|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 2 |
| Practical 3 |
| **Searching and Bookmarking** | |

**OBJECTIVES**

To be able to perform:

1. Searching using keywords.
2. Bookmarking data found in search hits.

Preparation: (the following steps must be performed each time you use EnCase.)

1. Boot the computer to Windows 10.
2. Ensure that the Windows Firewall and Symantec Anti-virus are turned off.
3. Enable the wired network adapter and set the IP address to dynamically assigned, then disable the wireless network adapter.
4. Ping 10.1.0.1 and ensure that you receive reply from the SAFE server (Secure Authenticate for Encase)
5. Start EnCase v21.3 application.
6. You should see the panel showing “**EnCase Forensic Training**” rather than “EnCase Acquisition”.
7. Refer to the case write-up on Conspiracy.
8. Tutor will be providing the evidence files: ***Laura.EXX***

**If you still do not see “EnCase Forensic Training”, inform your tutor.**

**Creating a case Laura and adding Evidence Files to the case**

**Refer to Week 1 Practical 1 for detailed steps.**

Create a new case in EnCase. Name the case as *Laura*.

Add Laura evidence file into the case.

Laura evidence file can be found in **C:\Evidence Files\Laura**

*Note: It is not necessary to add files E02, E03, E04 etc. as they are added automatically by EnCase.*

**Part A: Searching the Case**

EnCase provides a powerful search engine to locate information anywhere on the physical or logical media. After creating a case file, a raw keyword search operation may be conducted. The method of query detailed is called “raw keyword searching”. It bears this name because certain words or string text is used to search against raw binary evidence data. Keywords may be created with various options.

Within Encase, there are different methods to conduct a raw keyword search. It depends on the data set against which you want to focus your keyword searching. Encase allows raw keyword searching against all evidence, just selected evidence or a narrowed down result set.

We shall concentrate on searching by selected evidence using Raw Search Selected (i.e. a raw keyword search against blue checked or selected items).

Q1. Explore 3 different ways in which you can create raw keyword searching. (You may need your tutor’s help)

Raw Keywords can be done through:

* Search for keywords – conducted within the Evidence processor
* Raw Search All – conducted from the Evidence view
* Raw Search Selected – conducted from the Entries view

Adding Keywords

Always create an appropriate keyword list prior to beginning the case.

In Encase, click **Open** on Laura Evidence file to proceed to the Evidence Viewing (Entry) page, **blue-check** D 🡪Users 🡪 encase01. Then click the **Raw Search Selected** menu. This will allow keyword (s) to be added under the **New Raw Search Selected**.

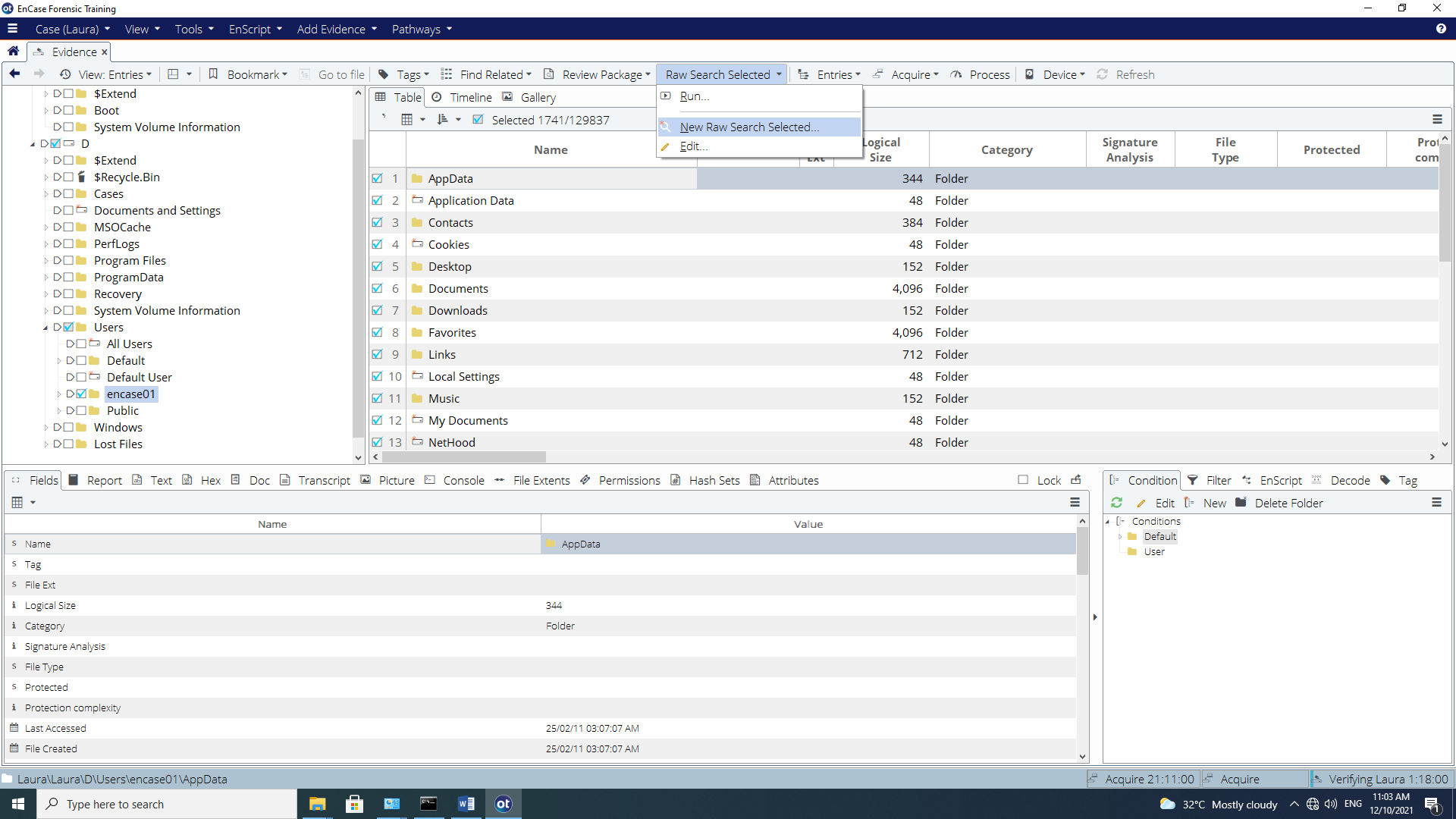


Figure A-1: “New Raw Search Selected in Evidence view

Note that the default location for saving this keyword file is within the User’s Document\ Encase\Search\ folder (.Keywords). You can rename your keyword search folder. Once you have built your investigative keyword files, you can easily run them from the Raw Search Selected menu with future cases.

