|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2020/21) Semester 4/6 | Week 4 |
| Practical 5 |
| **Hashing** | |

**OBJECTIVES**

1. To build hash set and hash library in EnCase.
2. To perform hash analysis on evidence.

Hashing is a vital part of the proactive auditing capabilities inherent to the EnCase methodology. Hash sets and library can be built and shared among examiners.

The hash feature of EnCase allows the investigator to create a hash value, a *digital fingerprint*, for any file. The hash value for each file is unique. Only a copy of a particular file will yield the same hash value. EnCase uses MD5 algorithm to create hash values. By building a library of hash values, EnCase is used to check any evidence file for the presence of any file that has a hash value contained in the Hash Library.

Q1. Explain the difference between hash items, hash sets and hash library. What is the purpose of creating hash set or hash library?

**Part A: Creating Hash Library**

Let’s create a new hash library. You only need Encase Forensic (Encase) open in order to create a hash library. From any view, click **Tools 🡪 Manage Hash Library …**

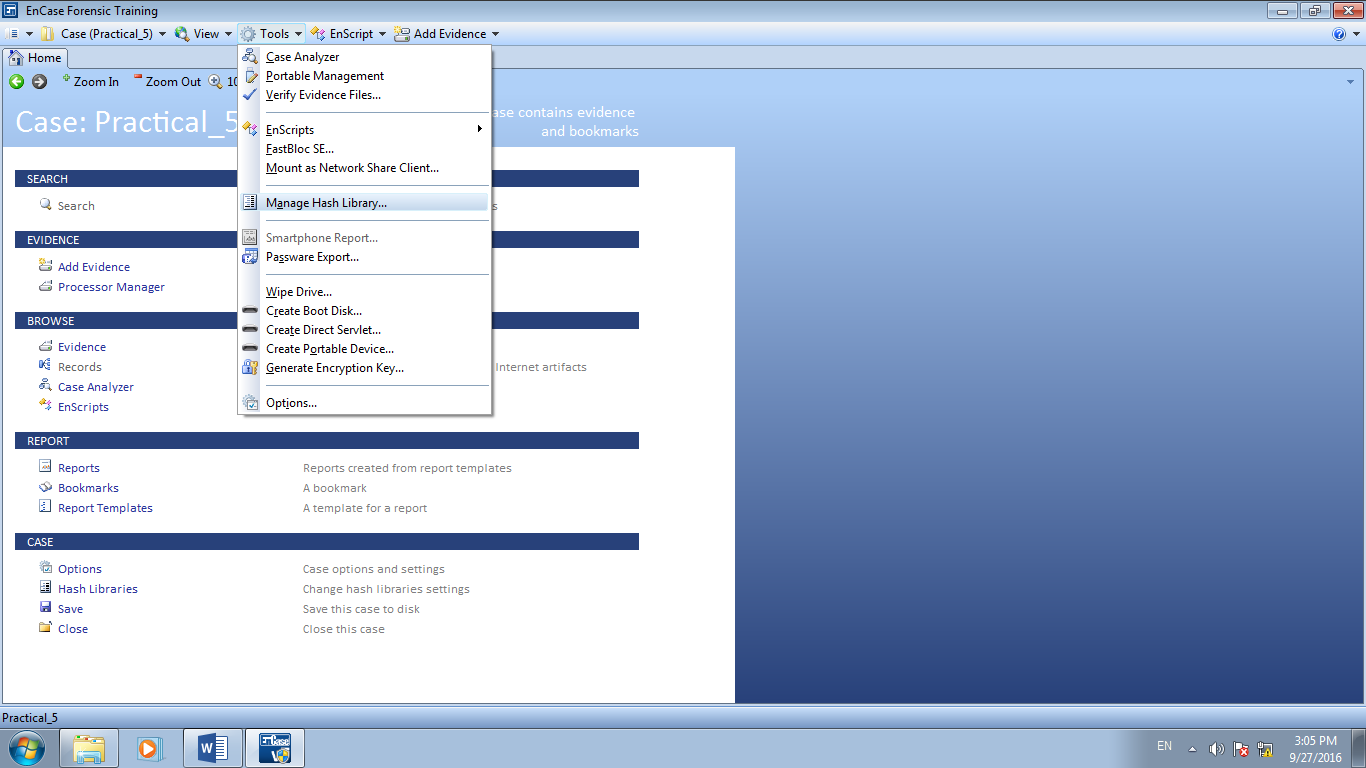


Figure A1: Managing Hash Library

If you receive the error shown in the following screenshot, it simply means that you had a hash library defined at one point and it has been moved or deleted. If you receive this error and you do not need the previous library, select **OK** to proceed. If you have not used hash libraries before, you will not get this error.

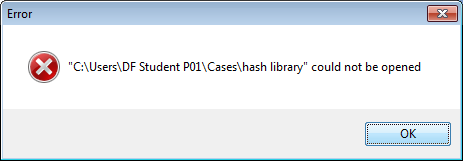


Figure A2: Error indicating a past hash library is no longer available

To designate a folder to contain your hash library, select **New** button.

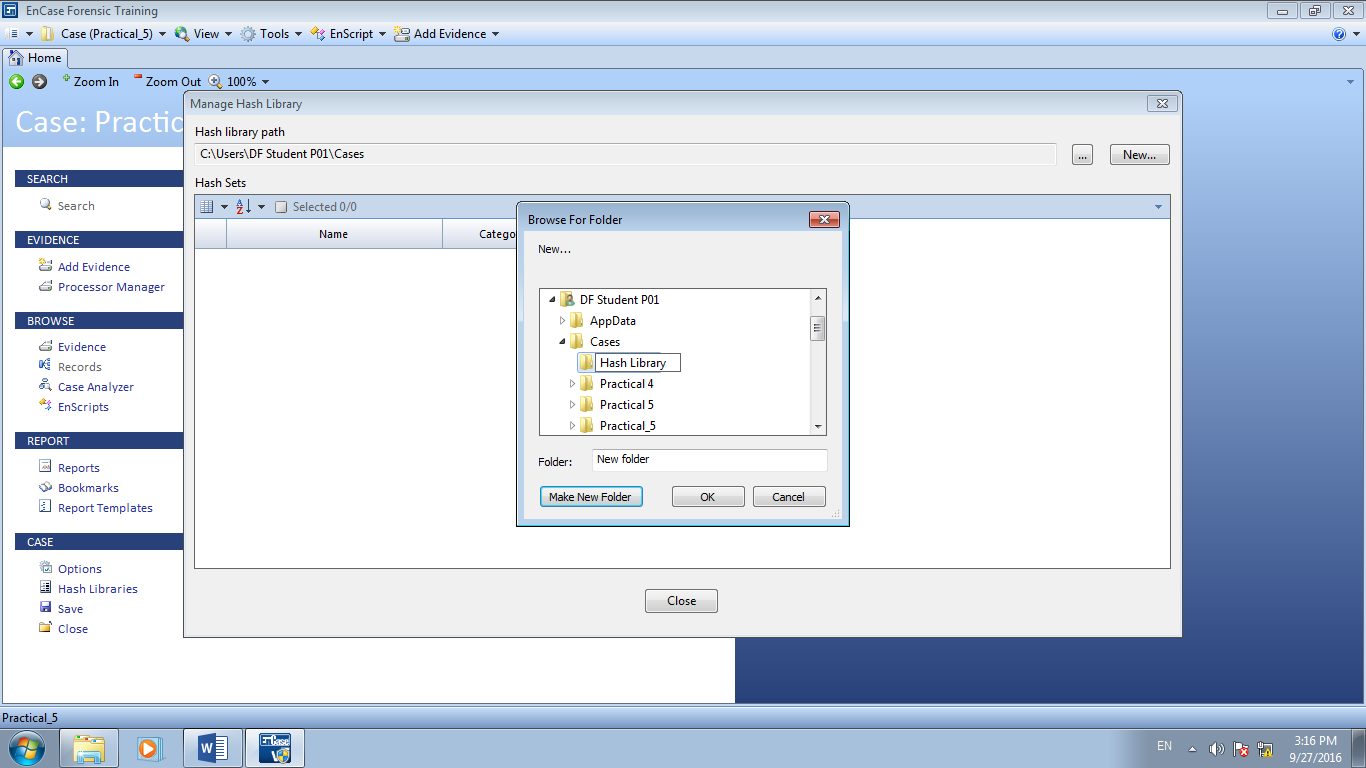


Figure A3: Designating folder to contain hash library

This will bring up a prompt to browse to a folder in order to select it to contain your hash library. This process will also create the foundation of your hash library by adding binary files to this designated folder.

