FORENSICS V2 LAB SERIES

Lab 06: Keyword Search & Analysis

Document Version: 2021-01-14

Contents

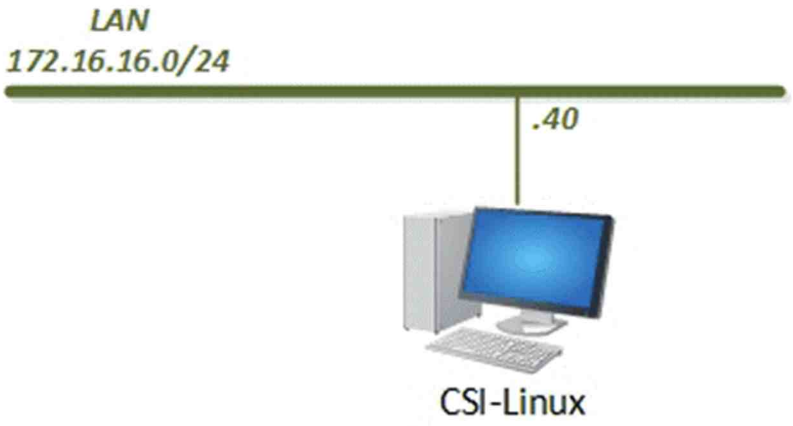
Introduction

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

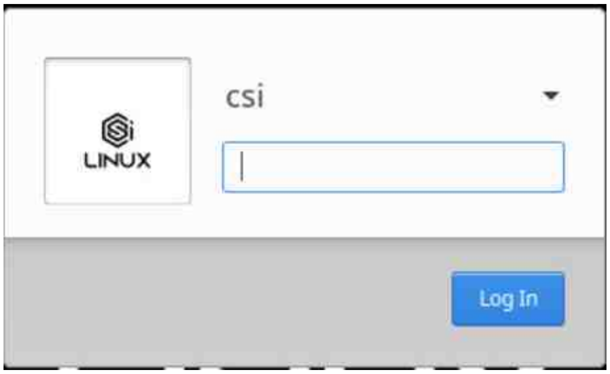
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

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

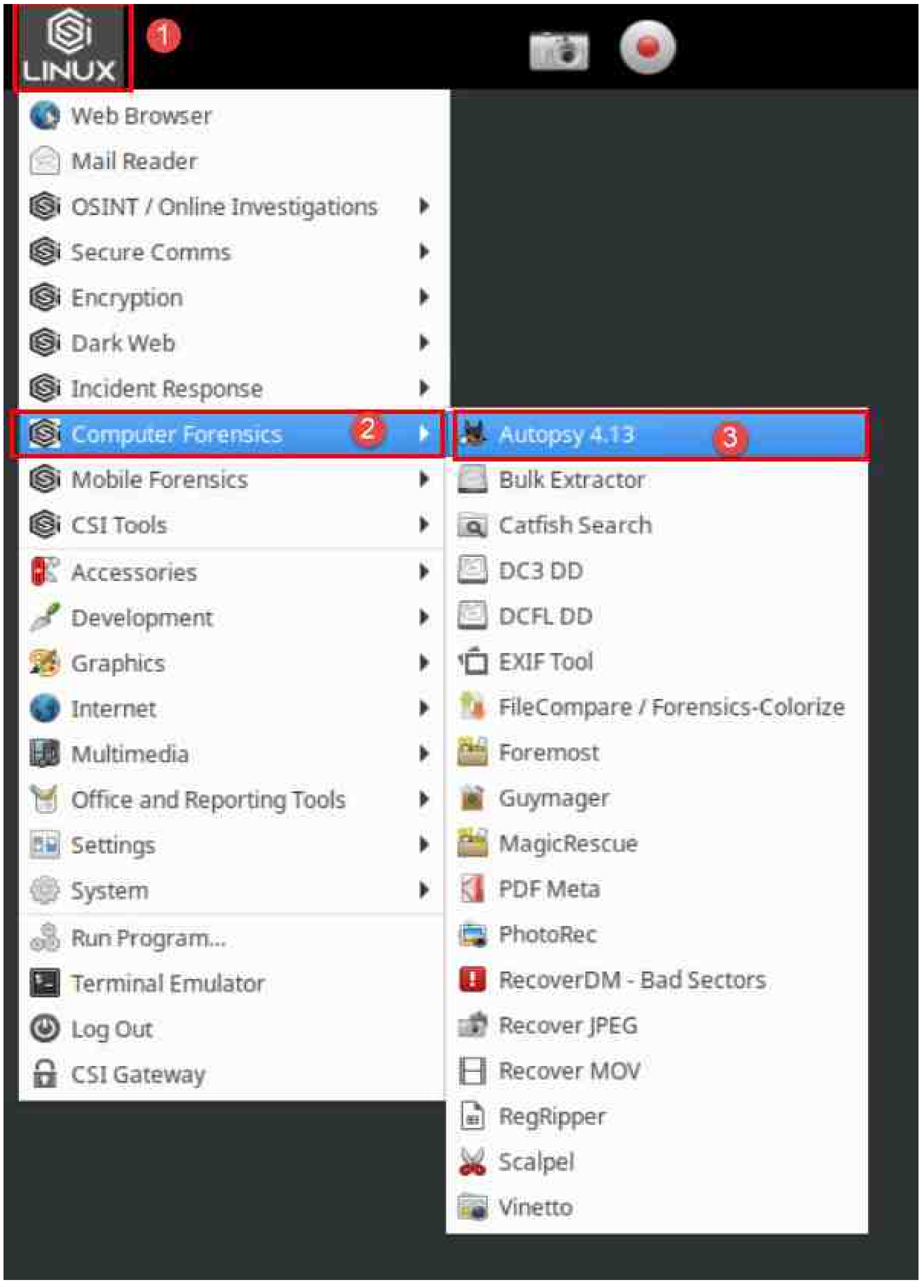
Learning to search through large volumes of data significantly speeds up investigations. In this lab, we will teach you to use a free forensic tool called Autopsy[1] to perform keyword searches in an evidence file. Autopsy™ is a digital forensics platform based on The Sleuth Kit™ that performs analysis, 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`