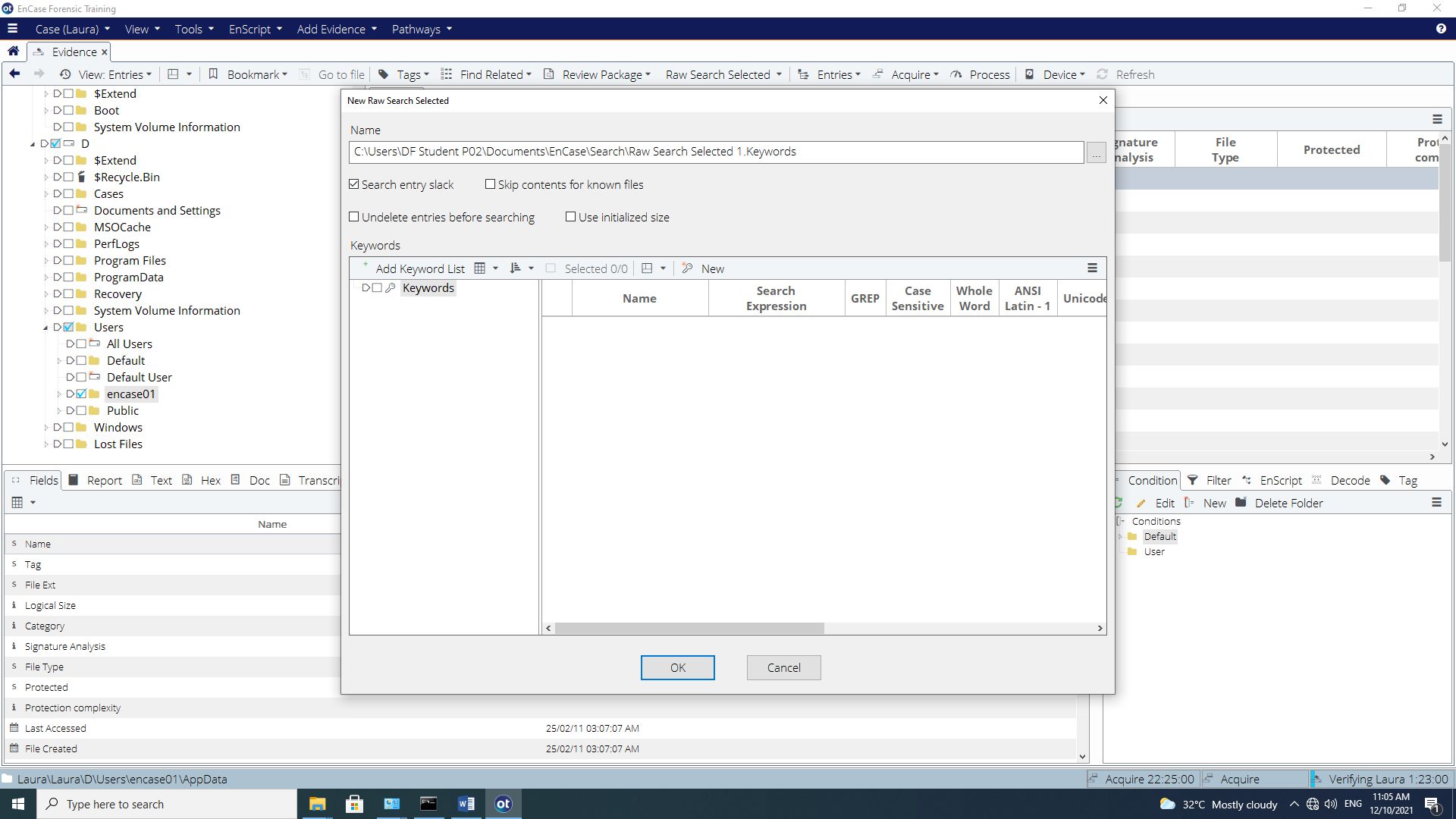


Figure A-2: New Raw Search Selected Window

The searching functions are listed as follows:

* Search entry slack – Search the slack area of the selected files along with the file’s content.
* Skip contents for known files – If utilizing analysis, this option can help to reduce the amount of searching by excluding files with hashes matching the hash sets categorized as Known.
* Undelete entries before searching. – Encase will attempt to find the starting cluster of a delete file. It will assume the unallocated clusters, following the starting cluster, belong to it in a contiguous manner. By default, Encase will only search the unallocated clusters individually, so it may miss content spanned across a contagious cluster boundary unless this option in checked.
* Use initialized size – Encase will search the initialized size of a file rather than the actual logical size. Using this option would speed up searching time by limiting the amount of area to search.

(For this exercise, tick the **Search entry slack)**

To perform only a single entry search, select the **New** button. This will bring up the **New Keyword** entry screen as shown below:

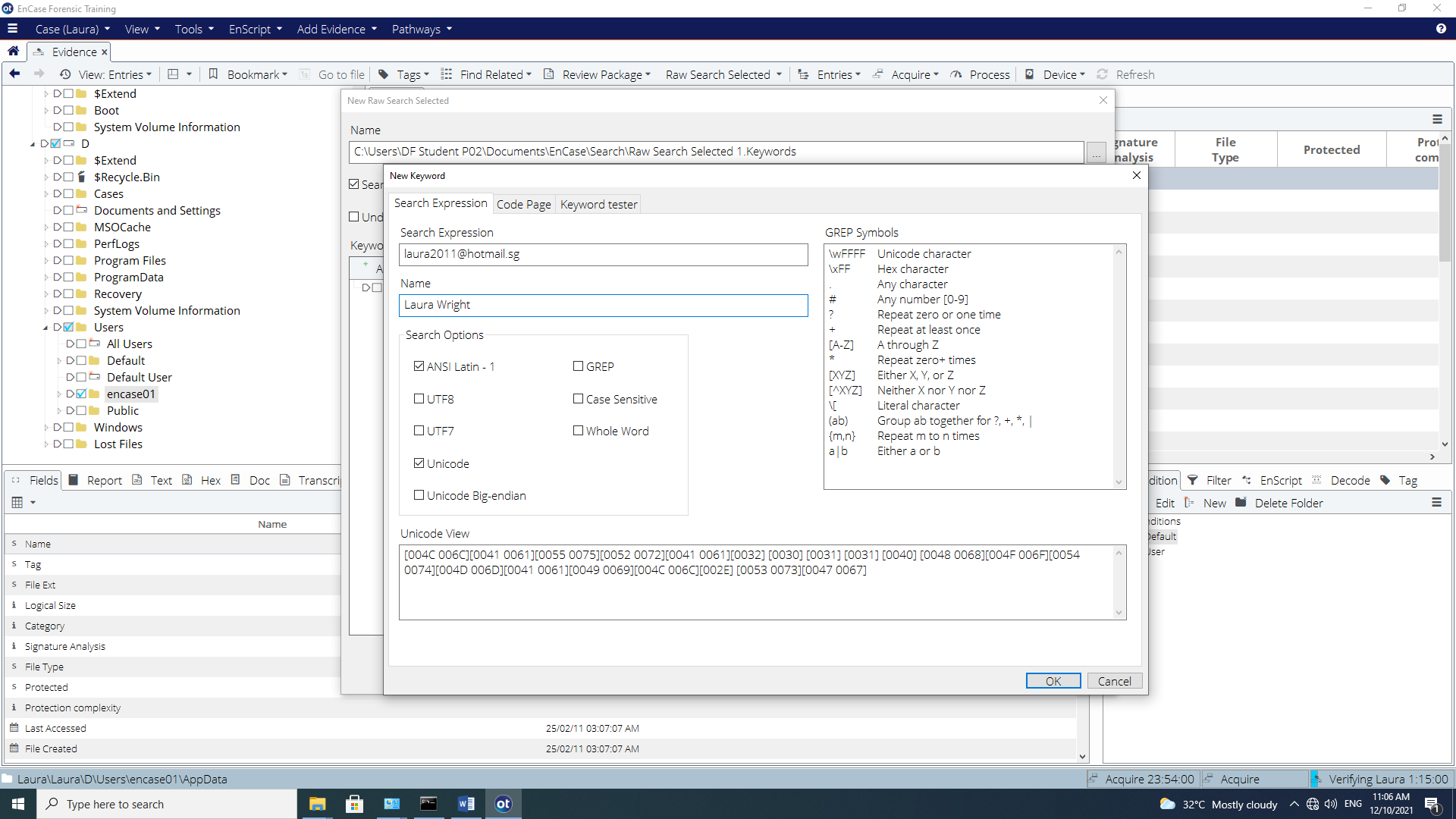


Figure A-3: Entering a Single Keyword

Enter Laura’s email address as keyword: [laura2011@hotmail.sg](mailto:laura2011@hotmail.sg) in the Search Expression field and Name it as Laura Wright. Select the rest of the options as shown in Figure A-3.

