|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 3 |
| Practical 4 |
| **File Signature Analysis & Searching Unallocated Space** | |

**OBJECTIVES**

To be able to perform:

1. Signature analysis on files.
2. Searching of a known file type in unallocated disk space.

**Part A: Signature Analysis**

A more comprehensive data analyzing method called file Signature Analysis is needed to support the process of digital forensics.

Perform research online to answer Q1 and Q2:

Q1: Explain what is a File Signature. Determine the signature for .GIF file (in hex).

There are thousands of file types, some of which have been standardized. When file types are standardized, a signature – or header – is recognized by the program the file belongs to. For example if one were to see a .DOC extension, it is expected that a program like Microsoft word would openm this file.

File signature for .GIF is 0x47 49 46 38

Q2: What is the purpose of performing signature analysis on files?

Many program’s rely specifically on the file extension to reflect their proper data type. Users may change the file extensions to hide the true nature of the files. By running signature analysis, we would be able to properly identify and classify files on a subject/s hard drive and to discover renames files.

By running the file signature analysis process, EnCase compares the file’s signatures with the extension of the file, and then compares both with a file signature table to determine if the file extension has been changed.

To better understanding on how this signature analysis process functions, open Laura’s case and look at the File Signature table. Click on **View 🡪 File Types** as shown in Figure A-1.

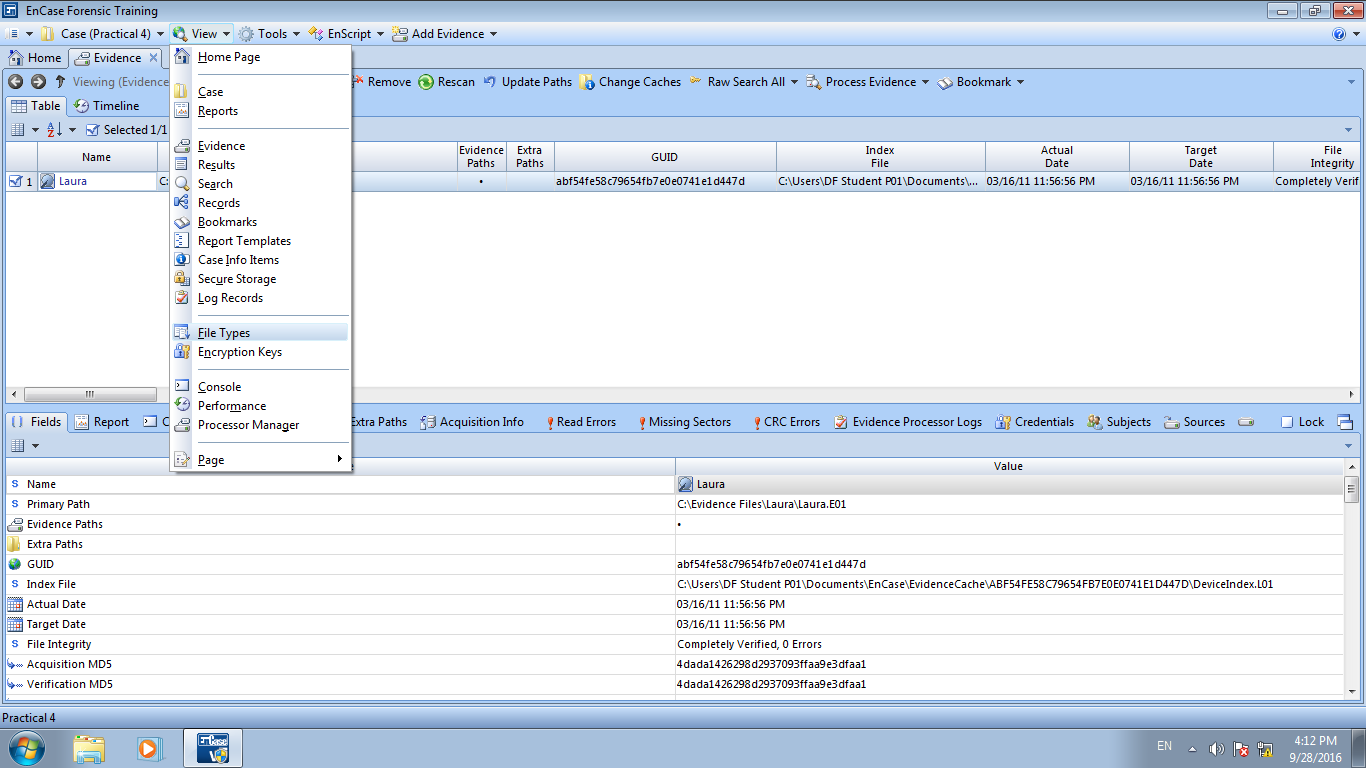


Figure A-1: Changing to the File Types view

The File Types Table view will open and display file types and file signatures. We can rearrange the columns so that the Header Signature column is next to the Name column. To move a column, left click and hold on the column description area and move the column to where you want to be placed. Drop it by releasing the left mouse button. Sort the **Name** column by double clicking on the header.

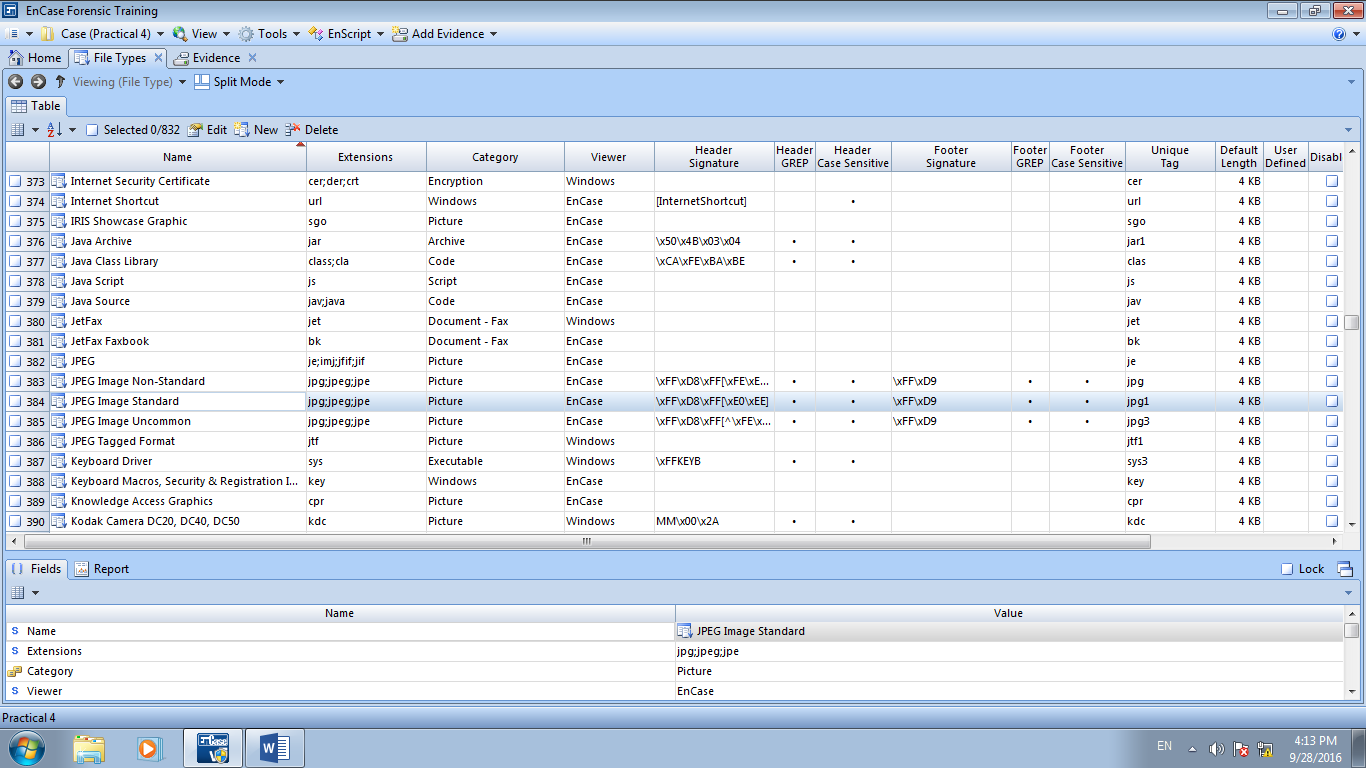


Figure A-2: File Types Table

It is important to understand that EnCase uses these search expressions in the Header Signature column to identify the headers within files and compares these headers with the extensions to identify files that may need further attention.

