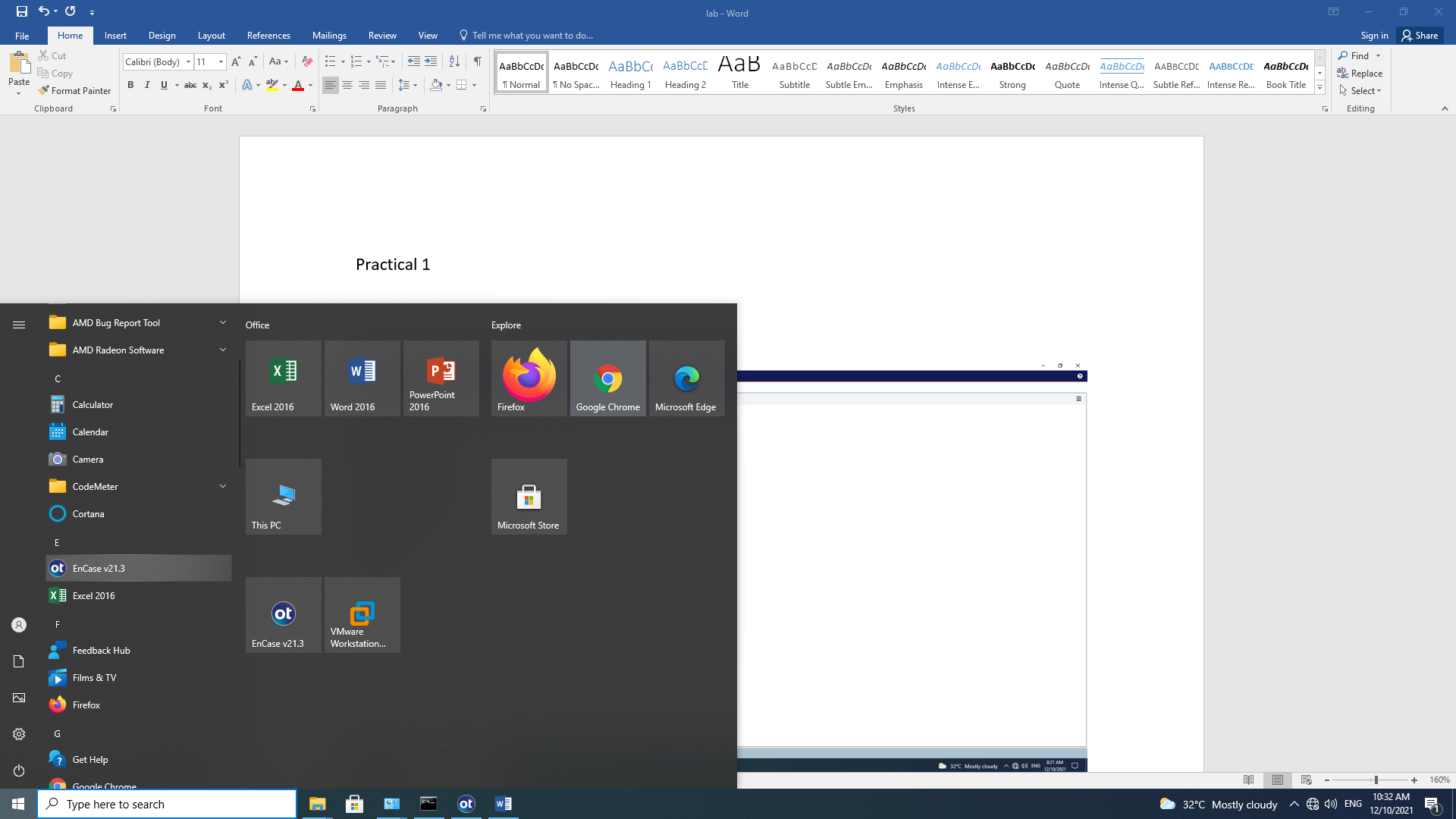
|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 1 |
| Practical 1 |
| **Familiarization with EnCase v21.3** | |

**OBJECTIve**

1. To be familiarized with EnCase environment
2. To be able to navigate and carry out simple functions in EnCase

**Preparation:**

1. Boot the computer to Windows 10.
2. Start EnCase v21.3 application.



1. You should see the panel showing “**EnCase Forensic Training**” rather than “EnCase Acquisition”.

If you see “EnCase Acquisition”, carry out the following steps to troubleshoot. Otherwise, move on to Part A.

* 1. Enable the wired network adapter and set the IP address to dynamically assigned.
  2. Ping 10.1.0.1 and ensure that you receive replies from the SAFE (Secure Authentication for Encase) server.
  3. Encase Licenses are provided by the SAFE server to the client PCs in the lab.

**Part A: Case Management**

**Important notes:**

* **All evidence files that will be used in this module are stored in “C:\Evidence Files”.**
* **Always copy the required evidence files to your own case folder before you start the investigation.**
* **You should stay at the same workstation throughout the semester.**

In Encase, a case is stored in a folder, with subfolders for case-specific information such as search results. The case folder and the components contained within that folder directly associate the investigative work you perform.

Encase automatically creates several folders when the case is created. These folders include:

* Documents
* Email
* Export
* Searches
* Tags
* Temp

When a device or evidence file is added to the case, the Evidence Cache folder is created.

1. Launch EnCase v21.3
2. After you launched EnCase, the Home page will be displayed:

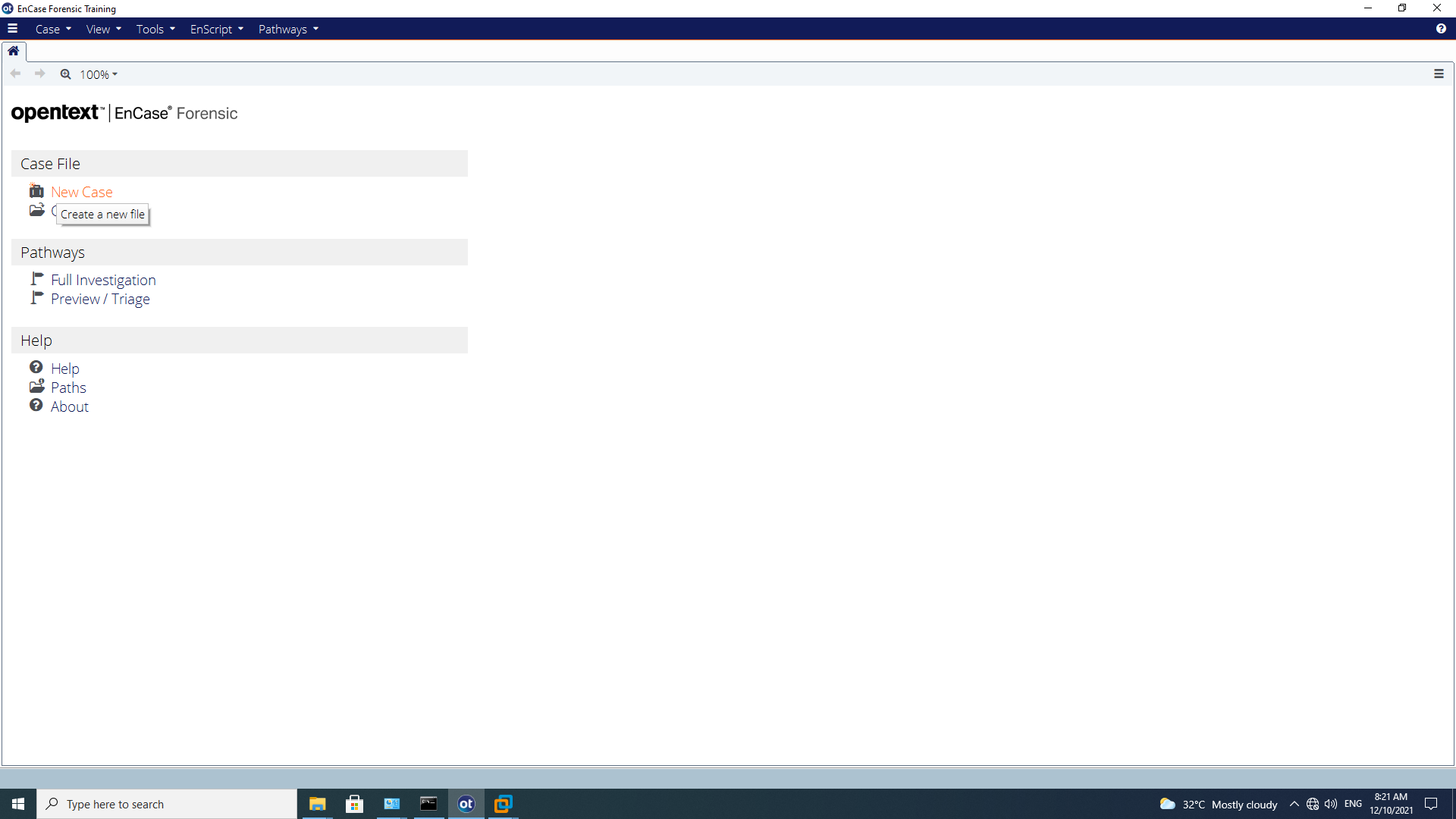


Figure A-1: Home Page

To create a new case:

1. Click **New Case** beneath the CASE FILE category.
2. The Case Options dialog displays. Use this dialog to select a case template and name the case.
3. In the figure below, the **#1 Basic** template is selected.
4. Enter a case Name, then click **OK**.