If the folder does not exist yet, we will want to select the **Make New Folder** button. We want our hash library in an easily accessible place. Create the folder “Hash Library” in C:\Users\%UserName%\Cases folder as shown in Figure A3.

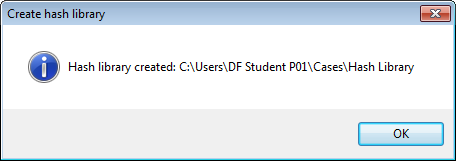


Figure A4: Successfully hash library creation

Select **OK** and the “Hash Library” folder will be created. You will be prompted about the successful creation of the library.

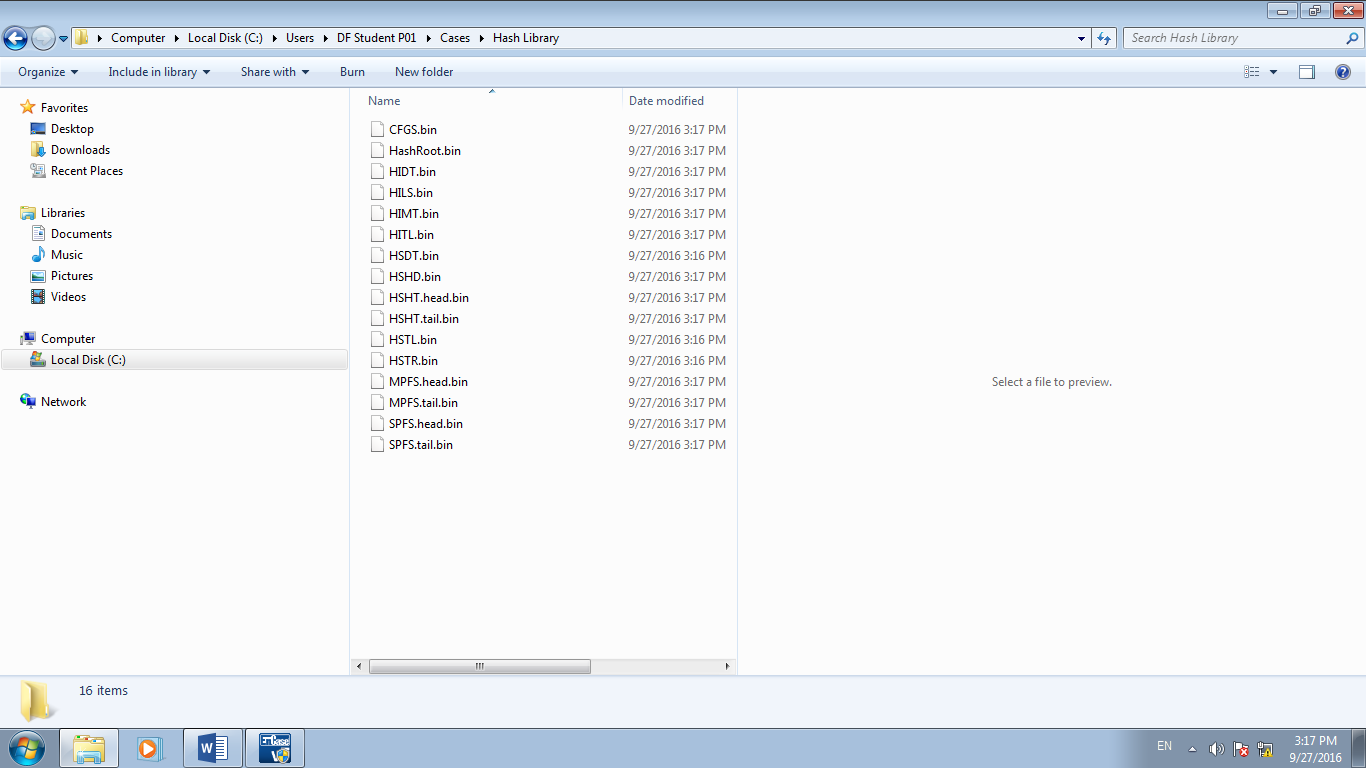


Figure A5: Hash library initial binary files

By navigating to the hash library folder that you have just created, we can look at its bare bone contents as shown in Figure A5.

**B: Creating Hash Sets through hash library management**

To hold hash values, we need hash sets. Hash sets are like containers that hold the hash values. The Encase hash analysis features allows us to create these hash sets now or later. If we know what the hash sets need to be named, it will save us time to create them now. We do not need to have a case open or any evidence loaded. Through hash library management, we can create them. Let’s create 1 hash set.

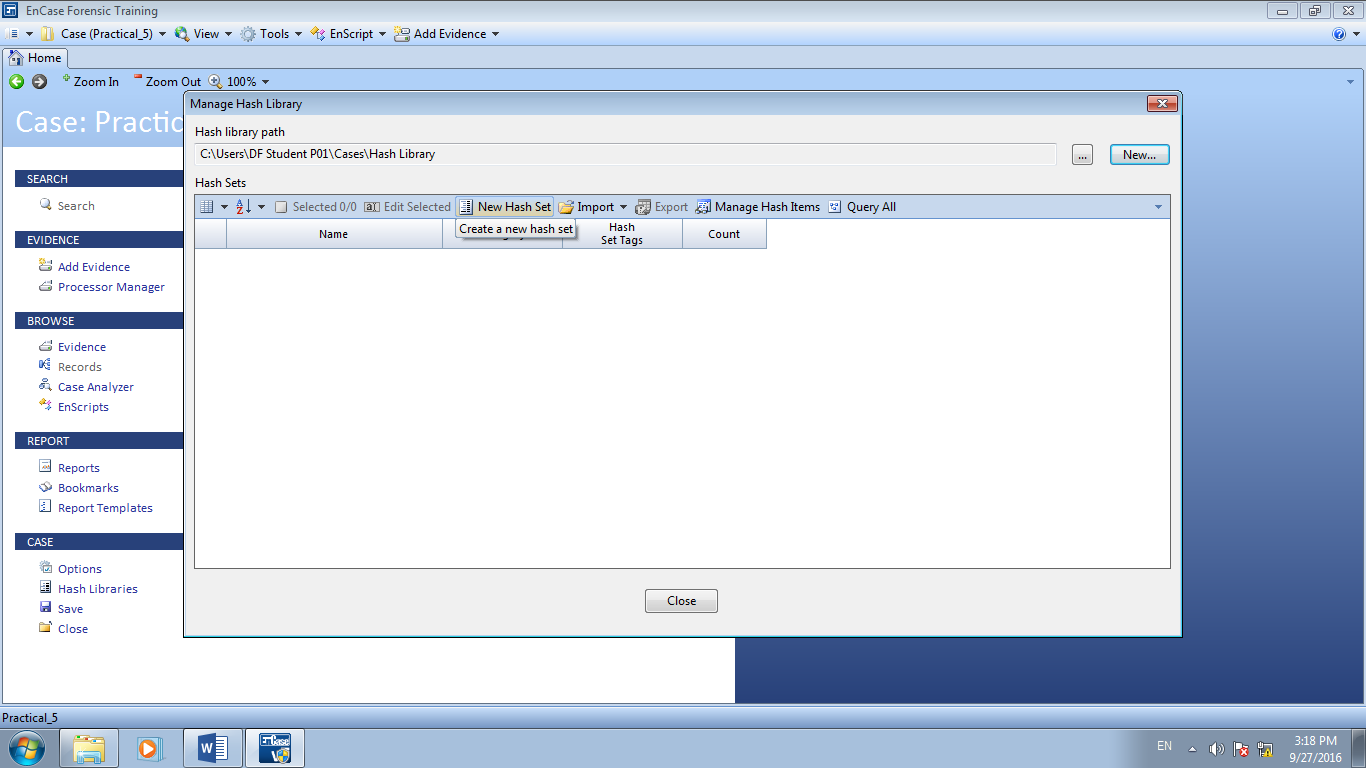


Figure B1: Creating hash set through library management

Through the hash library management screen we have been working in, click **New Hash Set**. This will bring up the Create Hash Set prompt.