**Starting an Analysis**

To perform a signature analysis on selected objects within a case, **blue check** the desired objects (**D drive from Laura’s hard disk**), **Right click** (within either the left or right pane) and select **Entries 🡪 Hash\Sig Selected…** The **Evidence 🡪 Viewing (Evidence)** view must be accessed at the end of the operation to refresh the appropriate column.

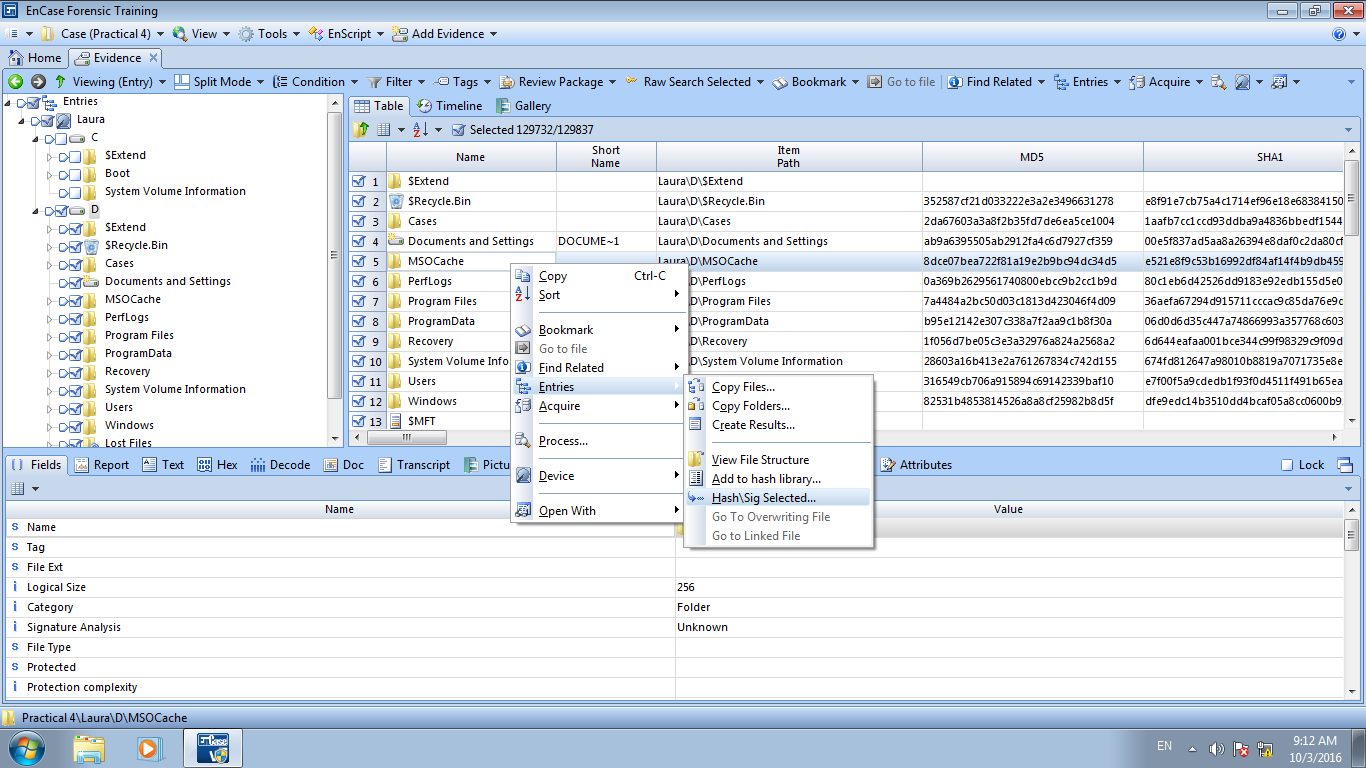


Figure A-3: Running signature analysis on selected items

Select the following options if the following screen appears:

Check **MD5**

Check **SHA1**

Check **Verify file signatures**

Click **OK**

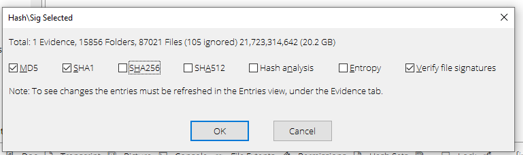


Figure A-4: Hash\Sig options

**Viewing the Results**

Within the Laura’s case from the **Evidence**, Viewing (**Evidence**) **View**, double click the evidence file to view, or select the **Open** button from the button bar.

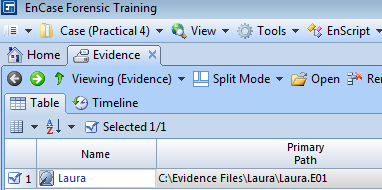


Figure A-5: Blue check evidence file, select “Open”

This should display the objects within the evidence file. Remove any blue checks and green, Set Include functions if necessary. To view the results of the signature analysis, display all files in the case. In the Evidence Tab, Viewing (Entry) view, click on the green **Set Include** on **Entries** in the tree pane.

In the Table Pane, scroll to the right and located the File Type and the Signature Analysis columns. Left click and hold the mouse on the **File Type** column then drag the mouse to the left of the Table Pane. Drop the File Type column next to the **Name** column by releasing the mouse button. Do the same thing with the **Signature Analysis** column until they are arranged as shown below.

Now that the columns are aligned, start examining the file signatures. Sort the columns in the Table Pane in the following order:

* First level: **Signature Analysis**
* Second level: **File Type**
* Third level: **Name**

The red triangles within each column heading should appear as that displayed in Figure A-6.

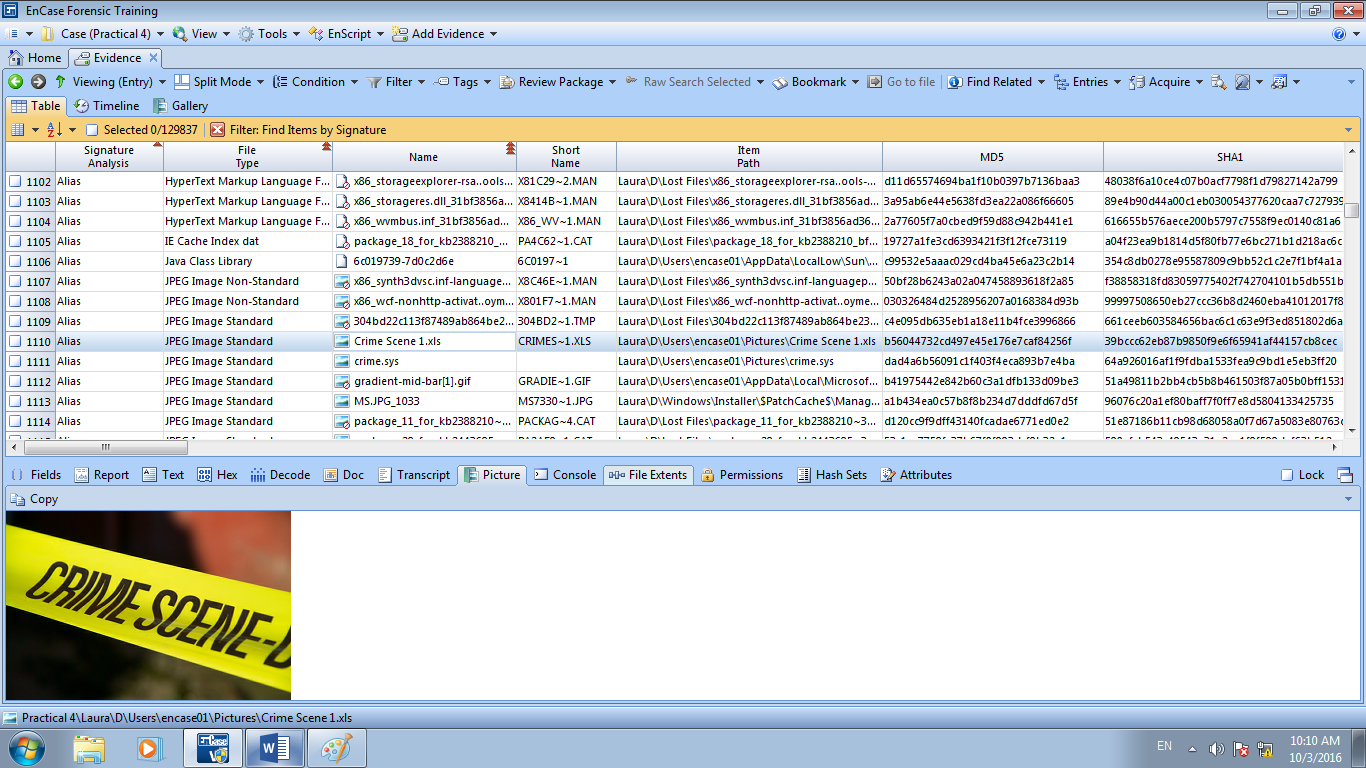


Figure A-6: Organize and sort the columns for analysis of results

NOTE: Shift-double-click to enable secondary sorts.