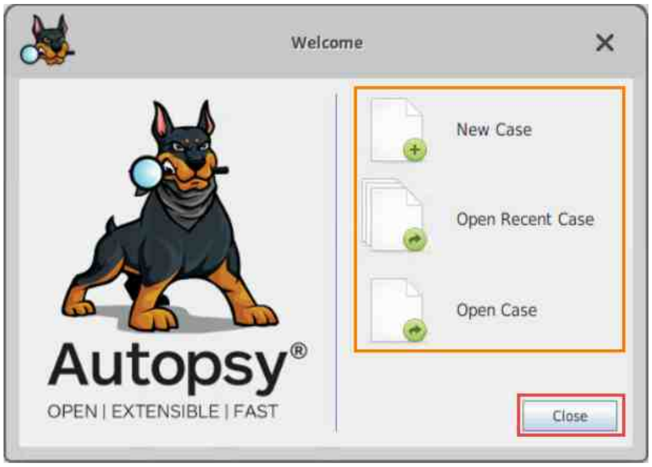


[1] https://www.autopsy.com/download/

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.

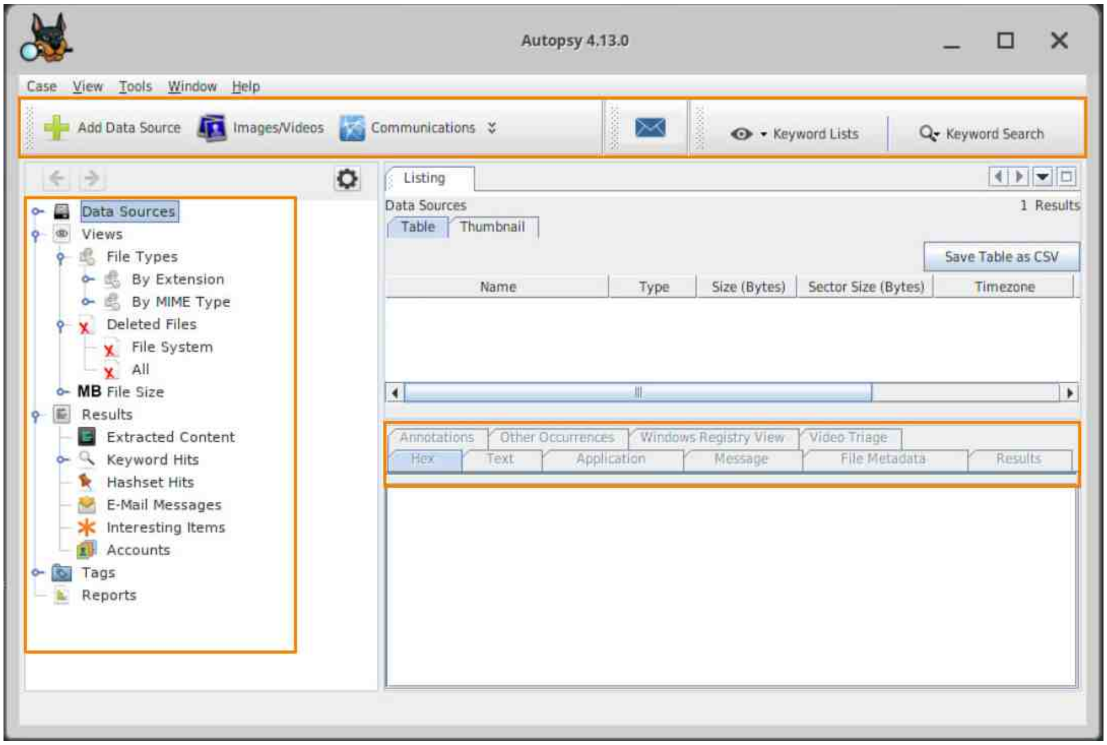


4. You will now be taken to the main GUI window. The table below will outline the features we will be using in this exercise. As always, please note that all the options are not listed here.

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

5. 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.