The hash set will contain hash values from crime images. We will use hash analysis to quickly search and locate these files in the evidence of Laura.

The **Hash Set Name** merely identifies the hash set. The **Hash Set Category** helps us to identify whether we are looking for this set or we already know of the hash set. The hash set name can be used as input to run filters. It is advisable to use the terms *Known* or *Notable*.

**Known** refers to data that the examiner knows is present within the evidence file, but wishes to exclude from examination efforts (e.g. MS Office software, OS files, etc)

**Notable** refers to data that the examiner wishes to find, such as hacker software and images files.

These have been accepted uniformly throughout the industry and some Enscript programs or filters may rely on that specific naming convention. **Hash Set Tags** serve to identify hash sets in another manner similar to hash set category. Hash set tags also help to find to suppress files.

Once we select OK to create the hash set, we get a prompt indicating success. Click OK on the success prompt and we can see the newly added hash set in the hash library management screen.

Enter Hash Set Name, Hash Set Category and Hash Set Tags as follow:

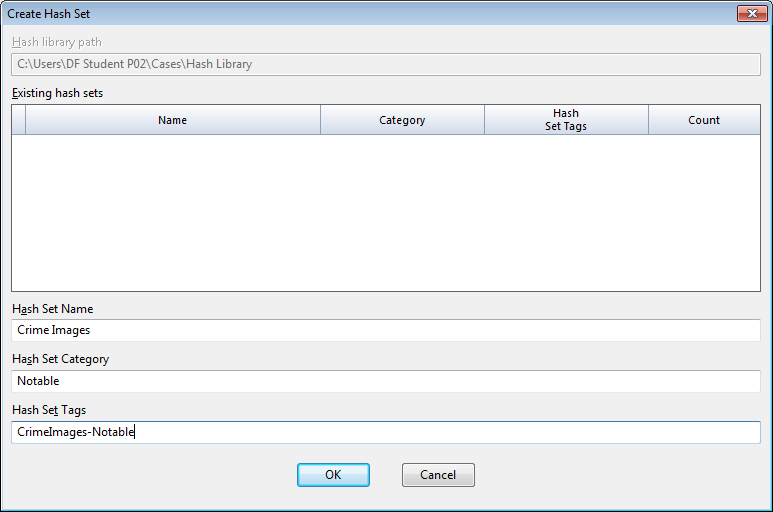


Figure B2: Creating hash set

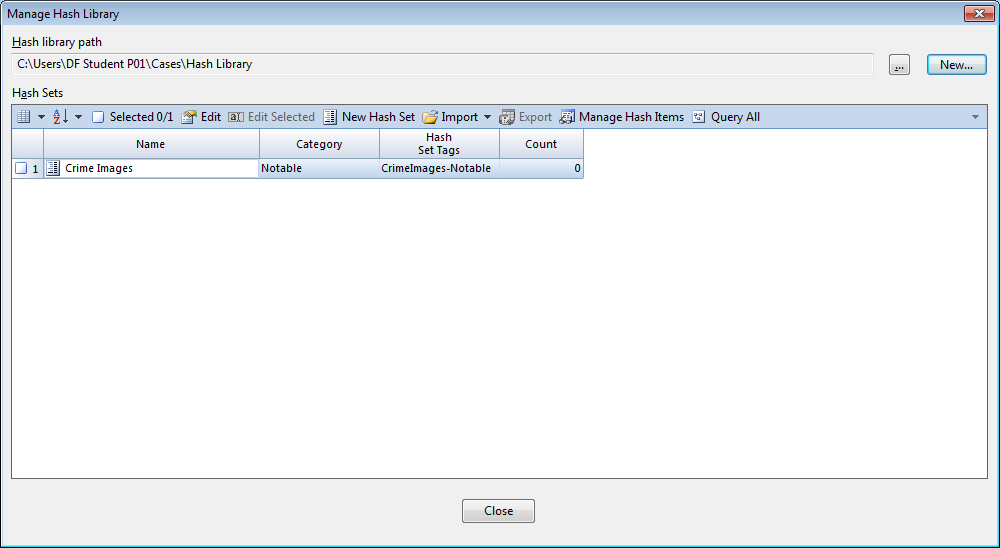


Figure B3: New hash set in hash library management

Click **Close** to continue

**C: Adding hash values to hash sets within First Forensic case**

Now we will open first forensics case so that we can bring in files to create the hash sets from. Open the evidence file and navigate to the folder as shown in Figure C1.

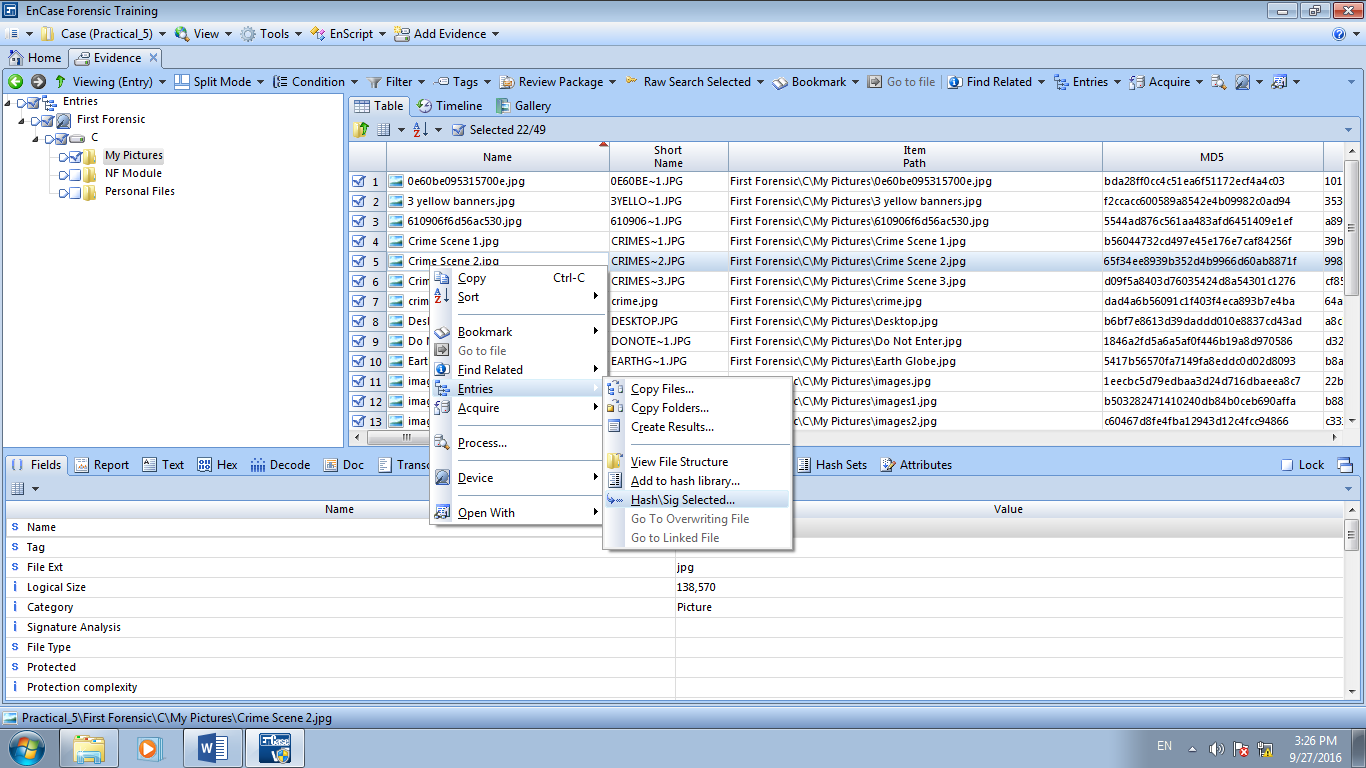


Figure C1: Select files to be added to hash set

Blue check the files as shown in Figure C1. To perform a hash value generation for all these items, right click anywhere and select **Entries🡪Hash/Sig Selected …**

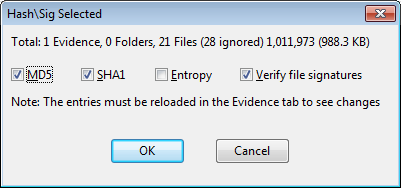


Figure C2: Hash/Sig Selected function options

The default options will be to perform MD5 and SHA1 hashing on the selected files along with verifying files signatures. Click **OK** to continue.

