Viewing the Search Results

Index and Raw searches are two methods of conducting searches within EnCase® Forensic v7 that have been discussed within a previous lesson. Index searches initially place results within the Search tab, but examiners have the option to save the results to the Results tab. Raw searches automatically record results within the Results tab.

Within the Results tab, to view and scroll through the index search hits, use the Transcript tab in the bottom pane; to view and scroll through the raw search hits, use the Text tab in the bottom pane.

A previous lesson produced several results sets within the Results tab.

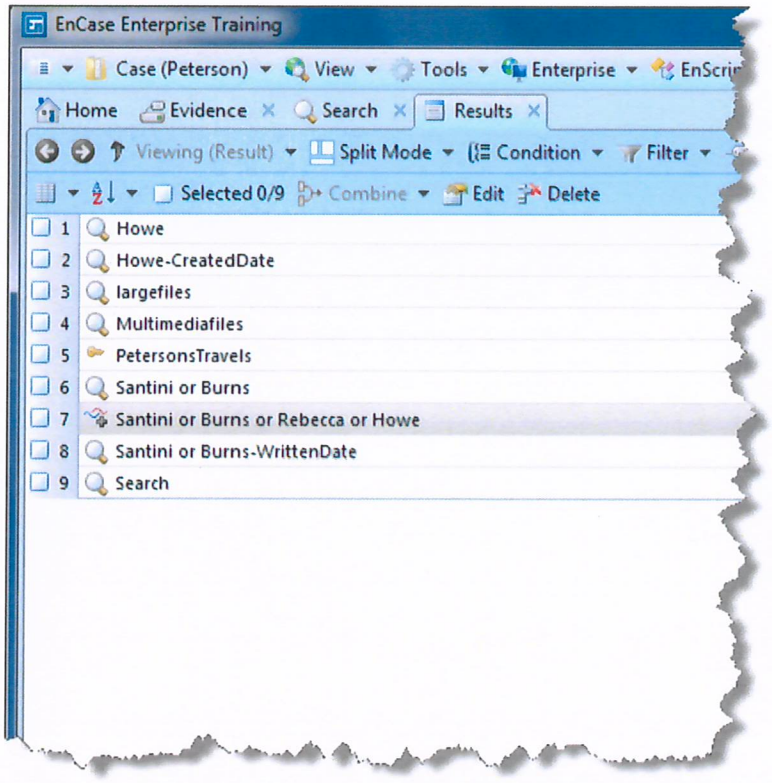

Figure 11-1 Results sets saved within Results tab

Overview of Examining Index Search Results

To examine the results of the Santini or Burns index search, access the **Results** tab. Highlight **Santini or Burns** in the Tree Pane and the **searchCA2CXMZ9** object in the Table Pane. In the View Pane, select the **Transcript** view.

