



FORENSICS V2 LAB SERIES

Lab 06: Keyword Search & Analysis

Document Version: 2021-01-14

Copyright © 2021 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and other countries. Google is a registered trademark of Google, LLC. Amazon is a registered trademark of Amazon in the United States and other countries.

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
1 Getting to Know Autopsy Forensics.....	6
2 Searching with Autopsy	10

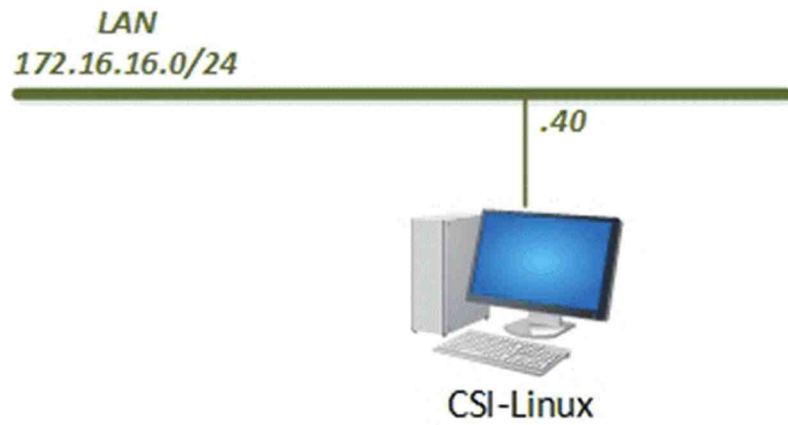
Introduction

With the volume of data existent on computers, finding a way to search through them is essential. This reduces examination time and helps to identify data that may have been otherwise overlooked. This module will cover types of keyword searches, how to perform them, and how to analyze the data found using them.

Objectives

-) Types of Keyword searches
-) How to create useful keywords

Lab Topology



Lab Settings

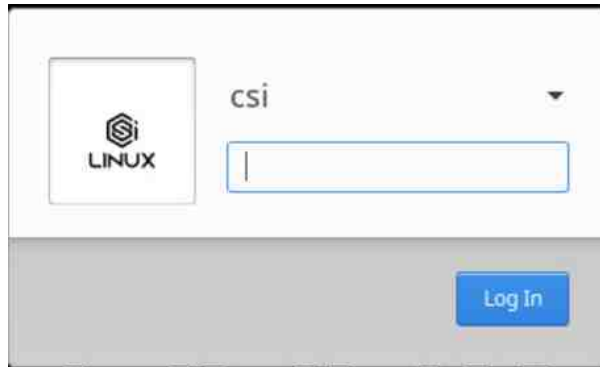
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address / Subnet Mask	Account (if needed)	Password (if needed)
Caine	172.16.16.30	caine	Train1ng\$
CSI-Linux	172.16.16.40	csi	csi
DEFT	172.16.16.20	deft	Train1ng\$
WinOS	172.16.16.10	Administrator	Train1ng\$

1 Getting to Know Autopsy Forensics

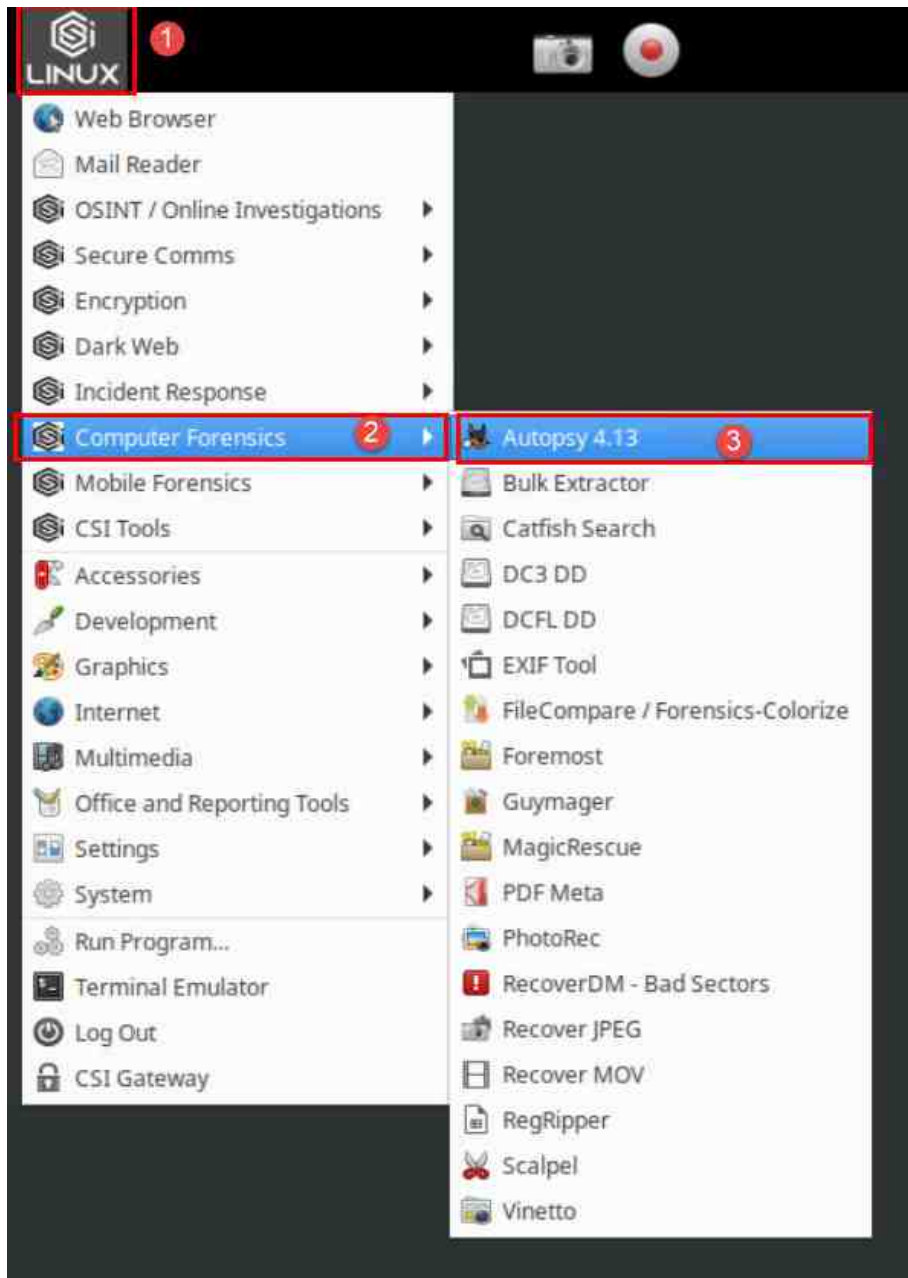
Learning to search through large volumes of data significantly speeds up investigations. In this lab, we will teach you to use a free forensic tool called Autopsy¹ to perform keyword searches in an evidence file. Autopsy™ is a digital forensics platform based on The Sleuth Kit™ that performs analysis, reports on findings, and preserves them in a forensically sound format.

1. To begin, launch the CSI-Linux virtual machine to access the graphical login screen.
 - a. Log in as `csi` using the password: `csi`



¹<https://www.autopsy.com/download/>

2. Once you are logged into the VM, launch the Autopsy program from the Start menu by navigating to Application Menu (top-left corner) > Computer Forensics > Autopsy 4.13. Alternatively, you can open Autopsy from the taskbar by clicking the Autopsy icon:



3. Autopsy may take a few seconds to open. Once it is up, you will be presented with a case creation wizard. This will walk you through the case creation process. As with most digital forensic software suites, a case needs to be created. This will allow you to load evidence; create and save tags; create bookmarks; generate reports, all while preventing cross-contamination of evidence. The Welcome screen highlighted below contains the New Case, Open Recent Case, and Open Case options. You can use this screen to create or reload a previously created case. For now, let us click Close as highlighted below.



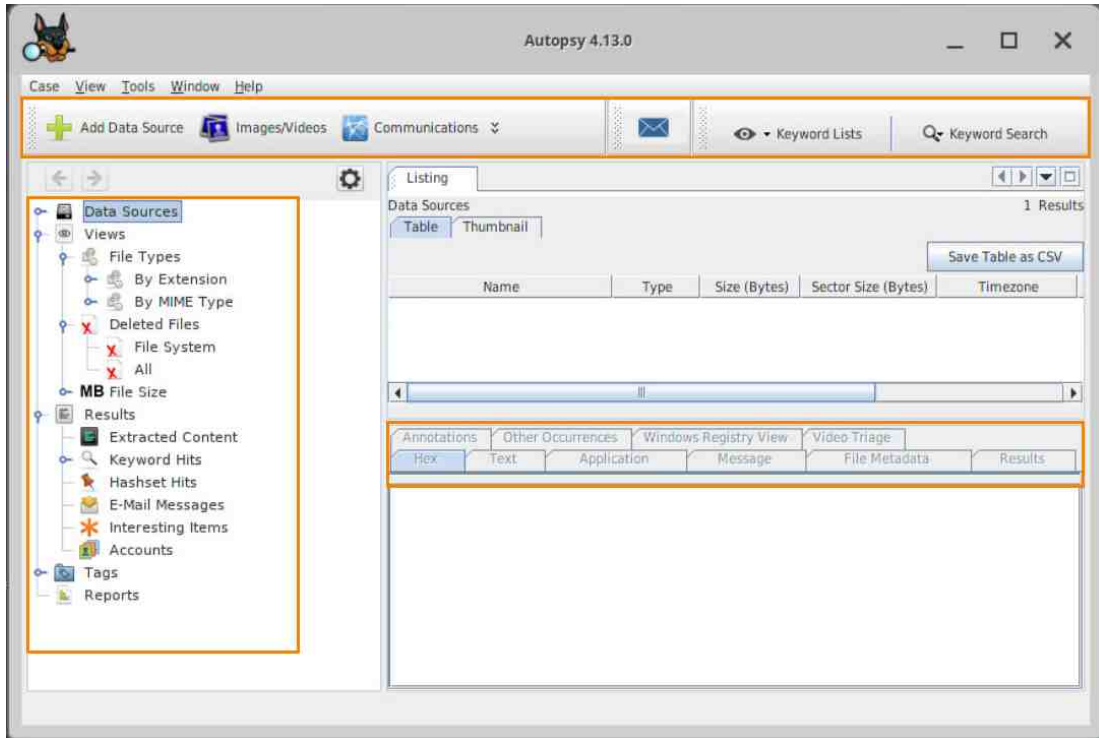
4. You will now be taken to the main GUI window. The table below will outline the features we will be using in this exercise. As always, please note that all the options are not listed here.

