpose for previewing a drive or examining an evidence file is to search it for a search expression or if GREP searches are to be used. Note that compressed or obfuscated compound files that are not mounted or interpreted may not yield anticipated results through a raw search.

NOTE: A previously run search may also be selected and modified if desired.

In this scenario, Norm Peterson is suspected of using Zerobit funds to further personal endeavors, namely personal travel. Specifically, we have been asked to locate any mention of Hawaii within Peterson's media. We could use an Index Search to accomplish this task, but let's use Hawaii as our raw search expression. From the Evidence tab, Viewing(Entry) view with at least the Peterson's HDD evidence file opened, blue-check the **Users** folder in the Tree Pane within the Peterson's HDD evidence file. From the button bar, click **Raw Search Selected→New Raw Search Selected**...

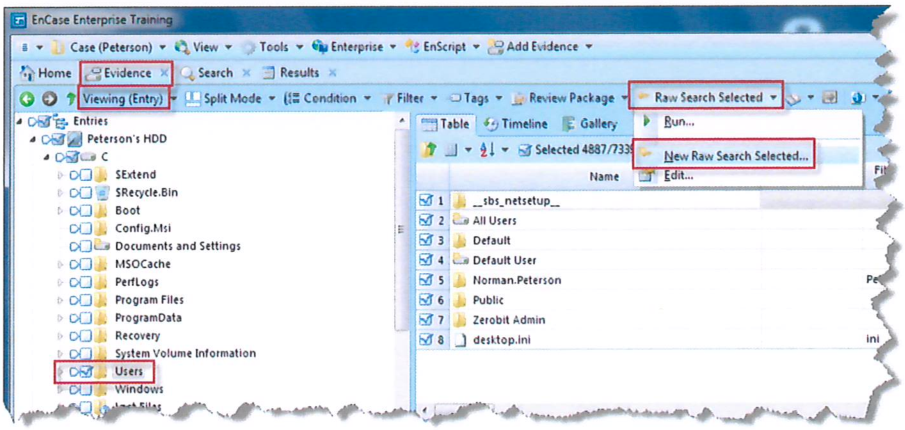
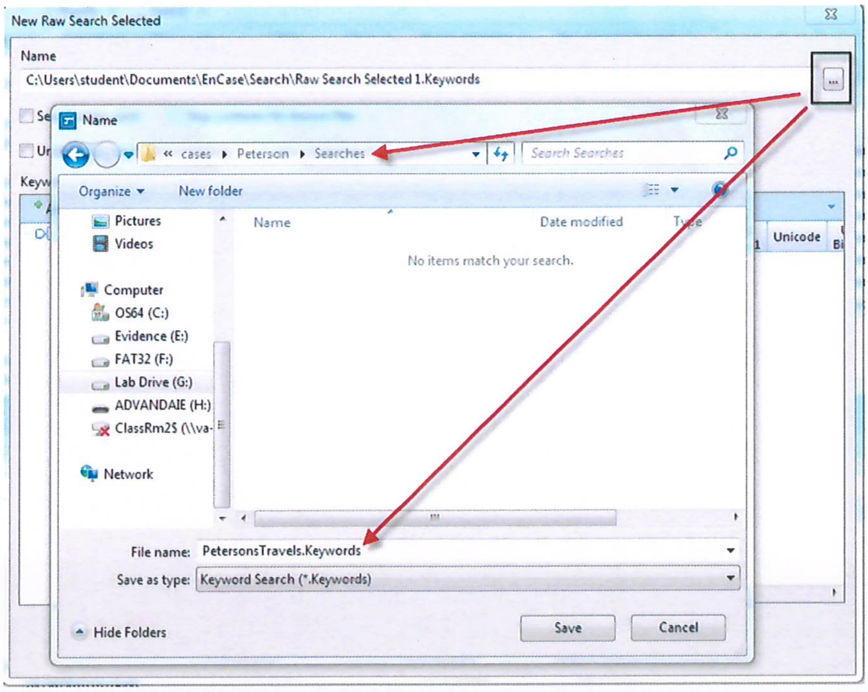


Figure 10-24 Blue -check Users folder, choose Raw Search Selected→New...

Browse to the \Cases\Peterson\Searches folder created previously, type the file name "PetersonsTravels," and click **Save**.