Explore the following options which can be set from this window:

* **ANSI Latin -1** – The default option will search for characters within the ANSI Latin-1 code page, which is the default code page for the Microsoft Windows operating system.
* UTF-8 – This is the 8-bit for of Unicode. It offers foreign language support. (more for HTML)
* UTF-7 – UTF-7 is a special format that encodes Unicode characters within US-ASCII in a way that all mail systems can accommodate. (more for emails)
* **Unicode** – Most MS Office products use Unicode as does Windows 2000, XP and Vista. *Enabling both ANSI Latin-1 and Unicode option will locate both ASCII and Unicode characters.*
* Unicode Big-Endian
* 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.
* Case Sensitive
* Whole Word – EnCase will locate the keyword as a whole word not within a larger word.

Q2. We have selected **Unicode** and **ANSI Latin -1** in our search options. What selections would you make if you are searching for Chinese characters found in an email message?

UTF-8 and UTF-7

Click **OK** and **OK** again at the Keywords window will start the keyword searching…

Searching updates can be seen at the lower right corner.

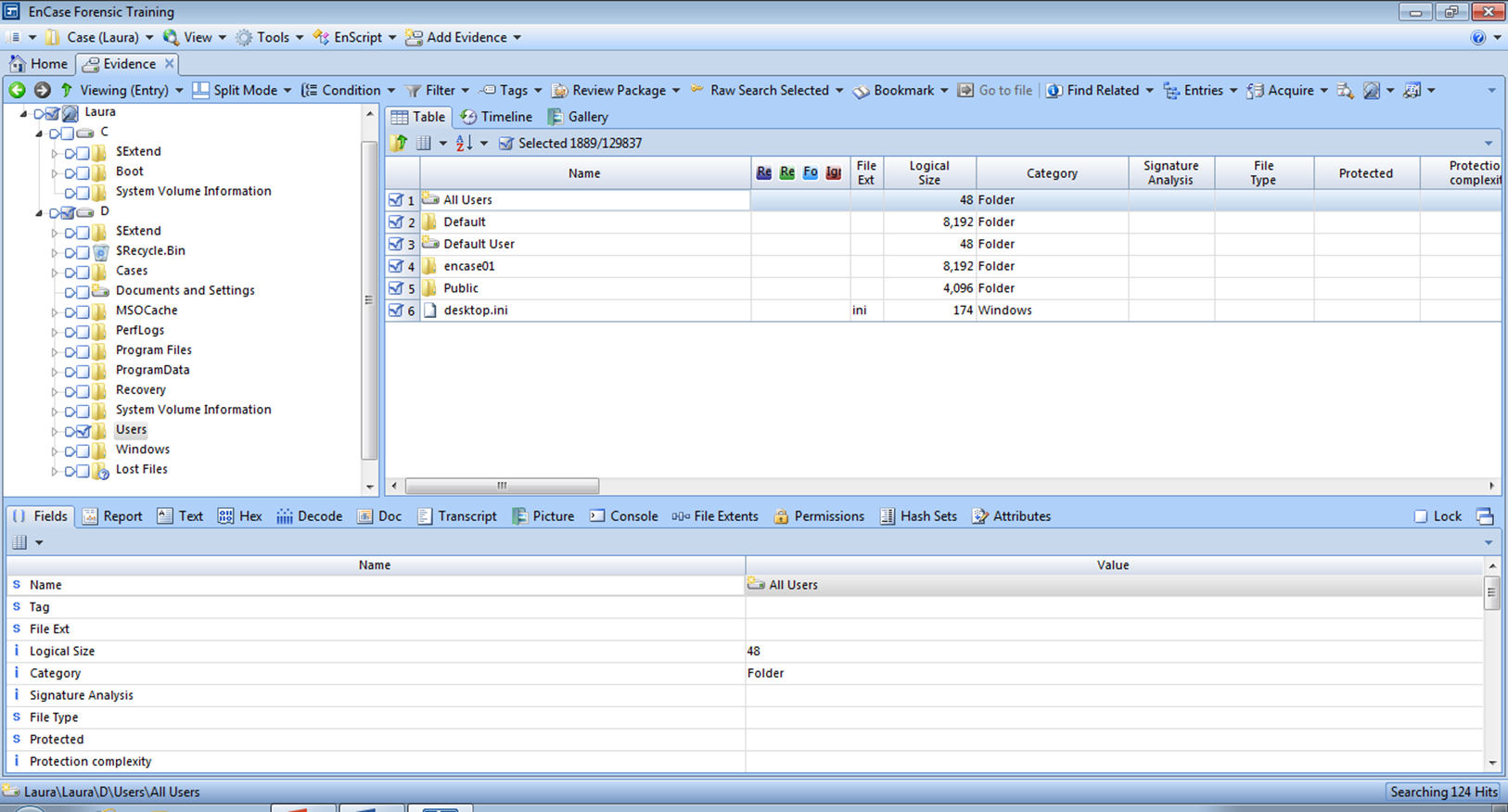


Figure A-4: Keyword Search Status

The keyword you have created will also be saved to the .Keywords file you named. (Default location for saving this keyword file is within the User’s Document\ Encase\Search\ folder (.Keywords). )

After Keyword Searching is Complete

The Result tab will automatically open upon completion of the search process. This tab is where you are initially taken to review the keyword search hits.