<i>Case</i>	The <i>Case</i> dropdown menu contains the options that allow you to manage case data and add data sources (<i>FEF</i> , local drives, etc.)
<i>Add Data Source</i>	The <i>Add Data Source</i> toolbar option allows you to add evidence files and other data sources
<i>Keyword Lists</i>	The <i>Keyword Lists</i> toolbar option allows you to perform keyword searches using keyword lists that you create, or you can use predefined ones.
<i>Keyword Search</i>	The <i>Keyword Search</i> toolbar option allows you to perform keyword searches



There are many other features that will not be touched in this course. If you would like to learn more about the tool, feel free to visit the Autopsy website <https://www.autopsy.com/> and learn more.

- Autopsy also has the tree-table display pane structure like FTK Imager. As highlighted below, browsing through the software is similar, although Autopsy does things differently in many other areas.

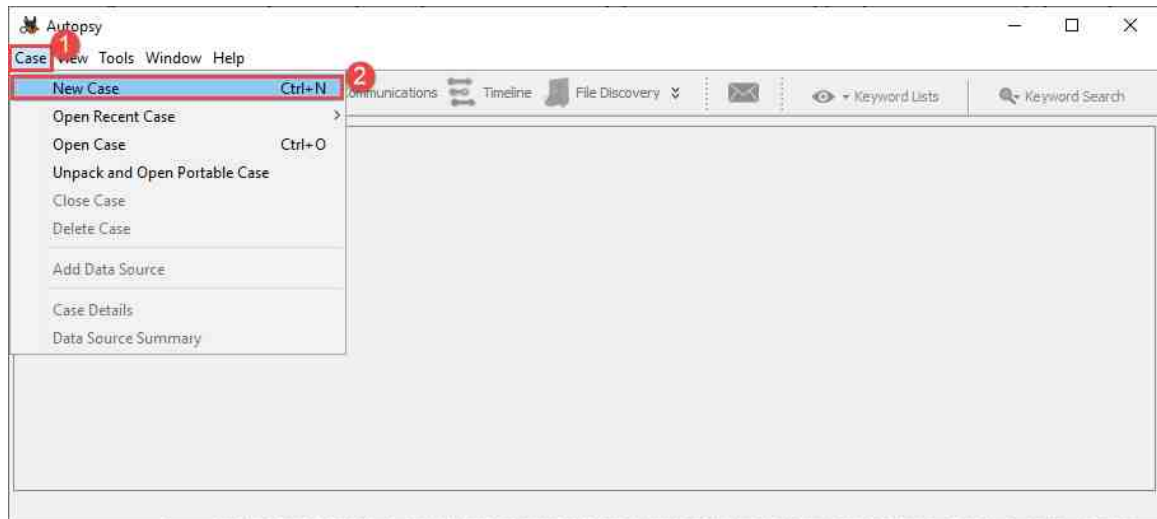


- The features we covered allow you to view and search the data. There are some additional features that we will cover during the exercise. For now, let us use what we know so far to create a case and load some data so we can perform some searches.

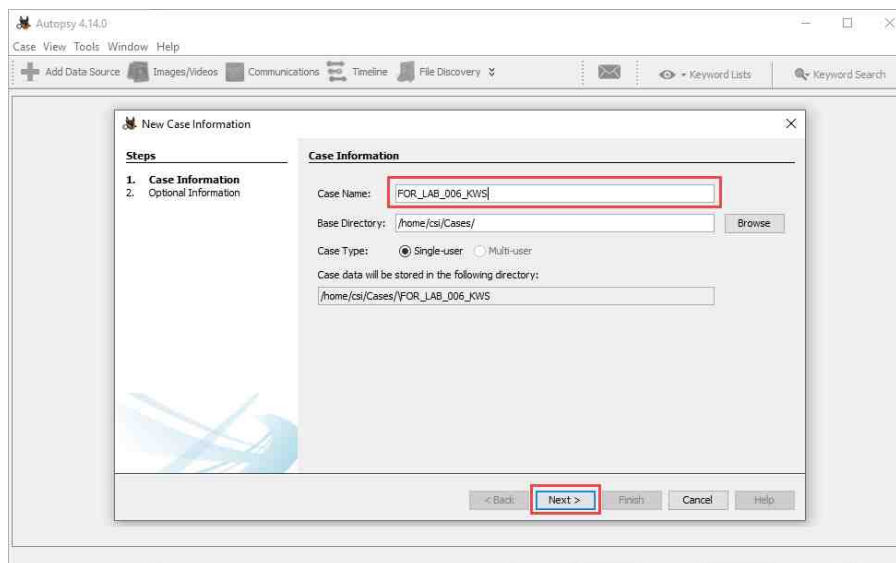
2 Searching with Autopsy

As we mentioned earlier, we need to create a case so that we can add and investigate data that is specific to the case. This means we will be creating names and unique case numbers and adding the appropriate evidence file.

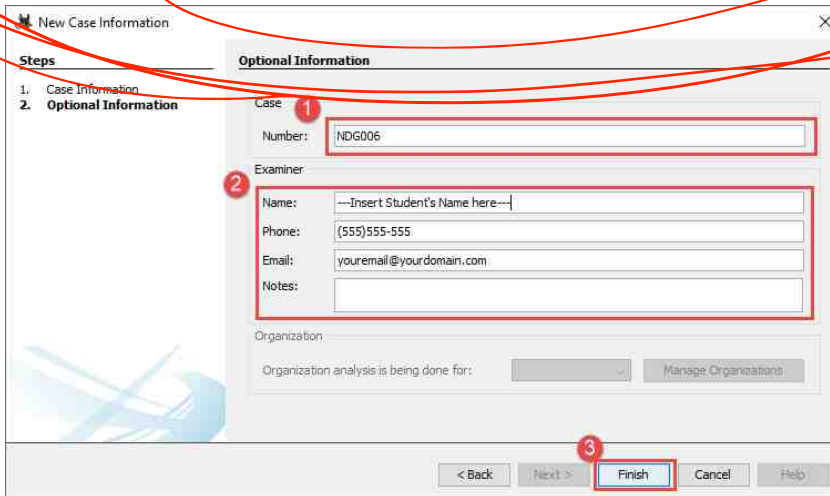
1. You should already have Autopsy open; if not, reopen it. Click the New Case option from the Case dropdown menu or press Ctrl+N as highlighted below. This will open the New Case Information window.



2. In the New Case Information window, enter FOR_LAB_006_KWS in the Case Name field. The Base Directory field is used to choose the location of the case folder. Let us leave that where it is in this exercise and click Next as highlighted below.



3. The next window in the New Case wizard is the Optional information window. Here you can type more information about the case and examiner. Fill in the information as seen in the fields below, and then click Finish when you are done. Remember, the Name field highlighted within the examiner section should contain your name.



New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case: 1

Number: NDG006

Examiner: 2

Name: --Insert Student's Name here--

Phone: (555)555-5555

Email: youremail@yourdomain.com

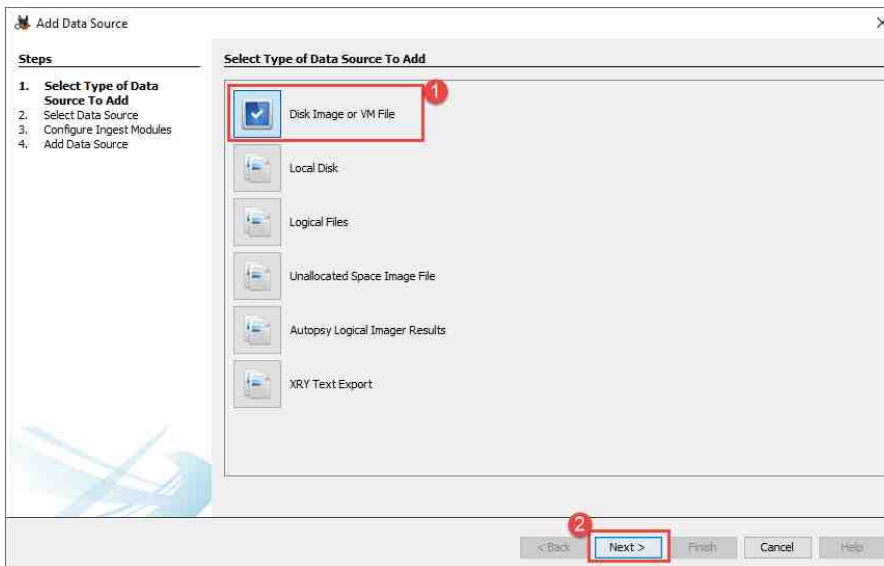
Notes:

Organization

Organization analysis is being done for: Manage Organizations

< Back Next > **Finish** Cancel Help

4. You will now be taken to the Add Data Source window. Here you can choose between different evidence sources. In this exercise, we will be using an FEF so let us select Disk Image or VM file and click Next as highlighted below.