Take note that the entries must be reloaded in the Evidence tab to see the changes.

You may want to close the evidence file and re-open it again to check that the hash values are populated.

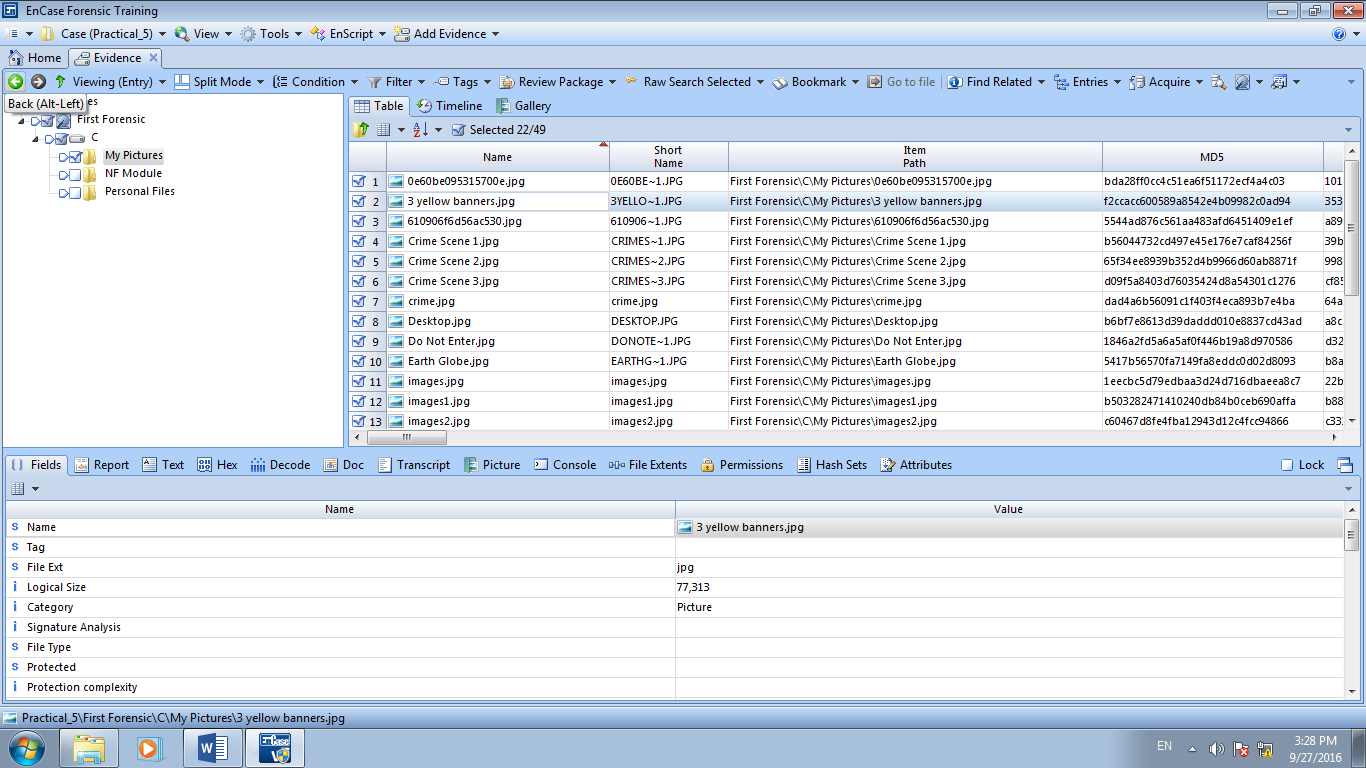


Figure C3: Navigating back to reload evidence

Q2. Encase uses MD5 algorithm to create hash values. What is the likelihood that any two files having the same hash value? How does this affect our work as a FI?

**D: Adding Hash items to hash set**

Right click the selected files as shown on Figure D1 and select Entries | Add to hash library

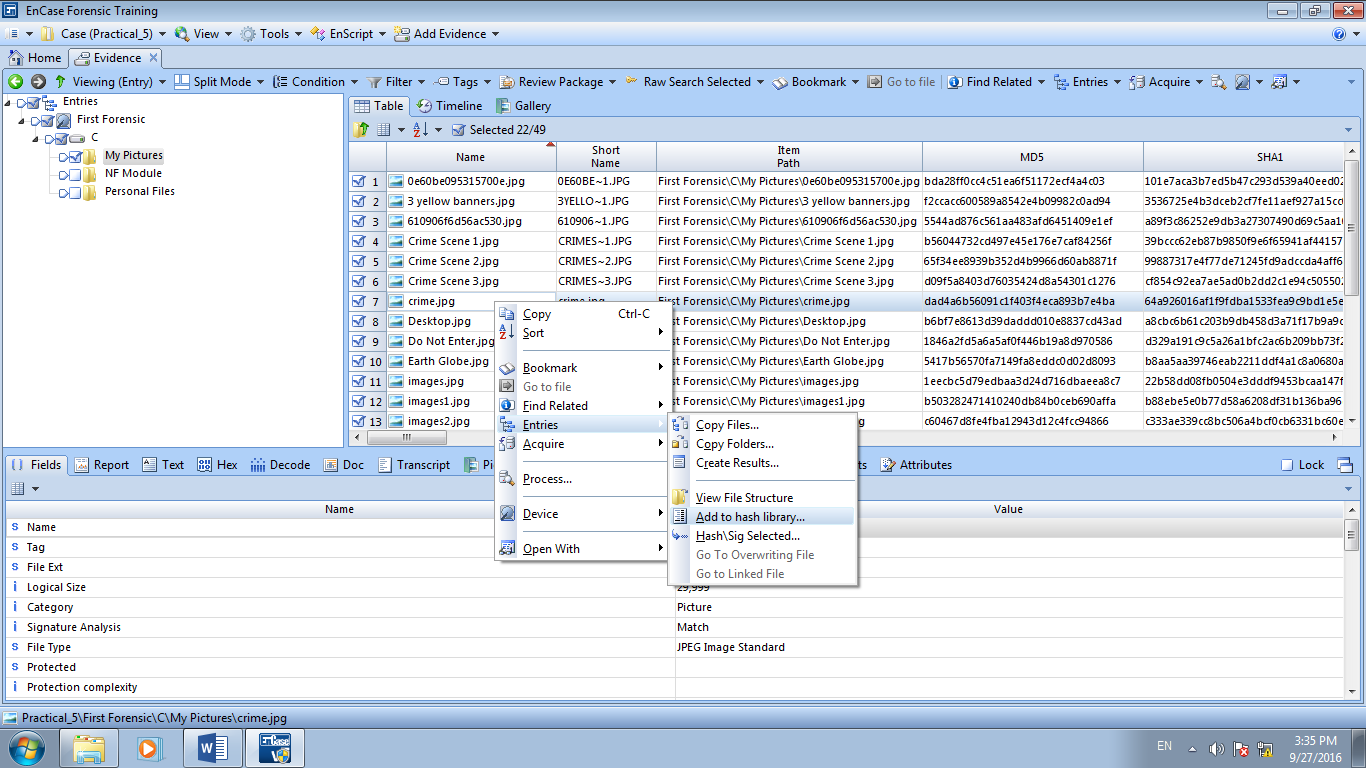


Figure D1: Add hash items to hash set

To view hash items which are added to hash set, click Hash Set **🡪** Tools **🡪** Manage **🡪** Manage Hash Library

By clicking the Tools **🡪** Manage Hash Library, we can see our hash library is in good condition and ready to be used. Now we are ready to close our case and utilize this hash library with the Laura’s case. Close the First Forensic case. We created the hash library in a folder separate from the First Forensic case, hence there is no need to save the first forensic case. The case was used only to hash the files and to add them to the hash set in the hash library.