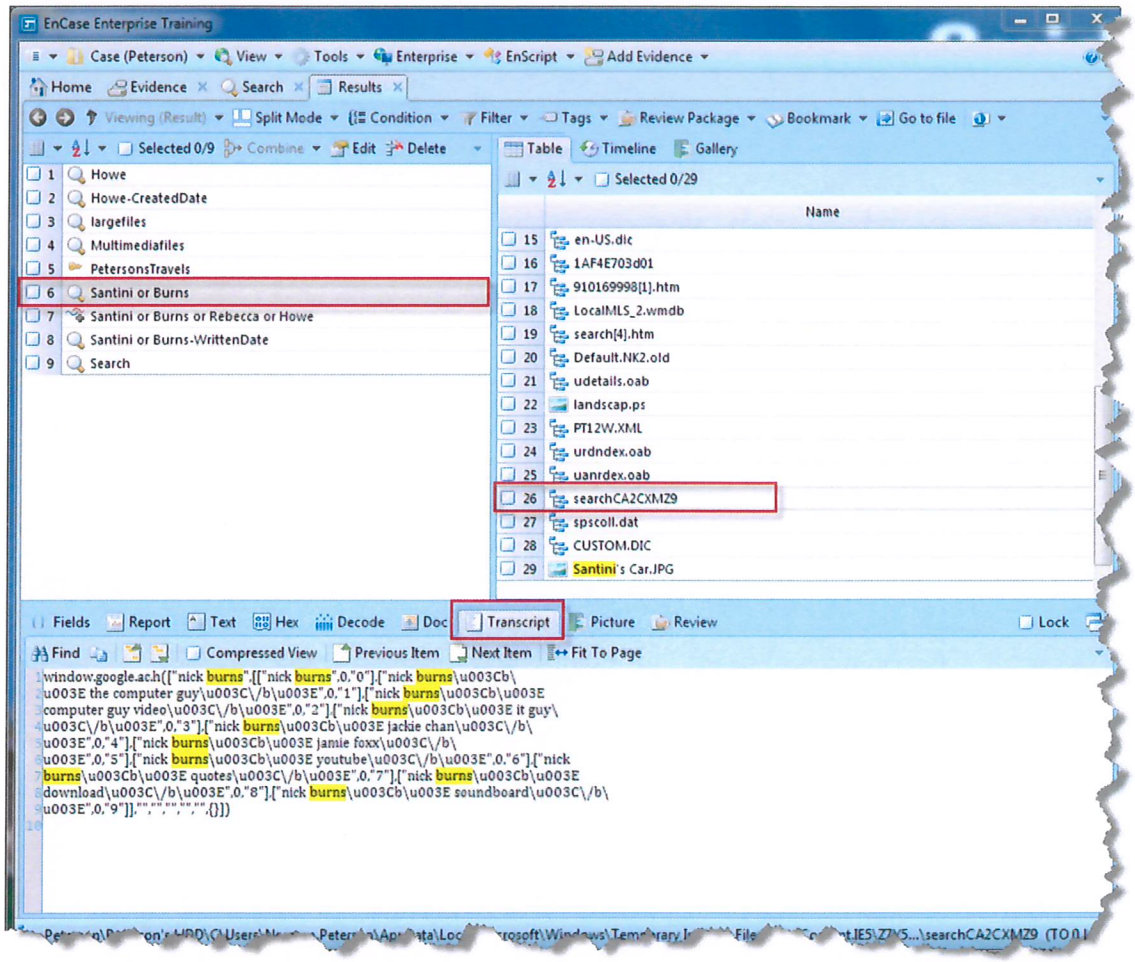

Figure 11-2 searchCA2CXMZ9 object contains index search results on "burns;" no slack

The term(s) that produced this object within the Search Results tab should be highlighted in yellow in the Transcript view. The Table Pane will display any object having at least one hit on the search terms. To access other search hits within the current object, the buttons **Next Hit** and **Previous Hit** are used. If the last hit within the current object is accessed, if the examiner clicks the **Next Hit** button again, the first hit within the next object in the Table Pane will be accessed.

NOTE: The Previous Item and Next Item buttons move from object to object in the Table view.

The Transcript view is related to the Doc view and the Stellent Outside-In Viewer. The purpose of the Transcript view is to filter out codes within the object to display user-readable text. Neither the Doc nor the Transcript view show slack data. The Doc view may also be used as it displays and interprets the file type of the search result object.

When an index search is executed, the expected views for examining the search results is Transcript.

If the Text or Hex views within the Results tab are used to review search hits, they will not be seen highlighted in yellow. Click on the Text view in the bottom pane and the yellow highlighting should disappear.