After Signature Analysis, the columns will display the results of the analysis:

1. \*[Alias]

The header is in the File Signature table and the extension does not relate to the header. This usually indicates a file with a renamed extension. The [Alias] represents the data in the Name column for that header in the File Signature table.

1. !Bad Signature

The extension is in the File Signature table, but the header does not relate to the extension, and the header is not in the File Signature table.

1. Match

The header matches the extension.

1. Unknown

Neither the header nor the extension is in the File Signature table.

Q3: Which of the above signature analysis results would the examiners be most interested to examine further? Explain why.

The examiners may often want to focus on those with a signature analysis result of Alias, as this usually indicates a file with a renamed extension.

This would indicate that the file extension has been changed and the files are likely been changed to hide its true intension.

The file, **D:\Users\encase01\Pictures\Crime Scene 1.xls** below is displayed as a picture as a result of the Signature Analysis.

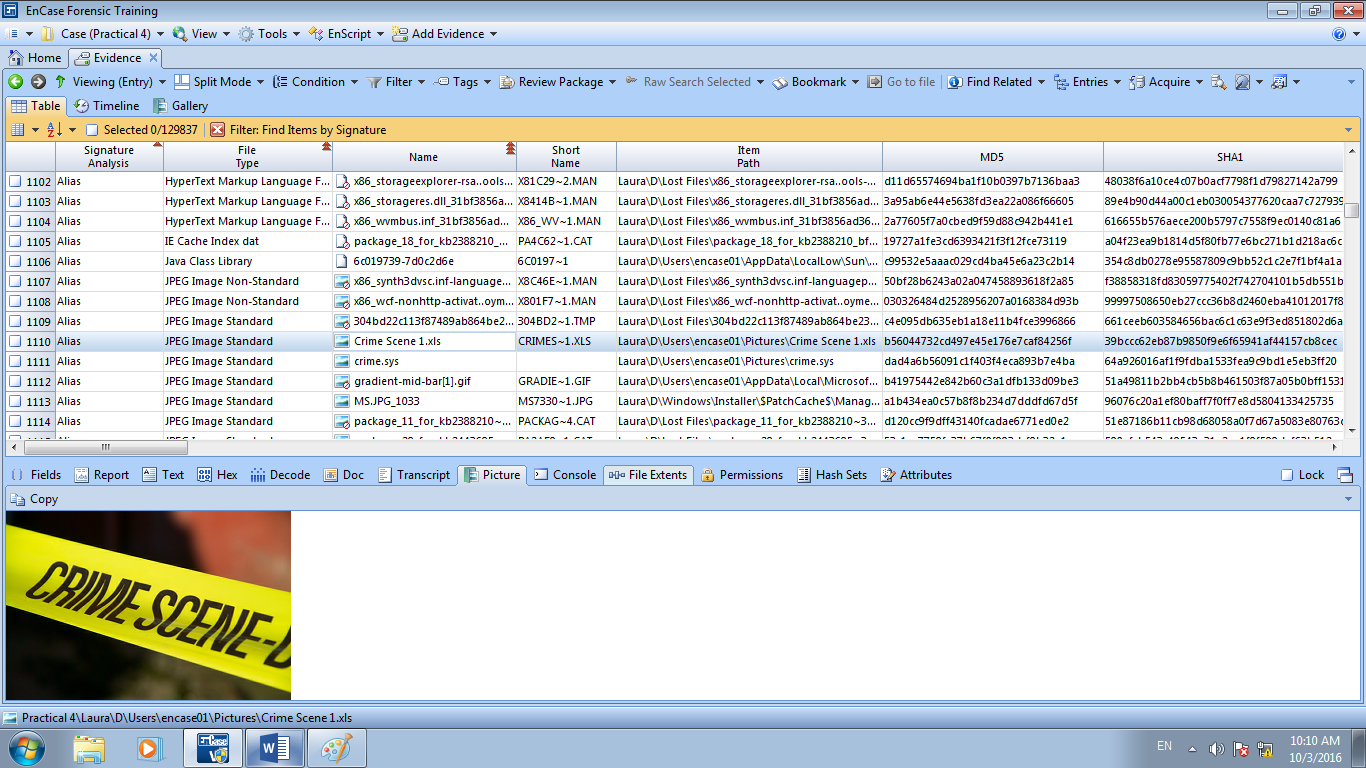


Figure A-7: Renamed JPG file displayed as an image

**Part B: Searching Unallocated Space (may take up to 30-40 min)**

After files are deleted, application programs and normal processes of most operating systems will overwrite their directory entries. In many cases the data is left on the disk with no indication that it is there. Searching the unallocated space for known file headers is one way of identifying such data.

This section illustrates the technique of searching for a JPEG header to locate JPEGs in unallocated space. It is important to note that not all files are recoverable, unless the entire file is obtained.

Q4: What situation may cause a file to be unrecoverable?

When a file is deleted and emptied from the recycle bin, the cluster it used will become unallocated and new files may overwrite these unallocated clusters.

If some of the clusters are overwritten with new files, we would not be able to recover the whole file.

In **Evidence 🡪 Viewing (Evidence)** view, highlight the volume whose unallocated space is to be searched. Highlight the **D** volume of Laura’s case. In the Table Pane, sort by **Name** column, scroll; down to locate the **Unallocated Clusters** entry and **blue-check** it. **Right click** and go to **Process**