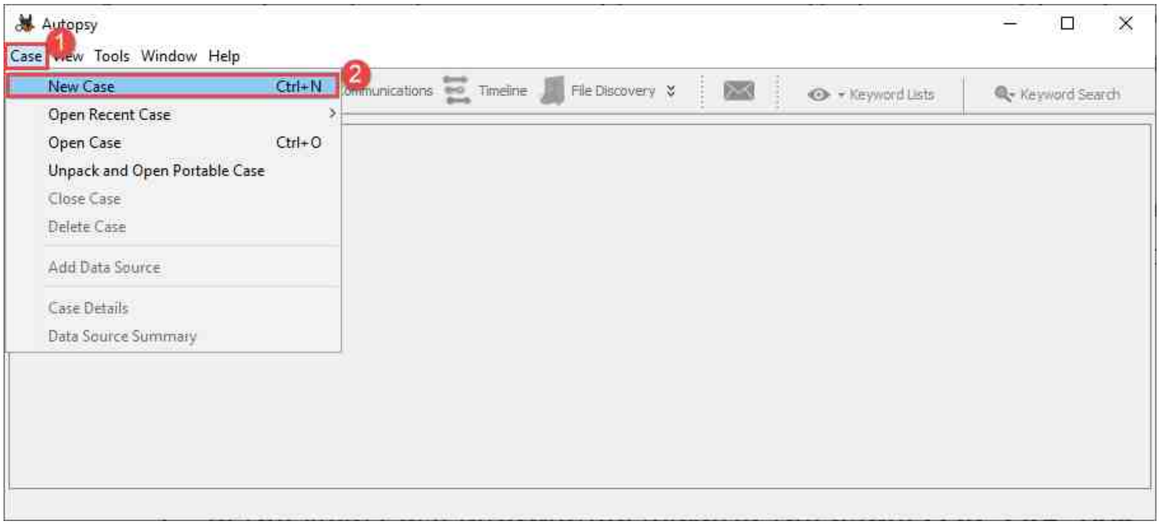


6. The features we covered allow you to view and search the data. There are some additional features that we will cover during the exercise. For now, let us use what we know so far to create a case and load some data so we can perform some searches.

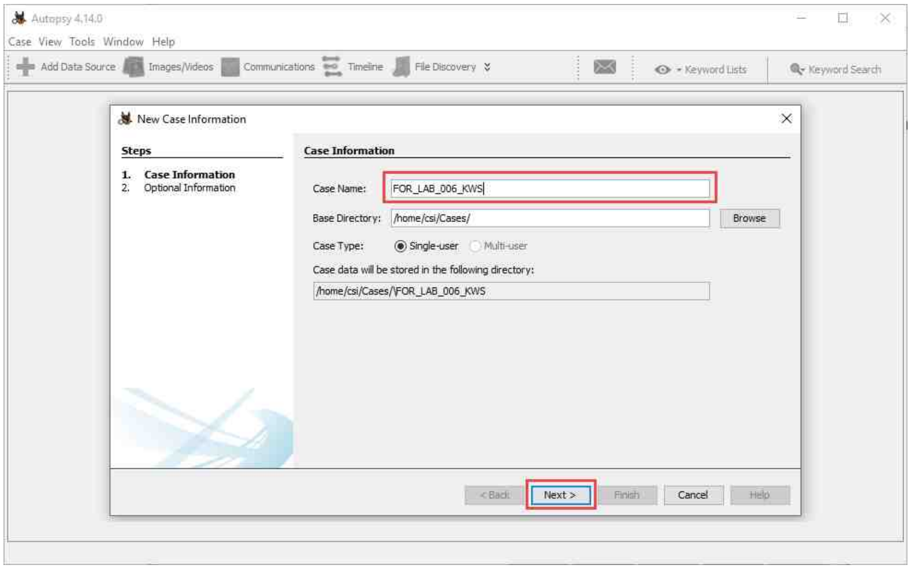
2 Searching with Autopsy

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.



New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: FOR_LAB_006_KWS

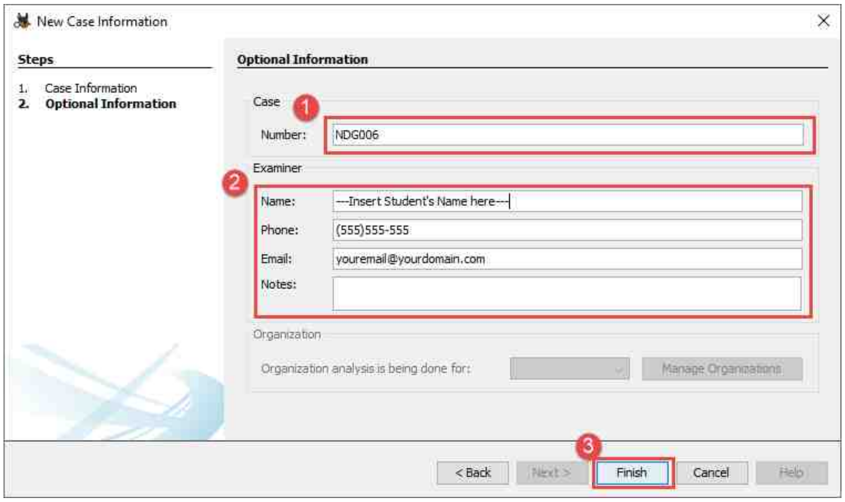
Base Directory: /home/csi/Cases/ Browse

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

/home/csi/Cases/\FOR_LAB_006_KWS

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.