Add Data Source

Steps

1. **Select Type of Data Source To Add**
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

☒ Disk Image or VM File 1

☐ Local Disk

☐ Logical Files

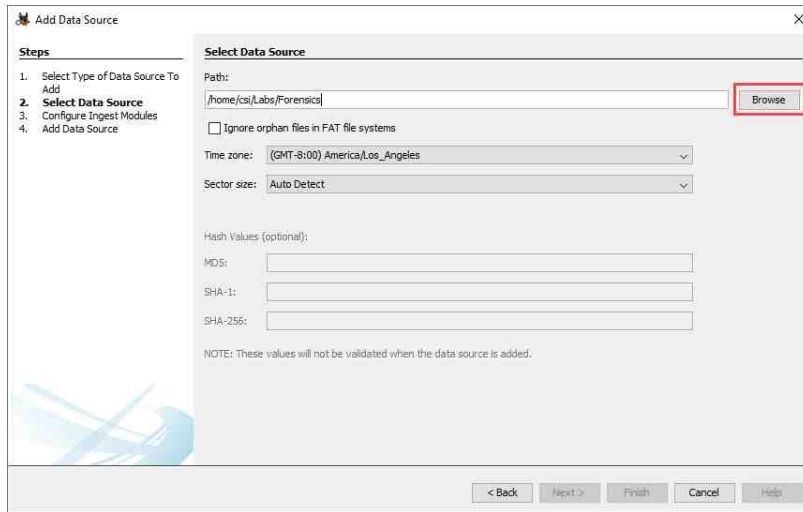
☐ Unallocated Space Image File

☐ Autopsy Logical Imager Results

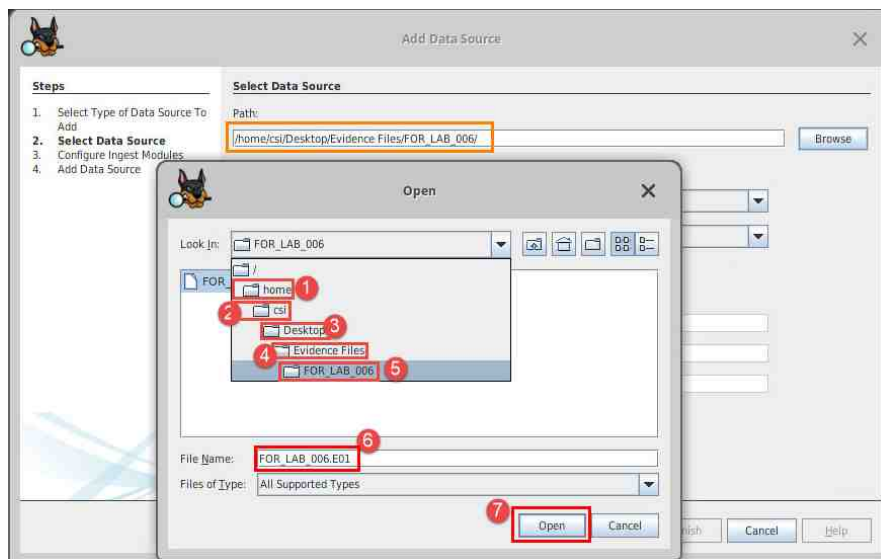
☐ XRY Text Export

< Back **Next >** 2 Finish Cancel Help

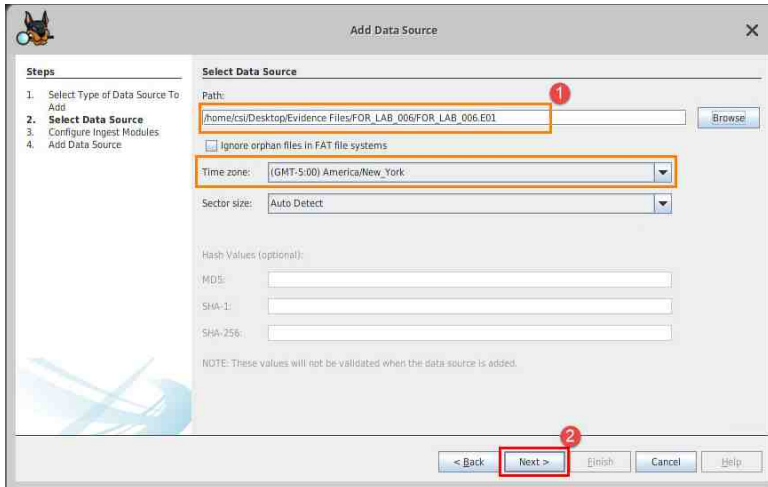
- The next window will allow you to choose the image you want to add to the case. Click the Browse button highlighted below to open the Open window that allows you to browse for the FEF.



- In the Open window, browse to Home > csi > Desktop > Evidence Files > FOR_LAB_006 and click the file called FOR_LAB_006.E01 and then click Open as highlighted below.



7. The image path will now appear in the Path field highlighted as item 1 below. We will leave the other options as-is for now and click Next highlighted as item 2 below.



The screenshot shows the 'Add Data Source' dialog box. On the left, a 'Steps' list shows '2. Select Data Source' as the current step. The main area is titled 'Select Data Source'. It contains a 'Path' text field with the value '/home/csi/Desktop/Evidence Files/FOR_LAB_006/FOR_LAB_006.E01', a 'Browse' button, an unchecked checkbox for 'Ignore orphan files in FAT file systems', a 'Time zone' dropdown menu set to '(GMT-5:00) America/New_York', and a 'Sector size' dropdown menu set to 'Auto Detect'. Below these are three optional hash value fields: 'MD5', 'SHA-1', and 'SHA-256'. A note at the bottom states: 'NOTE: These values will not be validated when the data source is added.' At the bottom right, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a red box and a red circle with the number 2.



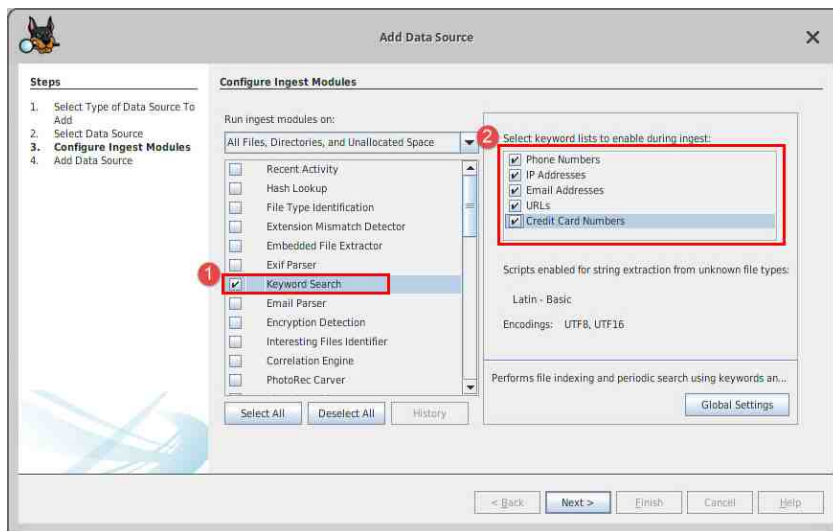
Time is adjusted based on the time zone of the evidence collected. If the time zone is not known, use the local time zone.

8. You will be taken to the Configure Ingest Modules step of the case creation process. Autopsy uses Ingest Modules to extract different types of data from data sources. The extracted data is then displayed in the main GUI window after the process is complete. In this exercise, we will only use the keyword search Ingest Module.

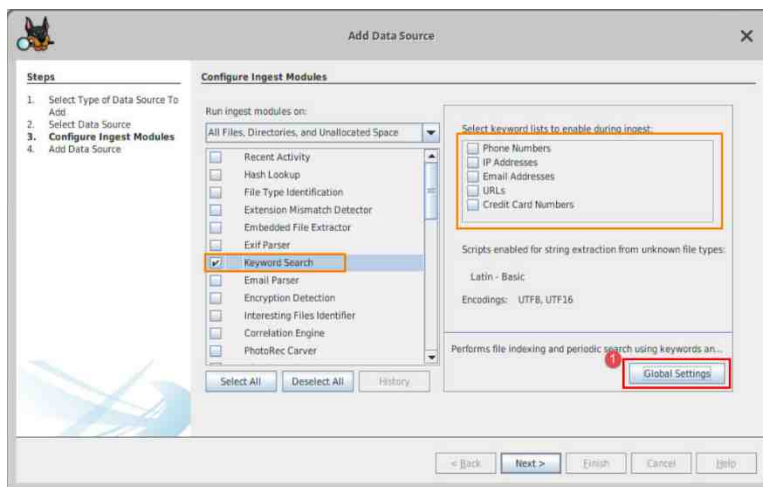


Autopsy has several 3rd-party modules that you can import in the application and use to perform additional decoding. Feel free to visit the website https://wiki.sleuthkit.org/index.php?title=Autopsy_3rd_Party_Modules and read more about the features.