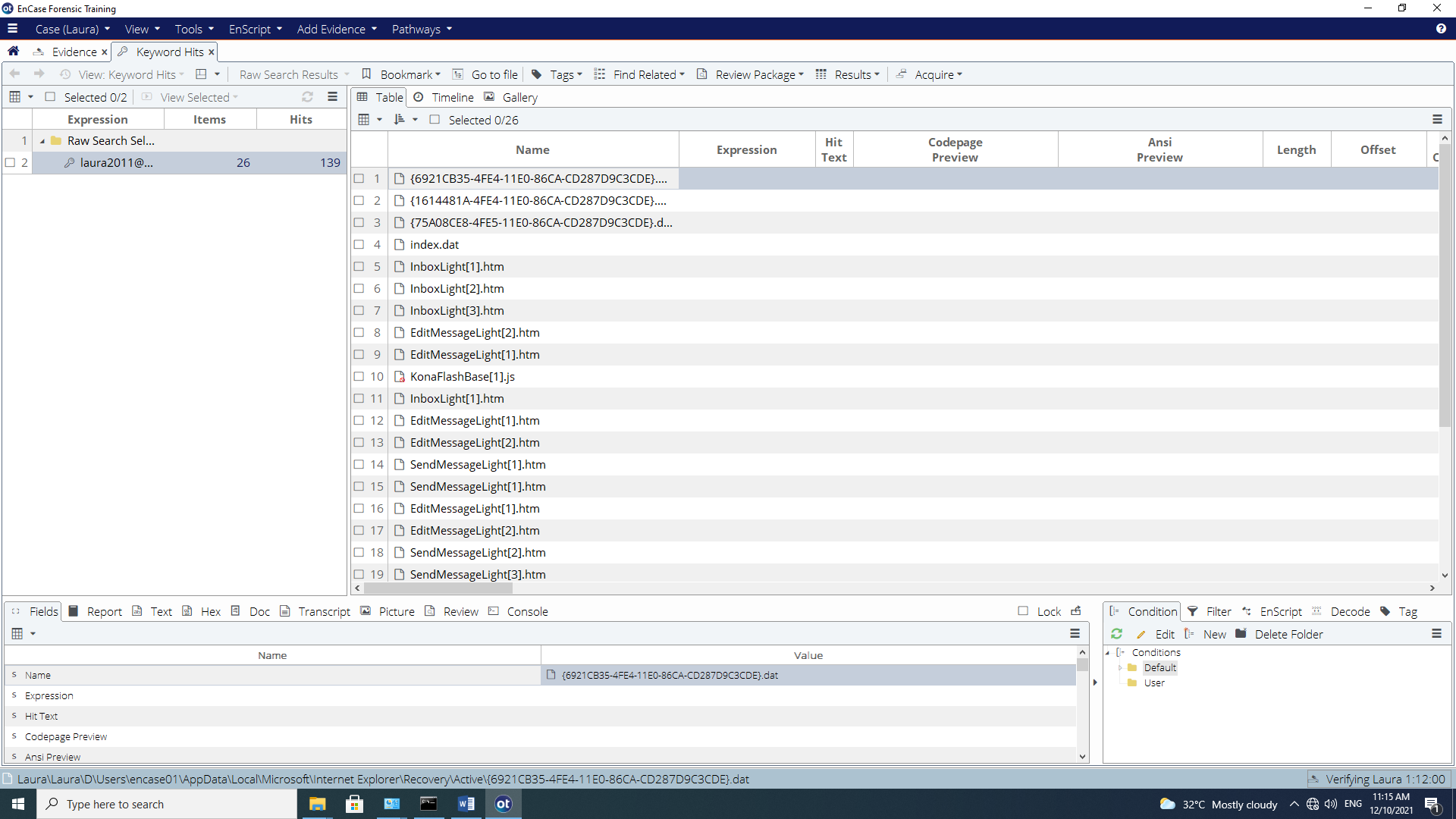


Figure A-5: Keyword Search Results

Viewing the Search Hits by Keyword

To view the search hits listed by the keyword, select **View** menu and choose the **Results** tab.