Number: NDG006

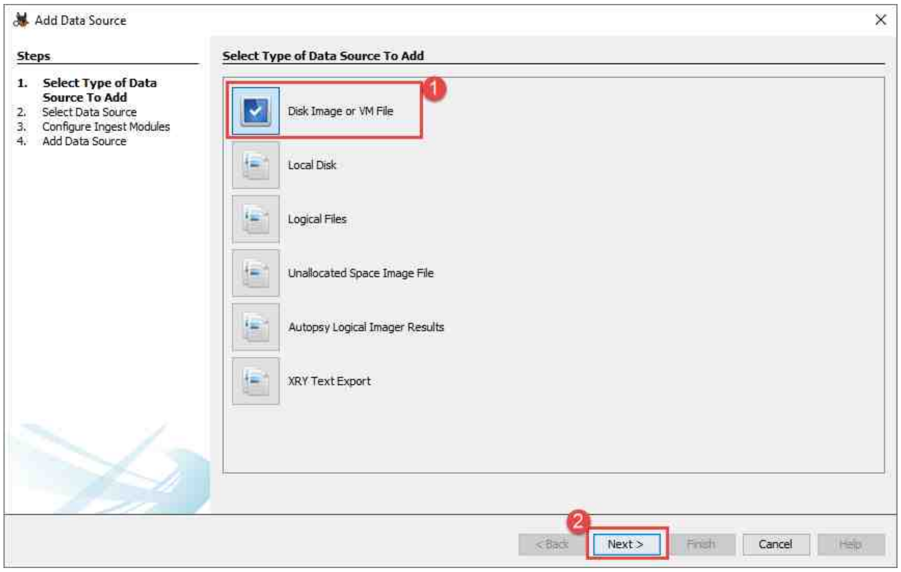
Name: ---Insert Student's Name here---

Phone: (555)555-555

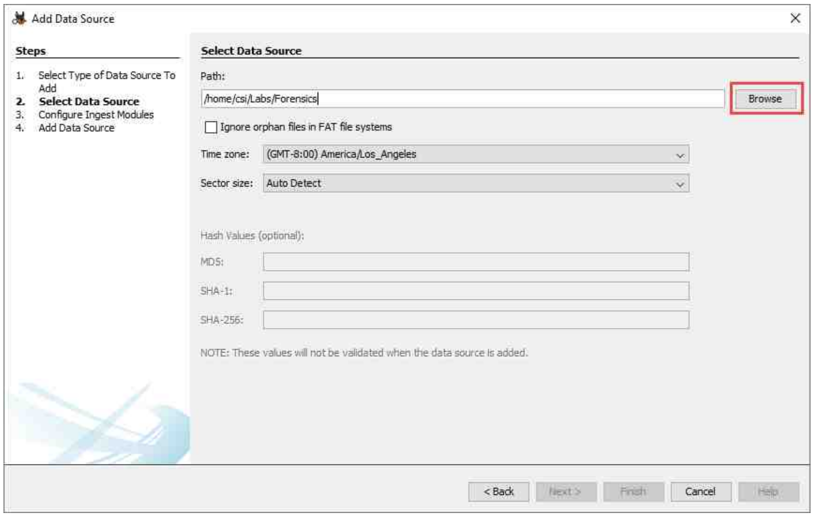
Email: youremail@yourdomain.com

Notes:

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
1
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
2
< Back
Next >
Finish
Cancel
Help

5. 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.



Select Data Source

Path: /home/csi/Labs/Forensics

□ Ignore orphan files in FAT file systems

Time zone: (GMT-8:00) America/Los_Angeles

Sector size: Auto Detect

Hash Values (optional):

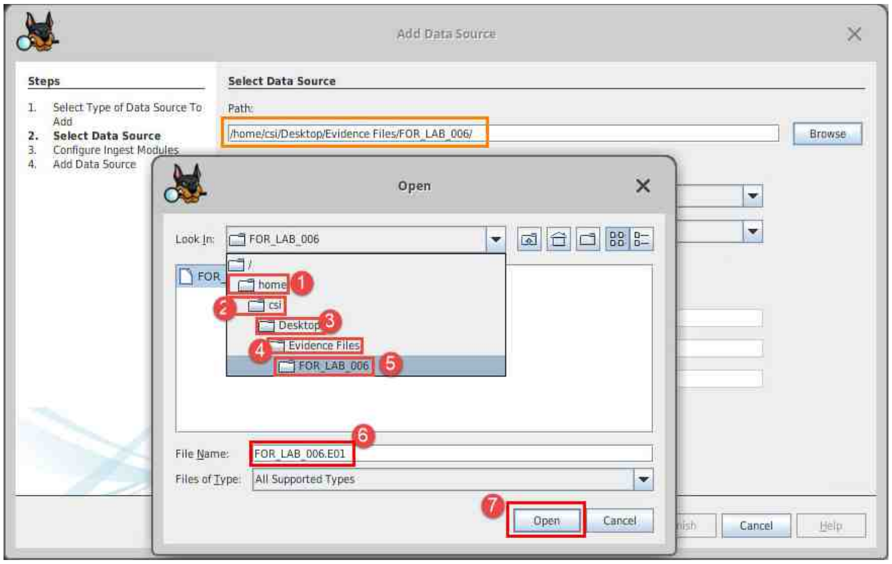
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

6. 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.