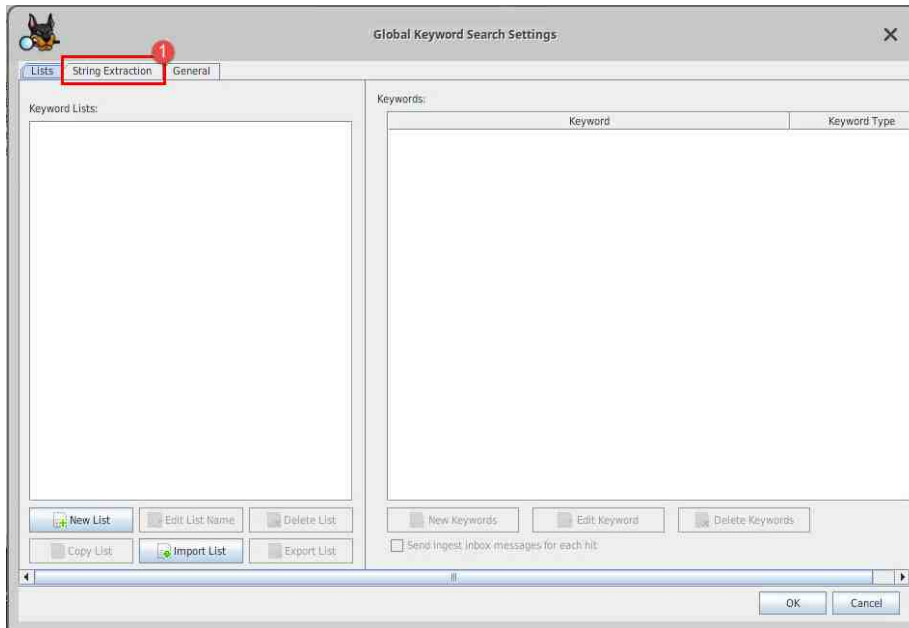
9. Let us begin by clicking the checkbox beside Keyword Search, as highlighted below. This module allows you to index and/or search the data. Once you enable the Keyword Search module, some options will appear in the right pane highlighted as item 2. These are the keyword lists that will be used to search the image. The lists highlighted in item 2 below contain default keyword lists that come with Autopsy (and most forensic software suites) and can be switched on or off. Let us verify that they are unchecked for this exercise by looking for a checkmark in the checkboxes seen in item 2 below. If there is a checkmark in the box, uncheck the box on the left of each keyword list.



10. Some Ingest Modules are simply on or off, while others contain additional settings and can be configured to provide the results you want. The Keyword Search Ingest Module is one such module; it can be configured. Let us look at some of its settings. Click Global Settings, as highlighted below.



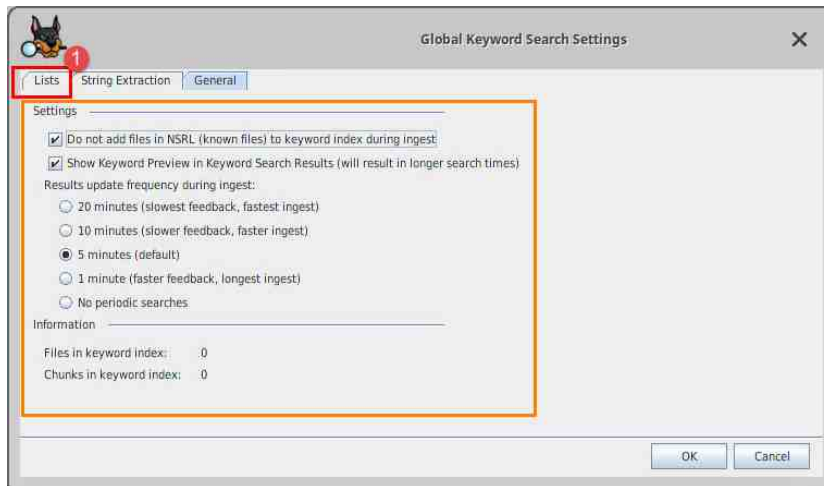
11. The Global Keyword Search Settings window will open. This window has 3 tabs. The first tab is called Lists and allows you to create, edit, copy, export, and delete keyword lists. We will come back to this tab later. For now, click the tab called String Extraction, as highlighted in item 1 below.



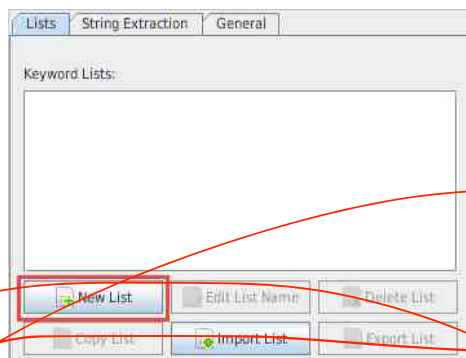
12. The String Extraction tab allows you to choose additional languages and font types to be indexed. It also allows you to enable Optical Character Recognition, which is a feature that identifies text in image files. It is only available for 64-bit Windows operating systems, though. Next, let us click the General tab highlighted as item 2 below.



13. The General tab contains general settings and allows you to change things like an NSRL list of files, show previews of the keyword search results while the search is running, and modify how frequently the previews get updated. Let us leave everything as is and go back to the Lists tab by clicking Lists as highlighted below.



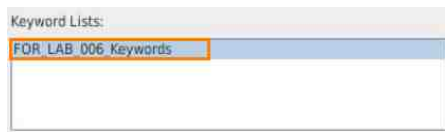
14. Now that we are back in the Lists tab, click the New List button as highlighted below.



15. The New Keyword List window will appear and prompt for you to enter a name for the list. Let us call this list FOR_LAB_006_Keywords highlighted as item 1 below. Once you have written the name, click OK highlighted as item 2. This will add the list to the Global Keyword Search Settings main window.



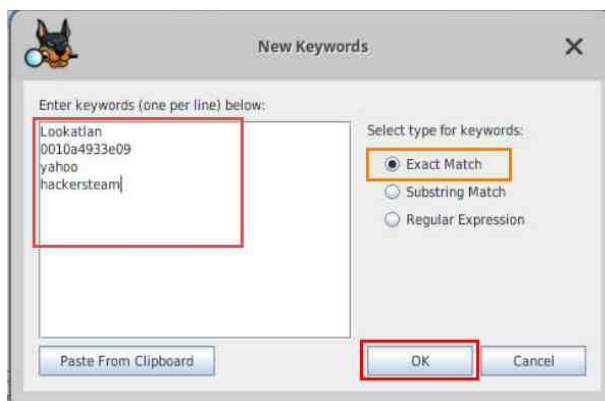
16. Back in the Global Keyword Search Settings main window, you will see the list you created. Now let us populate the list by clicking New Keyword as highlighted below.



17. The New Keywords window will allow you to type keywords and select what type of keywords they are. There are three options to select from, these are:

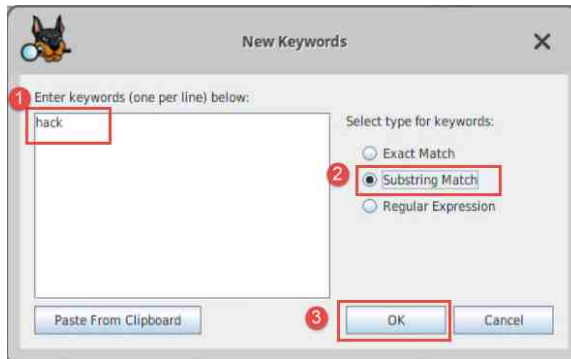
<i>Exact Match</i>	Provides results that match the term you type exactly
<i>Substring Match</i>	Provides results that contain a part of your keyword
<i>Regular Expression</i>	Provides results that match or contain your generated characters and defined search patterns

18. Before we begin, note that all options are case insensitive. Now, let us search for the same term using different types of keywords. Let us create an Exact Match keyword. In the Enter Keywords section, type these terms: Lookatlan, 0010a4933e09, yahoo, hackersteam, and then click OK as highlighted below to go back to the Global Keyword Search Settings main window.

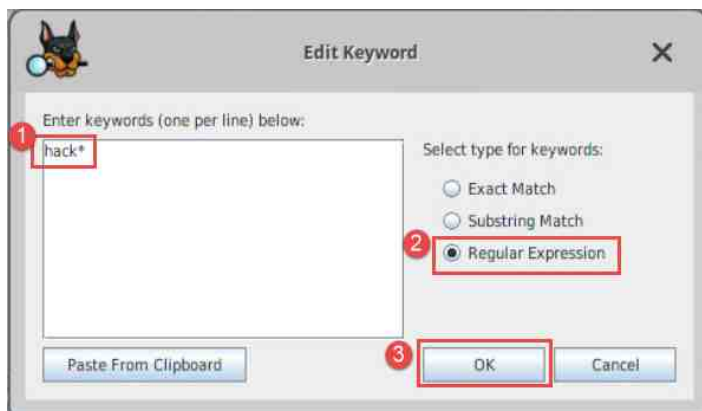


Enter each keyword on a separate line.

19. At times there is a need for variations in a search term just in case there are no results for the selected type. Let us click New Keywords again and type the part of the previous term `hack`. This time click the radio button beside Substring Match and then click OK as highlighted below.

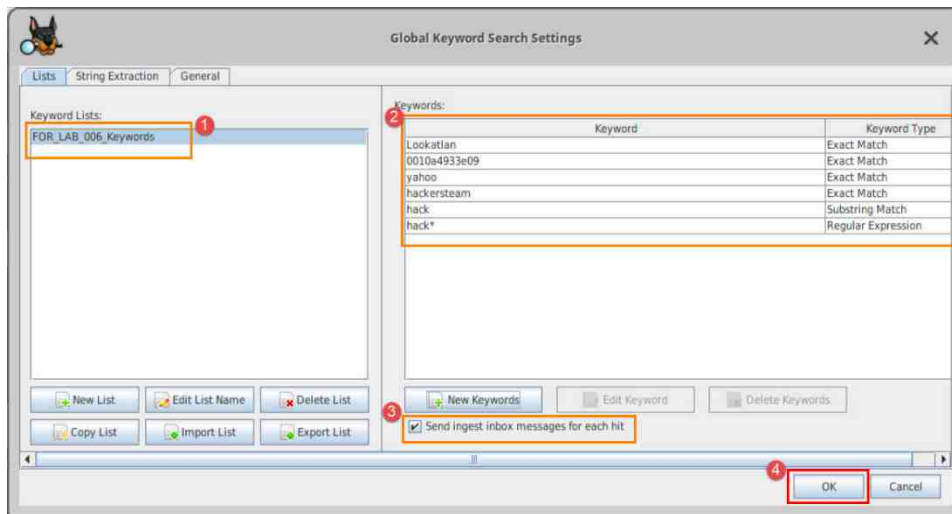


20. Let us click New Keywords again; this time, click the radio button beside Regular Expression. These patterns can be used to find terms in large volumes of data. We will use a simple expression for this exercise. Type `hack*` and then click OK as highlighted below.