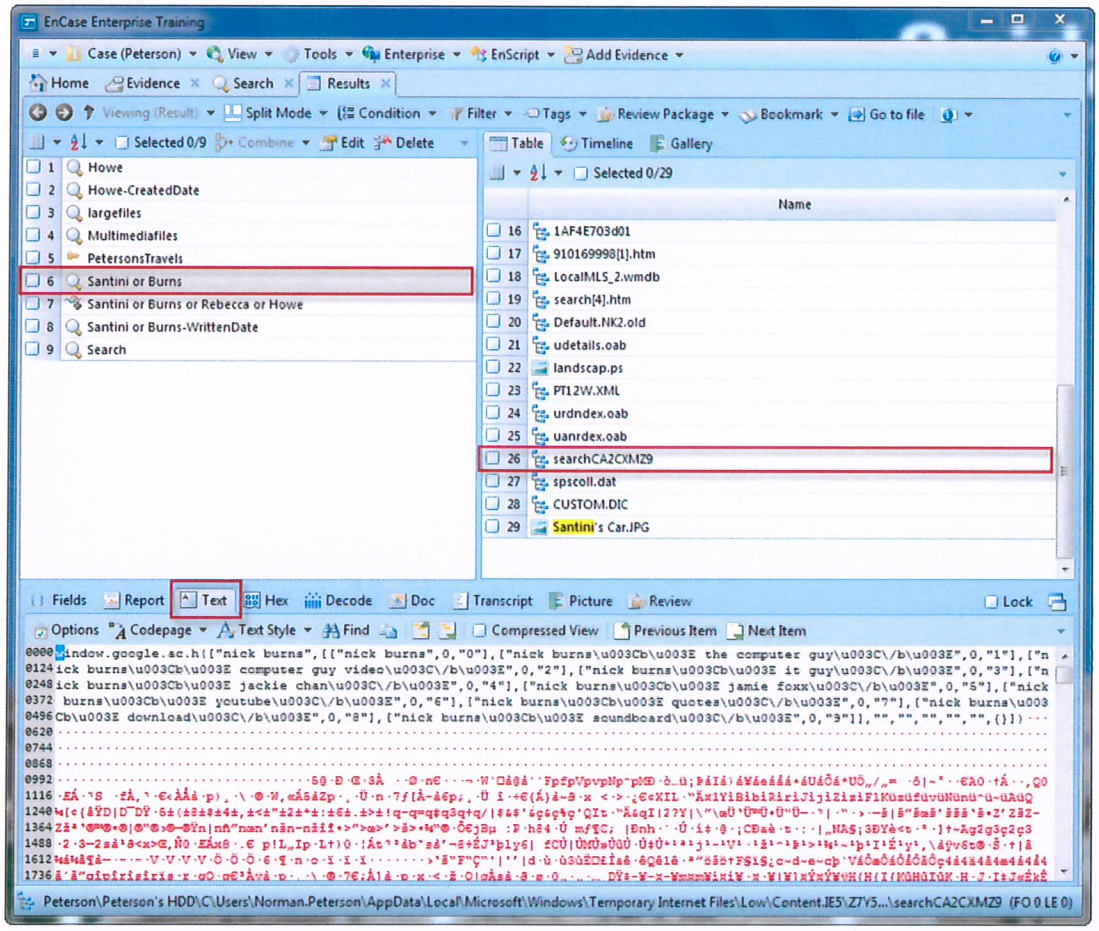

Figure 11-3 searchCA2CXMZ9 object in Text view, no search term highlighted, but slack is viewable

View the search results of the Santini or Burns index search within 910169998[1].htm. Highlight **Santini or Burns** in the Tree Pane and the **910169998[1].htm** object in the Table Pane. In the View Pane, select the **Doc** view. The Doc view interprets the data within the file as HTM data based on the header of the file.