Select Data Source

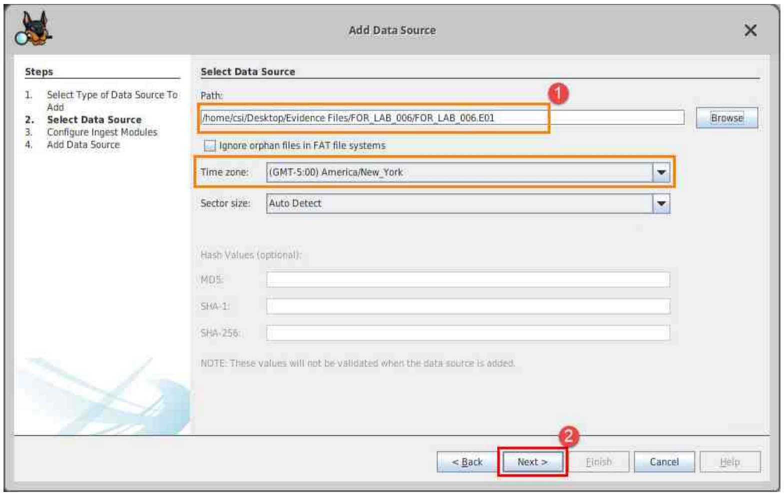
Path: /home/csi/Desktop/Evidence Files/FOR_LAB_006/

Look In: FOR_LAB_006

File Name: FOR_LAB_006.E01

Files of Type: All Supported Types

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.



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 Data Source

Path: /home/csi/Desktop/Evidence Files/FOR_LAB_006/FOR_LAB_006.E01

□ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/New_York

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

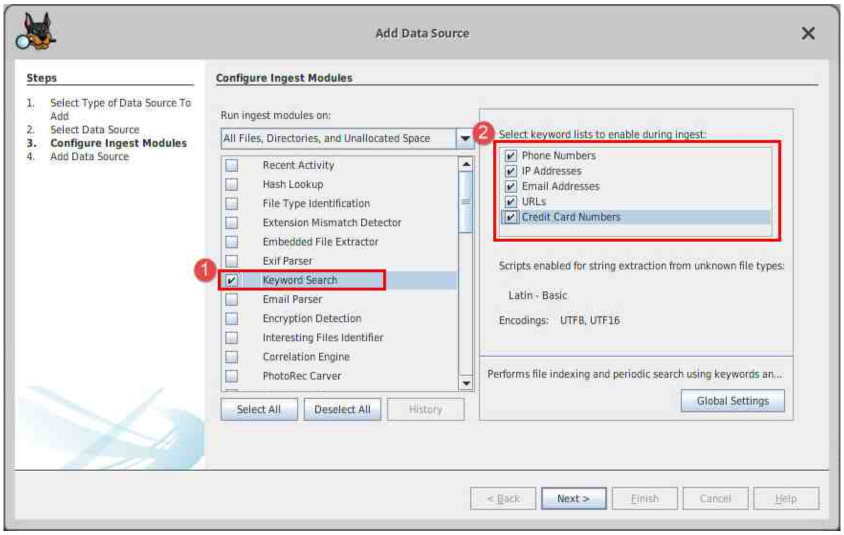
NOTE: These values will not be validated when the data source is added.

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

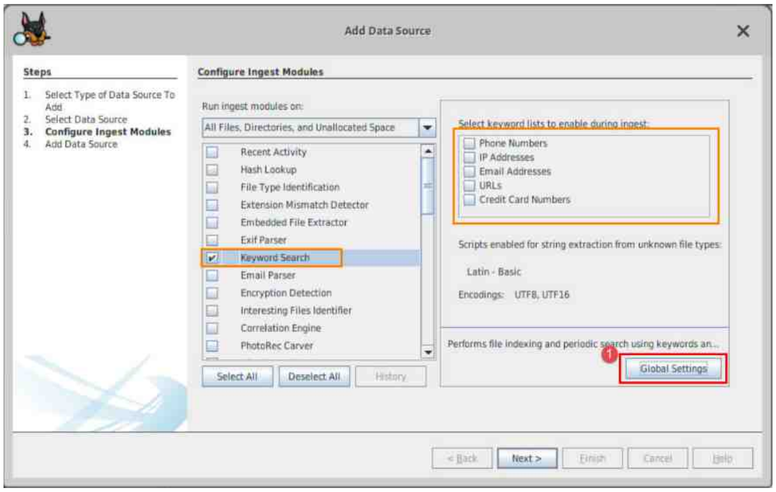
8. You will be taken to the Configure Ingest Modules step of the case creation process. Autopsy uses Ingest Modules to extract different types of data from data sources. The extracted data is then displayed in the main GUI window after the process is complete. In this exercise, we will only use the keyword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