New Raw Search Selected

Name
C:\Users\student\Documents\EnCase\Search\Raw Search Selected 1.Keywords

File name: PetersonsTravels.Keywords

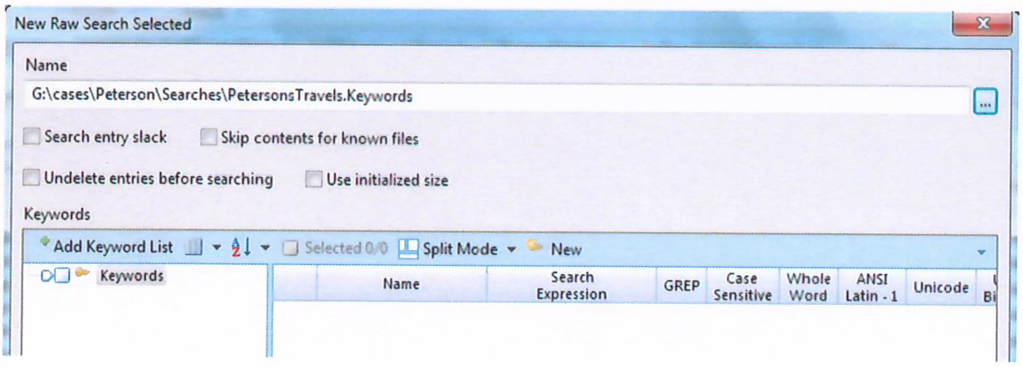
Save as type: Keyword Search (*.Keywords)

No items match your search.

Figure 10-25 Save the file to the \Cases\Peterson\Searches folder

Raw Keyword Search Options

There are four options available that will apply to all keywords searched for in this manner.