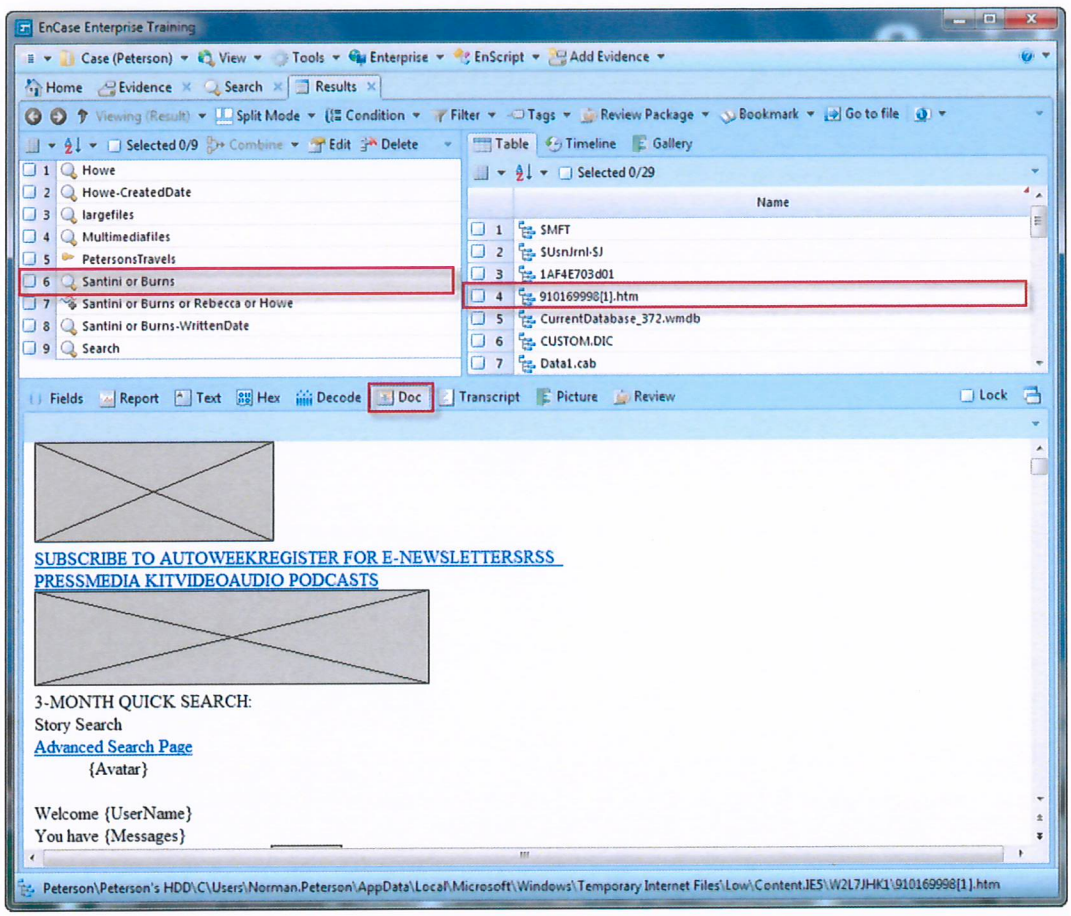

Figure 11-4 910169998[1].htm in Doc view

Neither **910169998[1].htm** or **searchCA2CXMZ9** contain any data relevant to our examination. Let's examine additional techniques to locate data regarding possible illegal and improper activities by Norm Peterson and Rebecca Howe.

USING COMPRESSED VIEW TO EXAMINE INDEX SEARCH RESULTS

Within the results set **Santini or Burns,** highlight the file **Default.NK2.old**. Select the **Transcript** view in the bottom pane. Click on the first byte of this file and click the **Next Hit** icon.

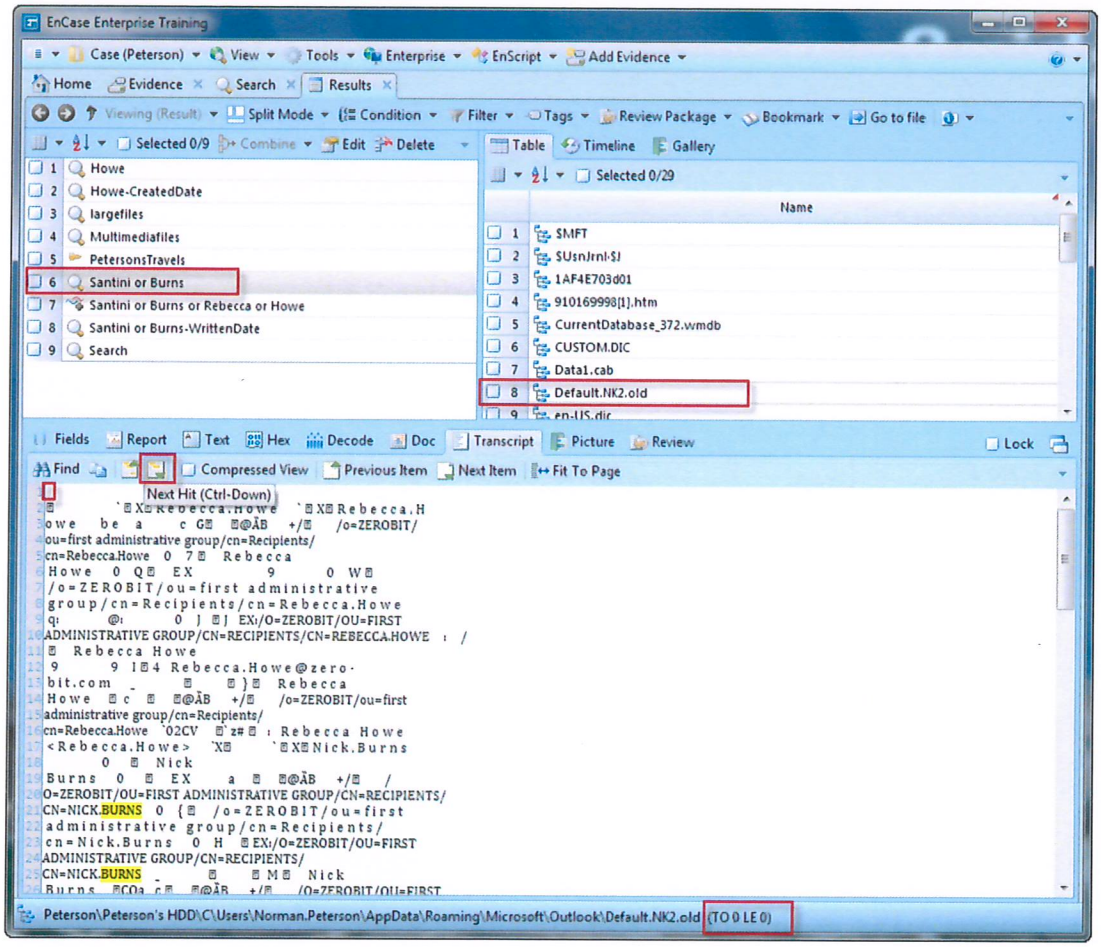

Figure 11-5 Default.NK2.old – next hit

The first hit within the file should be highlighted in blue.