**Running a Hash Analysis**

Now we can open up Laura’s case and associate this hash library to it. Once the Laura’s case is open, click **Case** menu and select **Hash Libraries**.

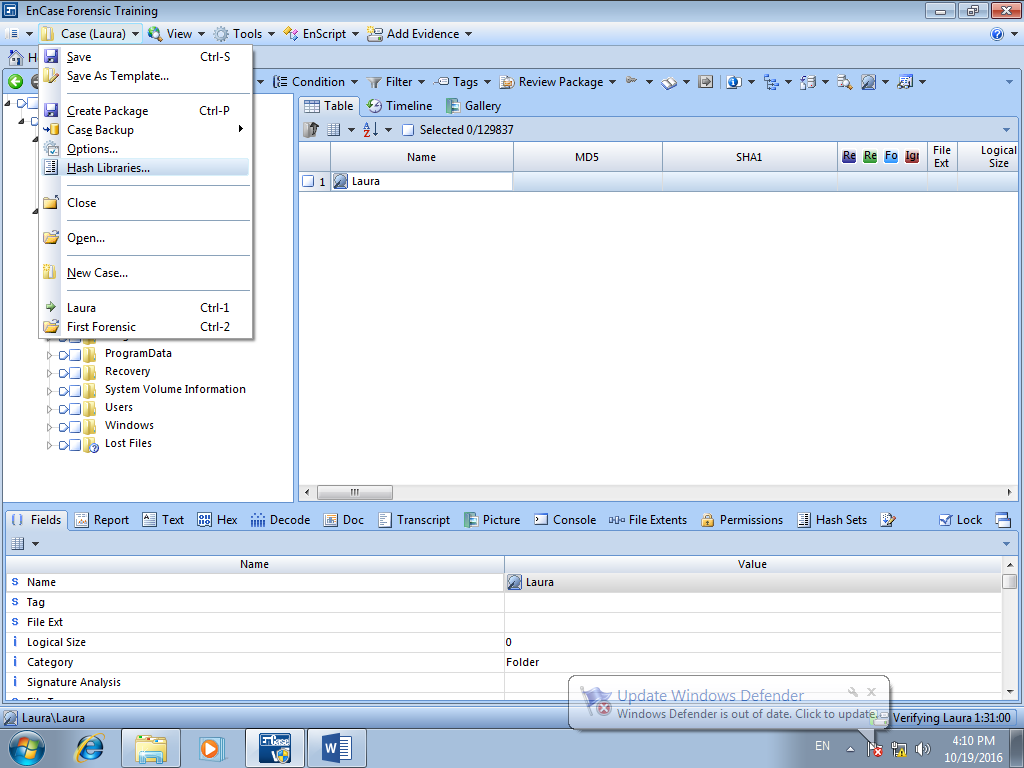
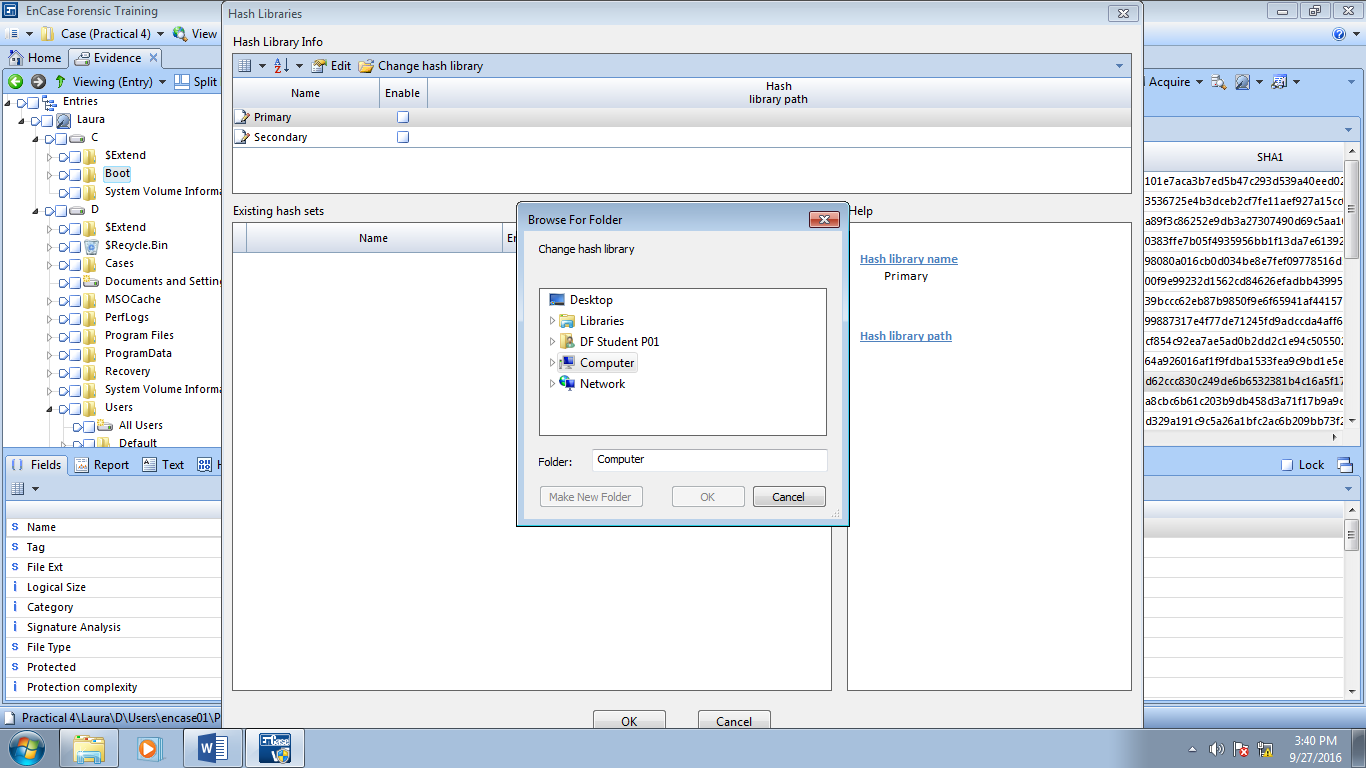


Figure D2: Add hash library access to Laura’s case

From here, we need to tell the Laura’s case where the hash library is. Double click the **Primary** line to browse to our Hash Library folder

Browse to the folder where hash library was created in C:\Users\%USERNAME%\Cases\Hash Library



**Double Click**

Figure D3: Linking the Laura’s case to the hash library

Highlight the Hash Library and click **OK**.

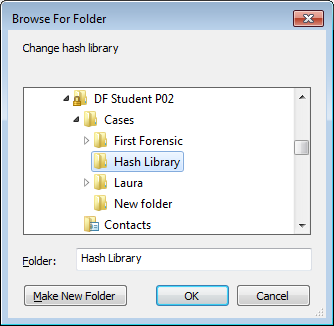


Figure D4: Browsing to the hash library

At this point, we will see the hash library contents and the hash set that it contains. From here, we will want to ensure the correct hash library and/or hash(s) set is/are selected as enabled or unchecked for disabled.

Click **OK** and we are ready to perform hash analysis.