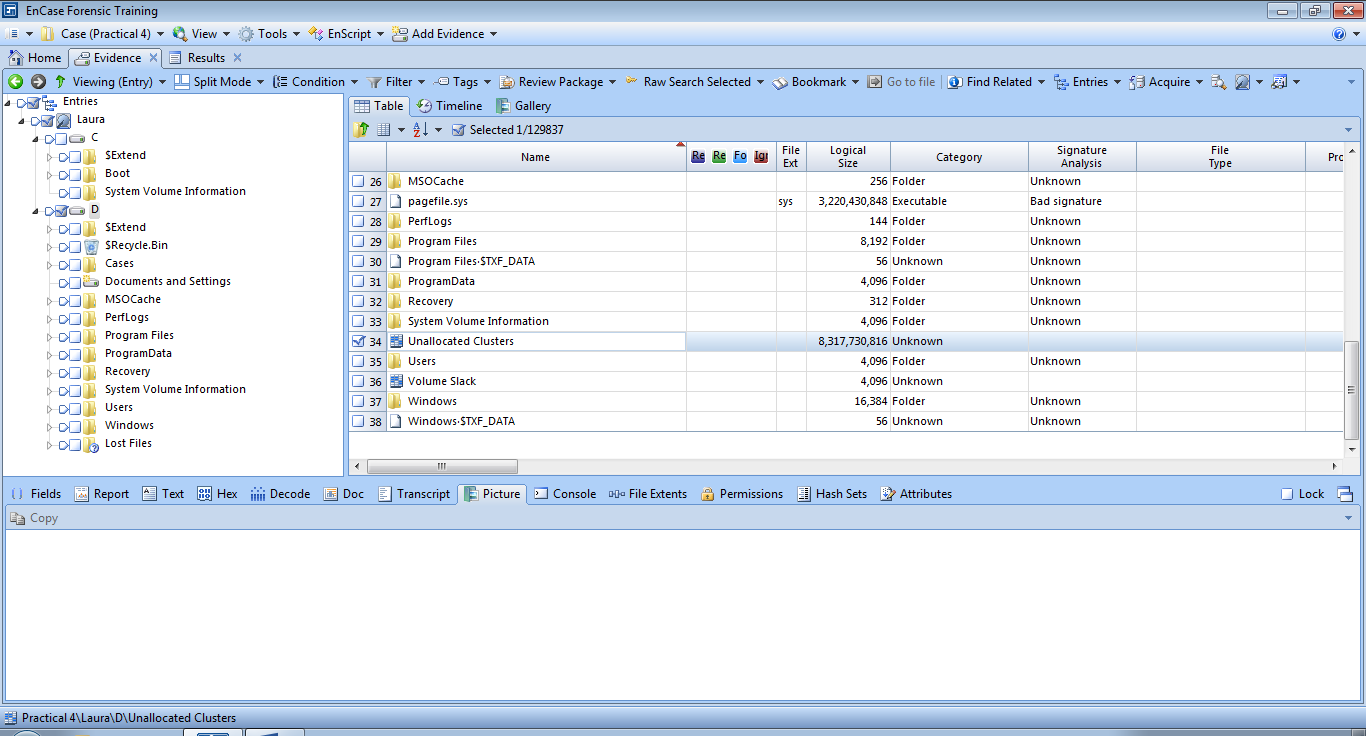


Figure B-1: Select unallocated space to be searched

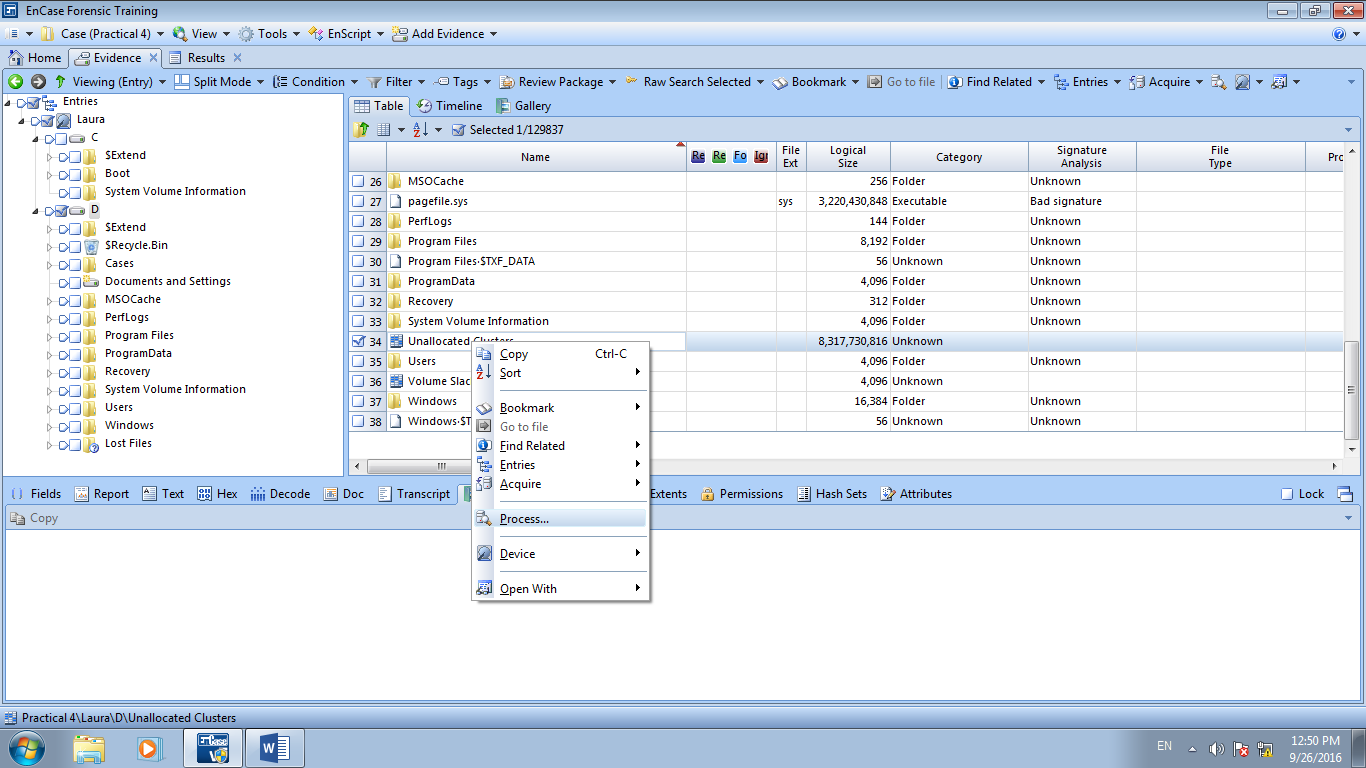


Figure B-2: Start process to search unallocated space on D drive

Enable **Search for Keywords,** Click **search for keywords** as shown in Figure B-3.