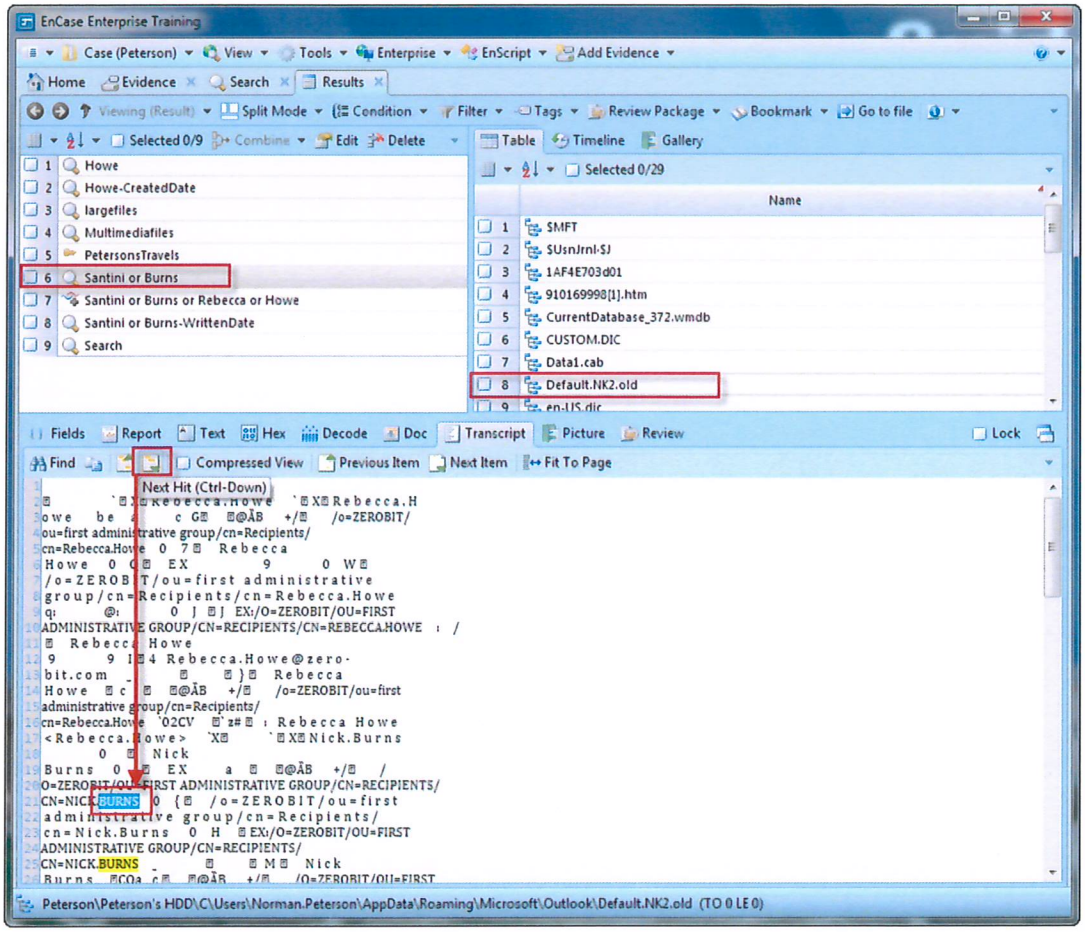

Figure 11-6 Default.NK2.old – hit highlighted in blue

Each time the **Next Hit** icon is pressed the next search hit is highlighted in blue. If all search hits are viewed within this file and the **Next Hit** icon is pressed, the search hit within the next object in the list will be displayed. This concept also applies in a similar way to the **Previous Hit** icon.

To quickly see each search hit within the context of the line it appears within, use the "Compressed View" button. Within the **Default.NK2.old** file and the **Transcript** view, blue-check the **Compressed View** option just above the bottom pane. This causes each search hit and a few words surrounding it to appear in the bottom pane.