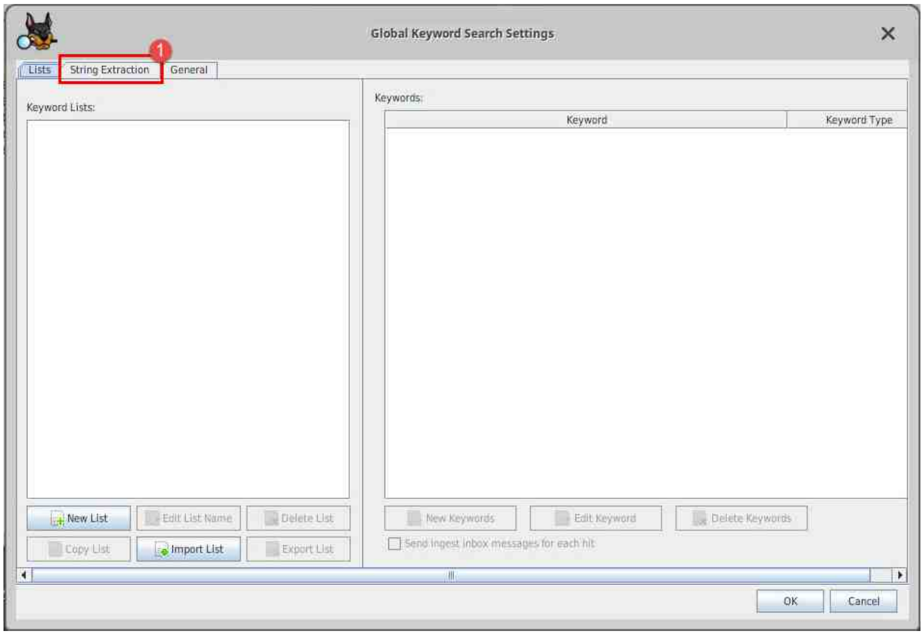
9. Let us begin by clicking the checkbox beside Keyword Search, as highlighted below. This module allows you to index and/or search the data. Once you enable the Keyword Search module, some options will appear in the right pane highlighted as item 2. These are the keyword lists that will be used to search 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.



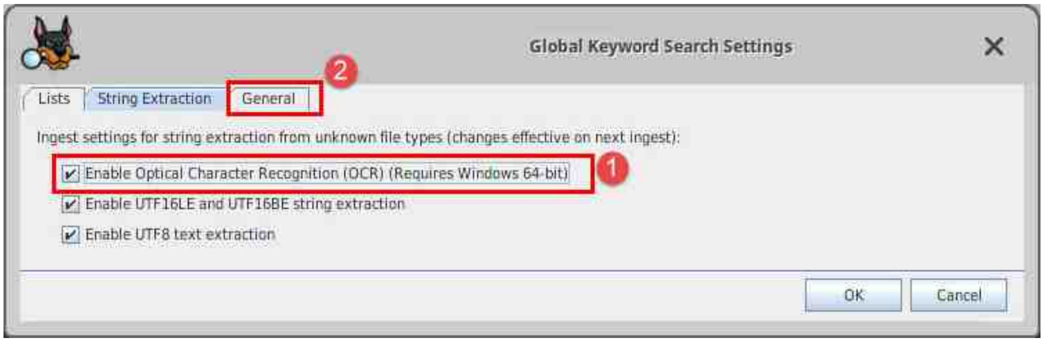
10. Some Ingest Modules are simply on or off, while others contain additional settings and can be configured to provide the results you want. The Keyword Search Ingest Module is one such module; it can be configured. Let us look at some of its settings. Click Global Settings, as highlighted below.



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.


Global Keyword Search Settings

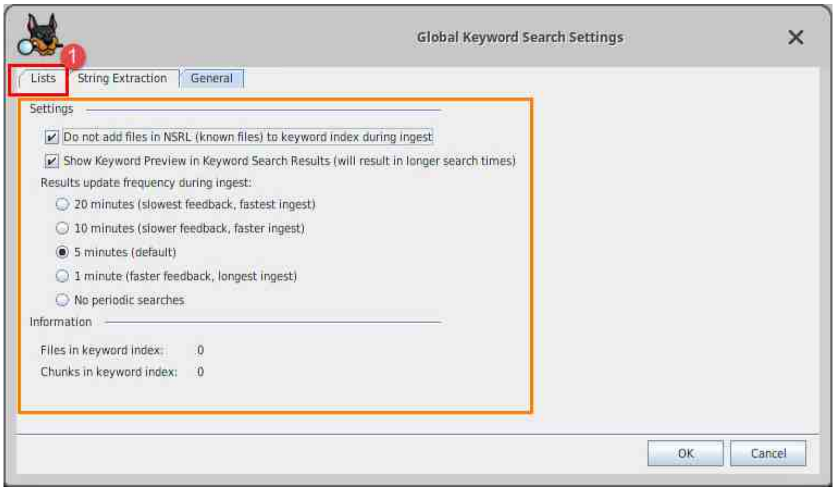
Ingest settings for string extraction from unknown file types (changes effective on next ingest):

☑ Enable Optical Character Recognition (OCR) (Requires Windows 64-bit)

☑ Enable UTF16LE and UTF16BE string extraction

☑ Enable UTF8 text extraction

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.