The character `*` in a regular expression means, match the preceding character zero or many times.

21. You will be back at the Global Keyword Search Settings main window with all the keywords you created shown on the right Keywords pane. Now that the keyword list is ready, click OK as highlighted below.

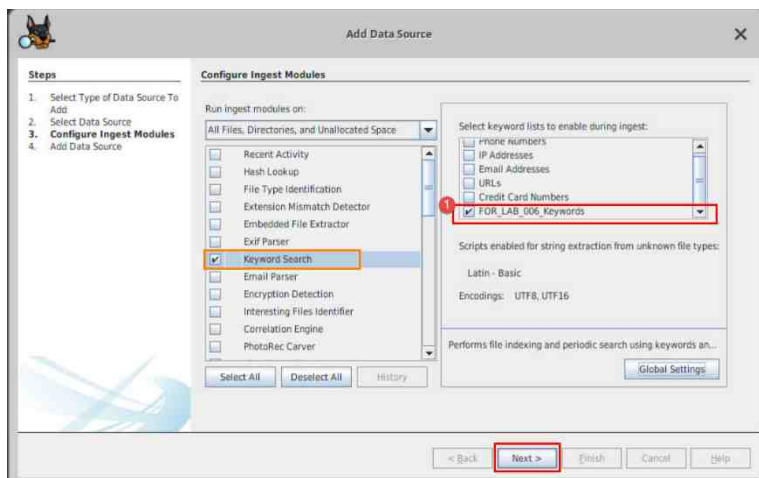


Please ensure that the keywords seen above match the ones you have entered. This will affect the results if the steps are not followed correctly.



By default, "Send ingest inbox messages for each hit" is checked. This is an interesting feature that displays all the hits that each keyword identifies in a list format during the analyzing process.

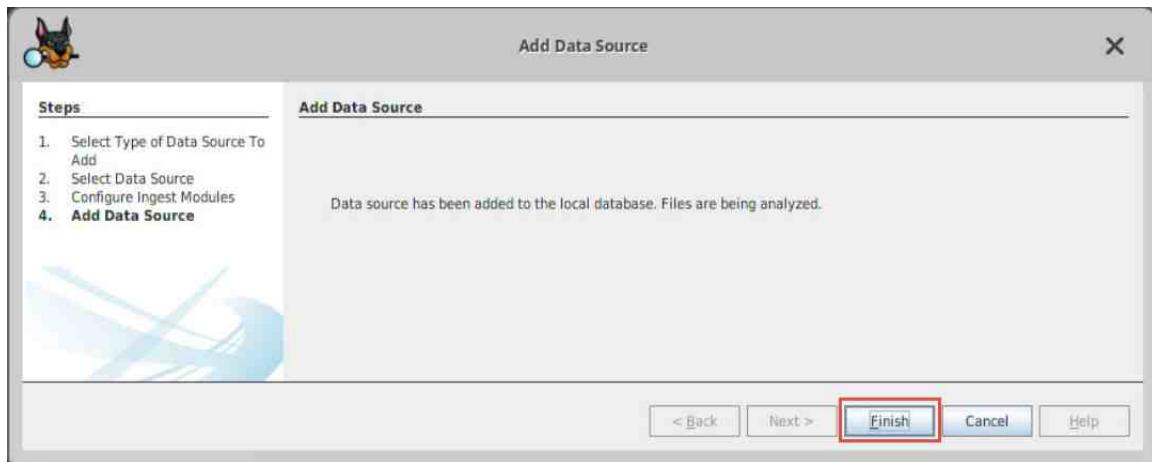
22. You will now be back at the Add Data Source window, and your new keyword list will be added to the Keyword lists pane highlighted as item 1 below. Since we will not be using any other modules, let us click Next as highlighted below.



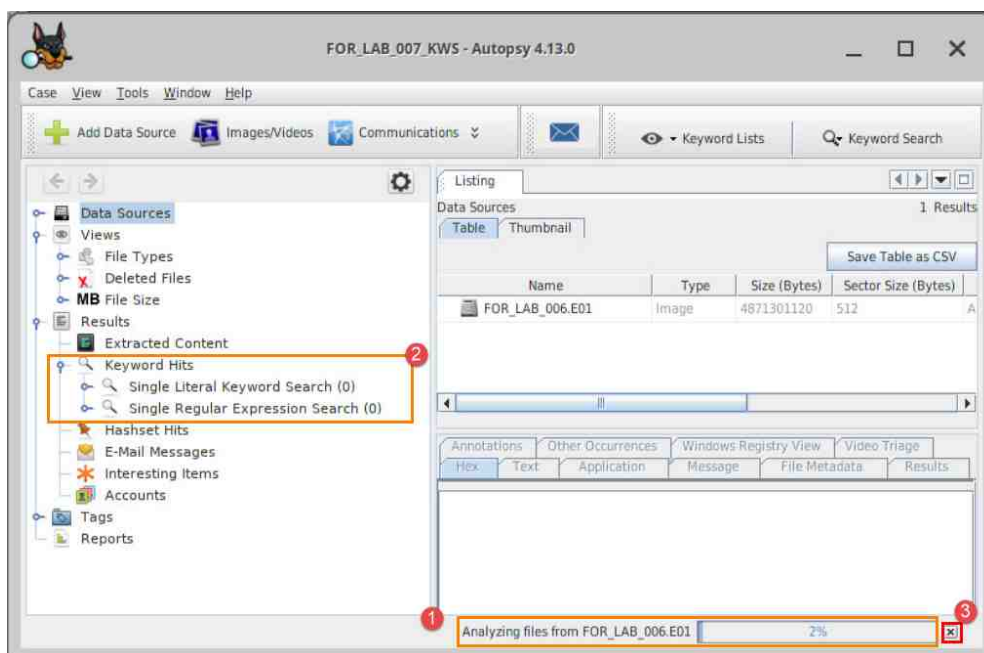


Again, ensure to uncheck the default keyword search lists before proceeding to the next step.

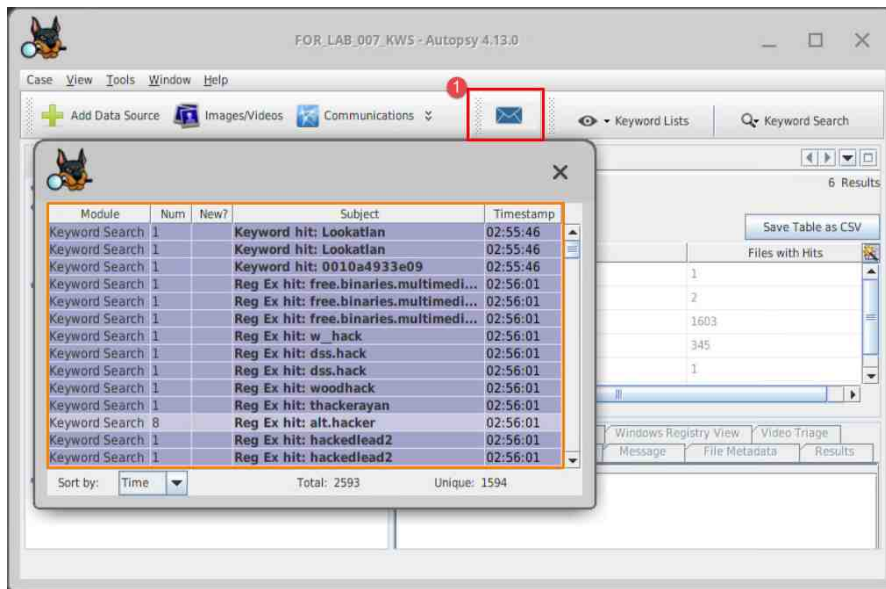
23. In the final window in the Add Data Source process, click Finish as highlighted below.



24. You will now be taken to the Autopsy main window. Here the Keyword Search Ingest Module will search the entire FEF; the progress is displayed at the bottom-right corner as seen highlighted at item 1. The decoded results will gradually populate the Keyword Hits section as highlighted at item 2. Processing an FEF for a case is very important and should never be skipped. However, due to time constraints, after the process reaches above 30%, you can cancel the keyword search by clicking the X at the bottom-right corner at item 3.