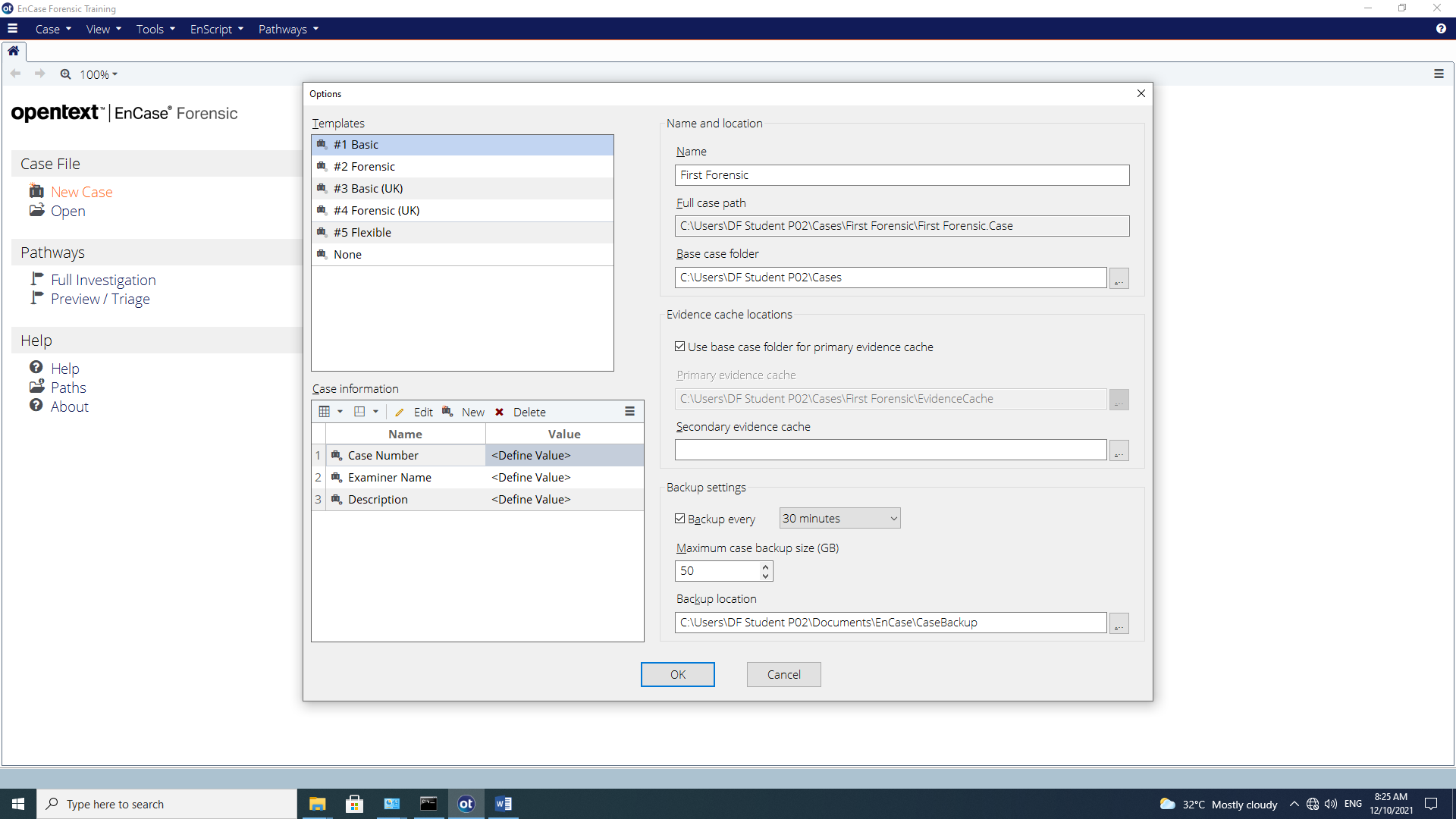


Figure A-2: Case Option Dialog

For this week, we shall use the Name, “**First Forensic**”.

**Full case path:** The folder in which the case file is stored. This path is determined by the Base case folder, followed by a subfolder with the case name.

**Base case folder:** The location where the above case folder is created. Change the Base case folder to **C:\Users\DF Student P0X\Cases where X is your tutorial group number.**

**You will need to create the Cases folder in your student account prior to this.**

No back-up is required in this exercise.

* **Uncheck Backup Every** (30 Minutes) check box. Click **Yes** when prompted with “Disable backup?” dialog box.

**Leave the rest of the settings as default.**

Q1: What do you understand about the .Case file?

The case file is a text file that contains info specific to a case. It is named as ‘.case’. It contains pointers to any number of evidence files or bookmarks, serach results, sorts etc.

**Part B: Adding Evidence to a Case**

Click OK to continue. The following display will appear:

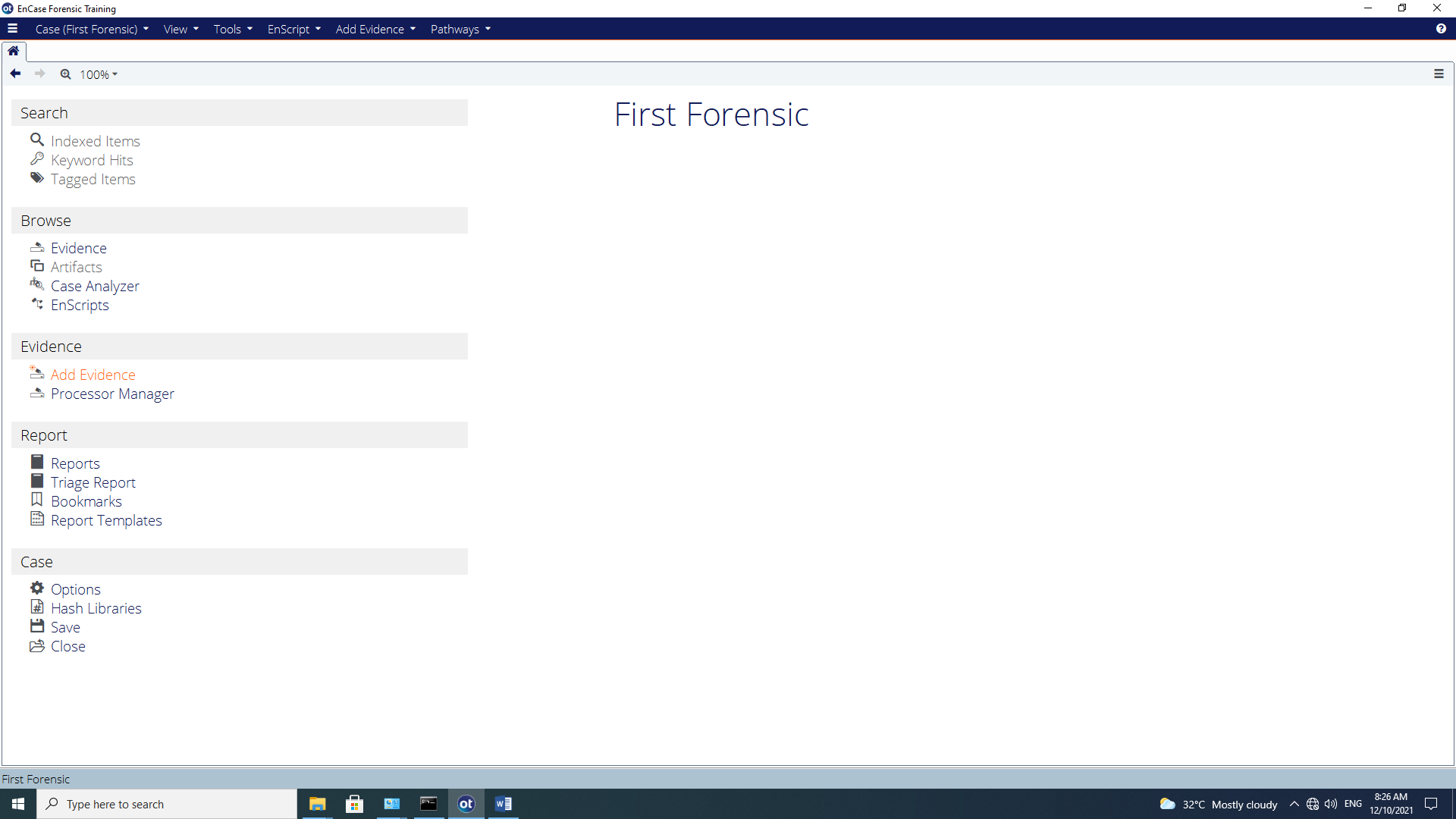


Figure B-1: Case Page List

You will need to add an evidence file. Select **Add Evidence.**

Select **Add | Evidence File**

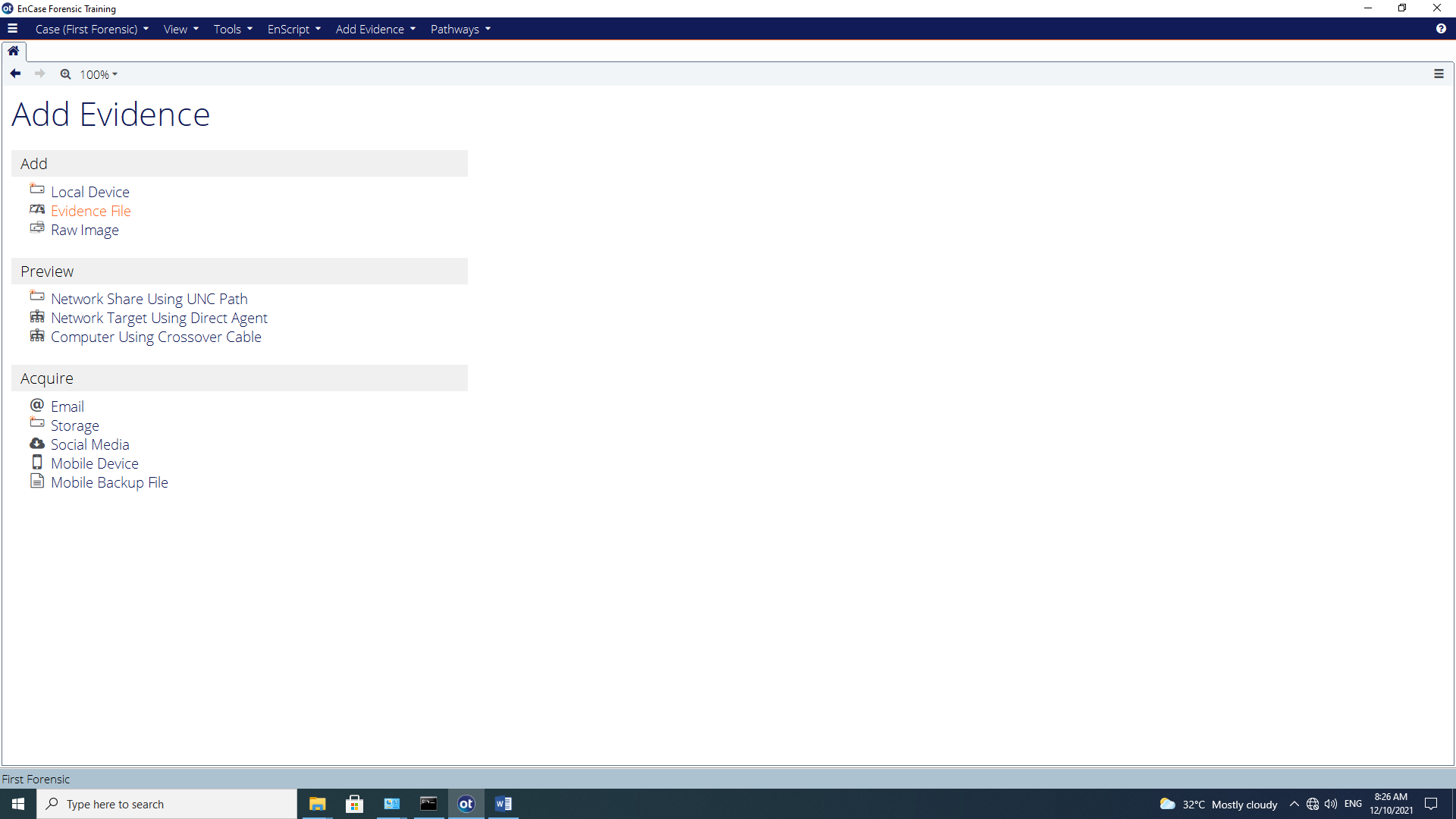


Figure B-2: Add Evidence Menu

Navigate to where the evidence file is stored (i.e. C:\Evidence Files\First Forensic\) and add the First Forensic.E01. Highlight the evidence file and click open.