Settings

☑ Do not add files in NSRL (known files) to keyword index during ingest

☑ Show Keyword Preview in Keyword Search Results (will result in longer search times)

Results update frequency during ingest:

○ 20 minutes (slowest feedback, fastest ingest)

○ 10 minutes (slower feedback, faster ingest)

● 5 minutes (default)

○ 1 minute (faster feedback, longest ingest)

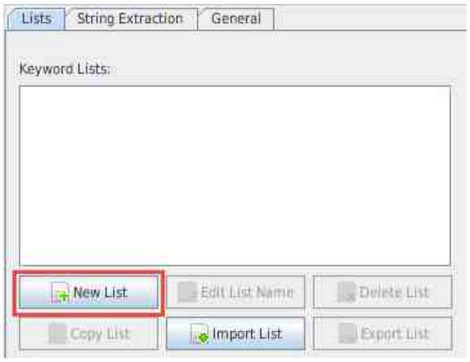
○ No periodic searches

Information

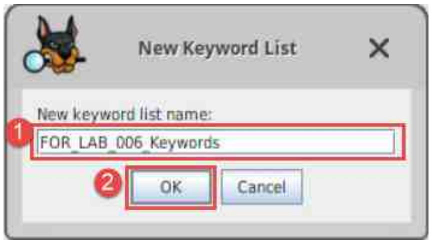
Files in keyword index: 0

Chunks in keyword index: 0

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

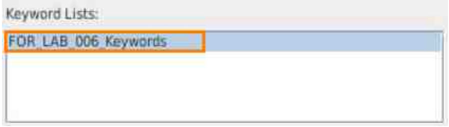


15. The New Keyword List window will appear and prompt for you to enter a name for the list. Let us call this list `FOR_LAB_006_Keywords` highlighted as item 1 below. Once you have written the name, click OK highlighted as item 2. This will add the list to the Global Keyword Search Settings main window.



New keyword list name: FOR_LAB_006_Keywords

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.



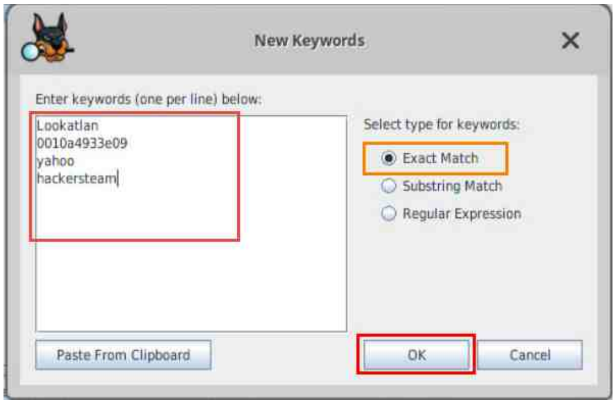
Keyword Lists:

FOR_LAB_006_Keywords

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:

Exact Match	Provides results that match the term you type exactly
Substring Match	Provides results that contain a part of your keyword
Regular Expression	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 keywords (one per line) below:

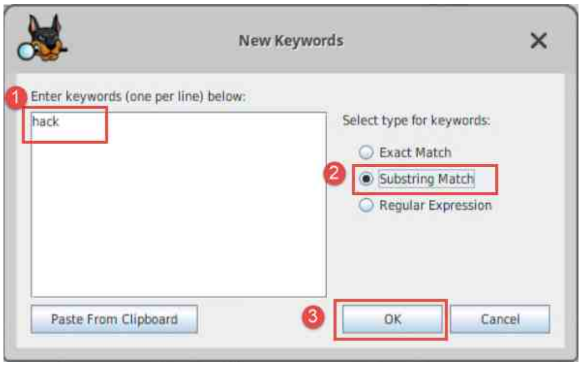
```
Lookatlan
0010a4933e09
yahoo
hackersteam
```

Select type for keywords:

● Exact Match
○ Substring Match
○ Regular Expression

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.



New Keywords

1 Enter keywords (one per line) below:

hack

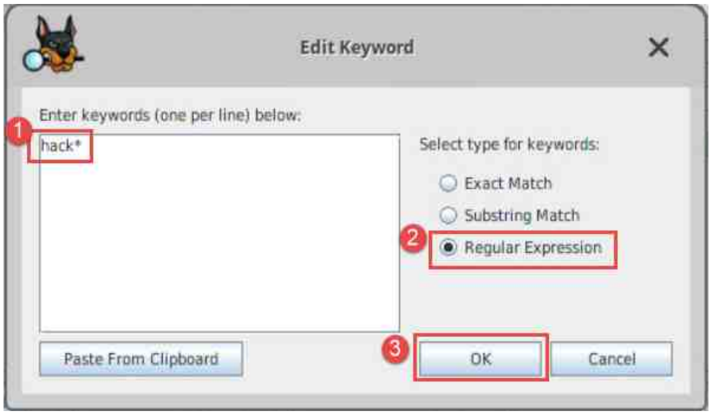
Select type for keywords:

○ Exact Match

2 ● Substring Match

○ Regular Expression

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.