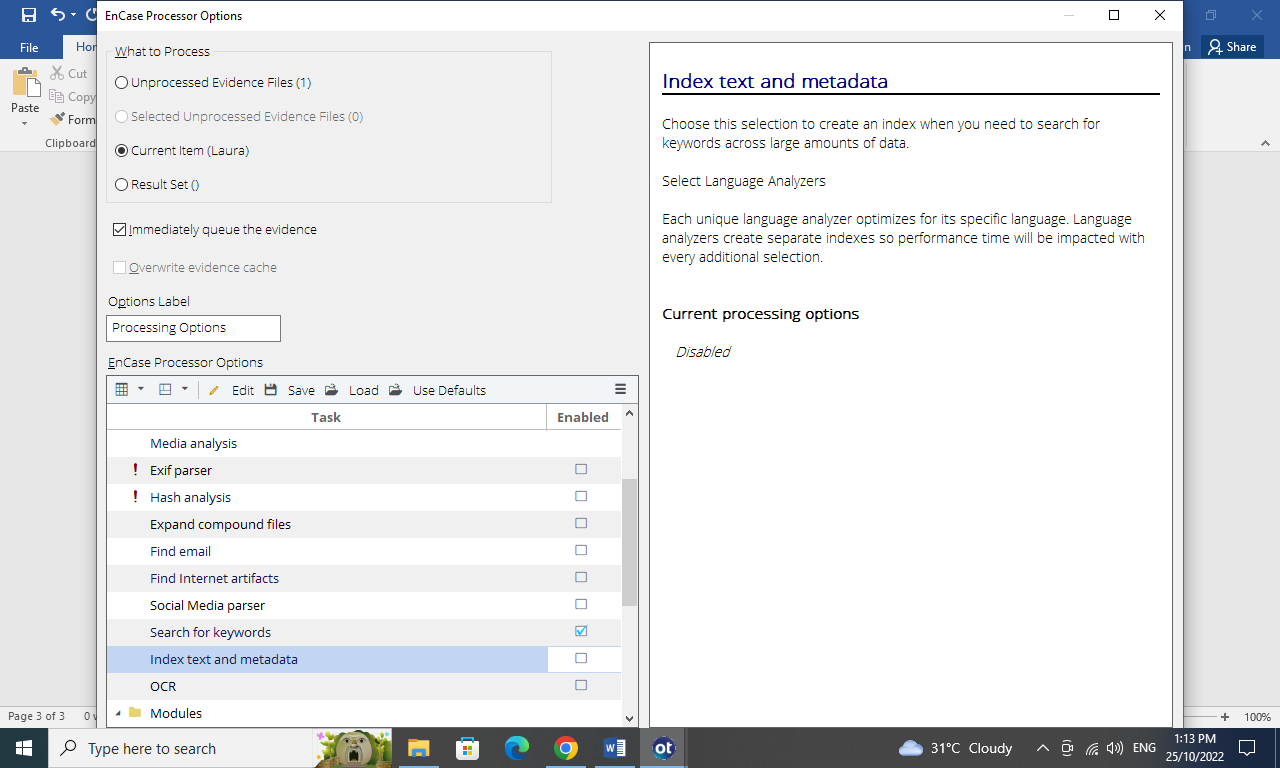


Figure B-3: Search for keyword

Click **New** to create new keyword as shown in Figure B-4

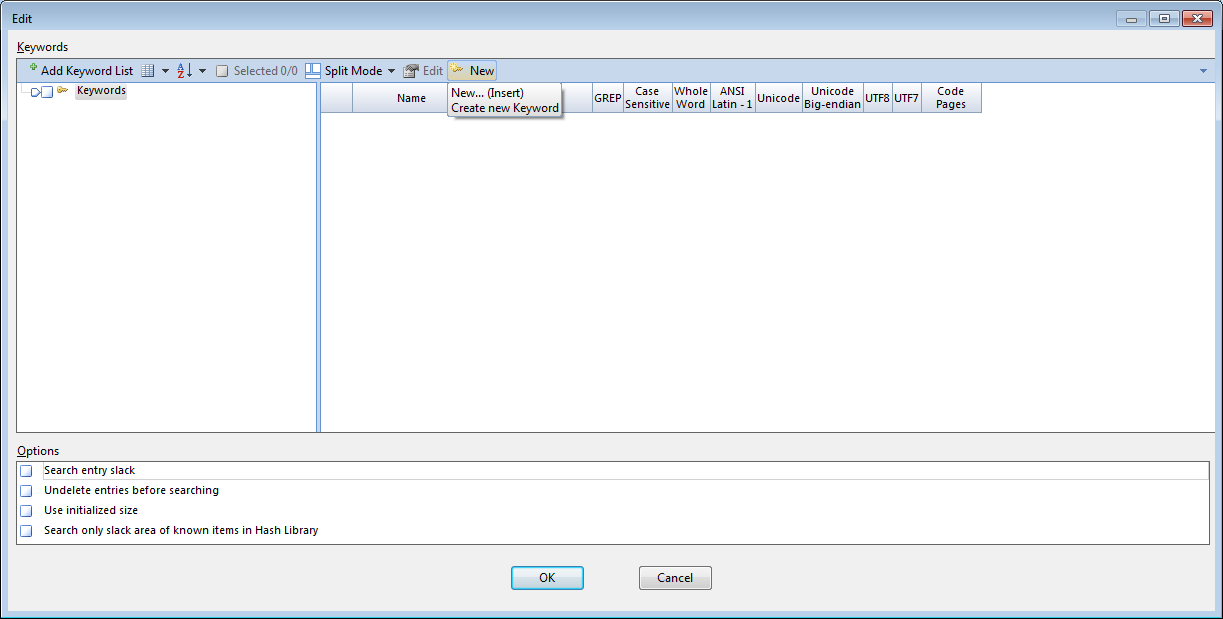


Figure B-4: Create new keyword

Go to view File Types view to locate JPEG Image Standard, right click **Edit**. Go to **Header tab** and right click **Copy.** Copy the search expression of JPEG Image Standard and paste it to the Search Expression field into the new keyword.

Choose the **Set Include Option** at the top of the tree in the Tree Pane, sort by the **Name** column in the Table Pane, and scroll down to the **JPEG Image Standard** entry. Right-click on the search expression column and select **copy**.