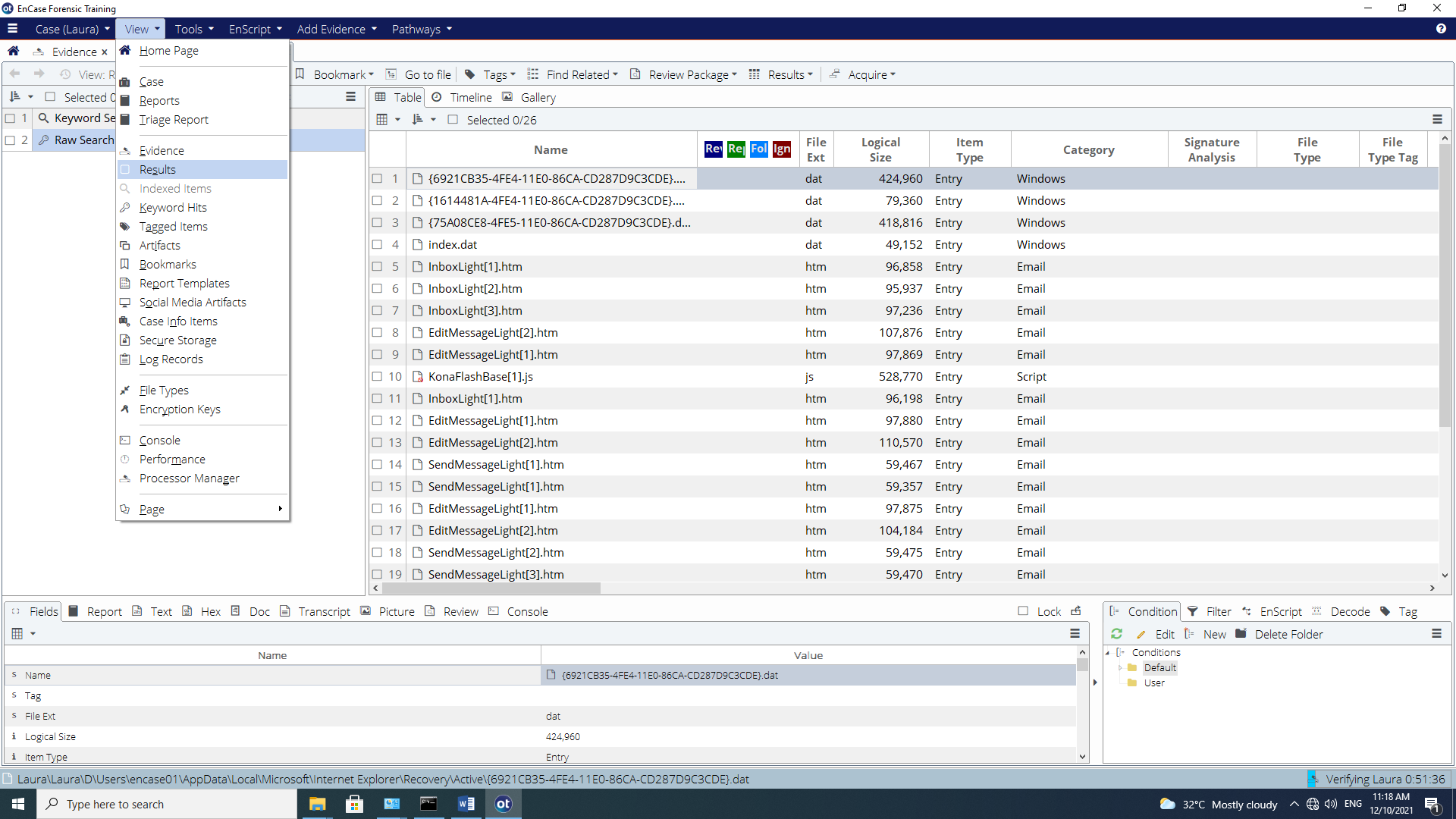


Figure A-6: Navigating to the Search Tab

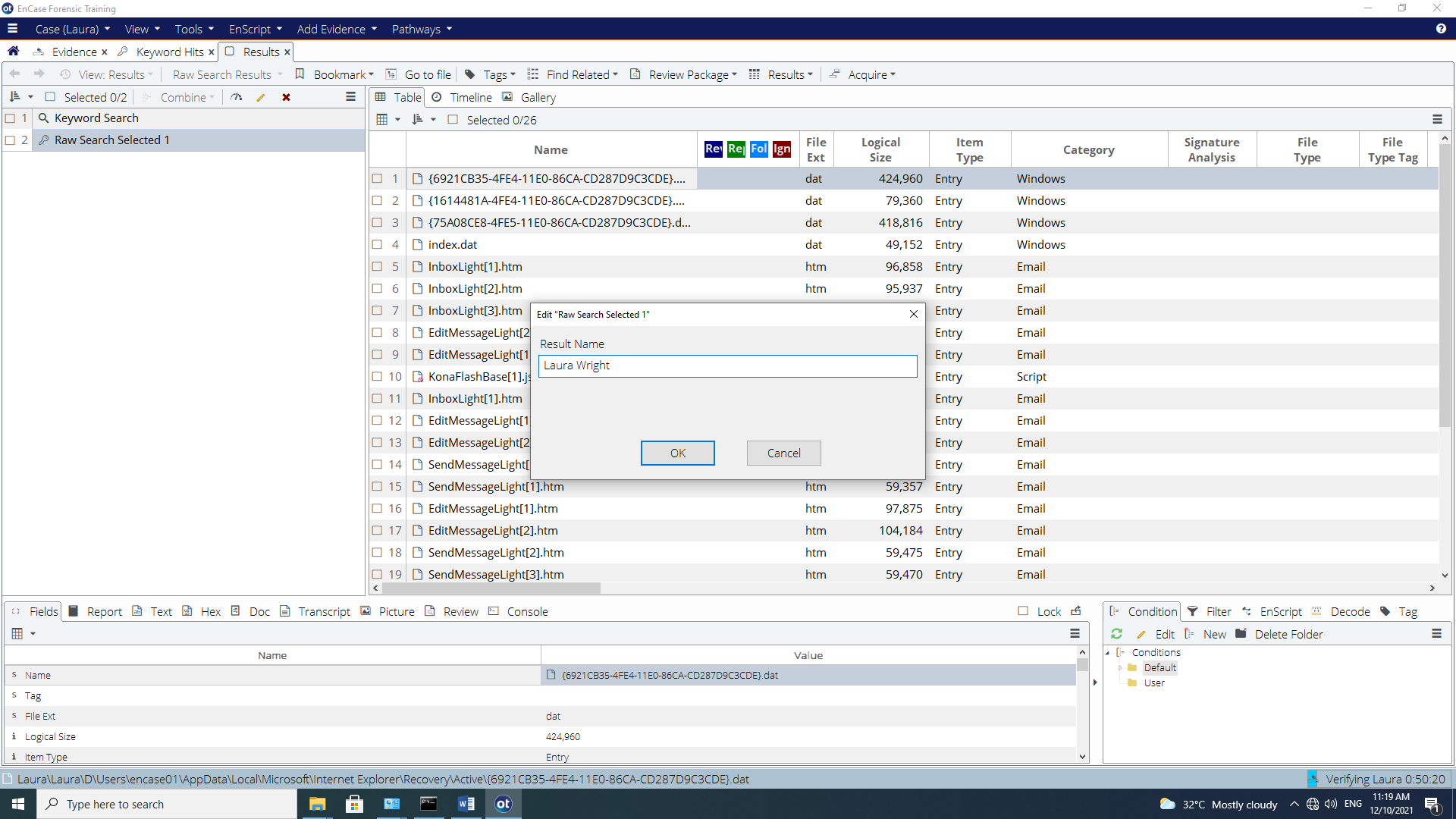
You can change the name of your keyword search by either by double-click the keyword or right-click at the keyword and select edit.

Figure A-7: Modifying Keyword Name

Reviewing Keyword Search Hits

The keyword search hits can be reviewed from either the **Results** tab or **Keyword Hits** tab.

In Keyword Hits, Click the **numbers** in the **Items** or **Hits** column to display the search hits.

At the Table view, the contents can be viewed in the Text tab of the View Pane. The search hits will be highlighted in yellow by default. (Essentially, we are searching for raw text or ASCII code page representation of the binary stored on disk).

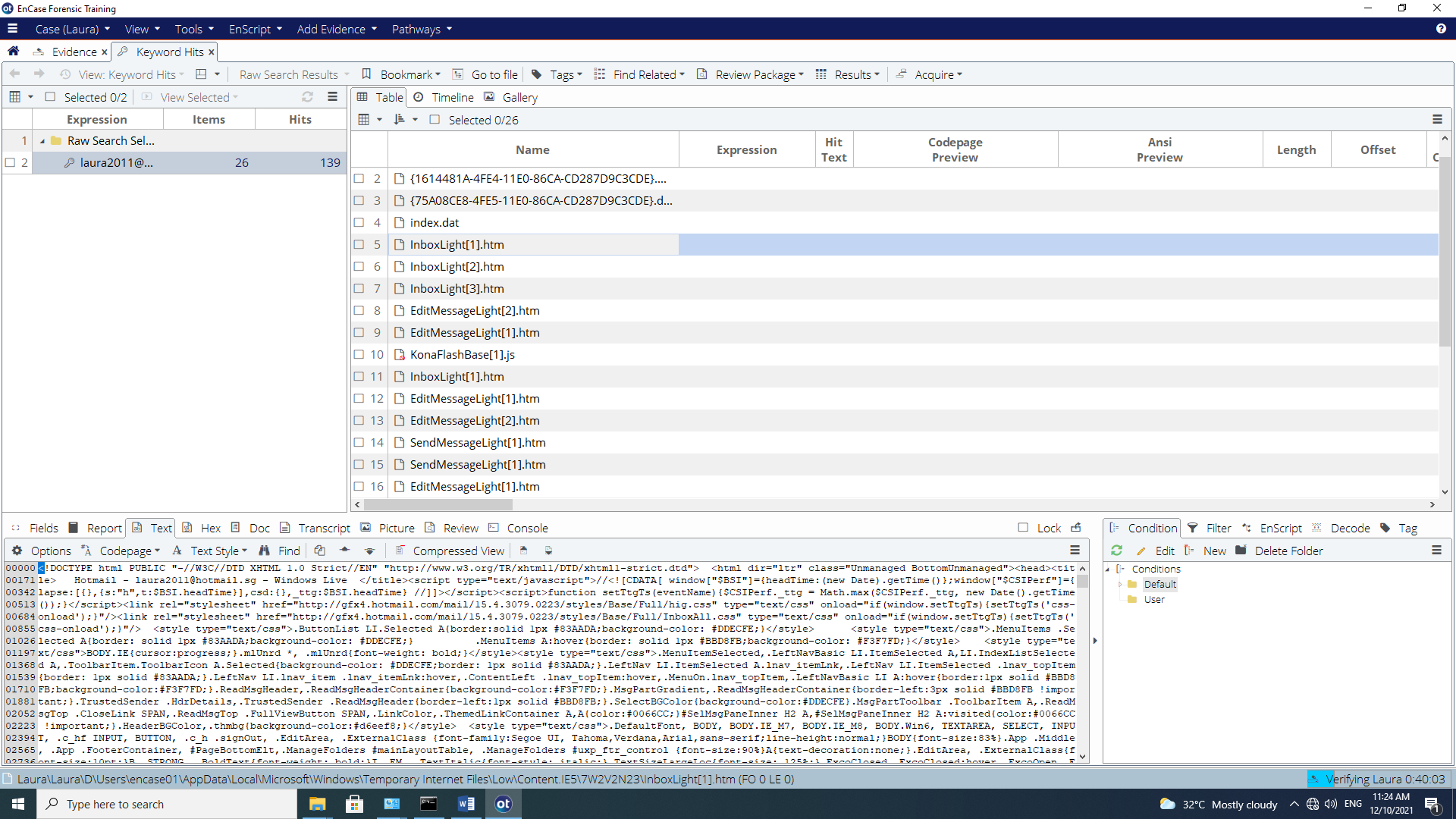


Figure A-8: Reviewing Search Hits by Keyword

[Note: You can also create a keyword list related to the investigation. This can be done by selecting **Add Keyword List.** at the **New Raw Search Selected** window. The Add Keyword List dialog box will appear:

[Explore and try this yourself.] You may seek tutor’s help.

Q3. Other using email addresses as keywords, what other keywords can you use to search for the case?