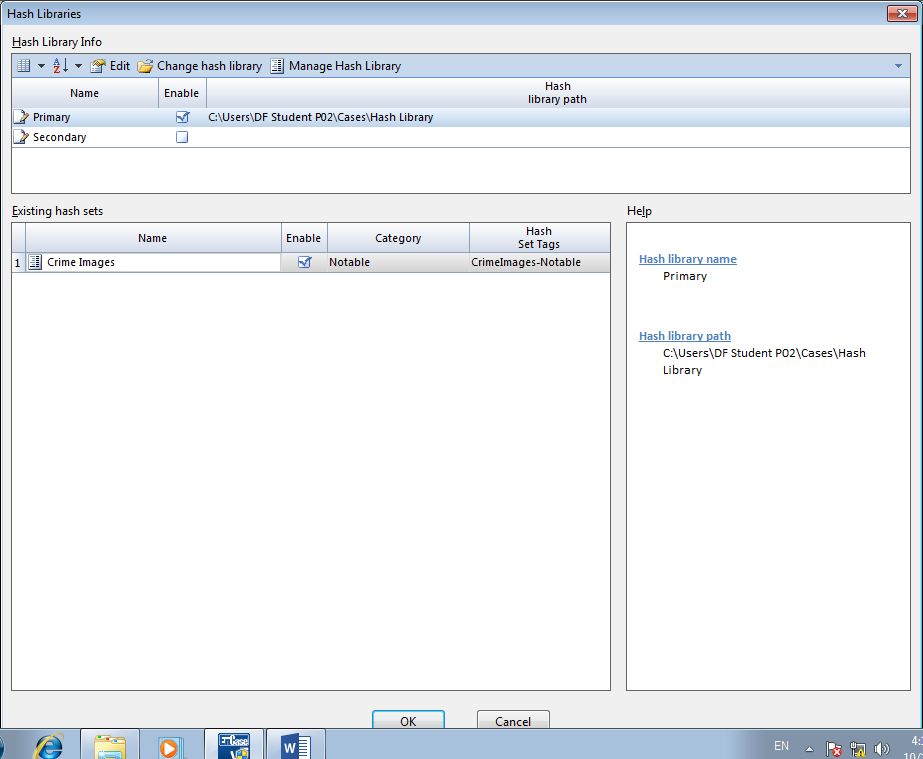


Figure D5: Hash Library linked to Laura’s case

Before we begin, be sure that you have created hash values for the files in the case against which you want to compare the hash library. This can be accomplished either by running the Hash Analysis through evidence processing function or by using Hash/Sig Selected on files that you want to work with. Lastly, remember to reload the evidence after the hash value creation function is complete in order for the hash values to be populated within Encase.

You can perform the hash analysis on Laura’s case by performing either of the followings:

a) Using the Processing function

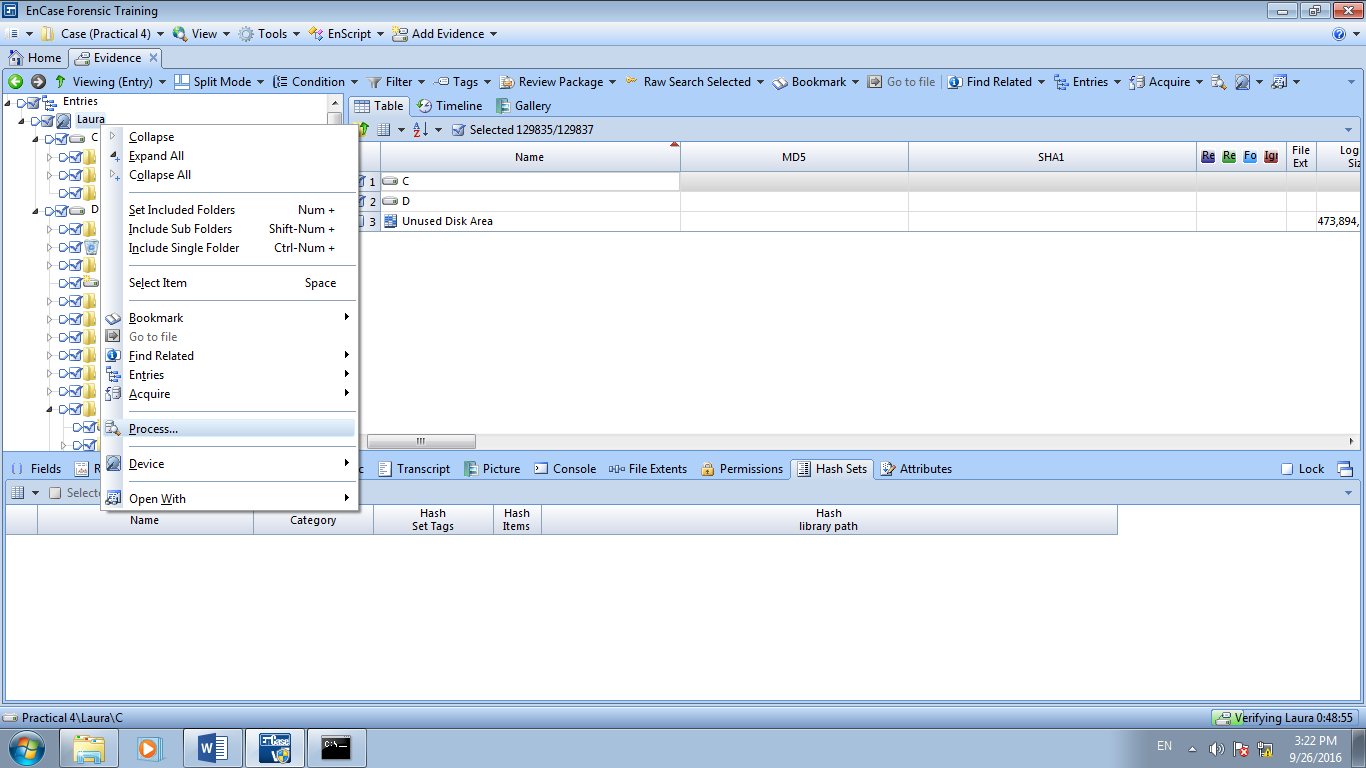


Figure D6: Blue Check selected files, Right Click **🡪** Process

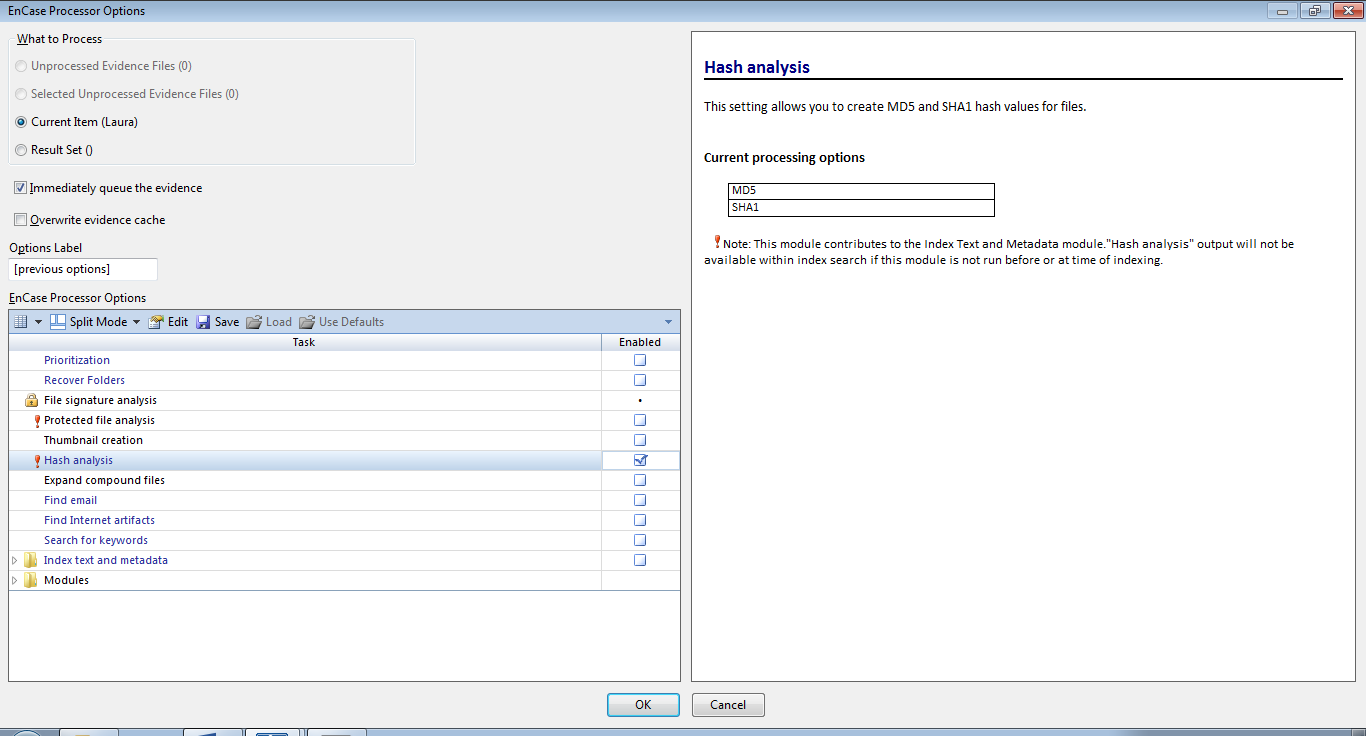


Figure D7: Enable hash analysis on selected items

Or

b) Using Hash/Sig Selected

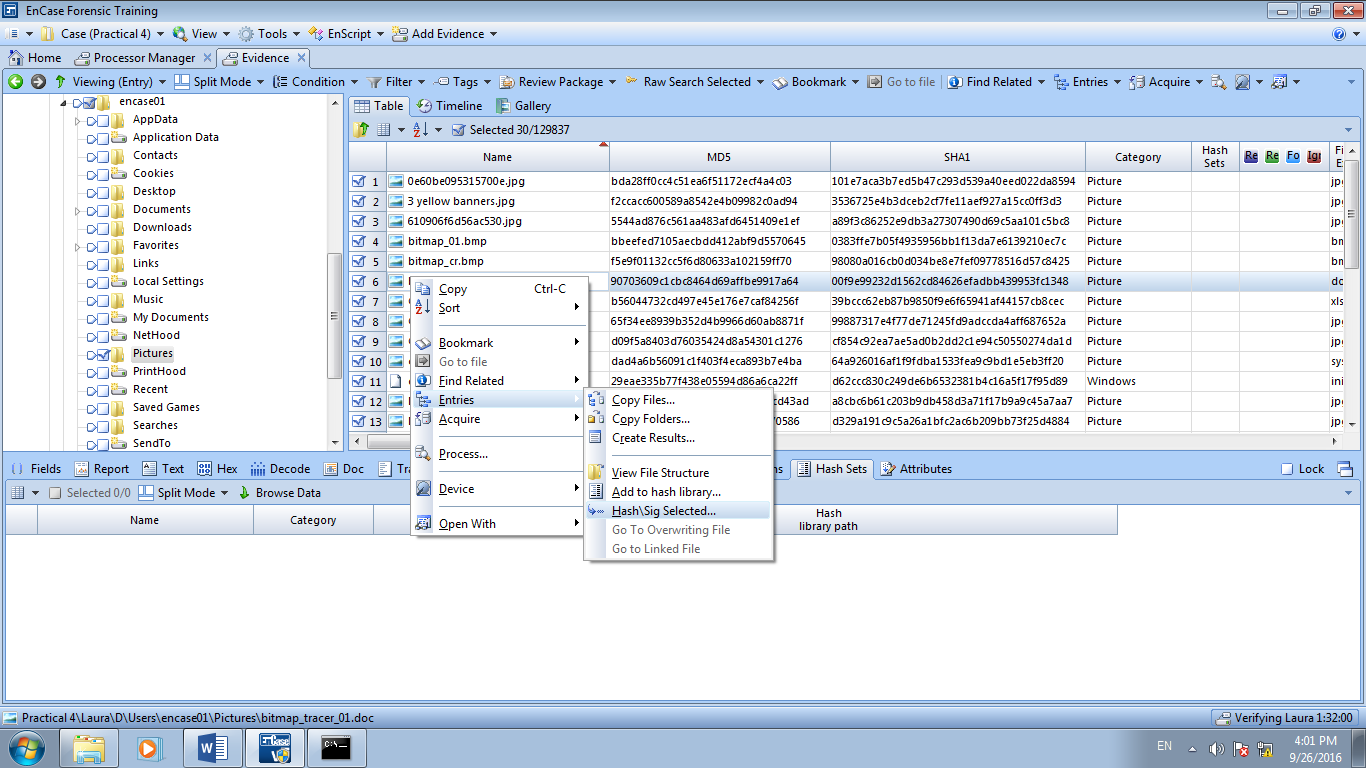


Figure D8: Blue check selected files, Right click Entries **🡪** Hash/Sig Selected

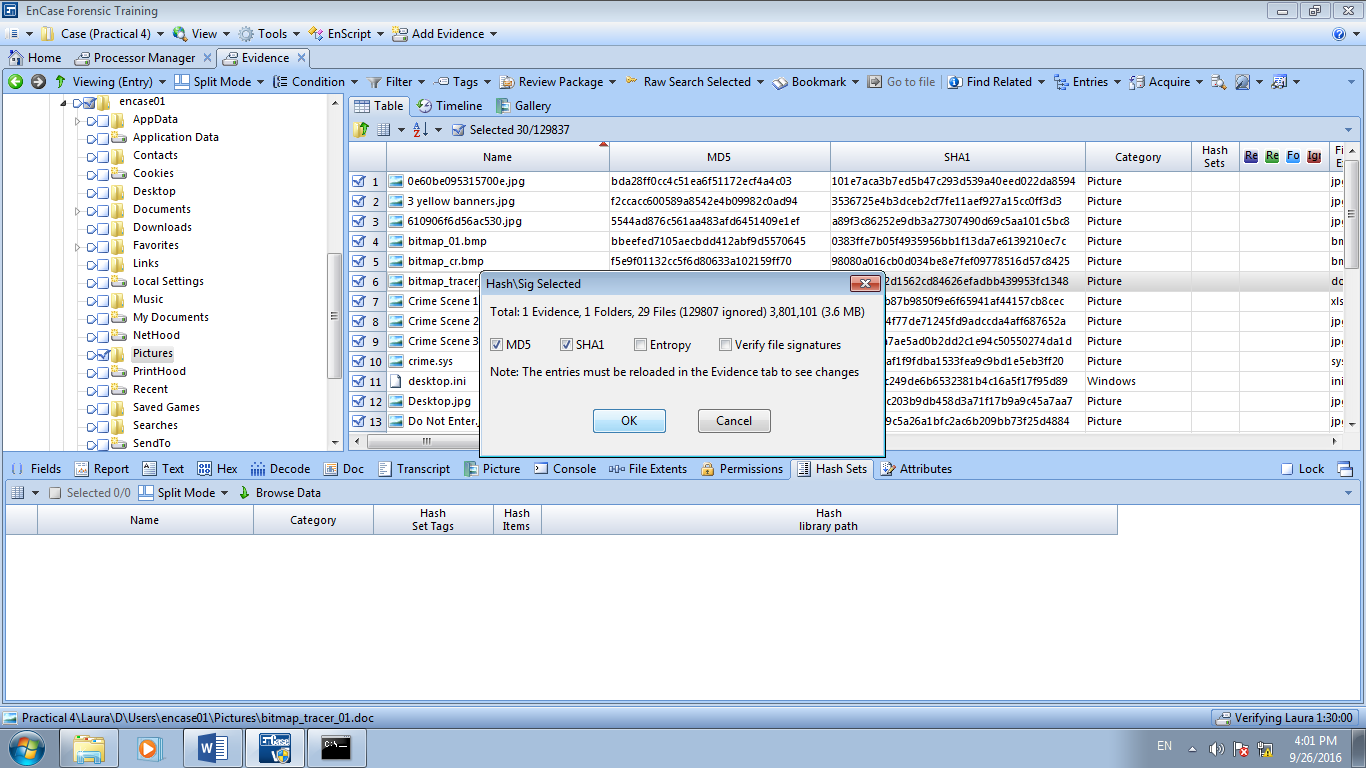


Figure D9: Running hash analysis on selected files

**Analyzing the Hash Results**

1. To analyze the hash results, we can apply filter. Back in the Entry view, we can run a filter. A filter is like a condition in that it will limit what is displayed. This filtering process on our data will assist us with locating or suppressing Notable or Known hash sets.
2. We are going to use the filter Find Items by Hash Category. To locate the filter, let’s click the Filter menu and then select Find Items by hash Category.