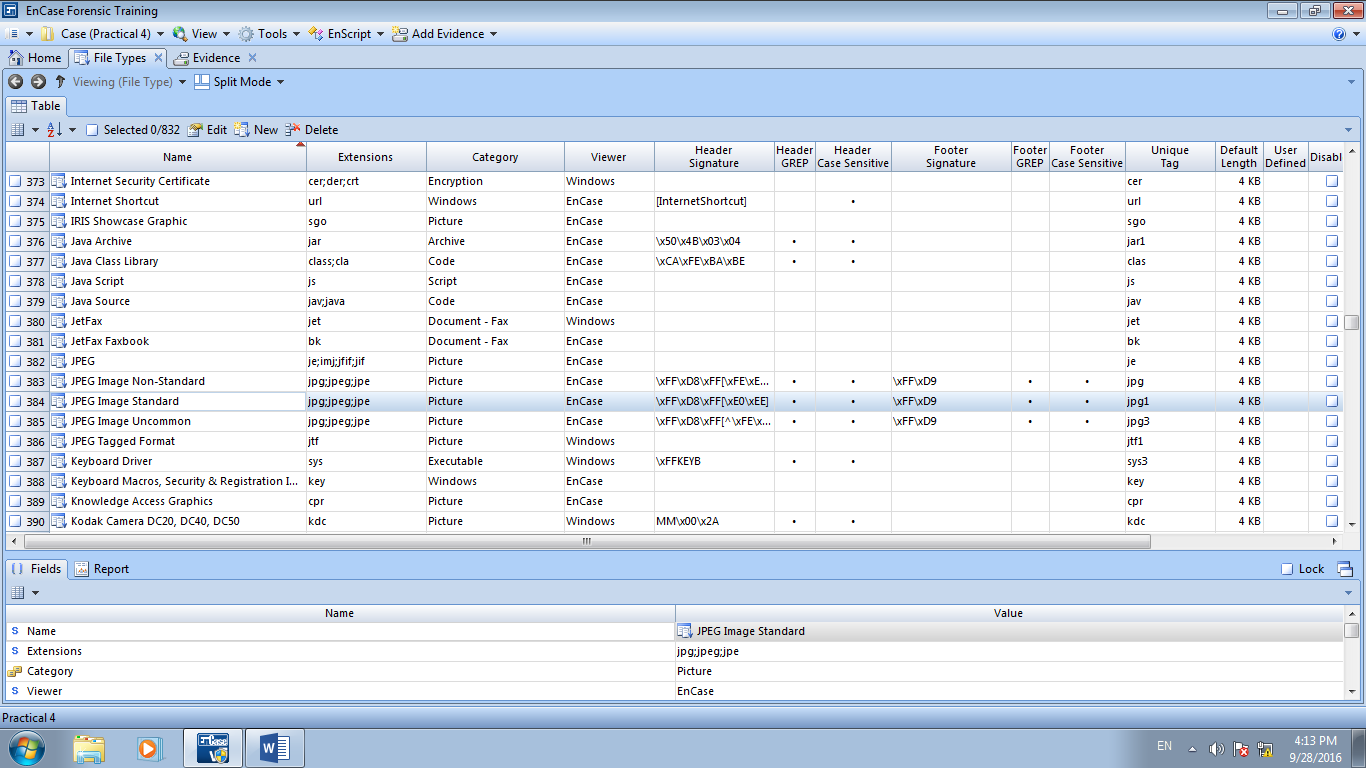


Figure B-5: JPEG Image Standard search expression

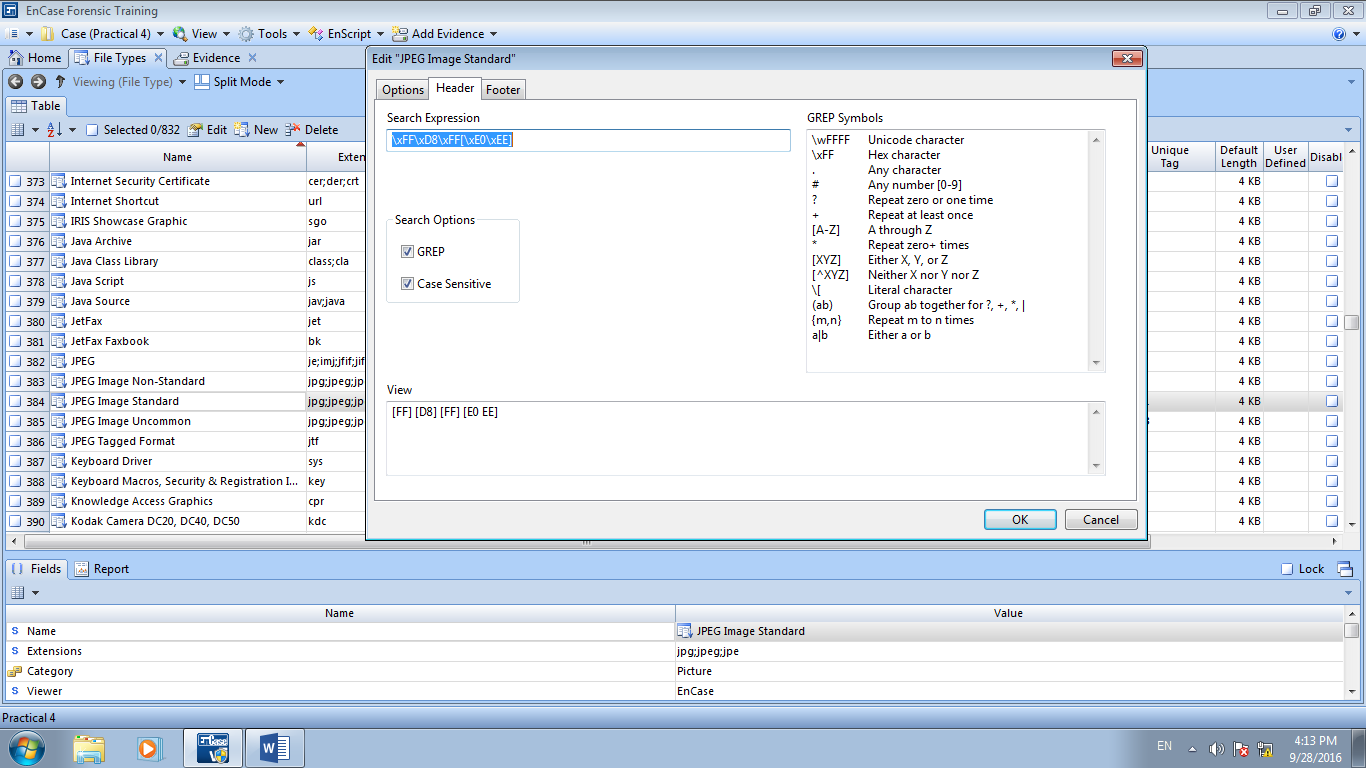


Figure B-6: Edit JPEG Image Standard

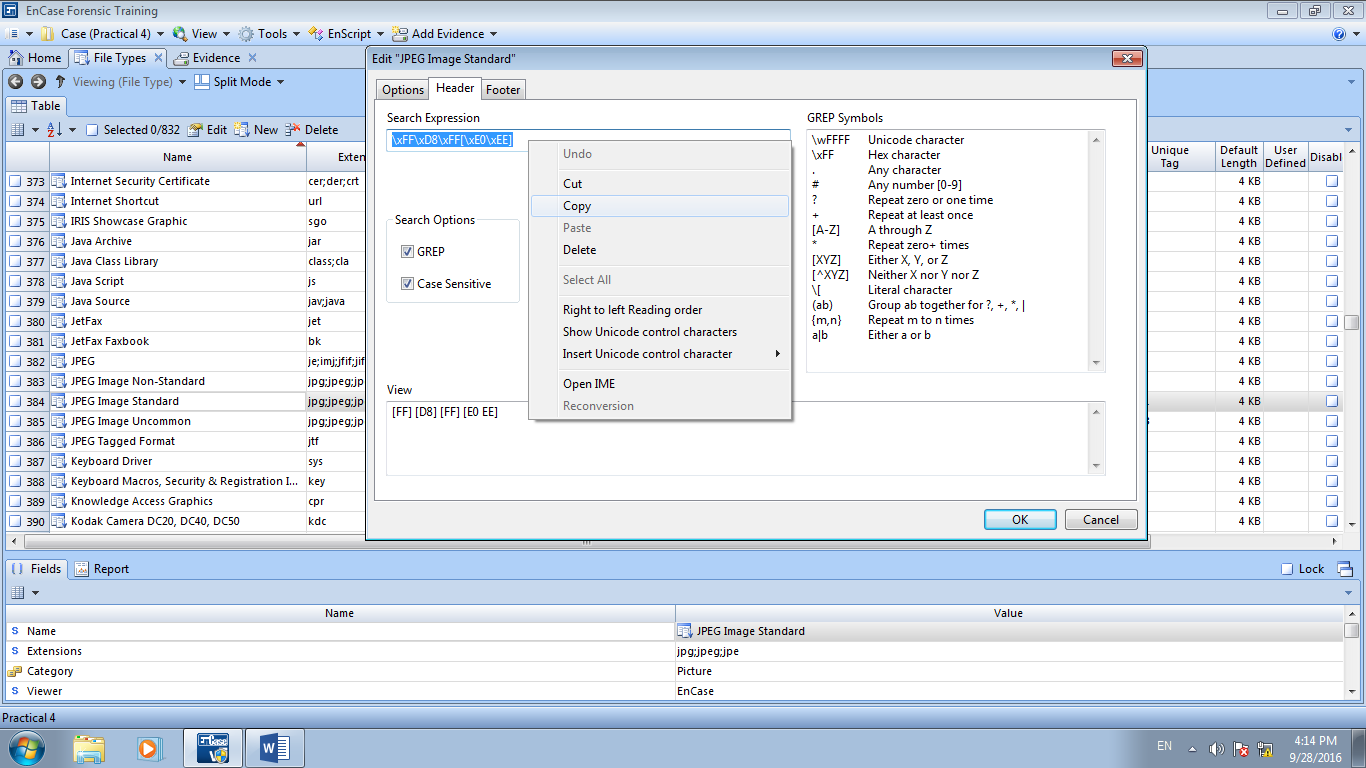


Figure B-7: Copy Search Expression from JPEG Image Standard

Select **Edit**, **right click** on the search expression of JPEG Image Standard and select **Copy**

Right-click in the **Search expression** field on New Keyword and select **Paste**. Make sure that **GREP** is selected. Type **JPEG** in the Name field to identify it for later use. Click **OK**.

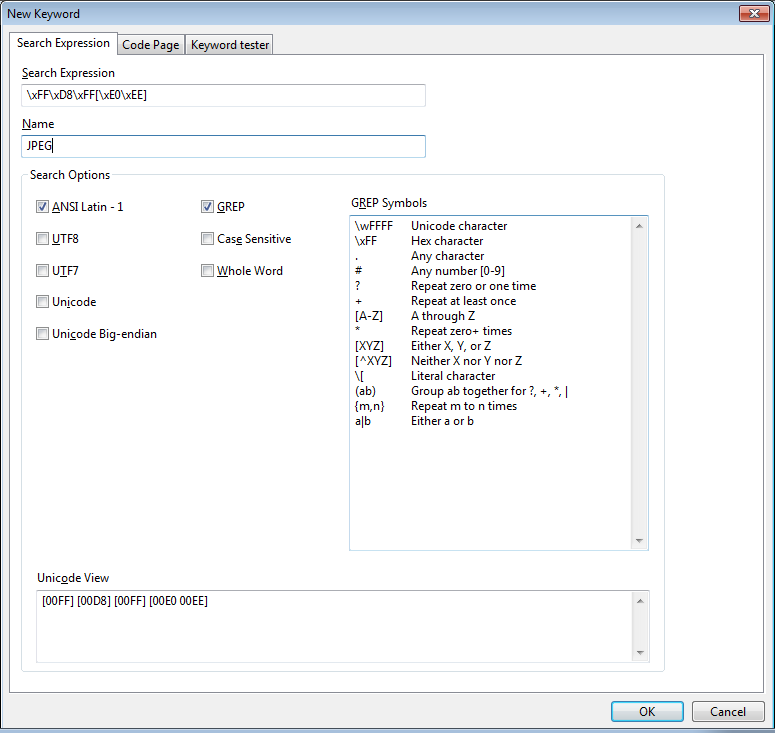


Figure B-9: Paste the JPG header in the Search expression field – click “**OK**”