Word or excel files

Biding

Price

Quotation

customer

**Part B: Bookmarking**

EnCase allows the examiner to document files, sections of files, or other objects of interest within the case. This is referred to as *bookmarks*, and the folders where they are stored are bookmark folders. Bookmarks and the organization of their folders are essential to creating a solid and presentable body of case evidence. You can examine bookmarks closely for their value as case evidence, and additionally, use the bookmark folders and their data items to create case reports.

Understanding Bookmarks

There are several different types of bookmarks. The more common ones are mentioned here.

**Highlighted Data Bookmark** – Created by sweeping data. This is normally done through Raw Text bookmark and /or Data Structure bookmark

**Notable File Bookmark** – Use notable file bookmarks to mark one or more files. You can assign notable files into a bookmark folder either singly or as a selection of files.

**Notes Bookmark** – Allows the writing of comments into the Report.

Bookmarking Highlighted Data: Raw Text Bookmarks

To create a raw text sweeping bookmark:

1. In the Evidence tab, go to the Table pane and select the file containing the content you want to bookmark.
2. In the View pane, click the appropriate tab (Text, Hex, or Decode).
3. Highlight the raw text you want to bookmark.
4. On the menu bar, click **Bookmark 🡪 Raw text** or right click the highlighted text and click **Bookmark 🡪 Raw text**.

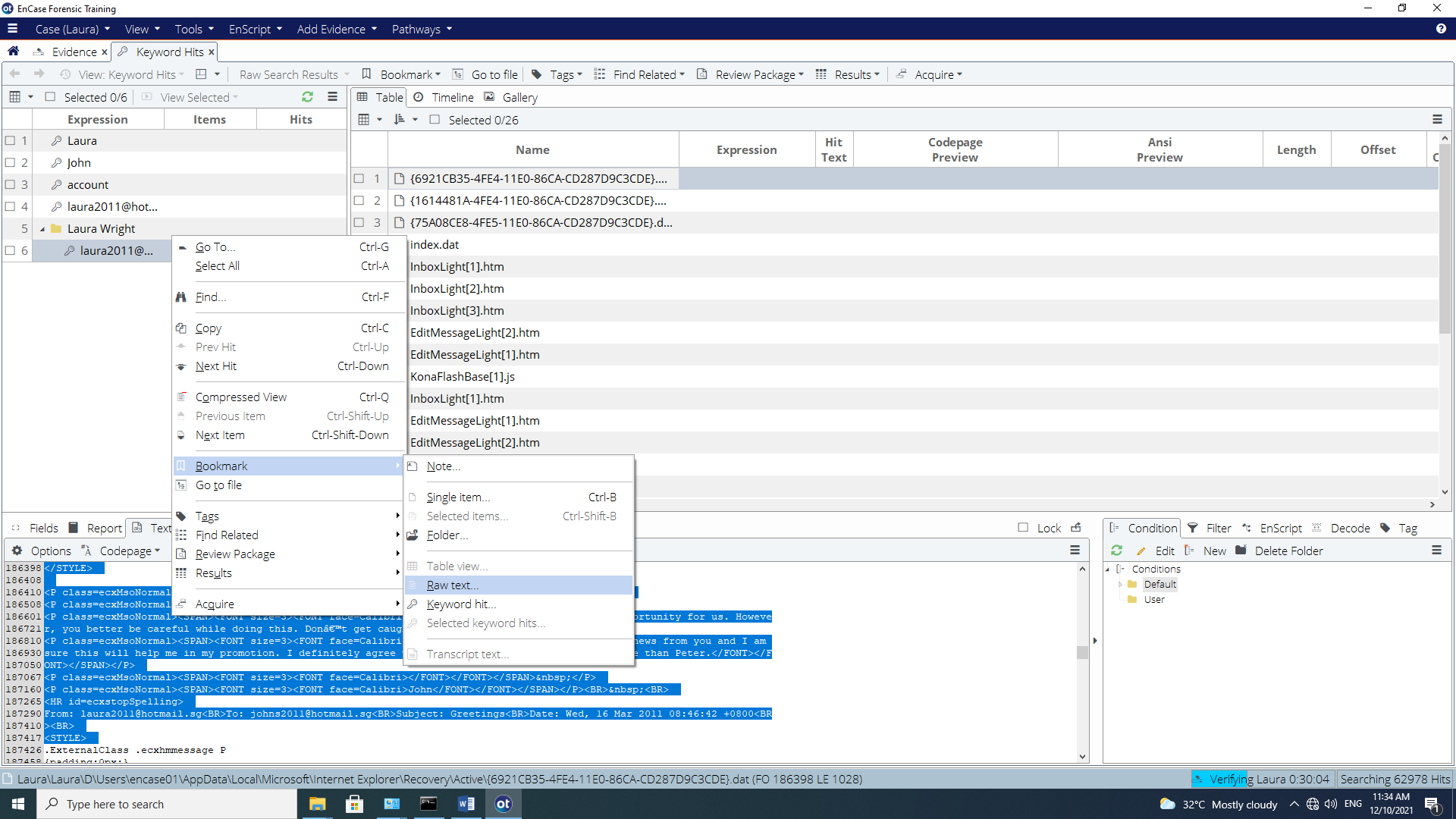


Figure B-1: Booking Raw Text

The Raw Text dialog displays. Type some identifying text in the **Comment** box on the **Properties** tab that makes it easy to identify the bookmarked content.