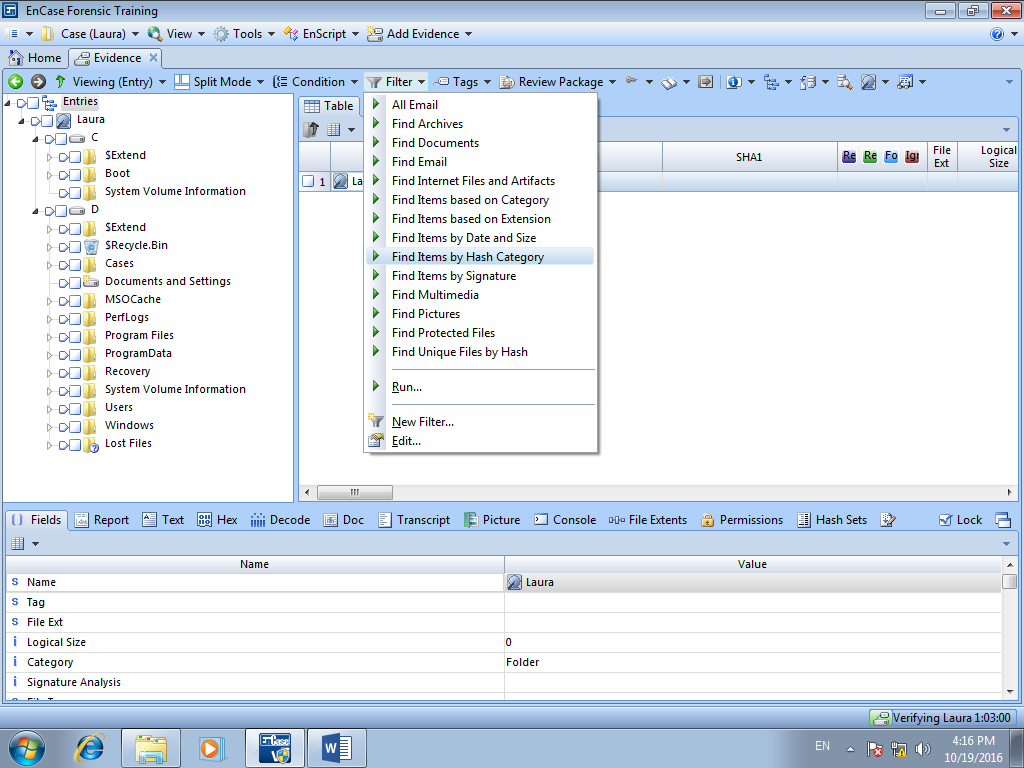


Figure D10: Filter menu

1. This is the options screen for our filter. This is the same screen you will see when running conditions. The result name is what you will either see displayed on the temporary filtered view or as the name of the created results set.

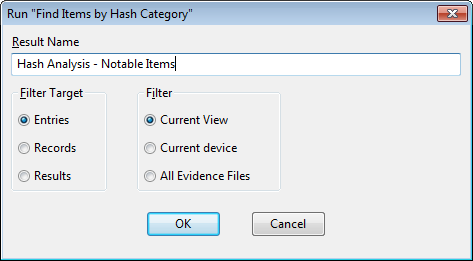


Figure D11: Filter options

Select **Current View** and title the Result Name “Hash Analysis – Notable Items.” After those items are complete, select **OK**.

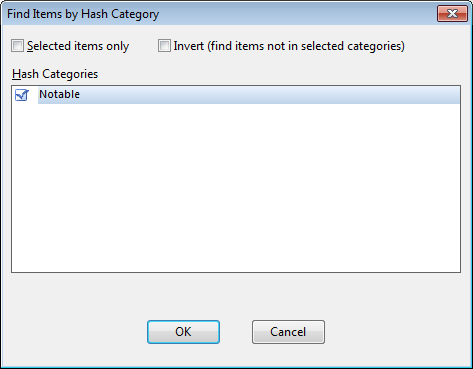


Figure: D12: Final filter options

In the final screen for filtering options we can define the Hash Category for which we wish to filter. If needed, we can run selected entries only. Select **Notable** Hash category and select **OK**.

We are done with our hash analysis. The files shown are exactly the same set of files that we have had previously created in the hash set in the hash library. You may blue check the files to be bookmarked for further analysis.

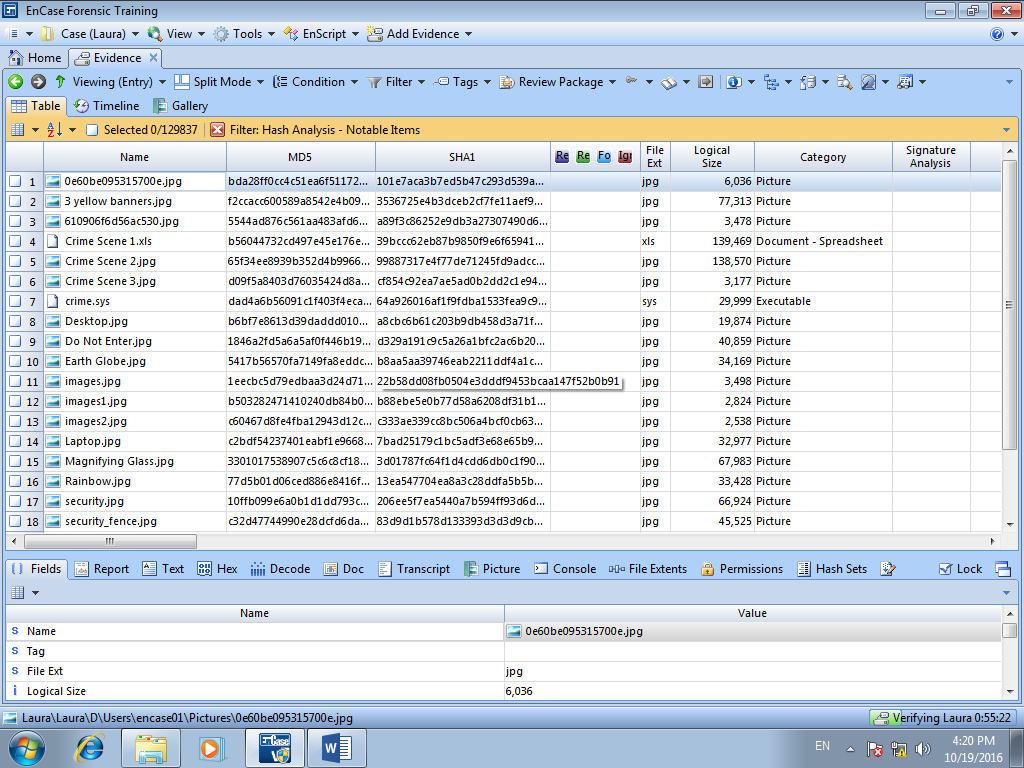


Figure D13: Filter results for Notable Hash Category in Table view

Q3. You are in the midst of analyzing a case and you found out that the hash value of a particular file is changed.

What would you do next? Explain how this affect the case.

Reflection: What have you learnt in this practical exercise?

Reference

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

- The End -