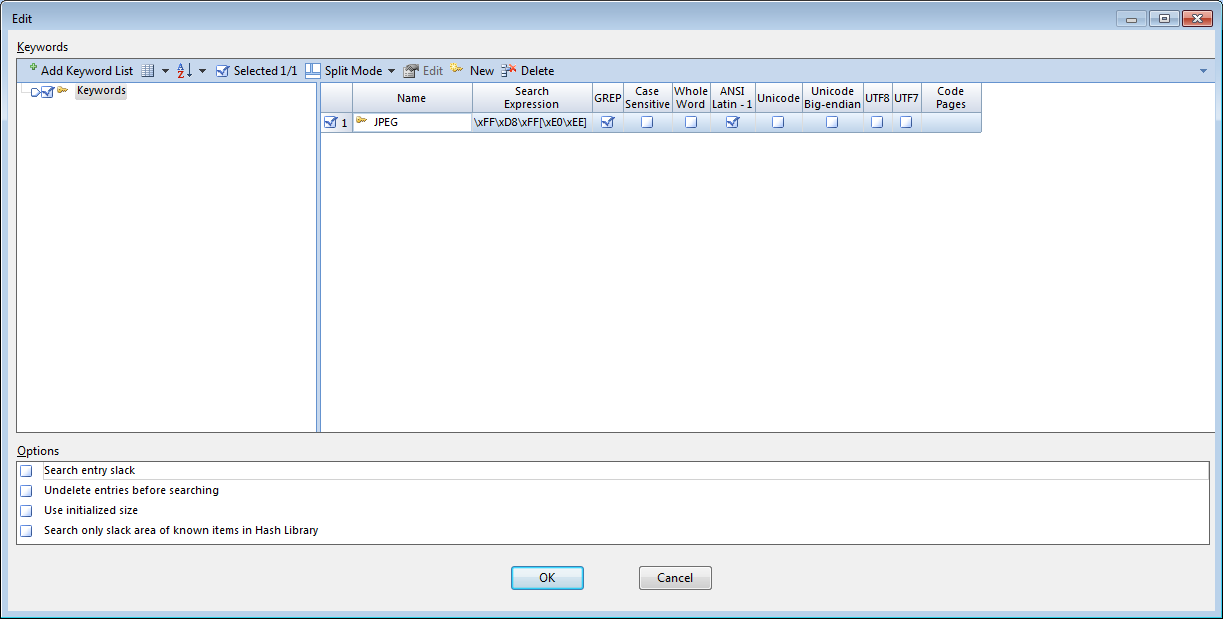


Figure B-10: New keyword JPEG with search expression created

Next, click **OK** to continue the search.

This process illustrates that evidence can be found in both allocated and unallocated space.

Review the hits by clicking **View** | **Keyword Hits** to determine the relevance to the investigation. Select the folder containing the search hits in the Tree Pane.

As this data is from unallocated space, not all the images will be intact. Some may have been overwritten with other data.

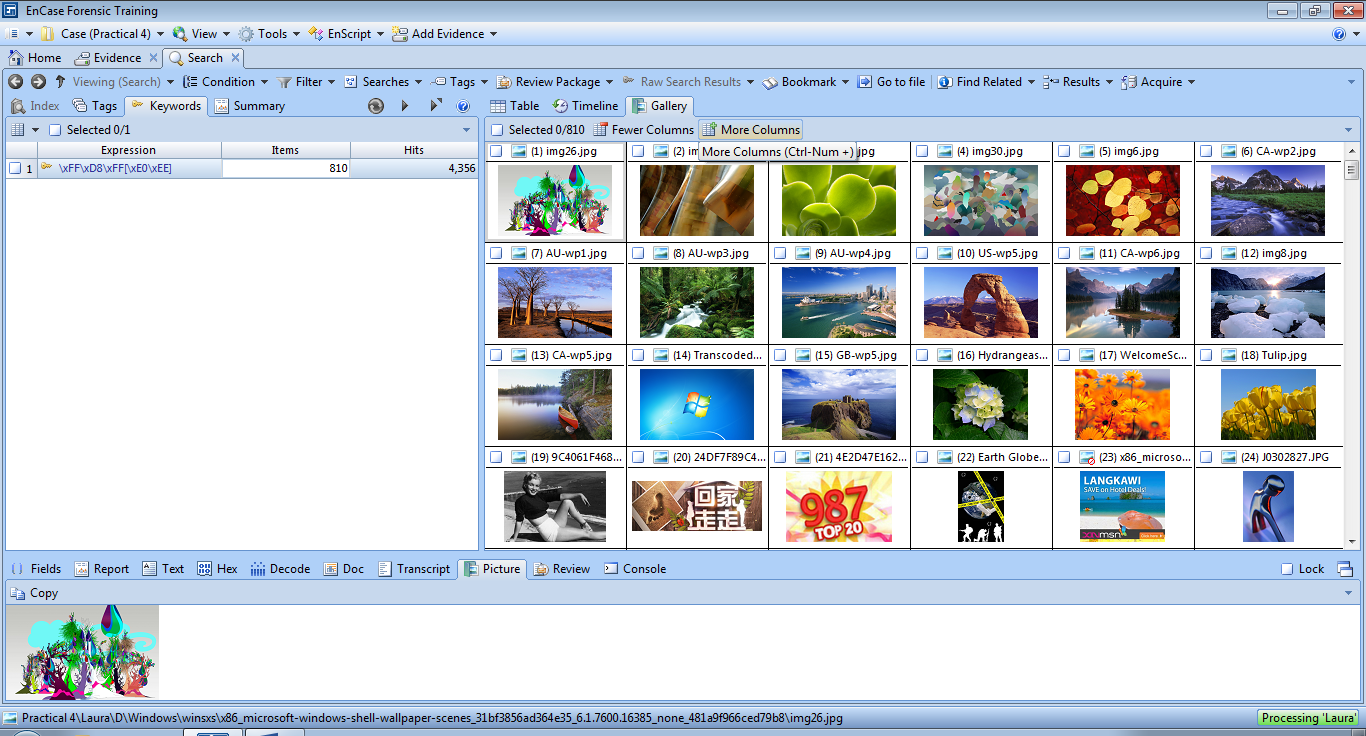


Figure B-12: Search hits in gallery view

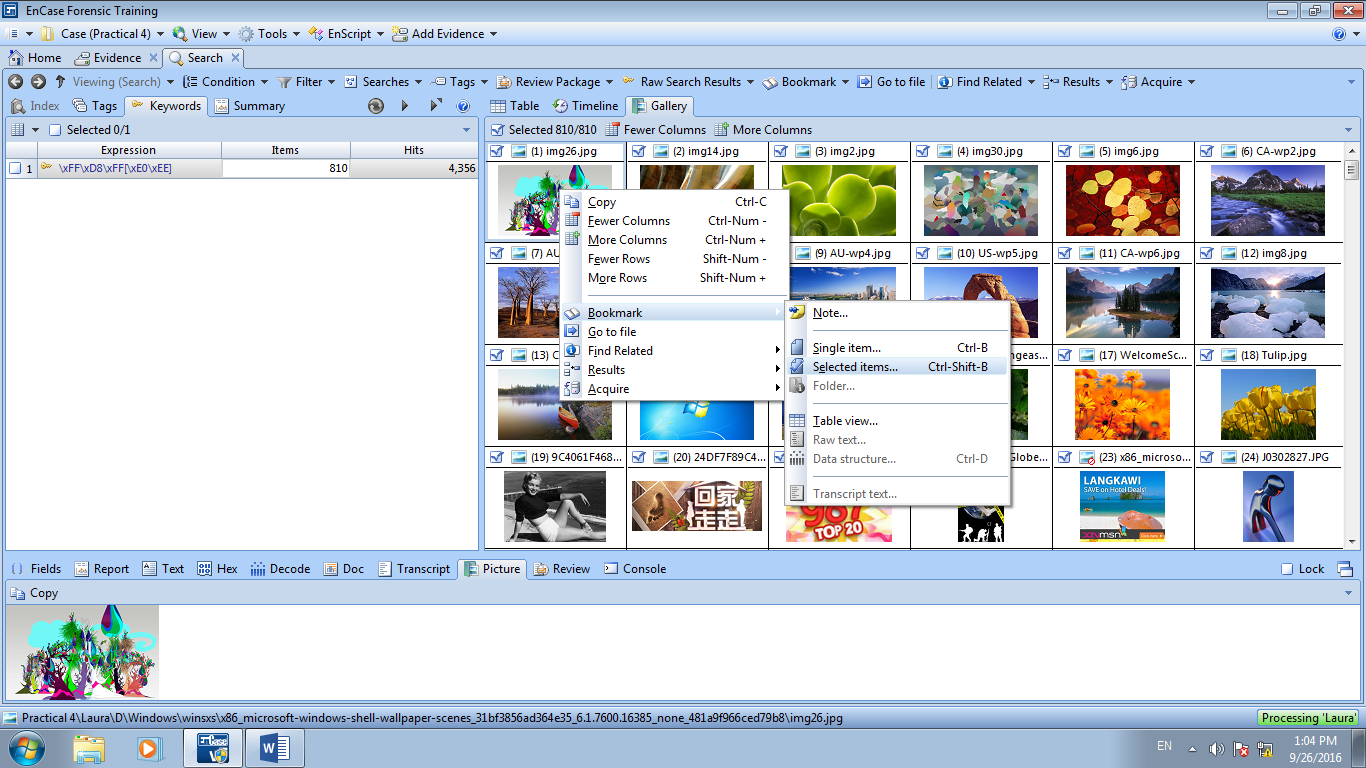


Figure B-13: Bookmarking selected items from search hits

To bookmark the pictures stored within unallocated space, select all search hits to be bookmarked, right-click and select **Bookmark Selected Items…**

Create a new bookmark folder to contain these images – name it as “**Images from unallocated space**”.