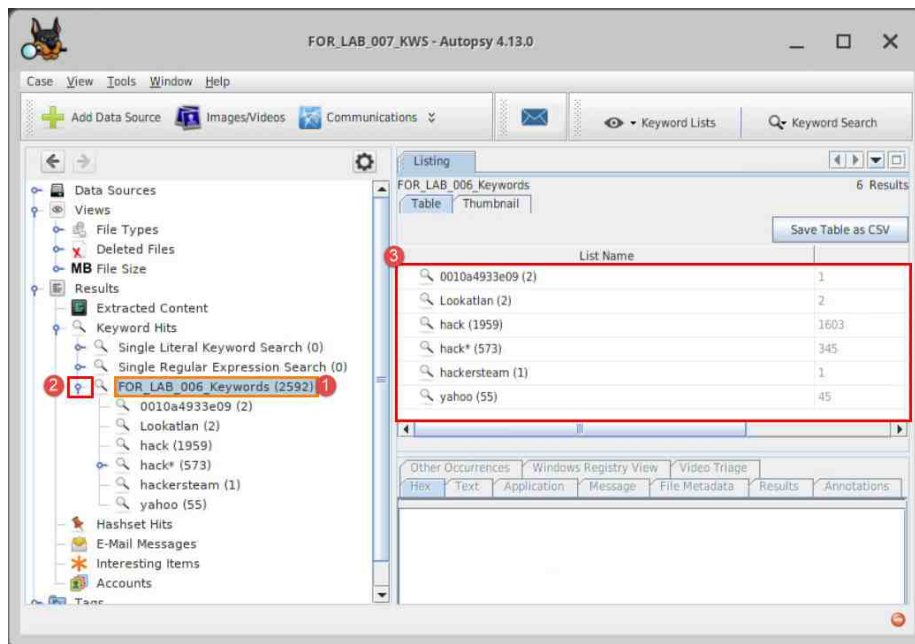


25. The icon highlighted below represents the Ingest Messages feature, which was enabled by default at step 21 above. The Keyword Search Ingest Module was able to identify 2593 hits, of which 1594 were unique.



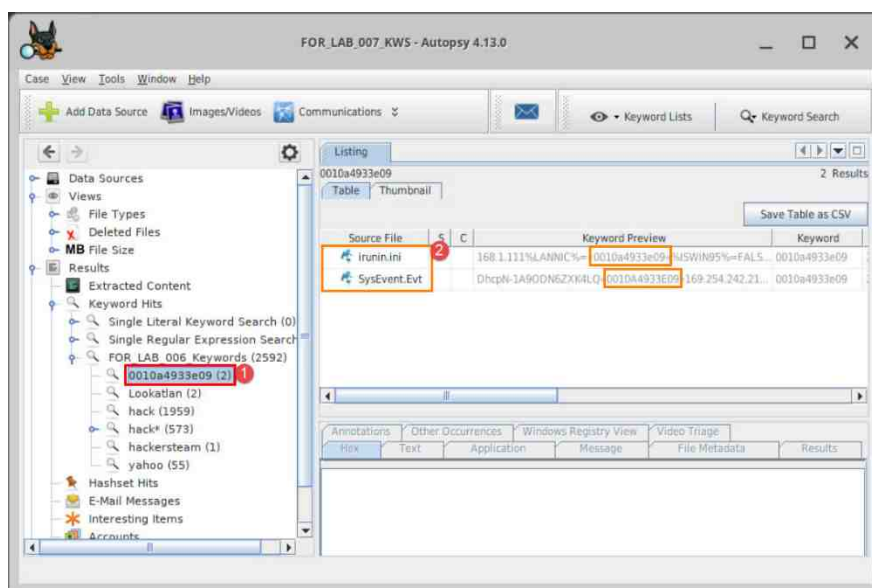
The total hits are from the completed keyword searches, as a result your total and unique numbers may differ, since you were instructed to cancel the process above 30%.

26. The search results are shown in the Keyword Hits section highlighted as item 1 below. The blue pin in item 2 below indicates that there is a subdirectory within the associated list item. Click the blue pin beside the list item called FOR_LAB_006_Keywords, highlighted as item 2, to reveal the results of the searches in the right view pane highlighted as item 3.

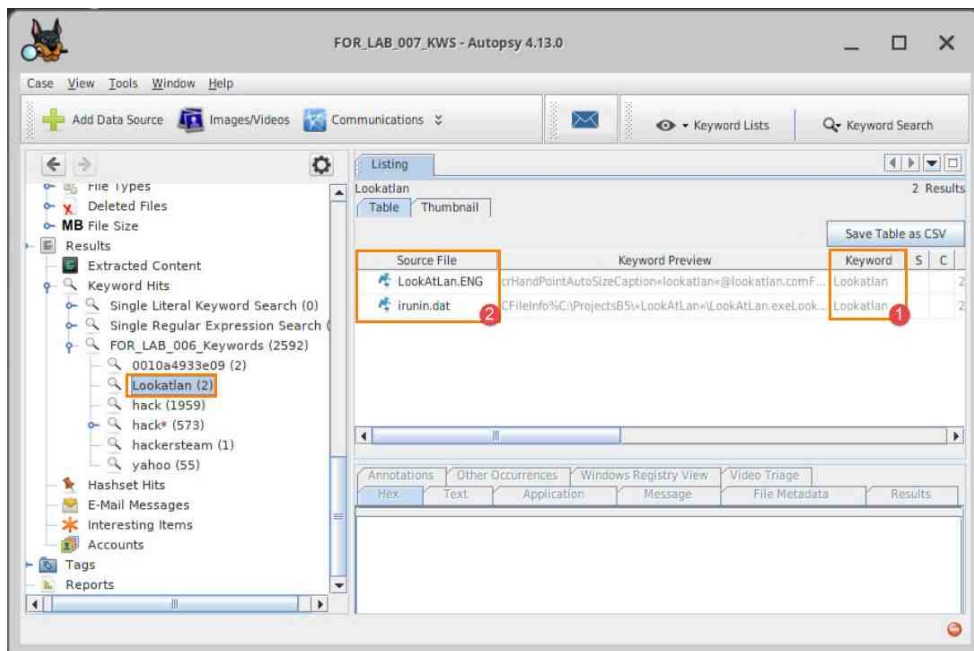


Expand all sub-directories to view the full directory tree pane.

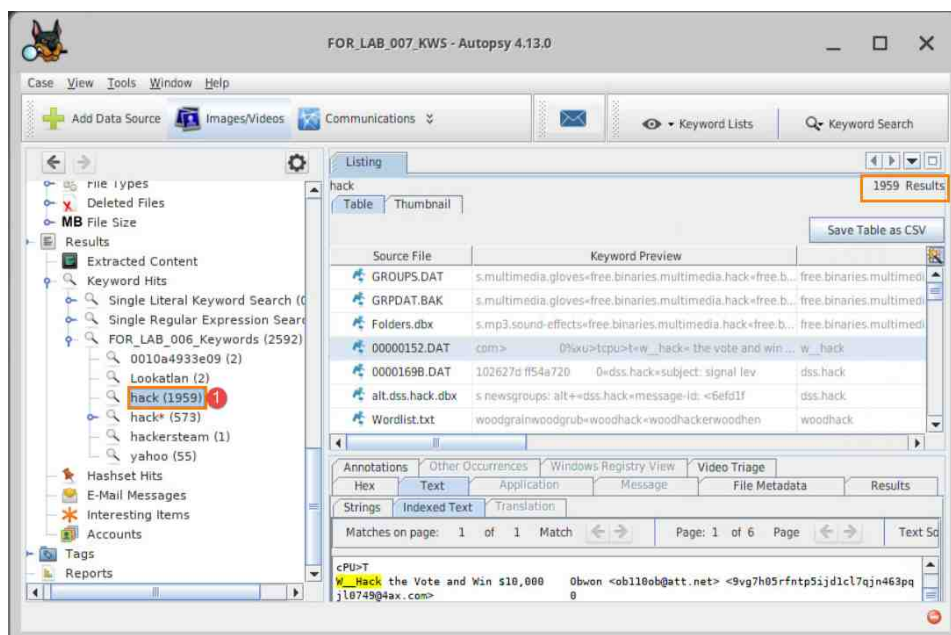
27. Let us review the matches for each search type. The Exact Match and Substring Match search types have accumulated results. The results for these search types can be found by clicking the first search term in the FOR_LAB_006_Keywords results, as highlighted as item 1 below. As you see in the view pane on the right, there are two files that contain search hits. The files are highlighted as item 2.



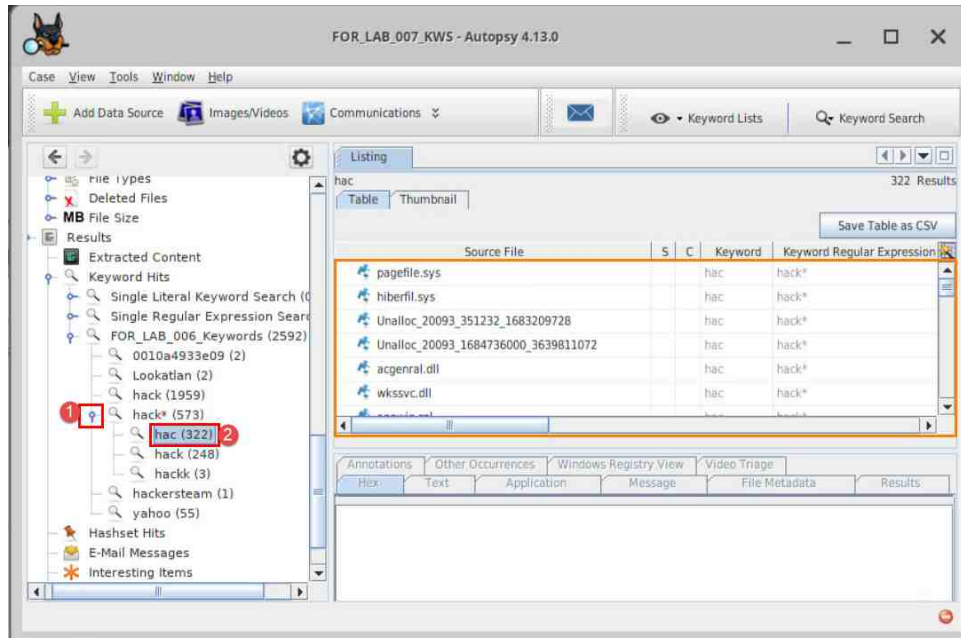
28. If you look at the keyword column highlighted as item 1 below, you will see the search term used to find each result. The result highlighted as item 2 is the Exact Match. This search term only identified the exact term lookatlan. If there were any special characters within the search term, then the Exact Match search would not identify the string. An example of this variation is look@lan.