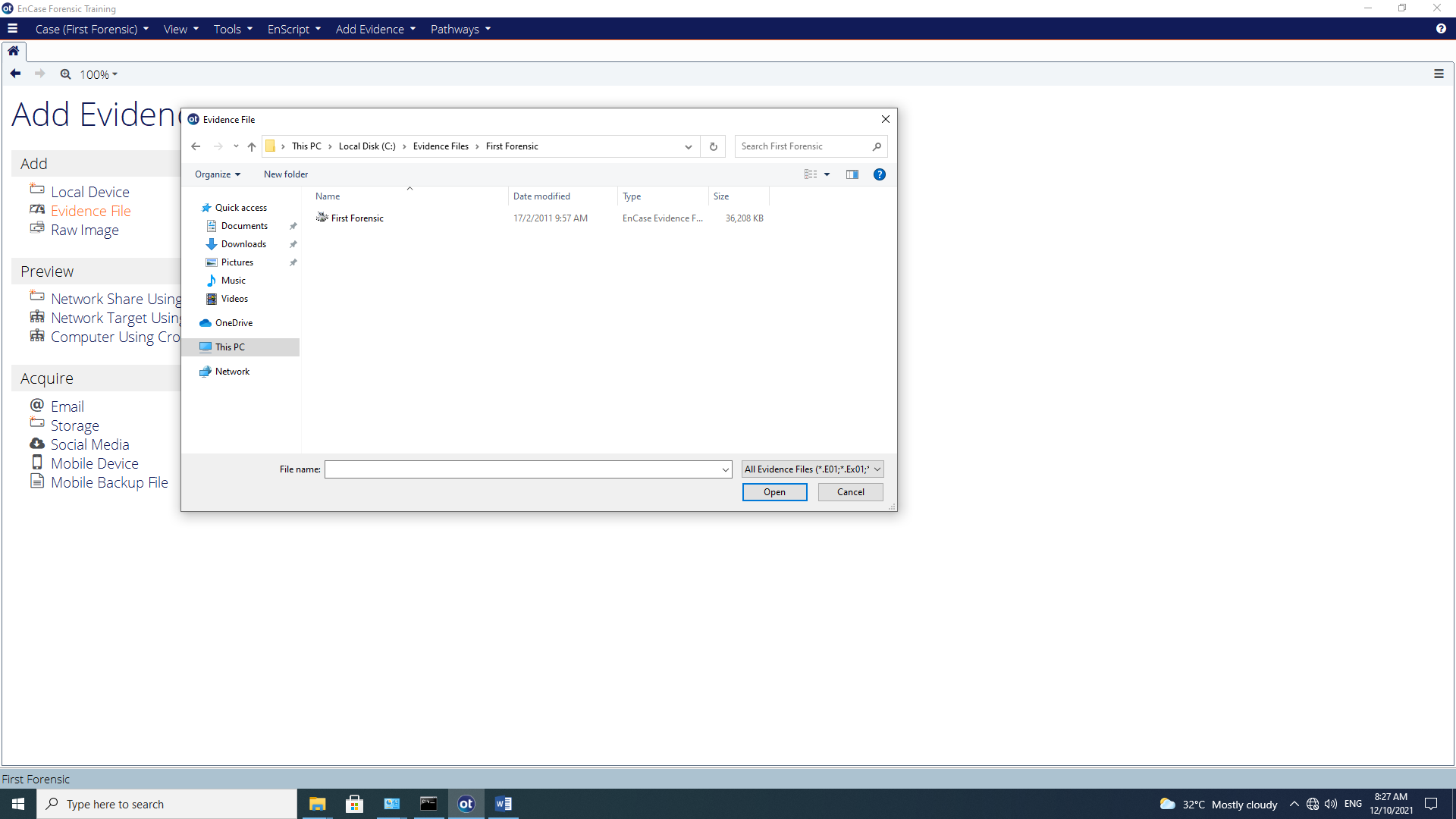


Figure B-3: Adding First Forensic Evidence file

Check “**Don’t notify me again**” and Click **OK** when prompted with Auto Evidence Processing Prompt.

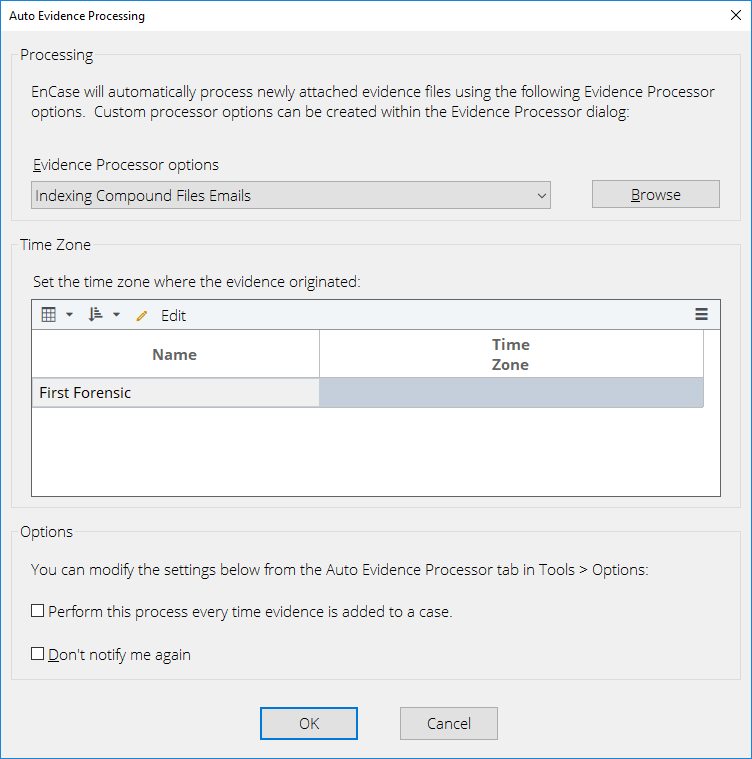
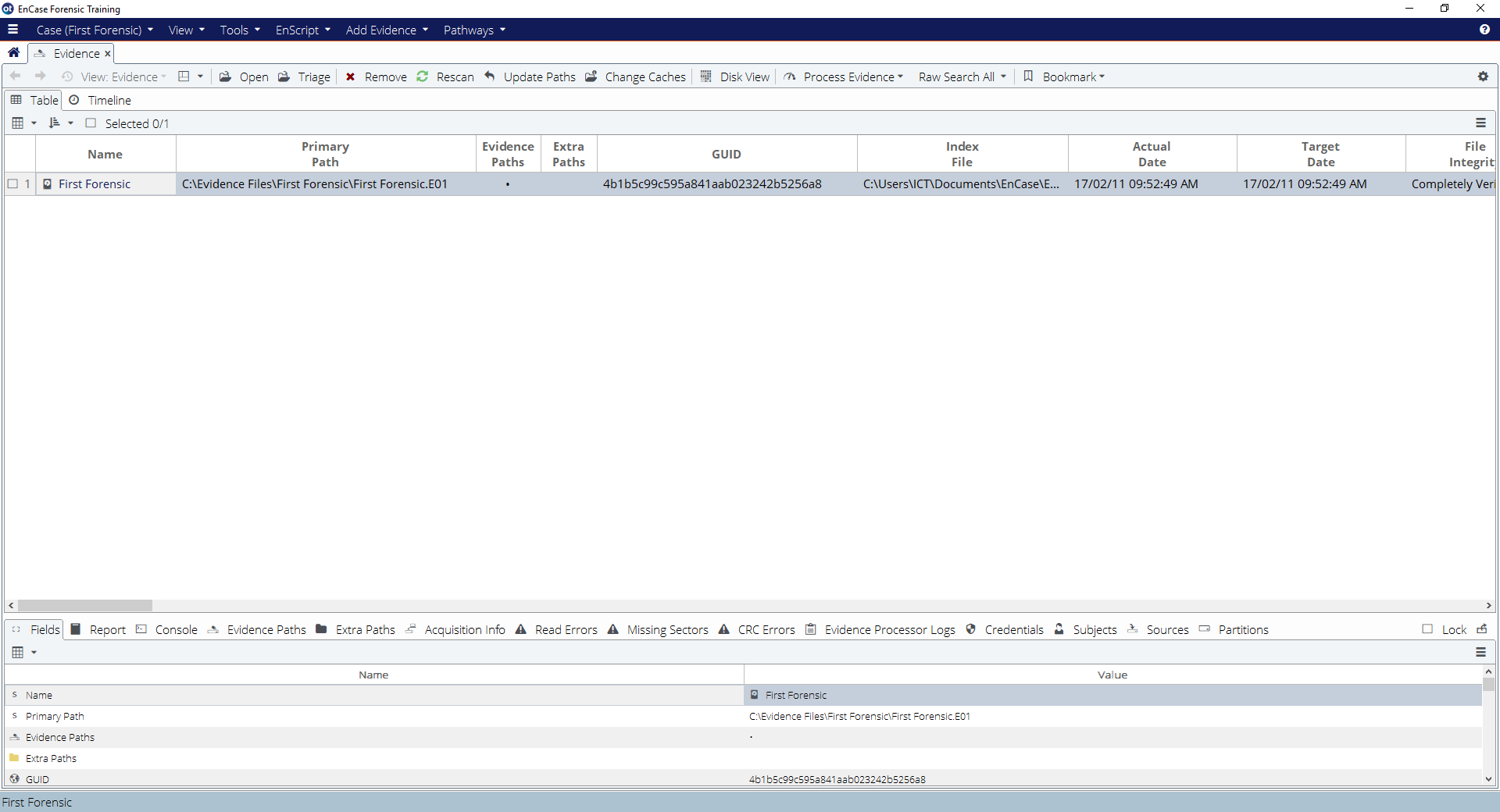