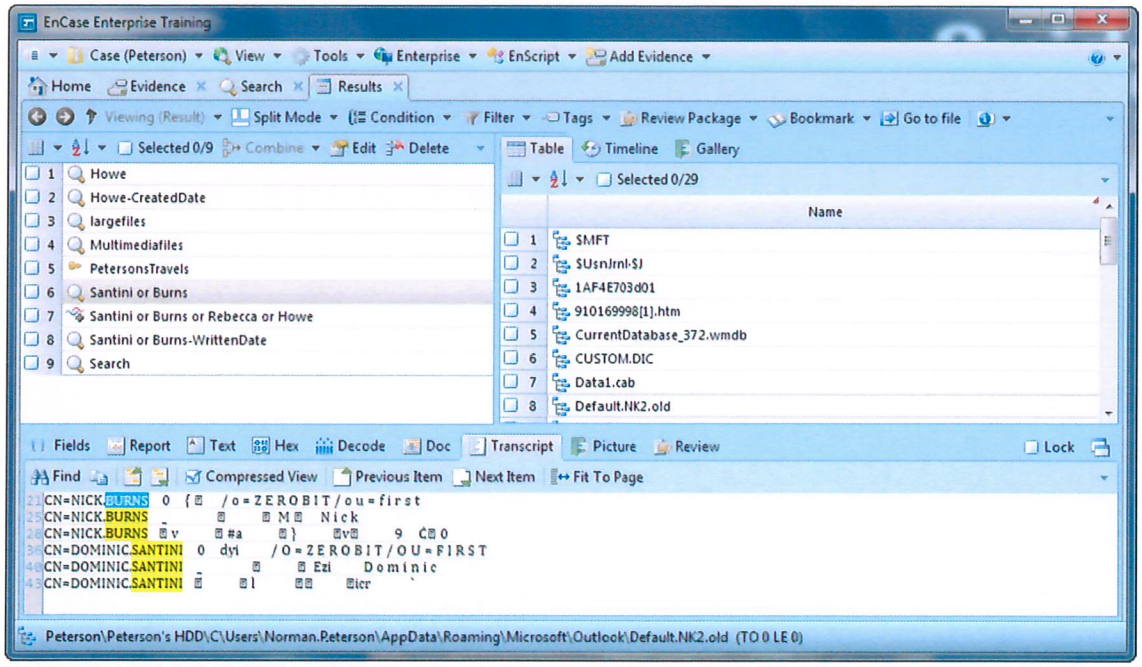

Figure 11-7 Clicking "Compressed View" button above View Pane

Six search hits are viewable in the context of the line in which they appear. To access the fourth line (first search hit on Santini), click on the "S" in Santini and remove the blue-check next to **Compressed View** by clicking on it. Additional data surrounding the search hit appears.