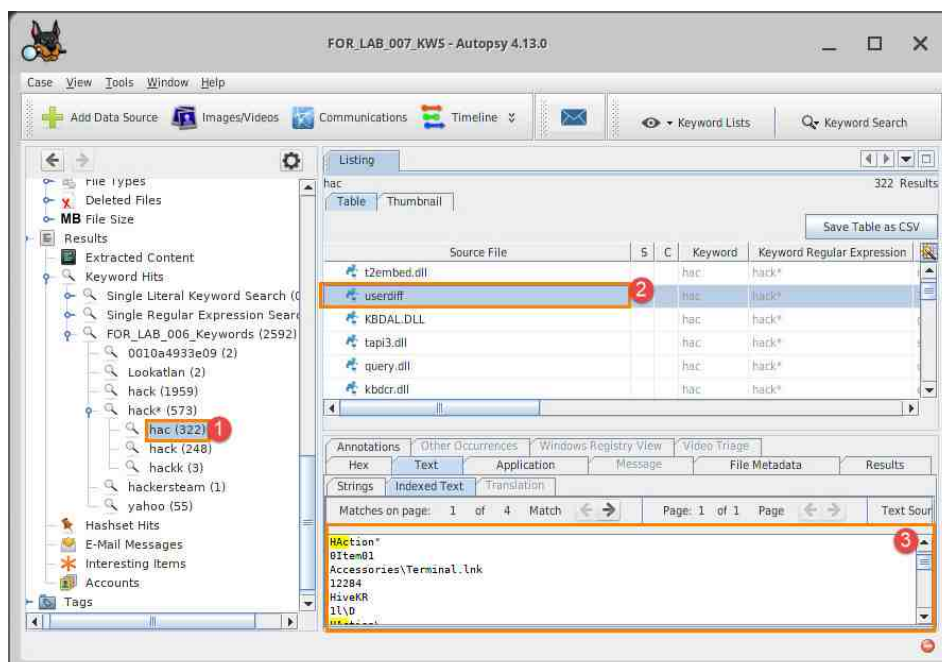
29. The third search result is the Substring Match search term. This is highlighted as Item 1, and the search term was hack. A key point to note with keyword searches is that they should not be ambiguous. Vague search terms may result in multiple hits that can be identified as false positives.



30. Now let us look at the Regular Expression search result. To access the Regular Expression search result, go back to the tree pane on the left and click the blue pin beside the search term `hack*`. This will expand and show any identified terms. Click the Regular Expression search result highlighted as item 2 below to view the search hits.



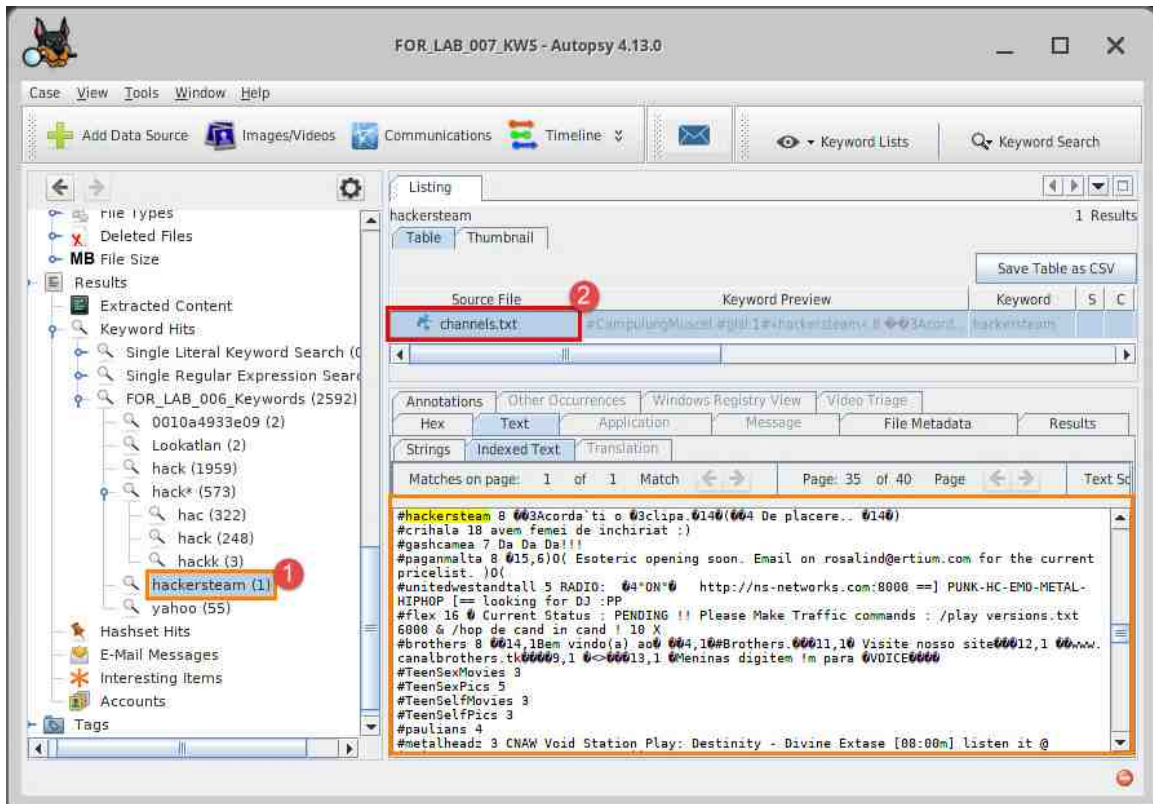
31. You can click each search result to view its location in the file. The contents will be displayed in the view pane as highlighted below. However, reviewing this many keywords can be time-consuming. So, let us filter the results a bit more.





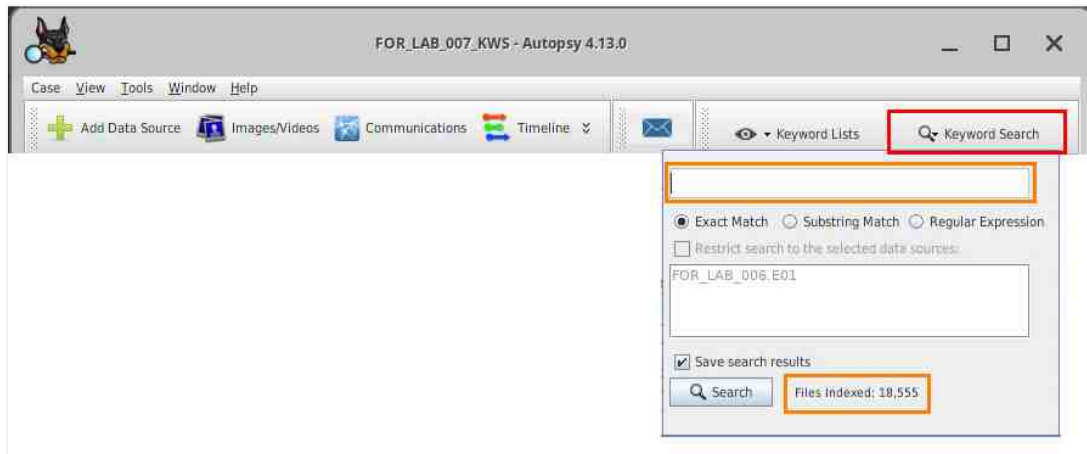
Ambiguous keywords can sometimes yield results, but you may have to search for several hours before finding that critical evidence to support your case. So, it is best to have or create a refined keyword that will filter the data accordingly.

32. Now that we have identified the different types of keywords and the possible results that can be recovered from each, let us look at some ambiguous search terms vs. refined ones. Let us say we wanted to find the term hackersteam. As you saw earlier, the search term hack had over 1000 results. The term hackersteam is guaranteed to be among the thousands of results, but it would be very time consuming to find it there. Let us compare those results to the results for the term hackersteam. As you can see, highlighted as item 1 below, the search term hackersteam provided one hit. This is more acceptable and would be specific to the data we are seeking. Let us click the file channels.txt, highlighted as item 2, to view the search hit inside the file. As you can see from the search result, the Exact Match search for hackersteam brought us to the location of the search term within the file. Since it is the Exact Match, it will not have any additional characters attached to it. As you can see from this exercise, the type of search term and the type of keyword search you perform will determine how many results you get.

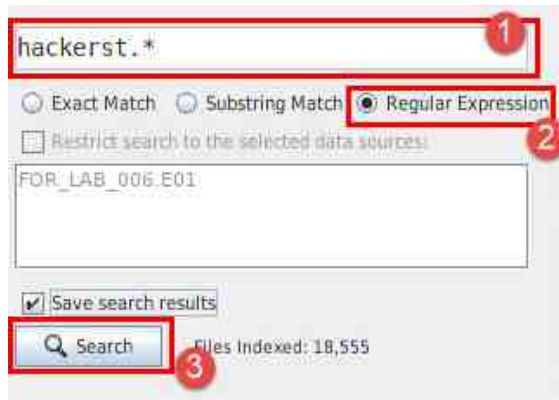


The screenshot shows the Autopsy 4.13.0 interface. On the left, the 'Results' pane shows a list of keyword hits. The 'hackersteam' keyword is highlighted with a red circle and the number 1. The 'Listing' pane on the right shows the search results for 'hackersteam'. The 'Source File' column shows 'channels.txt' highlighted with a red circle and the number 2. The 'Keyword Preview' column shows the search results for 'hackersteam' within 'channels.txt'. The 'Text' tab is selected, showing the search results in a text view. The search results show the term 'hackersteam' appearing multiple times in the file.