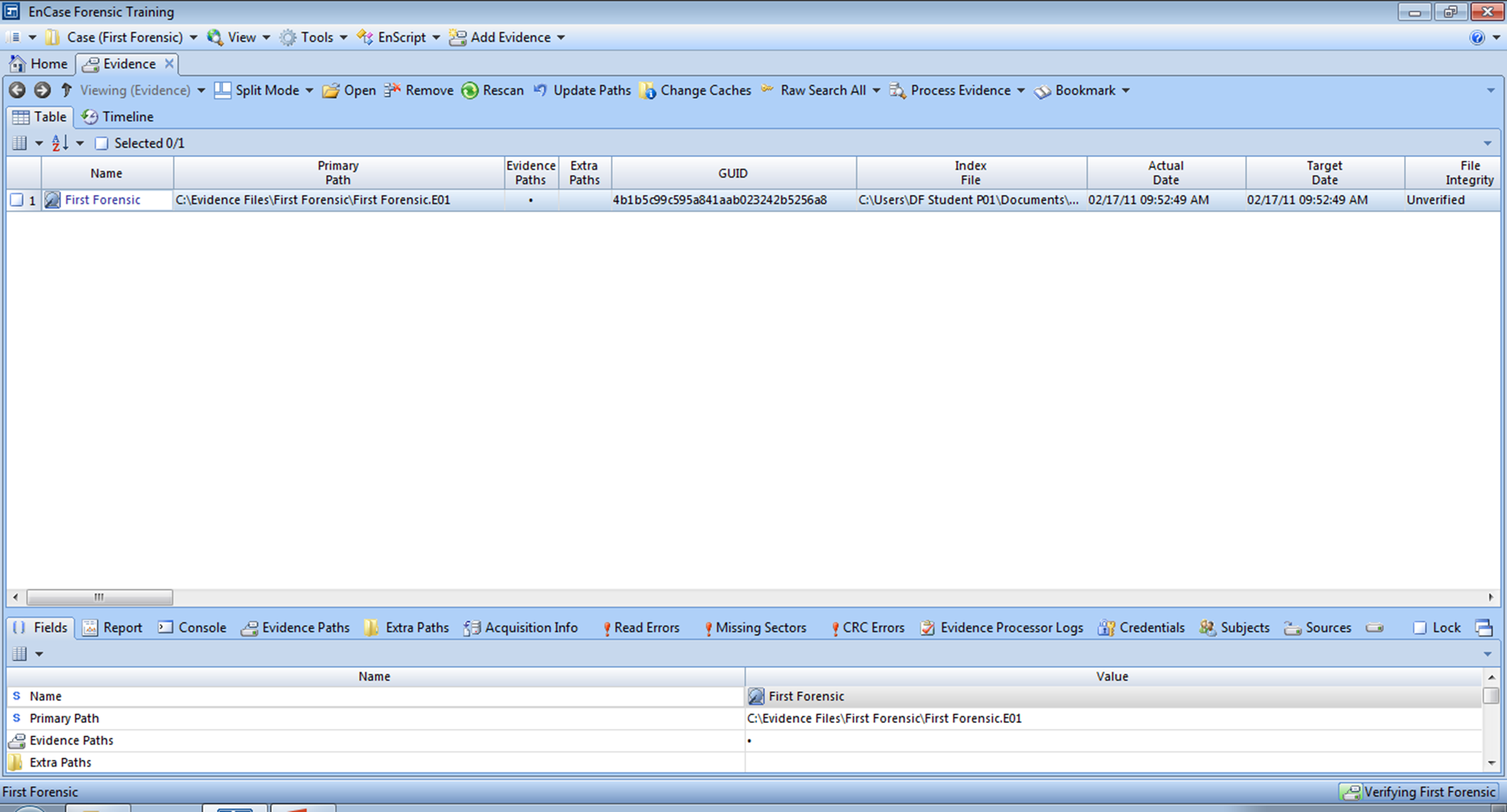
Figure B-4: Auto Evidence Processing

The Viewing (Evidence) screen will appear.

Figure B-5: Viewing (Evidence) screen

Q2: In what way do you think this evidence file was generated?

Evidence file was generated by bit-stream copy of the original suspect’s drive. E01 represents the EnCase Evidence file which is supported by most commercial open source tools.

Blue check the First Forensic evidence item entry and click **Open** or double click the  icon.

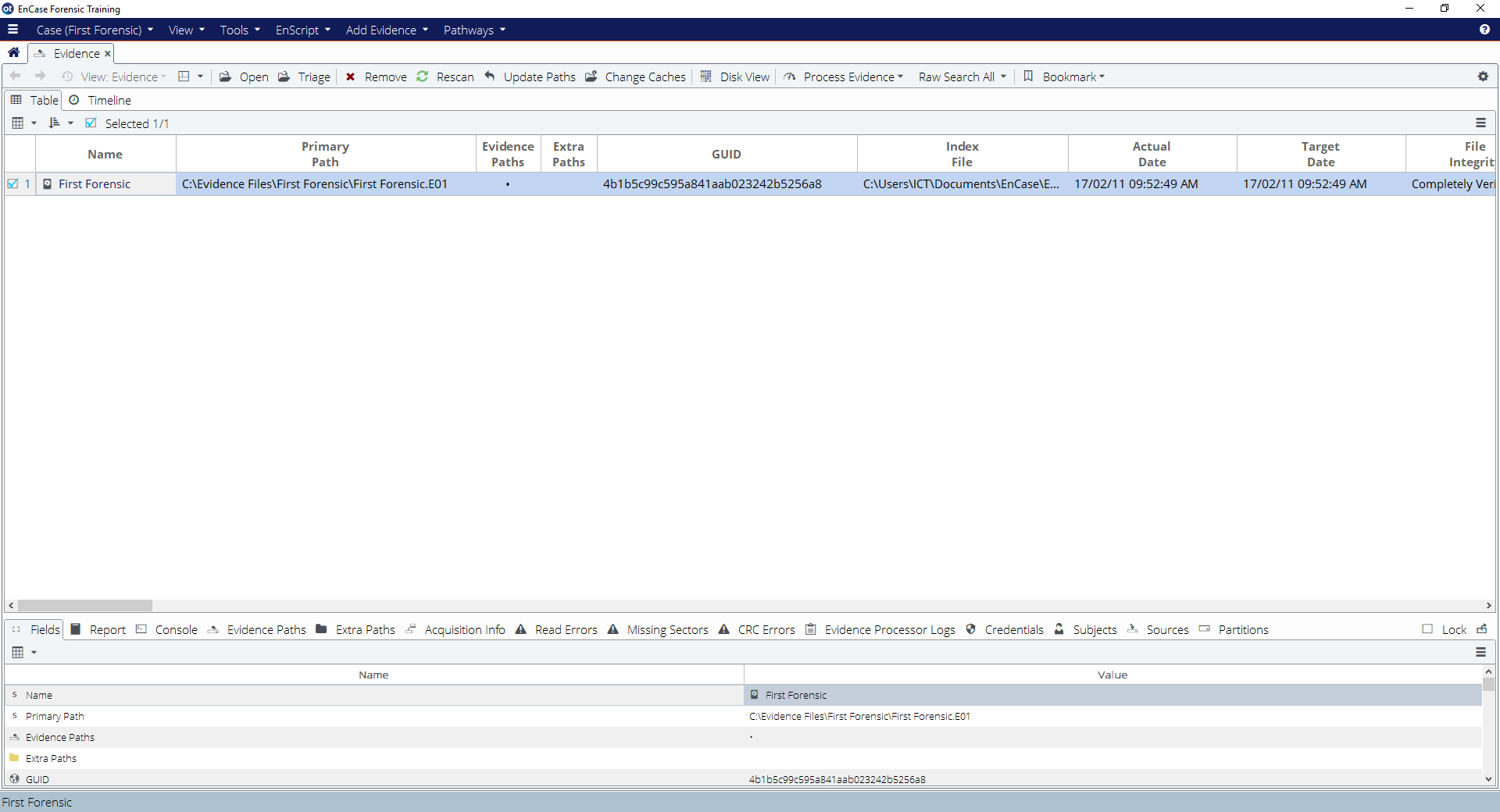


Figure B-6: Blue Check First Forensic Evidence File

The evidence will load and be cached automatically. Once this process is completed, you will be brought to the Viewing (Entry) screen.