New Raw Search Selected

Name

G:\cases\Peterson\Searches\PetersonsTravels.Keywords

□ Search entry slack □ Skip contents for known files

□ Undelete entries before searching □ Use initialized size

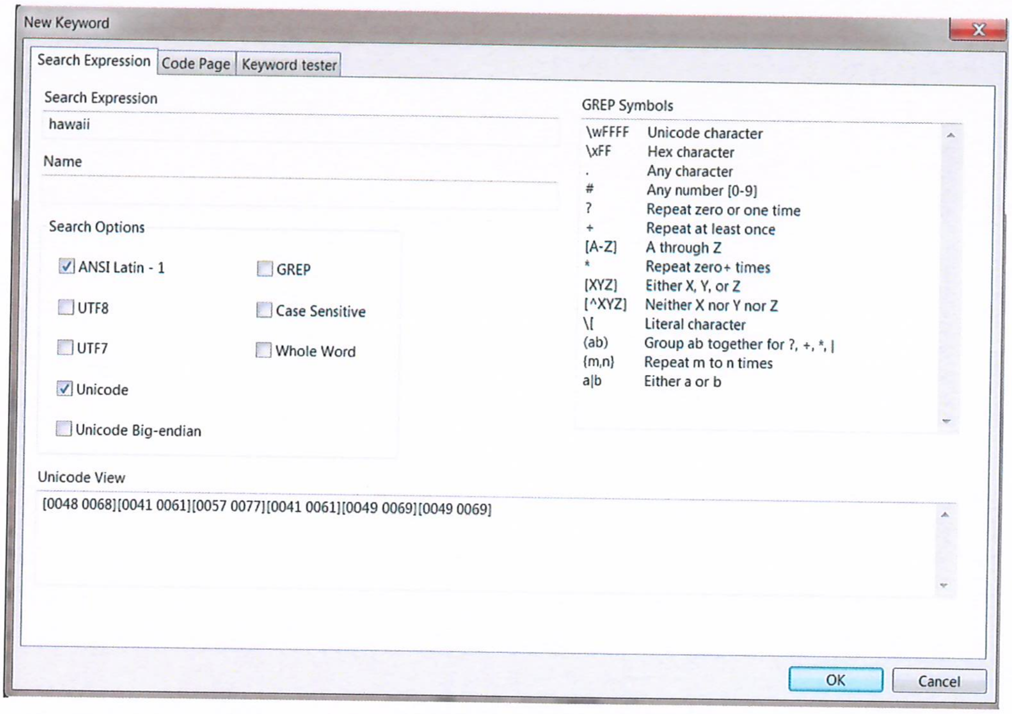
Keywords

Figure 10-26 Four options for raw keyword searching

- **Search entry slack** – This option tells EnCase to search the slack area, which exists between the end of the logical file to the end of the physical file for all items searched.
- **Skip contents for Known files** – This option is used in conjunction with a hash analysis. If a file is identified as *Known* from the hash library, then it will not be searched. However the slack area behind the file (if selected previously) will be searched. If this option is turned off, EnCase will ignore the hash analysis. Hash Analysis will be discussed in more detail later.
- **Undelete entries before searching** – This option will logically "undelete" deleted files prior to searching. If a file is deleted, EnCase and other tools can determine if the assigned starting cluster is not currently assigned to another file (if it is assigned, then the file is deemed deleted/overwritten). The unallocated clusters after the starting cluster may or may not belong to the deleted file. Choosing this option assumes the unallocated clusters after the starting cluster do belong to the deleted file. This is the same assumption made when copying out a deleted file. Choosing this option will find a keyword fragmented between the starting cluster and the subsequent unallocated cluster. If determining the presence of a keyword on the media is critical to an investigation, you should also search for portions of the keyword, including utilizing GREP search expressions for fragments of the keyword.
- **Use initialized size** – This option tells EnCase to search only the initialized size of an entry as opposed to the logical or physical size. When a file is opened on the NTFS file system, if the initialized size is smaller than the logical size, the space after the initialized size is zeroed out. Searching the initialized size searches only data a user would see within a file.

Create a New Keyword/Search Expression

Click the **New** button on the button bar. The New Keyword dialog appears. Enter "Hawaii" as the new search expression. Include the **Unicode** option – select **OK**.



Search Expression: hawaii

Name:

Search Options

☑ ANSI Latin - 1
□ UTF8
□ UTF7
☑ Unicode
□ Unicode Big-endian
□ GREP
□ Case Sensitive
□ Whole Word

GREP Symbols

\wFFFF	Unicode character
\xFF	Hex character
.	Any character
#	Any number [0-9]
?	Repeat zero or one time
+	Repeat at least once
[A-Z]	A through Z
*	Repeat zero+ times
[XYZ]	Either X, Y, or Z
[^XYZ]	Neither X nor Y nor Z
\[	Literal character
(ab)	Group ab together for ?, +, *, |
{m,n}	Repeat m to n times
a|b	Either a or b

Unicode View

[0048 0068][0041 0061][0057 0077][0041 0061][0049 0069][0049 0069]

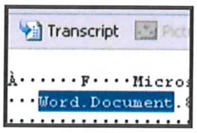
Figure 10-27 New Keyword dialog

The options that may be set differently for each search expression are:

- **Search Expression** – Enter your search expression in this box. It may be a simple keyword, phrase, or a GREP expression.
- 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.
- **Name** – Although not required, you may enter a descriptive name that will help you remember what the search expression will search for. This is very useful with GREP search expressions and foreign language searches.
- **Case Sensitive** – EnCase will locate the keyword regardless of the individual characters' case unless this box is checked. If checked, EnCase will only locate the keyword if the case sensitivity is the same as the search expression entered.
- **GREP** – The GREP option must be selected when utilizing GREP search characters. GREP is used to narrow the search, limit false-positive search hits, and in those cases where only certain portions of the keyword being sought are known.

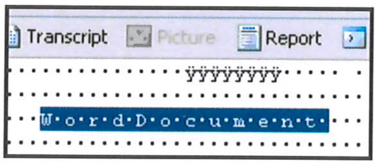
- **ANSI Latin -1** – This default option will search for characters contained within the ANSI Latin-1 code page, which is the default code page for the Microsoft Windows operating system. In earlier versions of EnCase, this option was called "Active Code Page." Since the active code page varied according to the active code page enabled on your computer, this option was replaced by ANSI Latin-1 to ensure consistent results.

- **Unicode** – Unicode was developed in direct response to foreign language character sets. Most MS Office products use Unicode as does Windows 2000, XP, Vista, and 7. Enabling both ANSI Latin-1 and Unicode options will locate both ASCII and Unicode characters. However selecting the Unicode option alone (without the ANSI Latin-1 option or appropriate code page selected) will find data stored in Unicode only. For more details on Unicode, please see http://www.unicode.org.



```
À······F····Micro
···Word.Document.
·················
```

Figure 10-28 Example of plain text



```
··············ÿÿÿÿÿÿÿÿ·····  ·
······························
···W·o·r·d·D·o·c·u·m·e·n·t····
······························
```