33. Next, we will review the Index Search. When the Keyword Search ingest module was running, it created a database of all the searchable text found on the FEF. This index database references the location of all the text in the FEF, which makes it quick and easy to search through large volumes of data on evidence files. To access the index search feature in Autopsy, click the Keyword Search dropdown window as highlighted below.

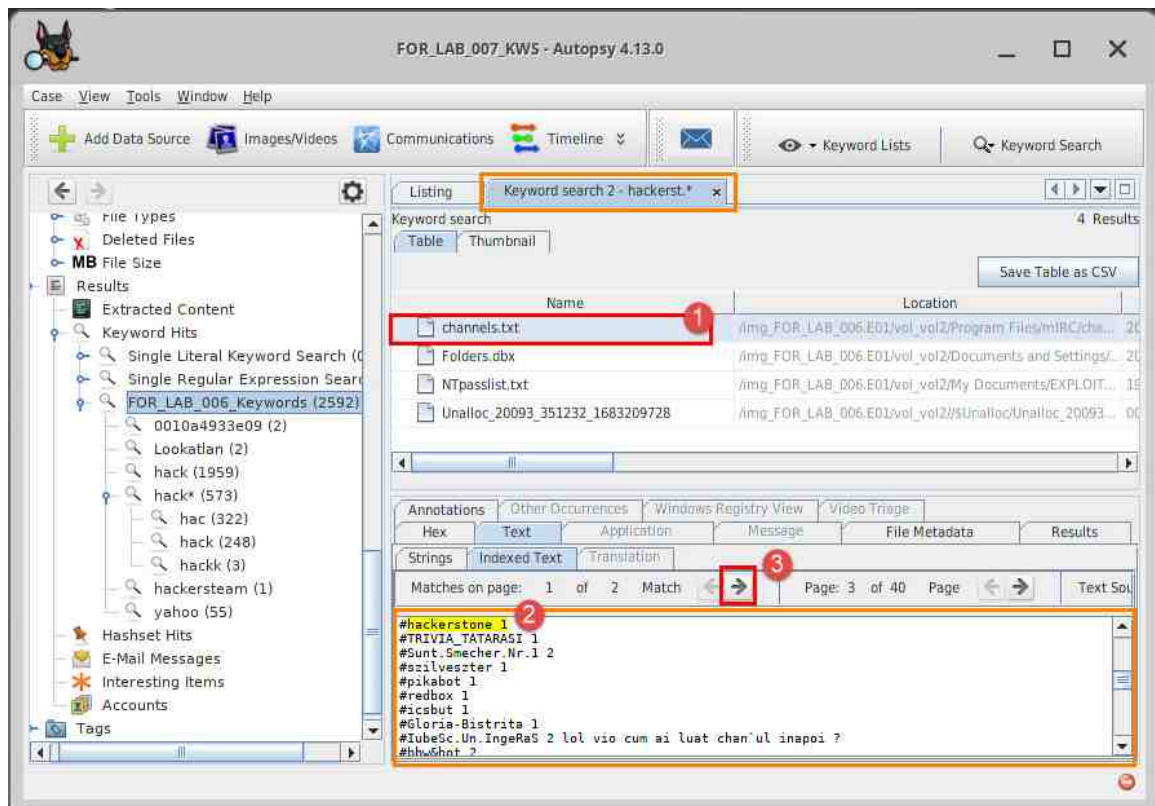


34. The dropdown window that appears will allow you to type a search term and select between Exact Match, Substring Match, and Regular Expression. Let us do another Regular Expression search. Type the term `hackerst.*` in the Search field highlighted as item 1 below. Click the radio button beside Regular Expression, highlighted as item 2 below. Finally, click Search highlighted as item 3 below, and the index search will begin.

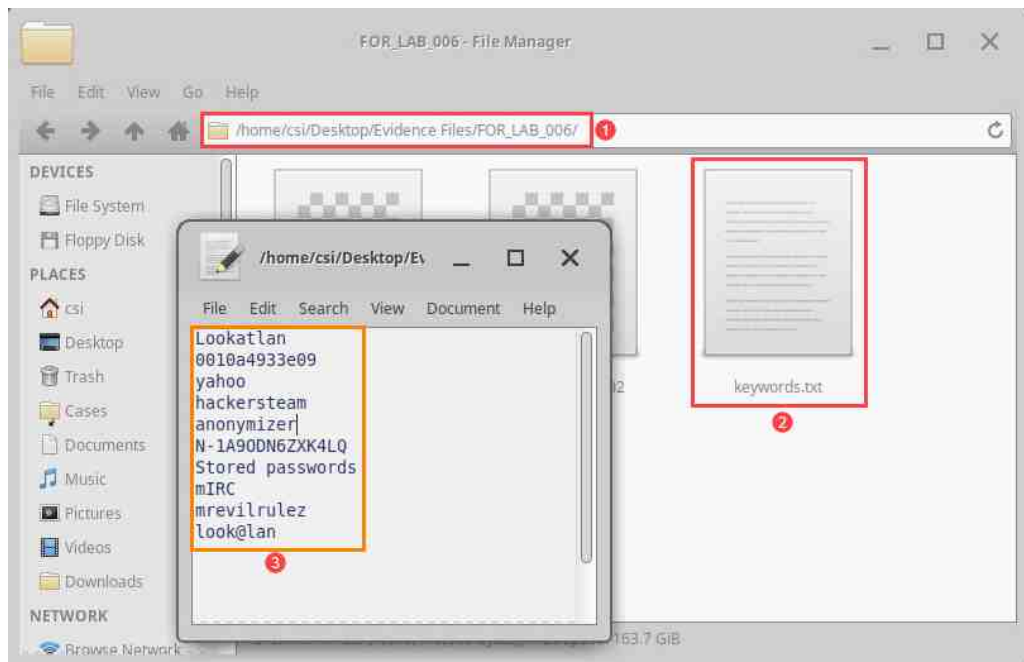


The Save search results option, if selected, will allow the search results to populate the tree-pane to the left under Single Regular Expression search. If unchecked, the results will not be saved, and you will have to perform the search again to find the results.

35. The index search should be quick, and the results should increase in comparison to our previous search for the term hackersteam. The Regular Expression term `hackerst.*` searches for all terms that start with the letters hackerst and will find any occurrence of it regardless of the string that follows it. To see an example of this, click the file called `channels.txt` highlighted as item 1 below. This is the same file as before, but now the results contain the term `hackerstone` 1 highlighted as item 2 below. Click the arrow highlighted as item 3 below to view the other search hits within a file.

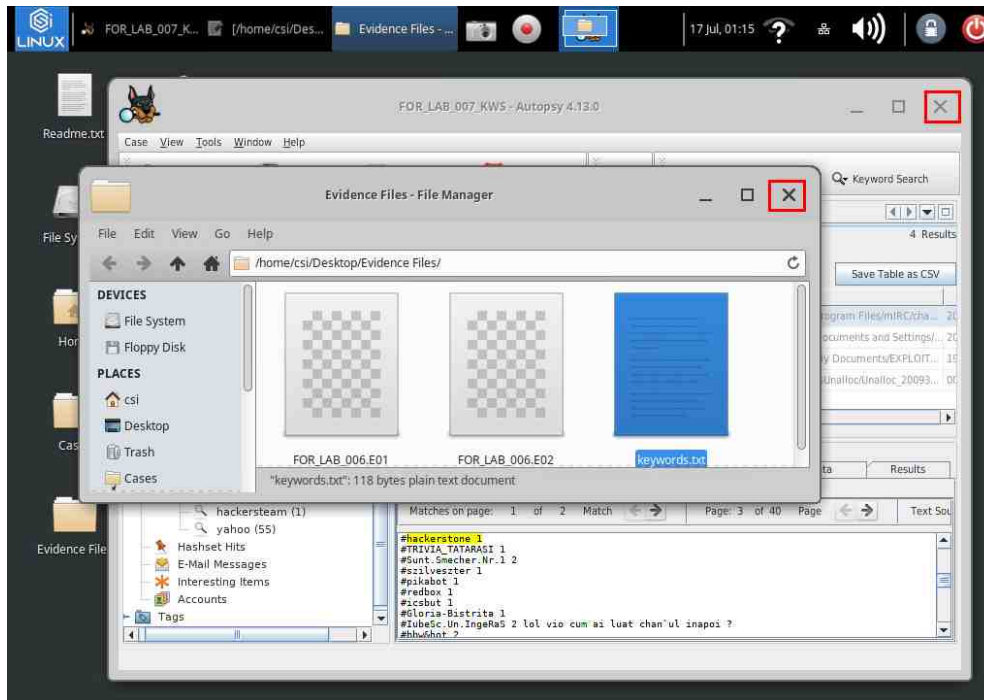


36. There is no limit to the number of keywords that you can search in a case. Navigate to the directory `/home/csi/Desktop/Evidence Files/FOR_LAB_006` seen in item 1. There you will find a text file titled `keywords.txt` seen in item 2. Double-click `keywords.txt` to open it in Mousepad text editor. The `keywords.txt` file contains several additional keywords that can be used to search the FEF. Please feel free to do an index search using any of these keywords and review the contents of the files that turn up. This will help you get an even better understanding of how keyword searching works.



37.

37. When you are done, click the X at the top-right corner of the open windows as highlighted below to close the programs.



38. In this exercise, you learned how to create a case in Autopsy and perform different types of keyword searches. These techniques will prove to be invaluable when performing forensic examinations, and as such, it is important for you to continue to build on this knowledge.