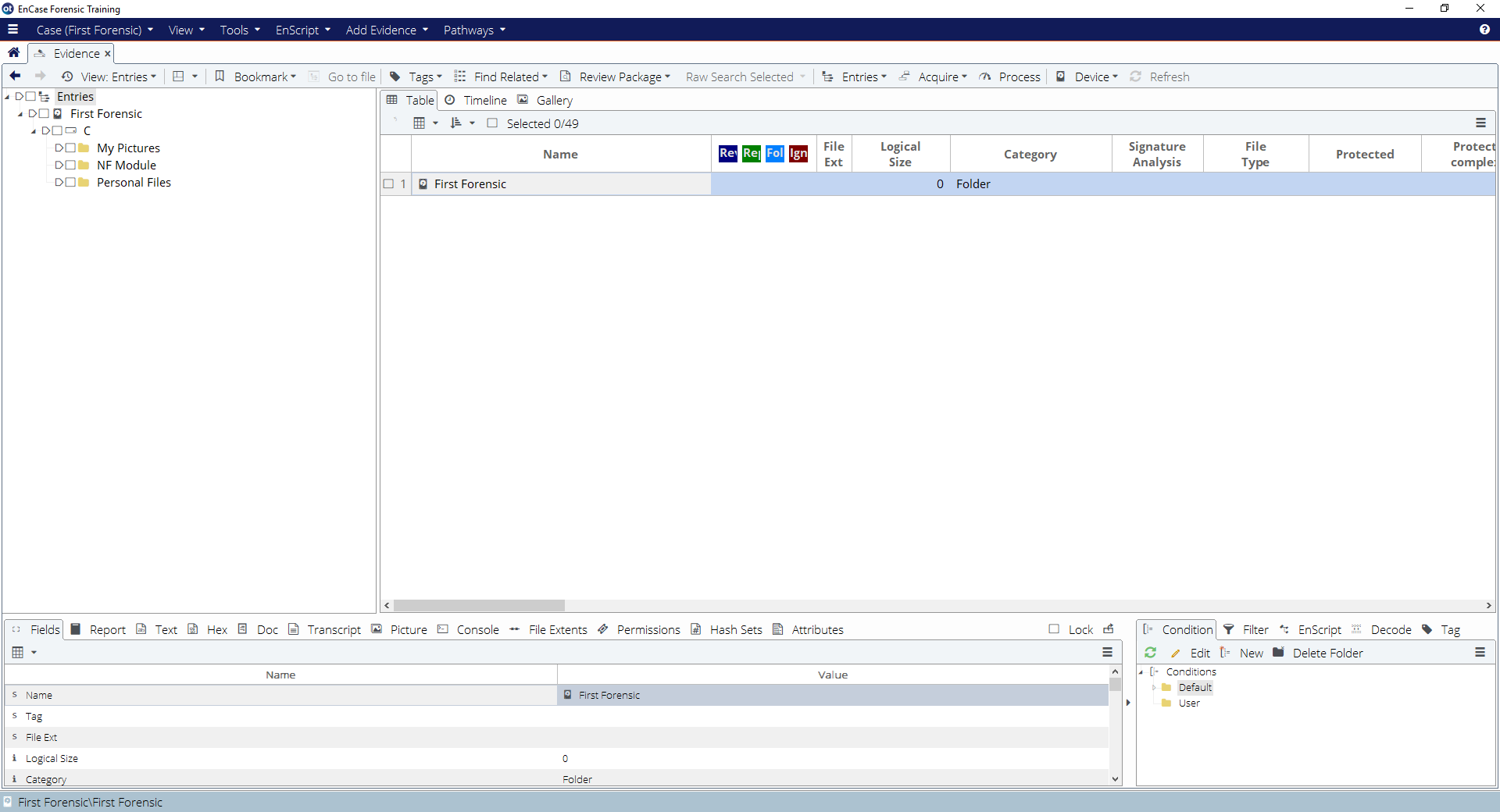


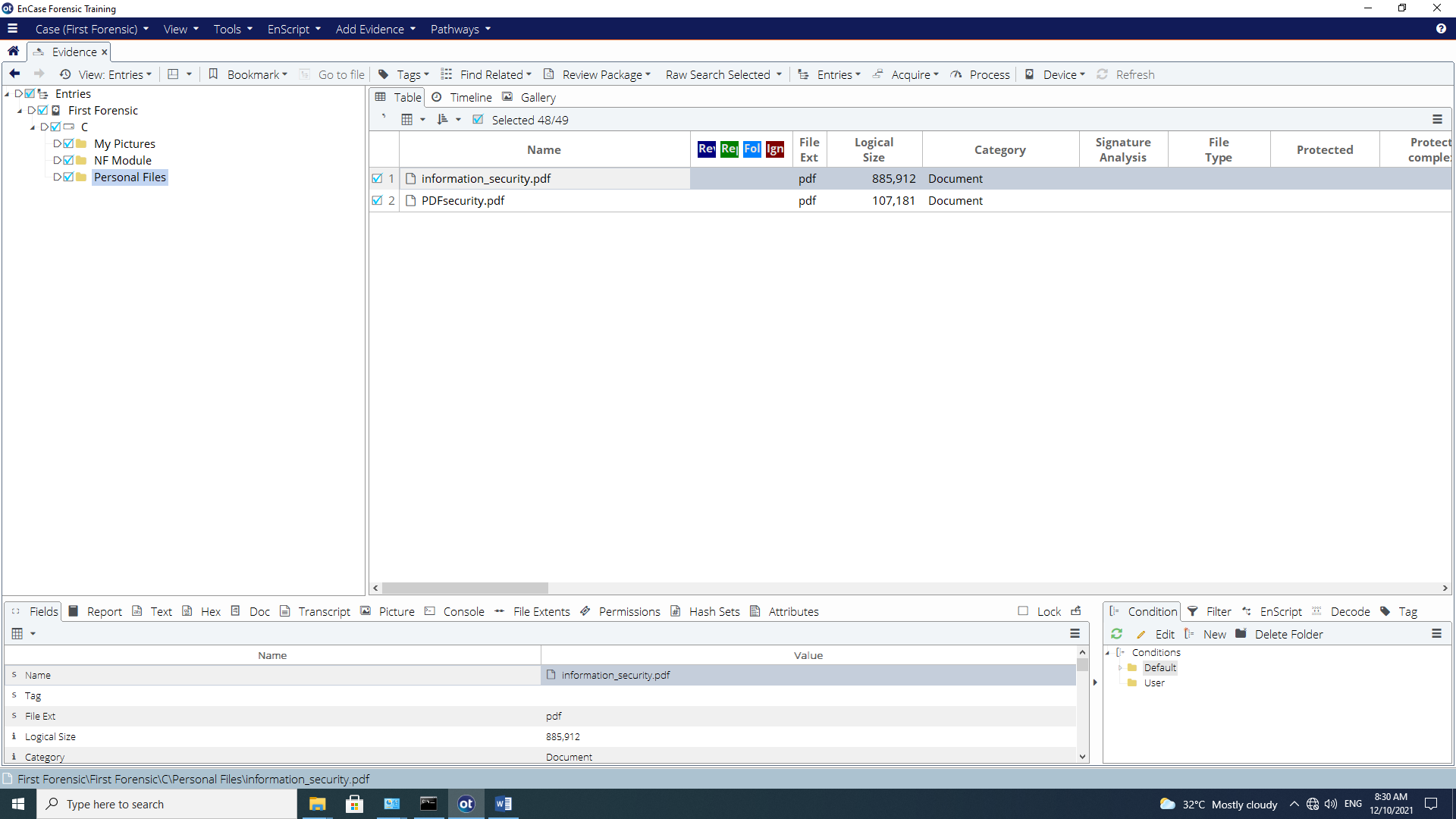
Figure B-7: Viewing (Entry) screen

**Part C: Navigating the EnCaseEnvironment**

The screen is initially divided into 3 sections:

* Tree Pane
* Table Pane
* View Pane

The Tree-Table shows the **Tree pane** on the left, the **Table pane** on the right, and the **View pane** on the bottom. This is the traditional EnCase entries view.



**Filter Pane**

**Tree Pane**

**View Pane**

**Table Pane**

Figure C-1: View of three panes

**Tree Pane**

The Tree view presents the evidence in a standard hierarchical folder structure. Only evidence files and the folders contained within them are displayed in this view. Individual files are displayed in the Table Pane. The arrows can be used to expand and contract the tree structure just as they are used in Windows Explorer.

Right-click on an object in the Tree Pane will bring up a context menu.

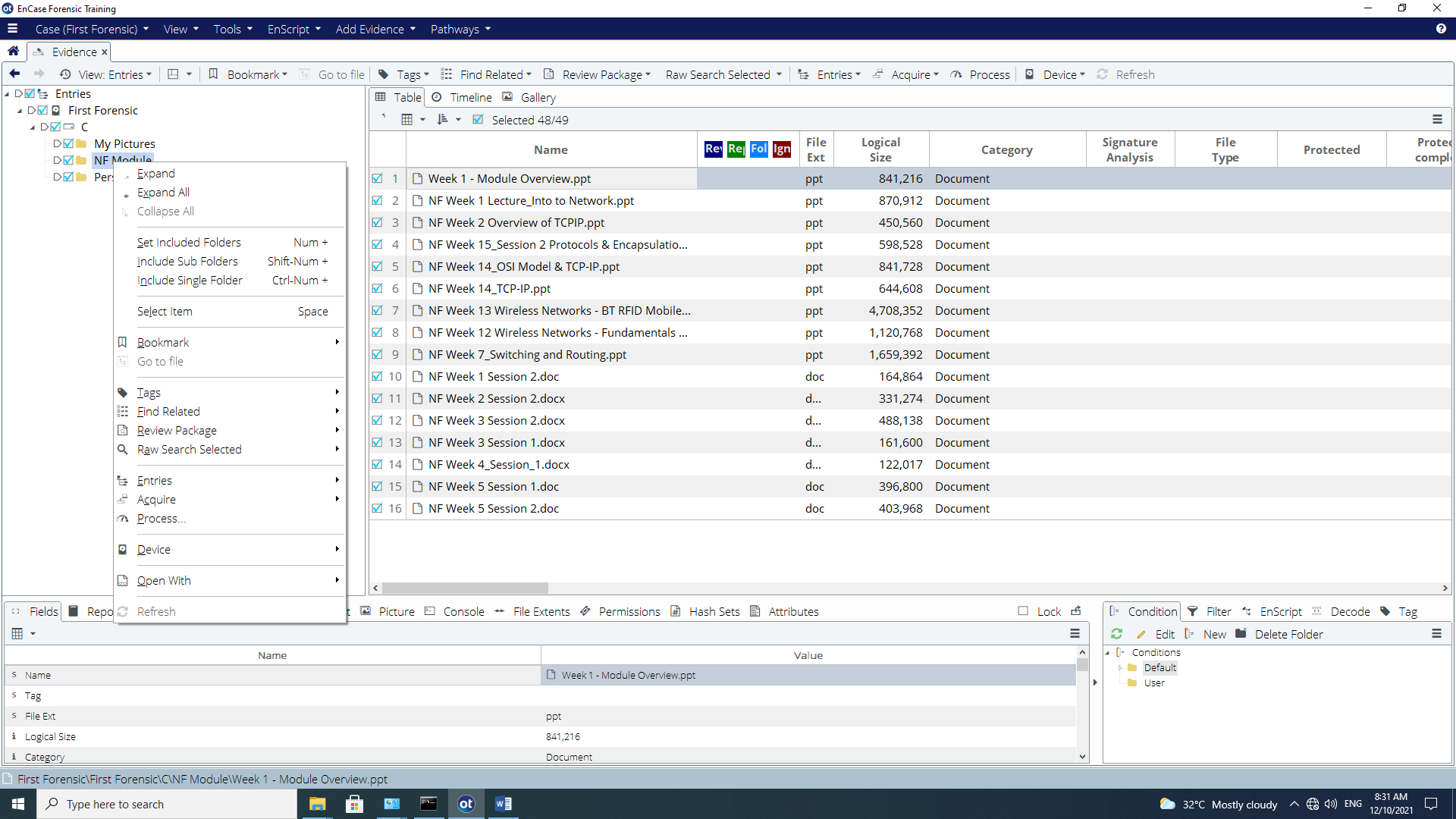


Figure C-2: Context Menu

There are 3 methods used within EnCase to focus on specific files or folders. These methods have different purposes:

* **Highlighting** a folder displays the entries within that folder in the Table Pane. This is used **for viewing** information only.
* The **Set Include Option** method displays all the entries, files, and folders for that folder and subfolders in the Table Pane. It overrides the highlighting option. This is used **for viewing** information only.

When a folder is included, the other folders are grayed out. All files and folders within the folder and subfolders are displayed in the Table Pane. To deactivate this function, click on the **Set Include Option** icon again or click twice on another include icon.