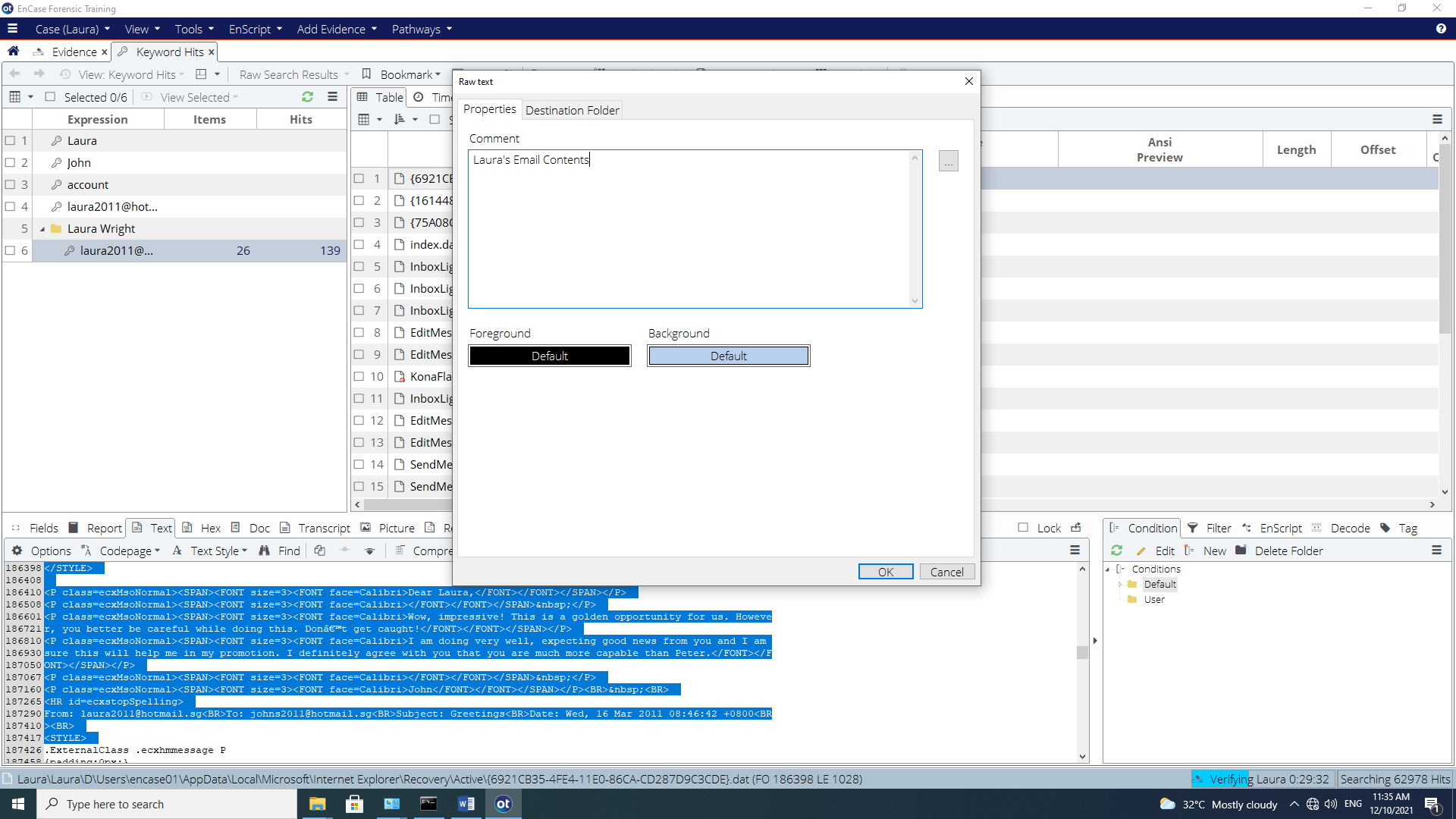


Figure B-2: Comment for Bookmark

Click the **Destination Folder** tab, which displays the bookmark folder hierarchy for the current case, and click the bookmark folder where you want to place this sweeping bookmark. You can either create a **New Folder** or make use of one of the appropriate sub-folders. (Note that you can always rename bookmark folders or move the bookmark later).

In this case, enter “**Email Content**” in the **New Folder** box. Click **OK** to create the bookmarked content in the folder.

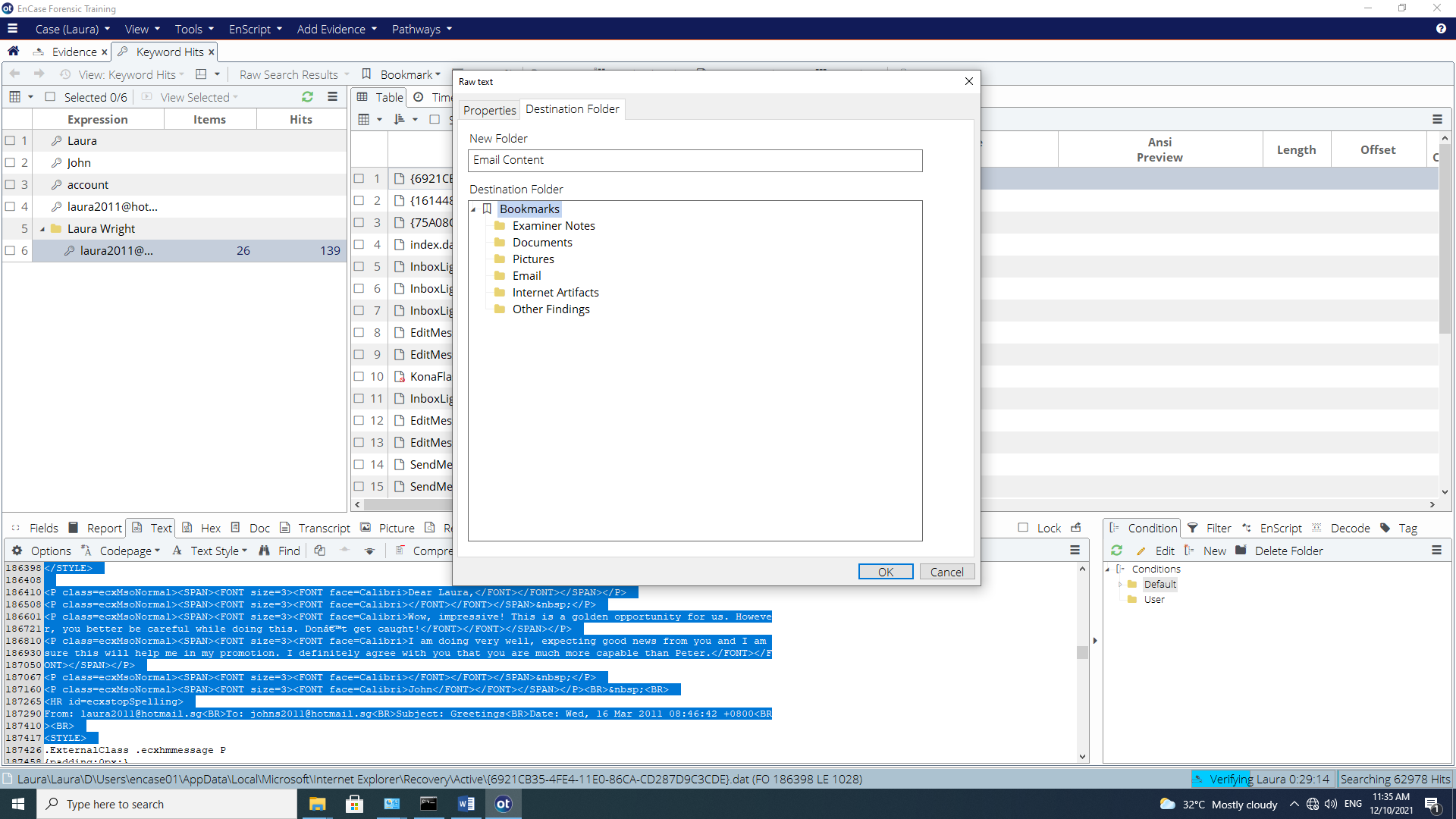


Figure B-3: Creating New Folder for Bookmark

By navigating to the **Bookmark** tab through **View 🡪Bookmarks** and clicking on the newly created folder (i.e. **Email Content**), the raw bookmarked raw text in the **Report** tab of the **View Pane** can be seen:

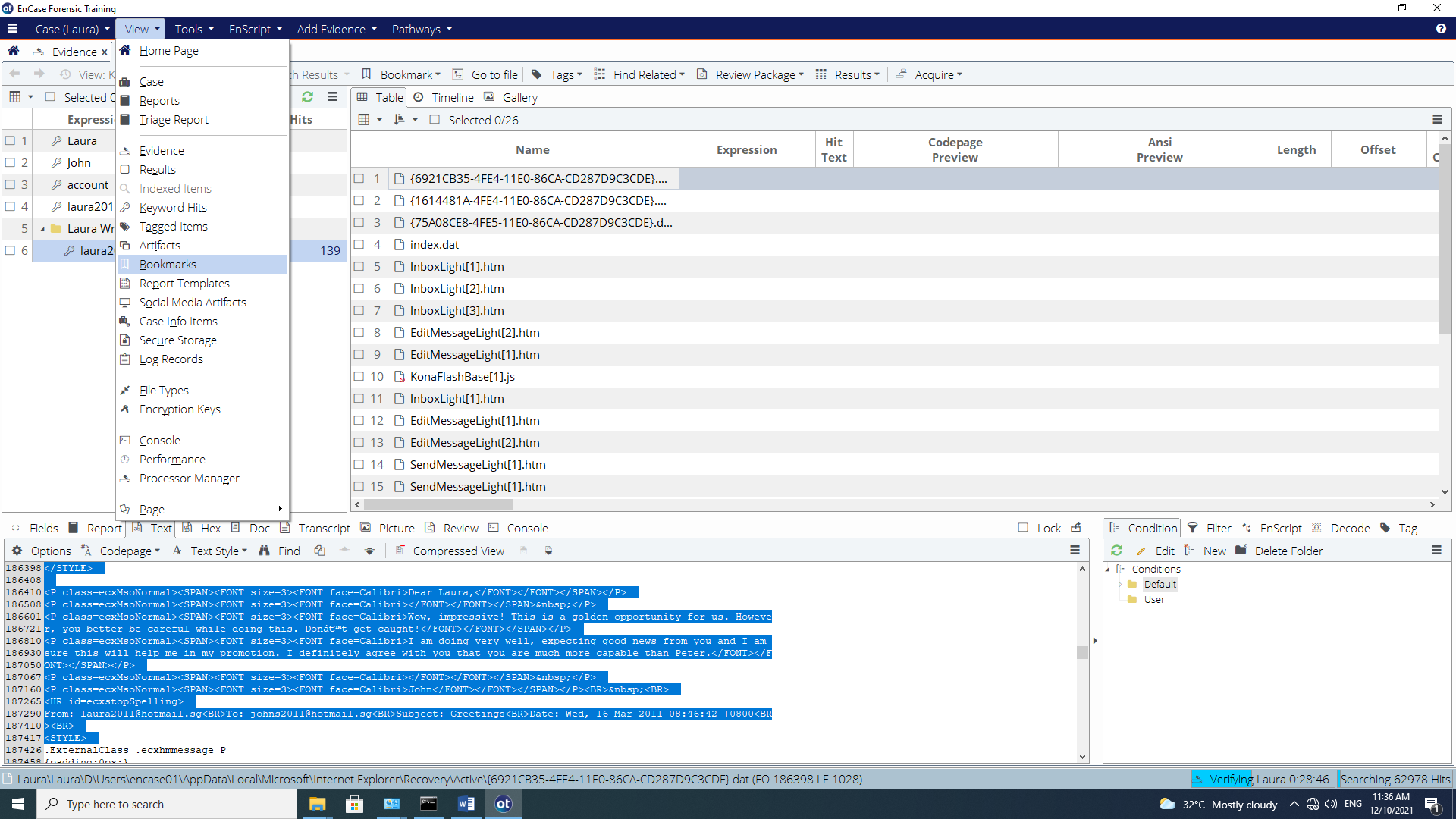


Figure B-4: Bookmarked Raw Text

Bookmarking a Notable File

Notable File bookmarks are used to identify individual files that contain important information to the current case. If the file is not an image file, the contents of the file will not be bookmarked. Only the administrative information about a non-image file is displayed in the report.

Single Notable File Bookmarks

To bookmark a single notable file:

1. From the **Evidence Tab**, select the folder **D:\Users\encase01\Documents** in the Tree pane. In the Table pane, select (Blue check) Peter’s Email Account .txt.

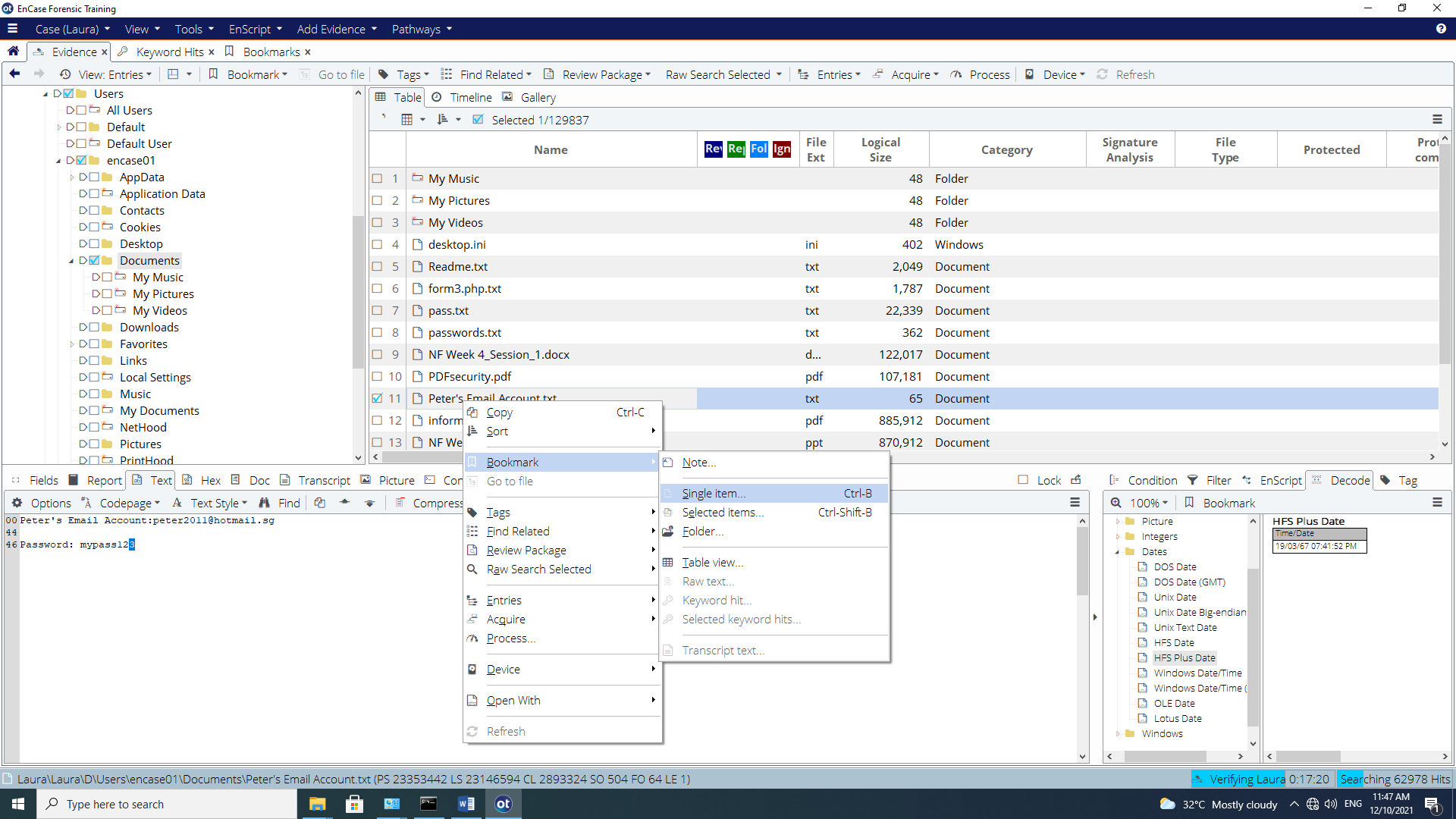


Figure B-5: Bookmark Single Item

1. On the toolbar, click **Bookmark > Single item**... (Note: Selected items can be used for selecting multiple notable files)
2. The Single item dialog opens. On the **Properties** tab, type some identifying text in the **Comment**. Alternatively, you can use the browse button to view a list of existing comments, and select one of those.
3. Click the **Destination Folder** tab to display the case's bookmark folder hierarchy. Click the bookmark folder where you want to store the bookmark. Click **OK.**

[You can also bookmark Notes, Pictures (Gallery), etc in the similar way. Try this out yourself]

Reflection: What have you learnt in this practical exercise?

- The End -