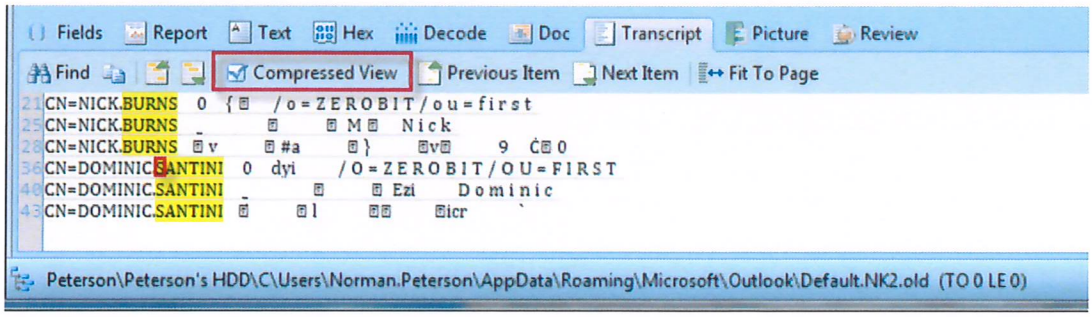

Figure 11-8 Place cursor at beginning of search hit to view in context

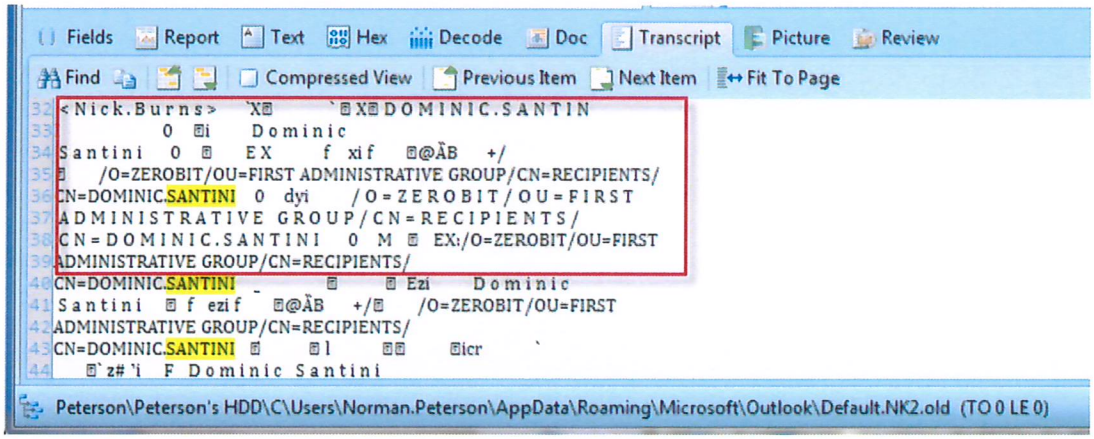

Figure 11-9 After removing Compressed View – see search hit in context

Scroll down to the end of this file. We find an e-mail address for an individual by the name of Cliff Cavin. Cliff Cavin is the CEO of Bull and Finch Enterprises, a competing government contractor. It is quite suspicious that Peterson has Cavin's -mail address documented within his computer system. We will explore this issue later.

If more room on the screen is needed to display the contents of the View Pane, undock the pane by clicking on the symbol on the far right of the button bar above the View Pane (to the right of the Lock option). The pane will detach and a new window will be generated. Close the window to redock the pane.