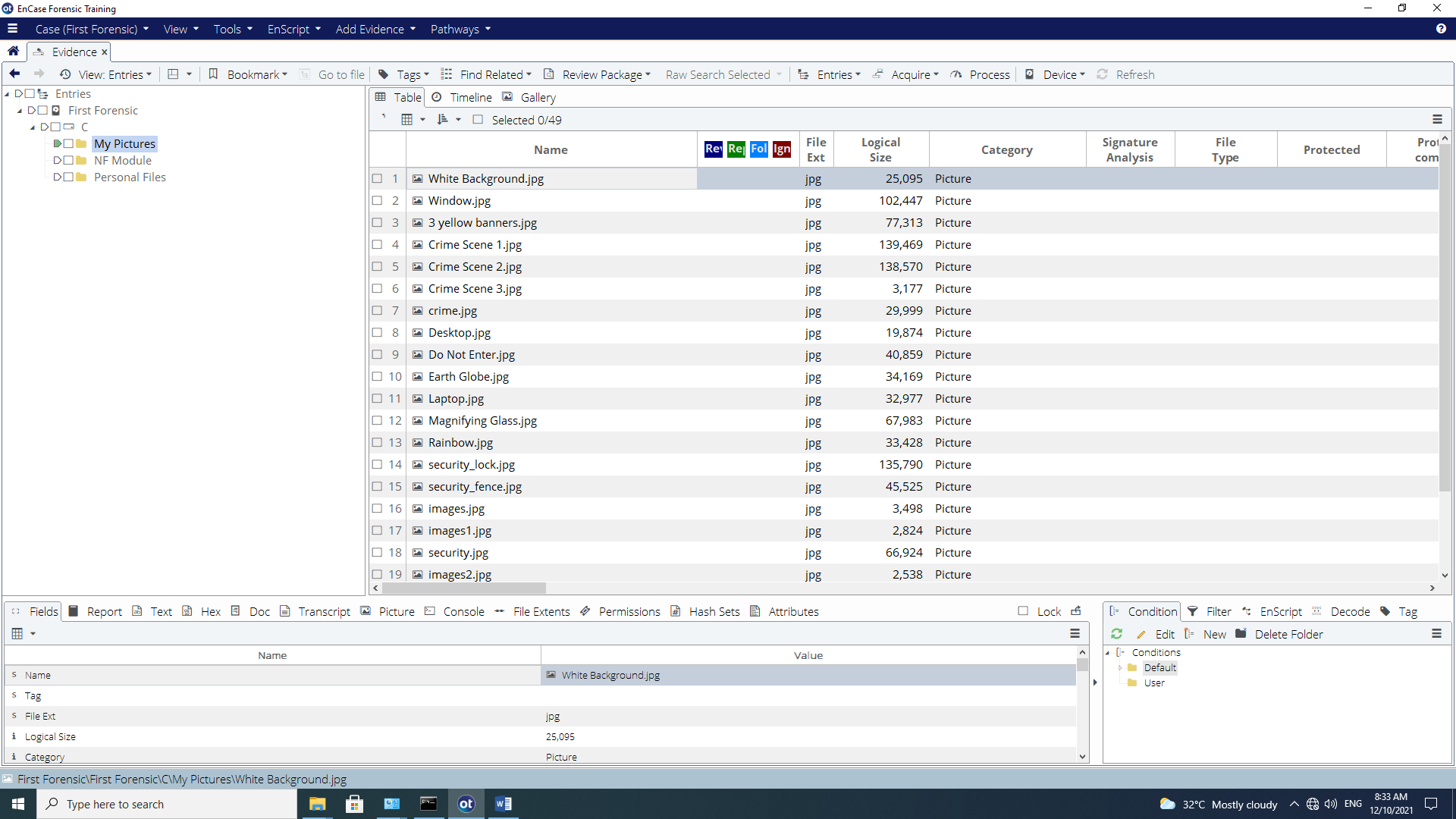


Figure C-3: “Set including” a Folder Structure

* The **Blue-check** [](http://www.dreamstime.com/register?jump_to=http://www.dreamstime.com/stock-images-blue-tick-symbol-image7330424)or **Select for future action** method is used for designating files or folders on which **to perform an analysis operation** such as keyword search. This can be implemented from a variety of views.

The **Dixon Box** can be found at the Table Pane that indicates how many entries have been selected.

To deselect all entries, click within this Dixon box to remove the blue check,

Try out these options.

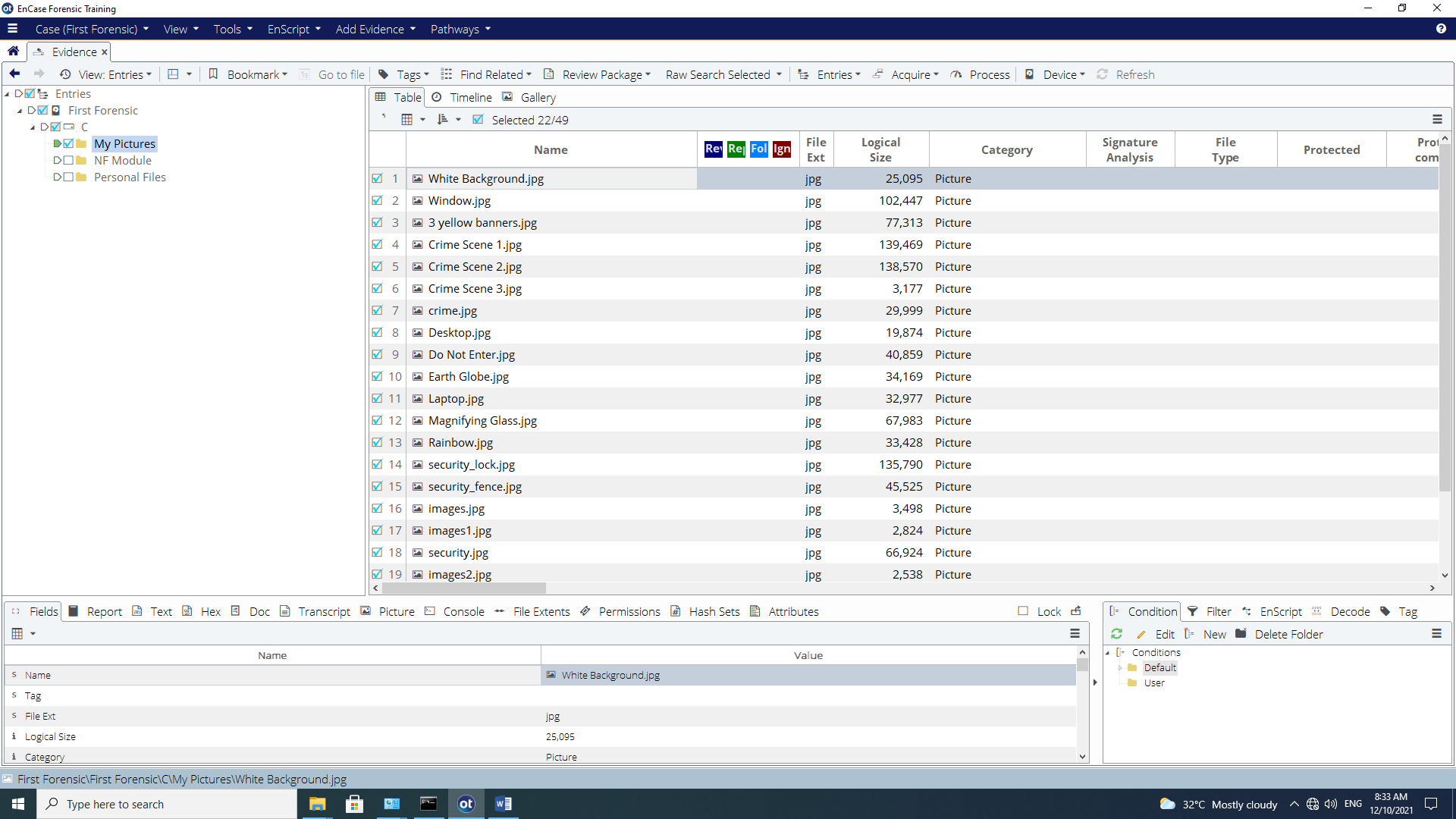


Figure C-4: “Blue-checking” entries and the Dixon Box

**Table Pane**

The Table Pane consists of three views:

* Table View,
* Timeline View and
* Gallery View.

By default, the Table Pane is in the Table View. Within this view are the subfolders and file objects that are contained within the folder(s) and are highlighted or included (Set Include) in the Tree Pane.

Highlighting an object in the Table Pane displays the object’s location in the Status Bar (bottom left-hand corner)

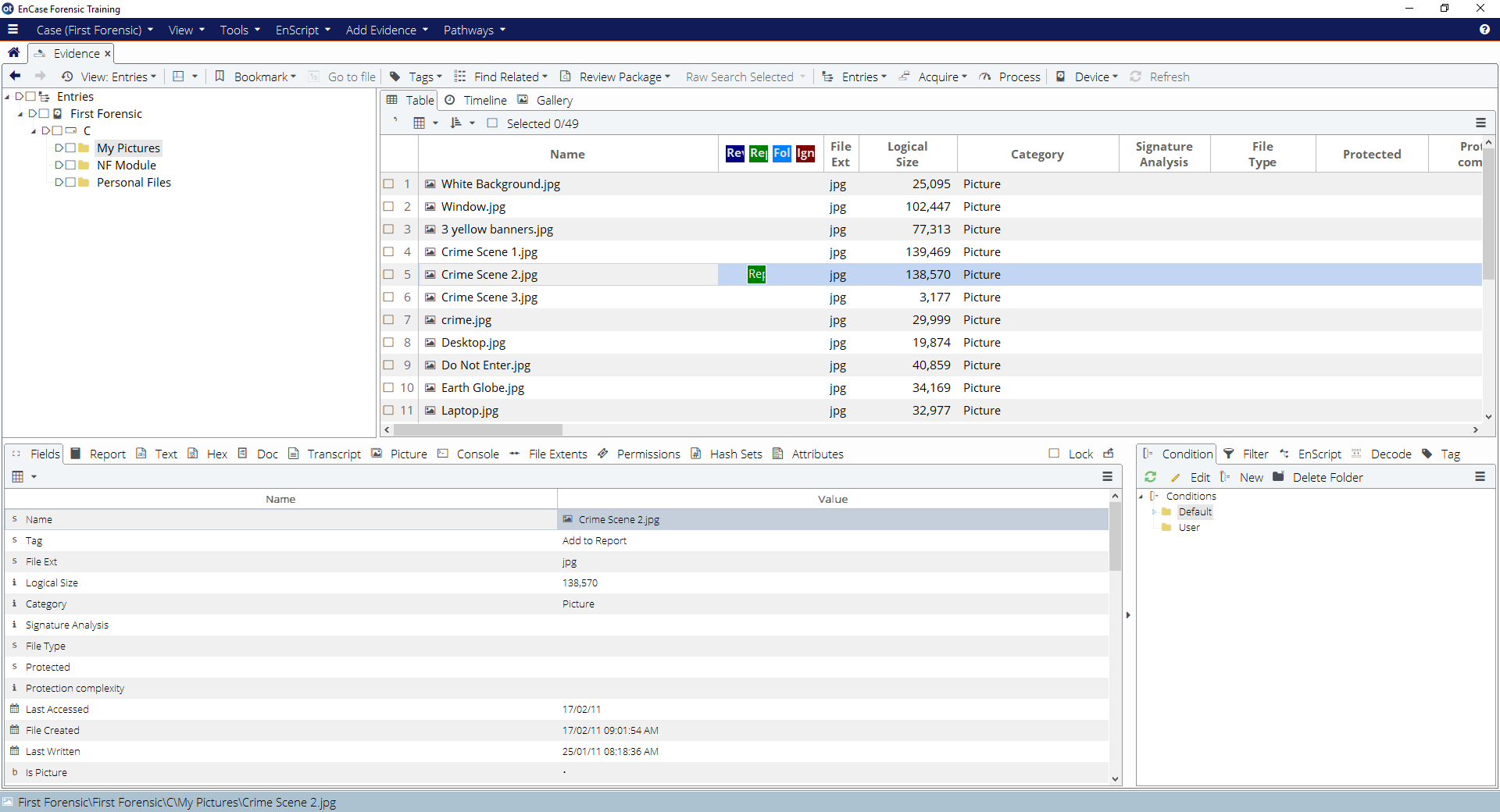


Figure C-5: Highlighting Crime Scene 2.jpg

The Table view in the Table Pane displays many columns of information about the displayed entries, notable, Name, File Ext, Logical Size, Category, Signature Analysis, File Type, Protected, etc.

The Timeline View in the Table Pane shows patterns of different types of dates and times.

The Gallery View in the Table Pane displays images in thumbnail view. These images are displayed (by default) based on their extension.