Figure 10-29 Example of Unicode

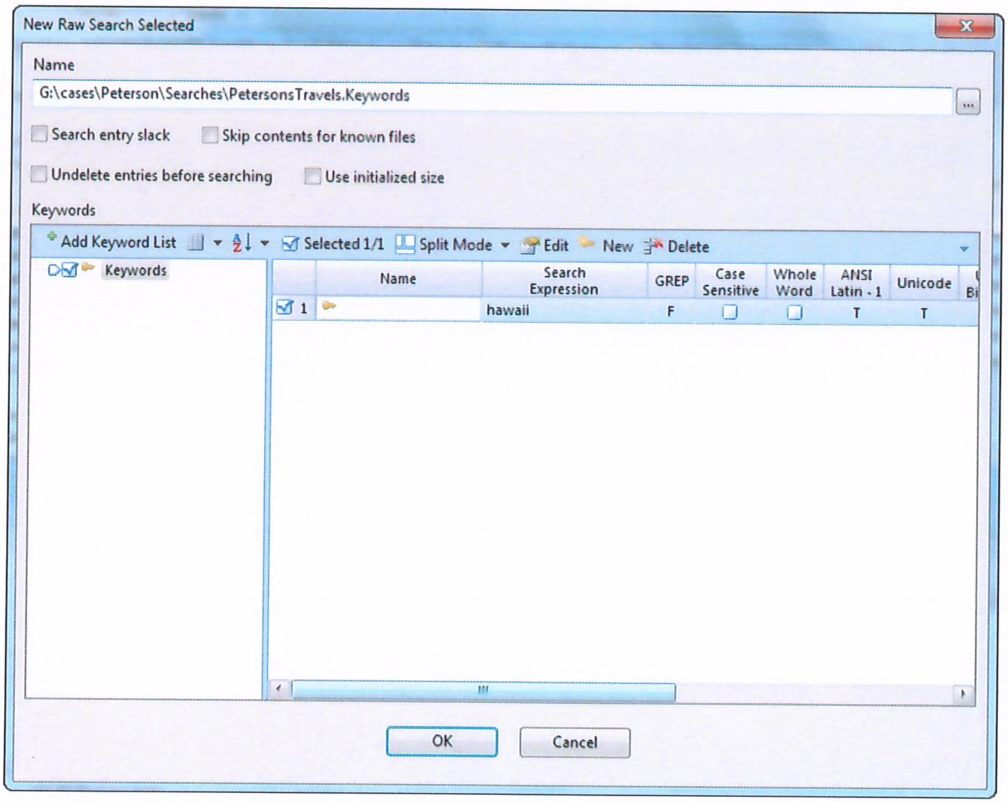
- **Unicode Big-Endian** – Non-Intel based data formatting scheme that stores multiple-byte numerical values with the most significant byte values first, which is the reverse of little Endian.

- **UTF-8** – UTF stands for Universal Character Set Transformation Format. Applications have several options for how they encode Unicode. The most common encoding is UTF-8, which is the 8-bit form of Unicode. This option offers foreign language support.

- **UTF-7** – UTF-7 is a special format that encodes Unicode characters within US-ASCII in a way that all mail systems can accommodate.

- **Whole Word** – EnCase will locate the keyword as a whole word not within a larger word (i.e., Chris not Christopher)

In this example, the only options selected are **Ansi Latin-I** and **Unicode**.



New Raw Search Selected

Name

G:\cases\Peterson\Searches\PetersonsTravels.Keywords

□ Search entry slack □ Skip contents for known files

□ Undelete entries before searching □ Use initialized size

Keywords

	Name	Search Expression	GREP	Case Sensitive	Whole Word	ANSI Latin - 1	Unicode	Bi
☑ 1		hawaii	F	□	□	T	T	

Figure 10-30 Completed entry of single keyword

This is the only raw keyword we will enter in this example, but additional search expressions may be entered if desired. To add a list of keywords, as opposed to adding one keyword at a time, select **Add Keyword List**. Keyword lists can be entered from the keyboard or pasted from a text document with one search expression and a line return per line. Options can be selected for all keywords and modified later if needed.

When all keywords are entered, blue-check the keywords to be run at this time and select **OK**. The search will initiate. A raw keyword search is much slower than an index search. Raw searches do not make use of the indexed data. The results will ***automatically*** appear within the Results tab. Viewing the search results will be discussed in a subsequent lesson.

Case and Evidence Keywords

Index and raw search terms may be saved within any folder desired by the examiner. Index search terms and options are stored within a file with the extension .EnSearch; raw search terms and options are stored within a file with the extension .Keywords. Searches may be recalled and run at any time, within any case, on any drives/evidence files. Keywords may be shared between examiners by simply sharing the created file. Keyword Search results are stored within the case folder structure and may be found within EnCase within the Results tab.