The bookmarked data in the selected folder will be displayed as an image within the Bookmark view as shown below.

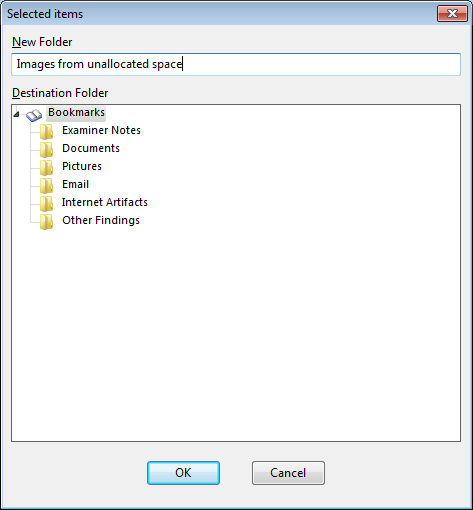


Figure B-14: New Folder in Bookmarks Folder

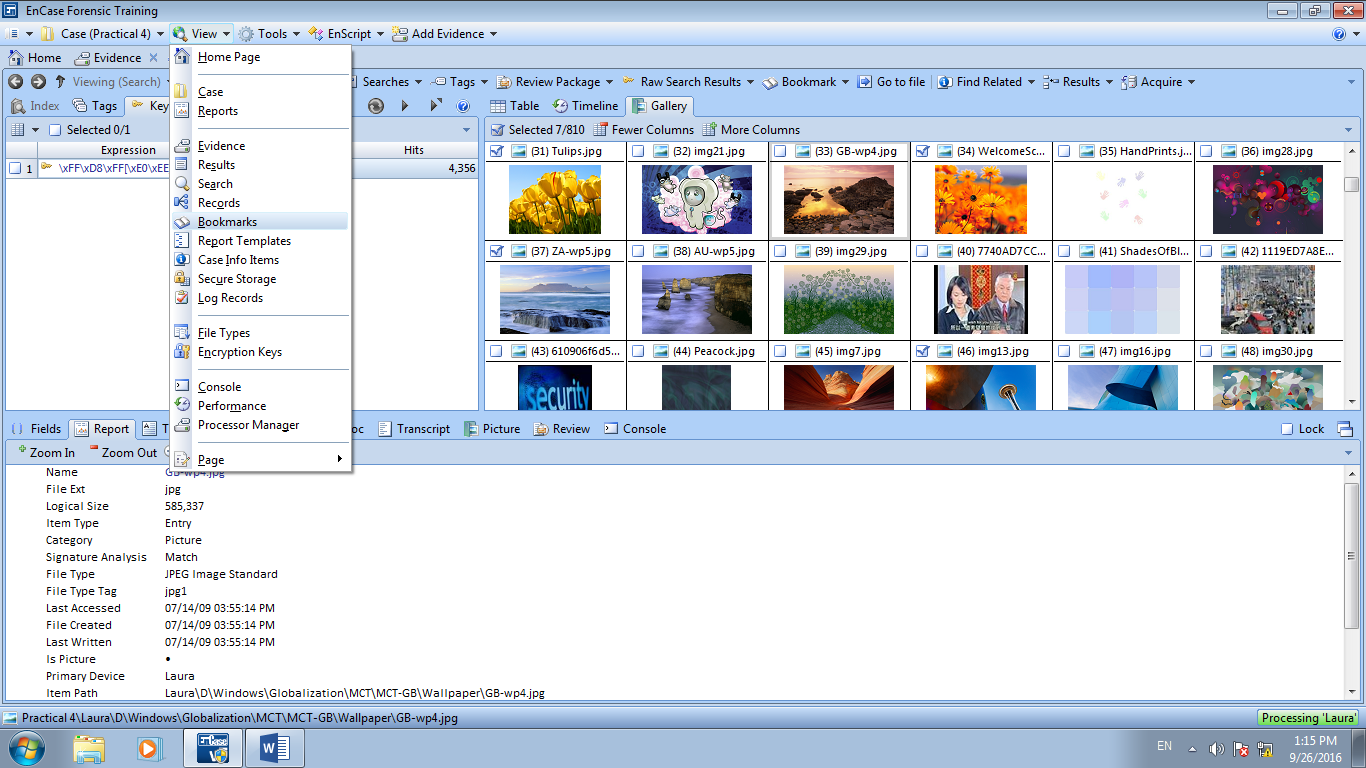


Figure B-15: Viewing Bookmarks

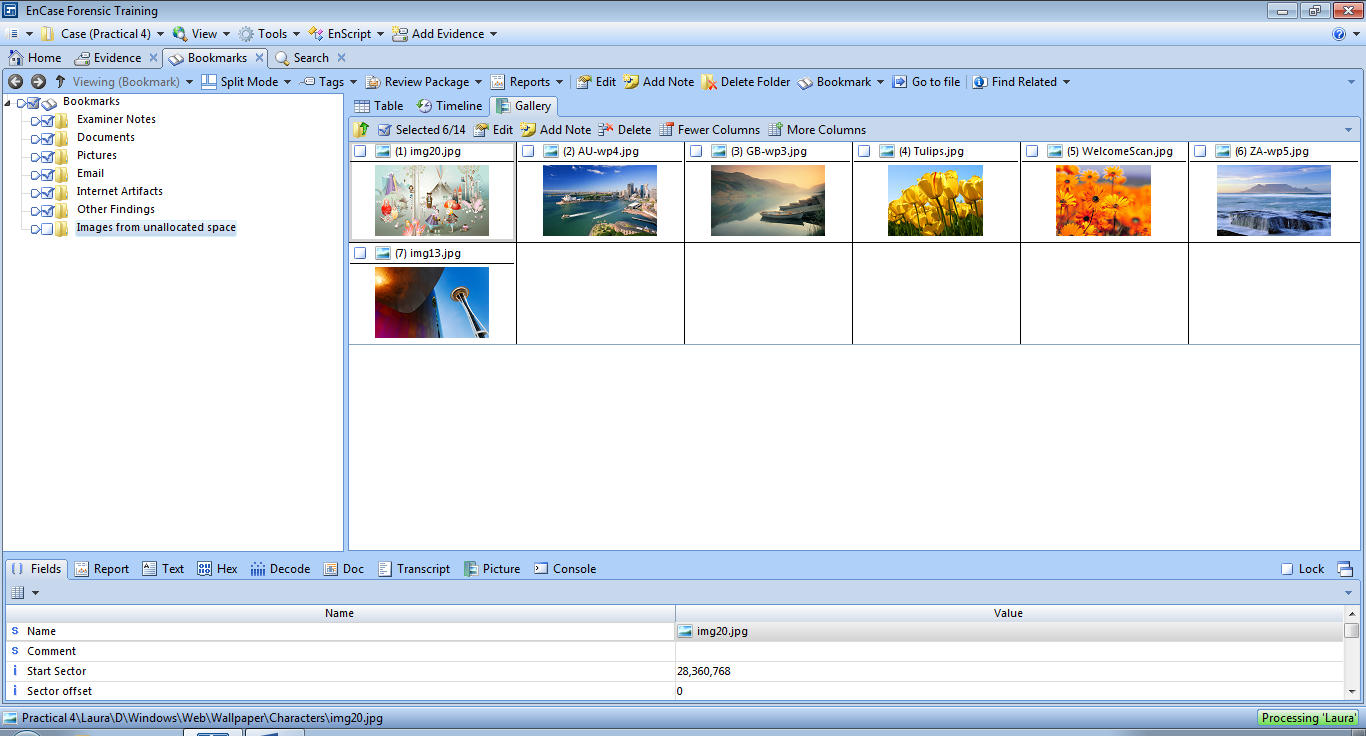


Figure B:16: Bookmarks View

Reflection: What have you learnt through this practical exercise?

Reference

* Guidance Software, Inc, *EnCaseComputer Forensics I* – v6.14psvi (12.03.2009).
* Guidance Software, Inc, *EnCaseComputer Forensics II* – v6.15psvi (02.11.2010).

- End -