**View Pane**

The View Pane displays the contents of the item highlighted in the Table Pane. The View pane provides several ways to view file content:

* The *Fields tab* displays all information available regarding an item. All fields shown on this tab are indexed.
* The *Report tab* provides a readable, formatted view of metadata.
* The *Text tab* displays files in ASCII or Unicode text.
* The *Hex tab* displays files as straight hexadecimal.
* The *Decode tab* lets you decode swept data in the Hex tab in a variety of different formats. You can then make that sweeping text into a bookmark.
* The *Doc tab* provides native views.
* The *Transcript tab* displays the same formats as the Doc tab, but filters out formatting, allowing you to view files that cannot display effectively in the Text tab.
* The *Picture tab* displays graphics files.
* *File extents* shows the sector information about the selected file. This works on entry evidence only.
* The *Permissions t*ab displays the security permissions for a file, including the name and security identification number (SID) of the user(s) who have permission to read, write, and execute a file.
* *Hash sets* show hash information for entry evidence only.

EnCase checks the contents of the file highlighted in the Table Pane to see if it is an image that can be decoded internally. If so EnCase will provide the ability for the user to select the Picture view in the View Pane and display the image.

If numerous files highlighted in the Table Pane are images, EnCase will default to the Picture view for subsequent images. Likewise, if a Microsoft Word document is highlighted, Encase will change the default view in the View Pane to Text.

If the examiner wishes to have every highlighted item displayed in the Hex or Text view, he need to click on the square box beside **Lock** to lock that view.

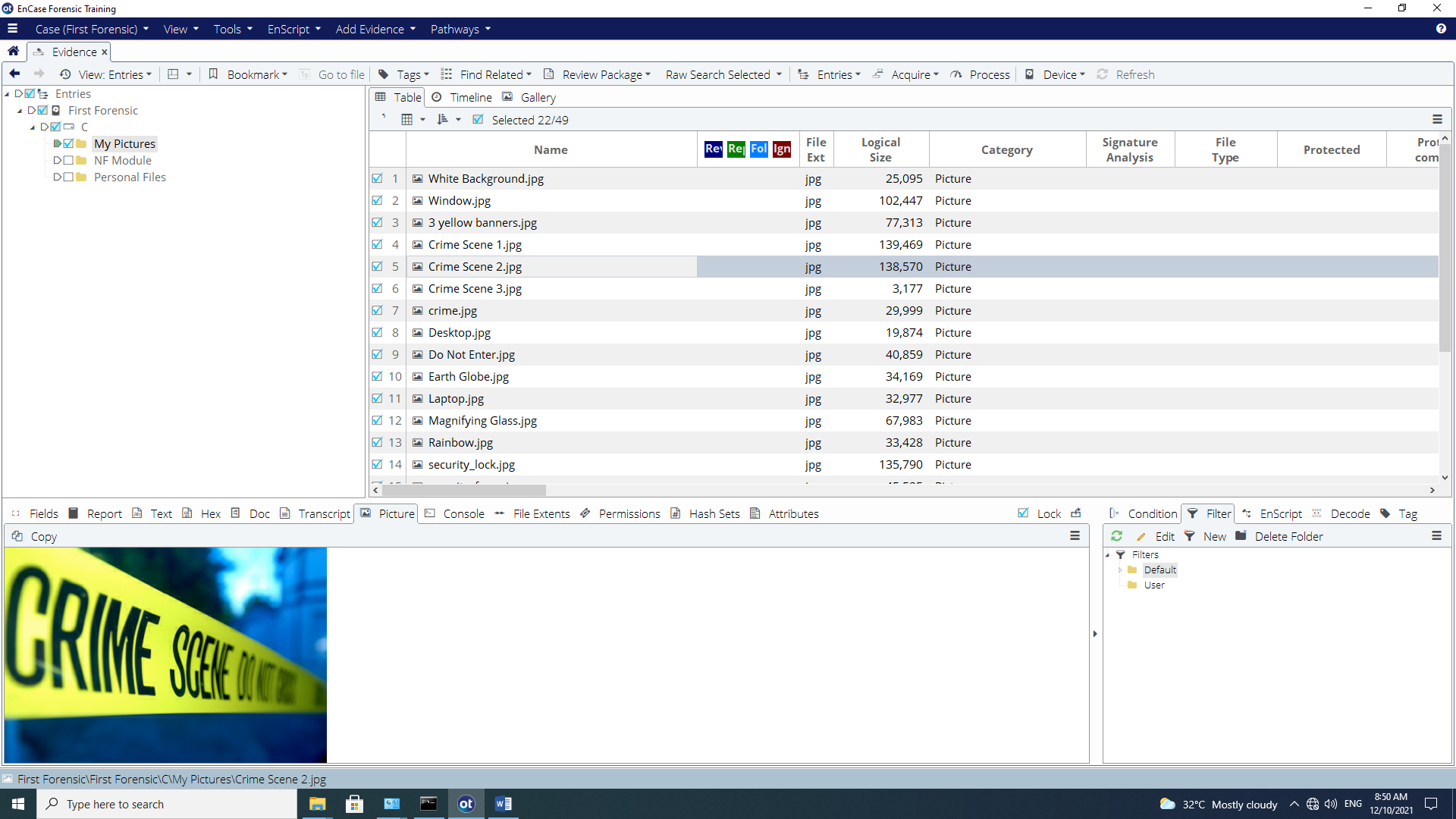


Figure C-6: Picture view in View Pane

To unlock, remove the blue check from the box.

Here is the same picture viewed in hexadecimal.

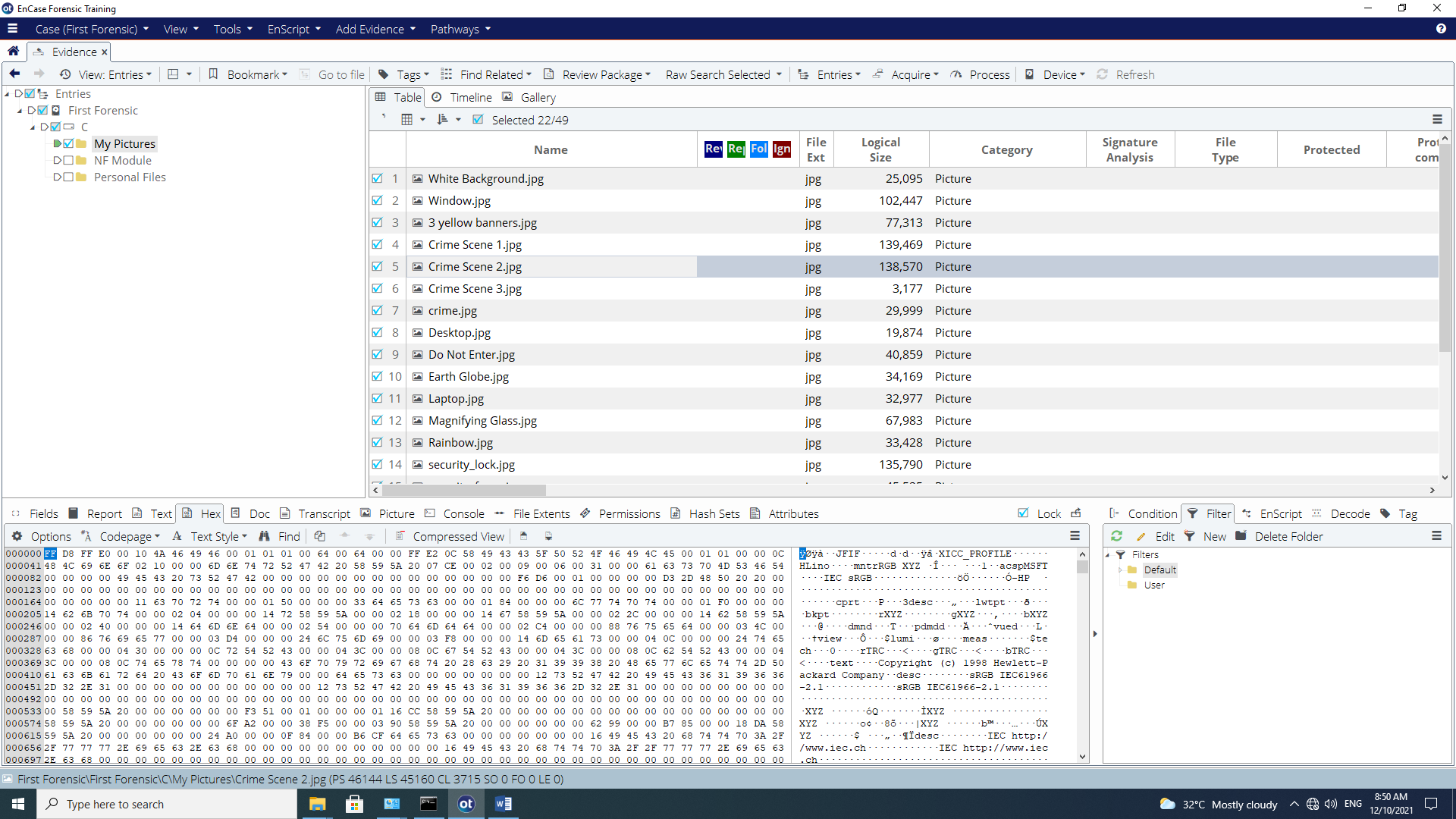


Figure C-7: Viewing in the View Pane as Hex

Here is a word file displayed in Doc view.