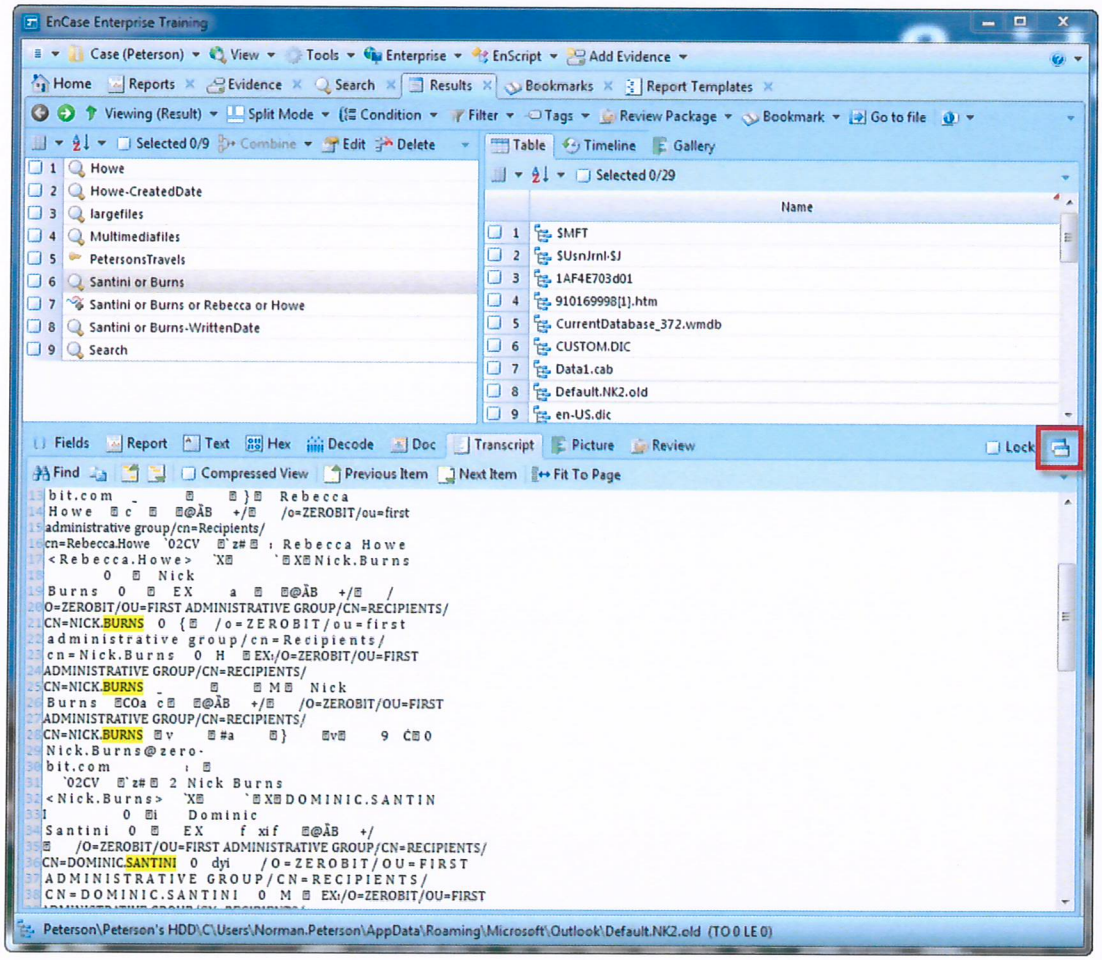

Figure 11-10 Click symbol above View Pane, to right of "Lock" to undock pane

Sometimes it is valuable to see what other files are in the folder in which the search result object resides. Within the Results tab, highlight **Santini or Burns** in the Tree Pane and the **Default.NK2.old** object in the Table Pane. Select the **Go To File** button in the button bar above the Table Pane.

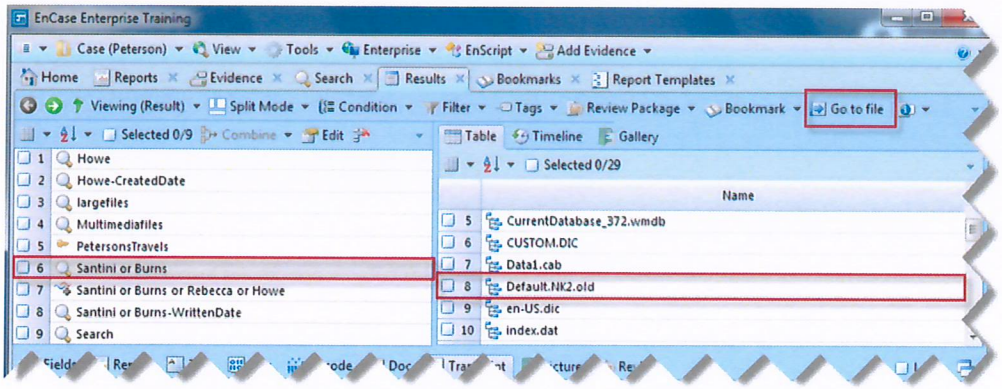

Figure 11-11 Click "Go to File" above Table Pane on right within button bar

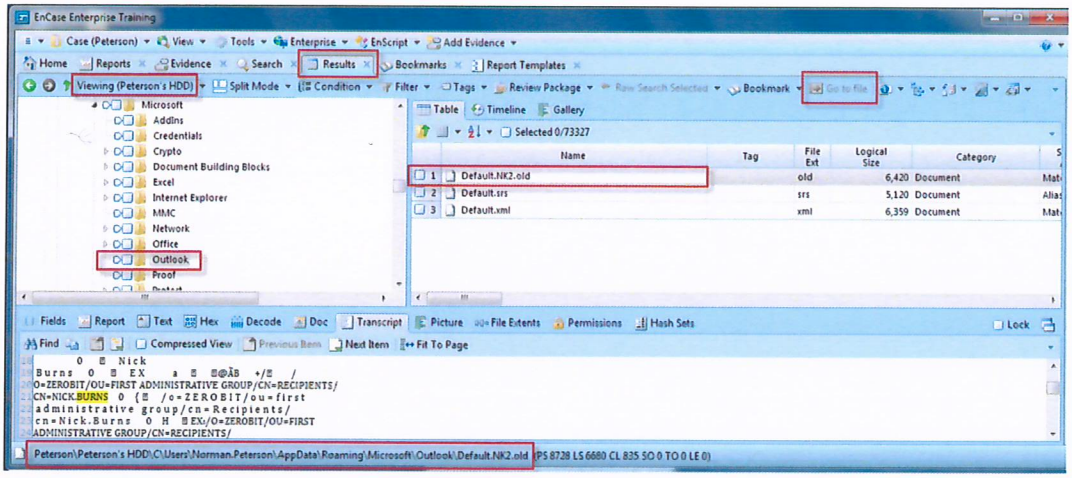

Figure 11-12 File displayed in folder within Viewing (Peterson's HDD) view still in Results tab

Click the **Back (Browswer-like)** button (to the left of Viewing (Peterson's HDD)) to return to Search Results.

Canceling a Raw Search

To cancel a search, double-click the blue status bar in the lower-right corner of the screen. Click **Yes** in the dialog box that appears to cancel the search.