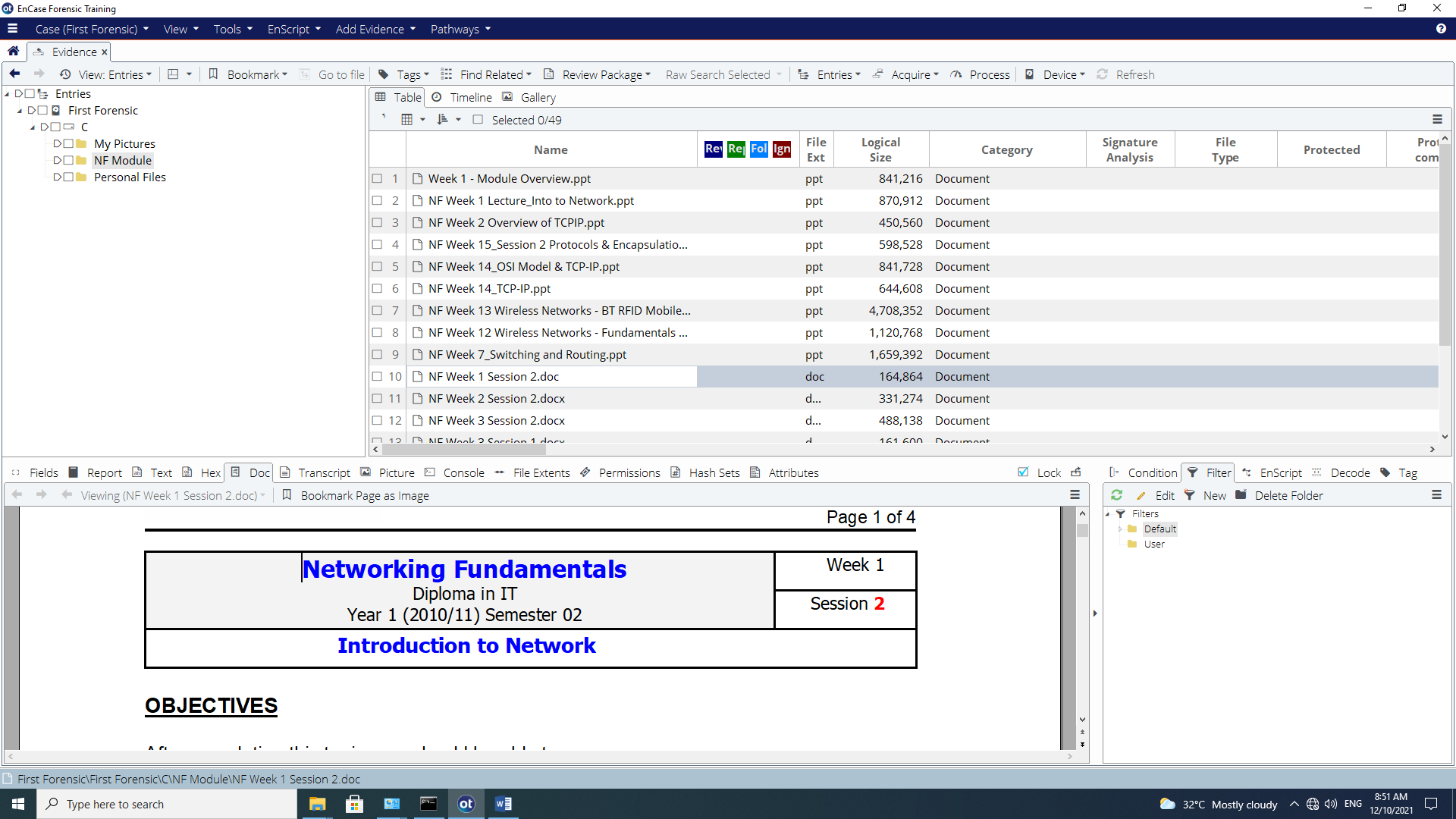


Figure C-8: Viewing in the View Pane as Doc

A ppt file displayed in Doc view.

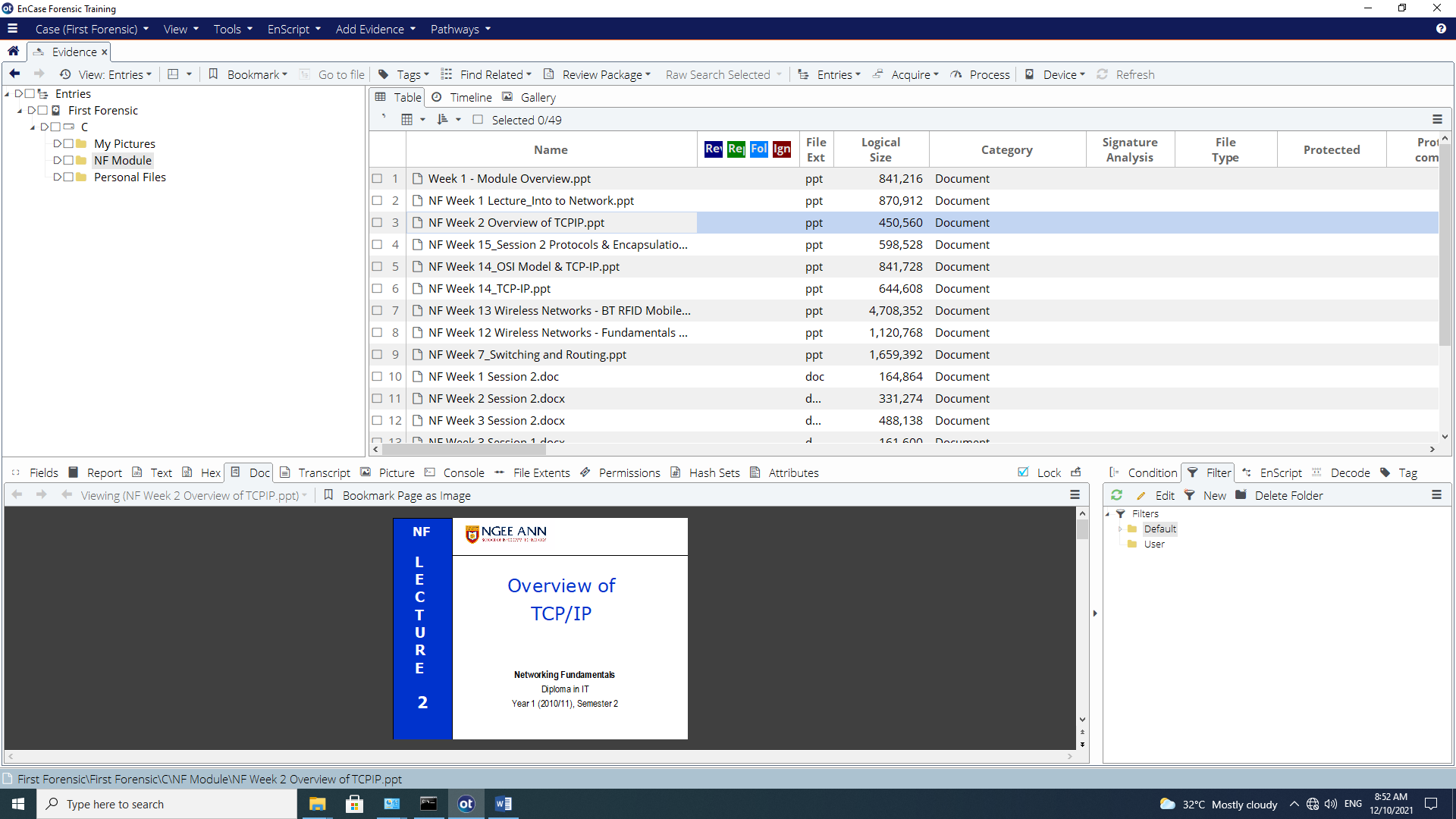


Figure C-9: Viewing in the View Pane as Doc for Powerpoint file

Q3: What are the 2 ways to view pictures/images in EnCase?

Use Picture in View pane or use Gallery in Table pane.

The text format may be improved by altering the text style from the **Text Styles** tab in the Filter Pane.

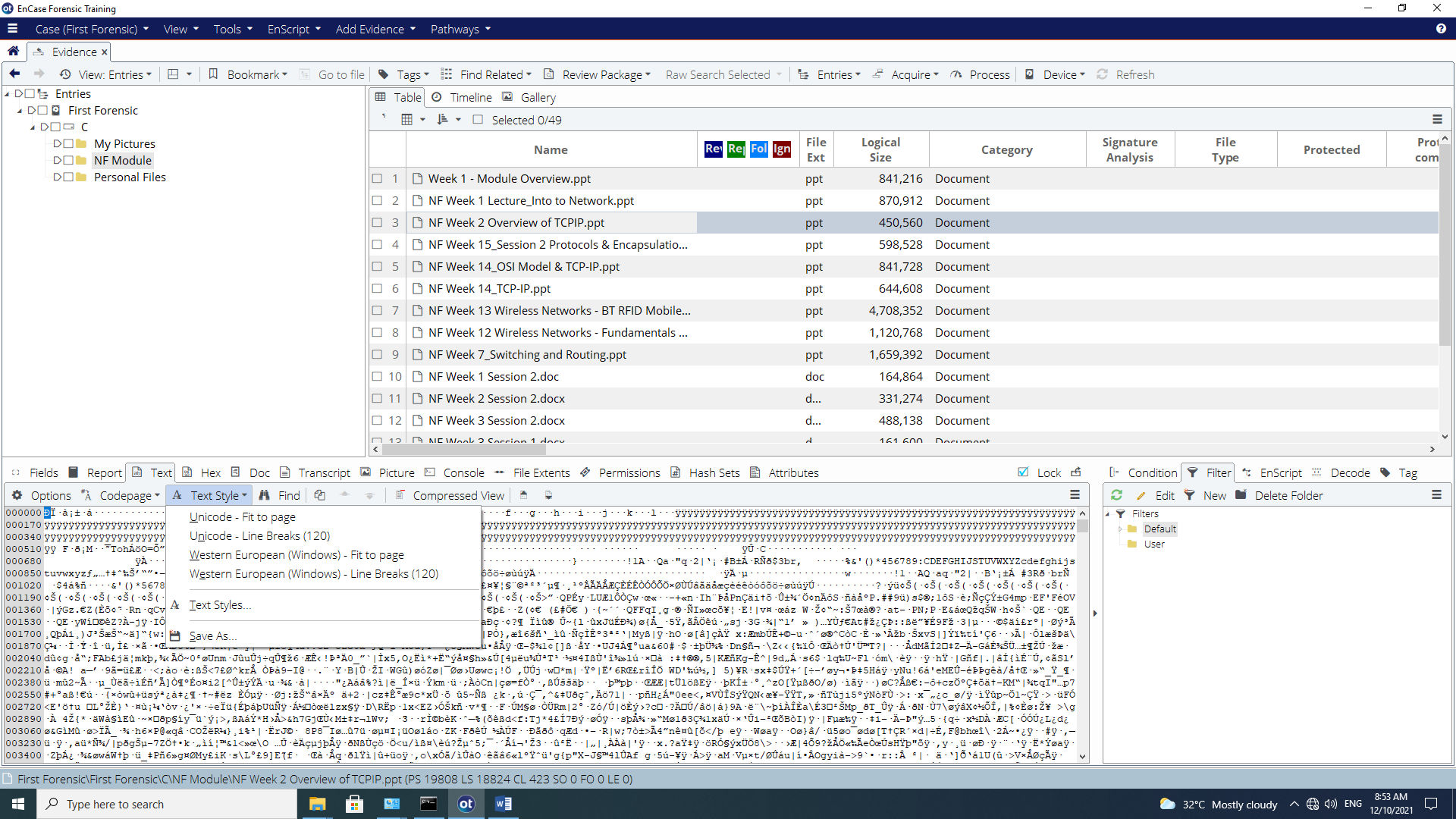


Figure C-10: Changing text style for View Pane

Q4: Do some research to find out more about the following character representations.

|  |  |  |
| --- | --- | --- |
|  | Character Representation | Description |
| 1 | ASCII |  |
| 2 | ISO Latin |  |
| 3 | Unicode |  |

The status bar found at the bottom of the screen provides information on the current position within a case.



Figure C-11: Status Bar

The codes are translated as follows:

**PS** Physical sector number

**LS** Logical sector number

**CL** Cluster number

**SO** Sector Offset – The distance in bytes from the beginning of the sector

**FO** File Offset – The distance in bytes from the beginning of the file

**LE** Length – The number in bytes of the selected area

Q5: Look for a file named *Rainbow.jpg* and record the following.

|  |  |
| --- | --- |
| PS | 46888 |
| LS | 45904 |
| CL | 3808 |
| SO | 75 |
| FO | 75 |
| LE | 1 |

Q6: Why is it important to know the current position within a case?

Text

Description automatically generated

Reflection: What have you learnt through this practical exercise?

A lot.

- The End -