Edit Keyword

1 Enter keywords (one per line) below:

hack*

Select type for keywords:

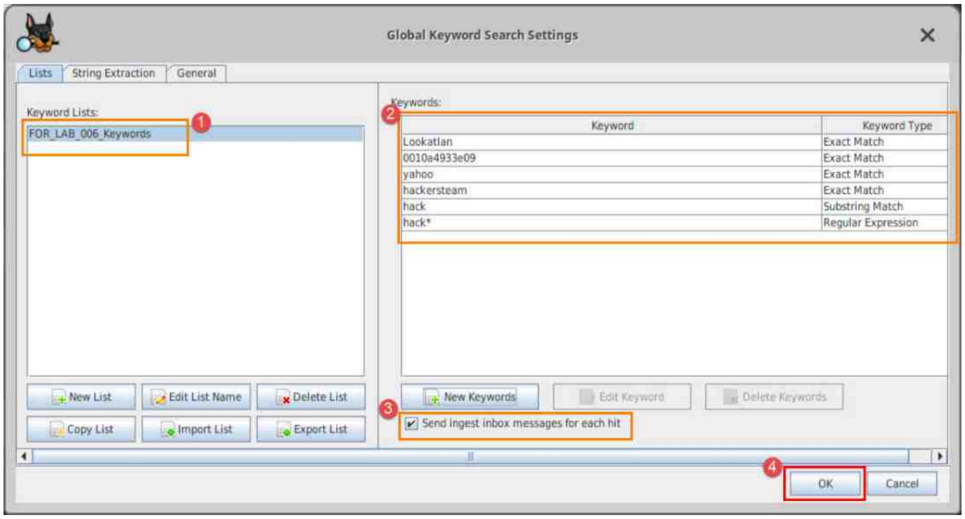
○ Exact Match

○ Substring Match

2 ● Regular Expression

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.



Keyword Lists:
FOR_LAB_006_Keywords

Keywords:

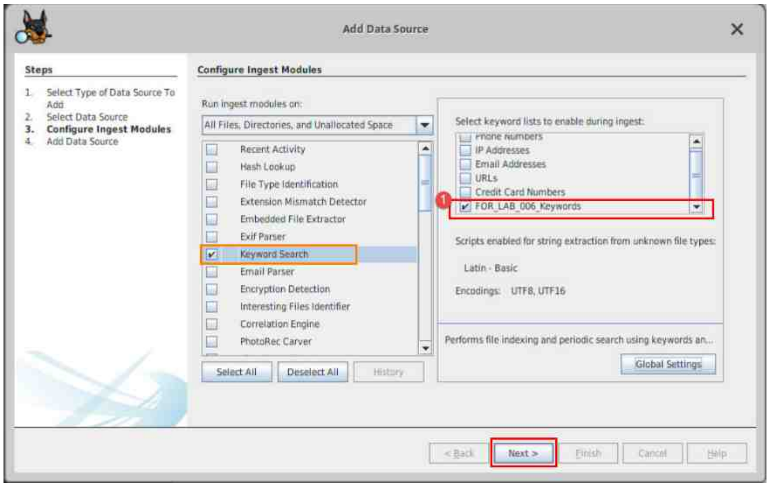
Keyword	Keyword Type
Lookatlan	Exact Match
0010a4933e09	Exact Match
yahoo	Exact Match
hackersteam	Exact Match
hack	Substring Match
hack*	Regular Expression

☑ Send ingest inbox messages for each hit

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.



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

Configure Ingest Modules

Run ingest modules on:
All Files, Directories, and Unallocated Space

□ Recent Activity
□ Hash Lookup
□ File Type Identification
□ Extension Mismatch Detector
□ Embedded File Extractor
□ Exif Parser
☑ Keyword Search
□ Email Parser
□ Encryption Detection
□ Interesting Files Identifier
□ Correlation Engine
□ PhotoRec Carver

Select keyword lists to enable during ingest:
□ Phone Numbers
□ IP Addresses
□ Email Addresses
□ URLs
□ Credit Card Numbers
☑ FOR_LAB_006_Keywords

Scripts enabled for string extraction from unknown file types:

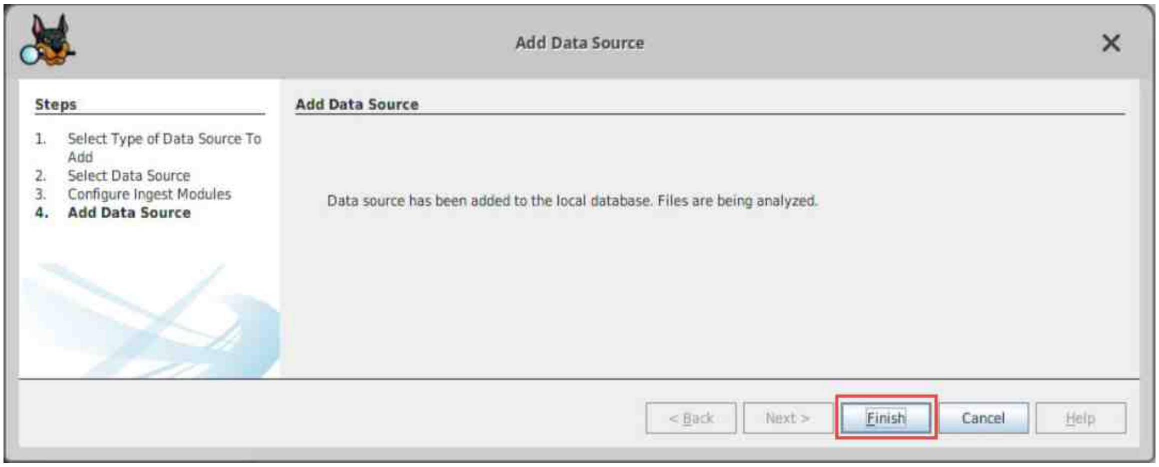
Latin - Basic

Encodings: UTF8, UTF16

Performs file indexing and periodic search using keywords an...

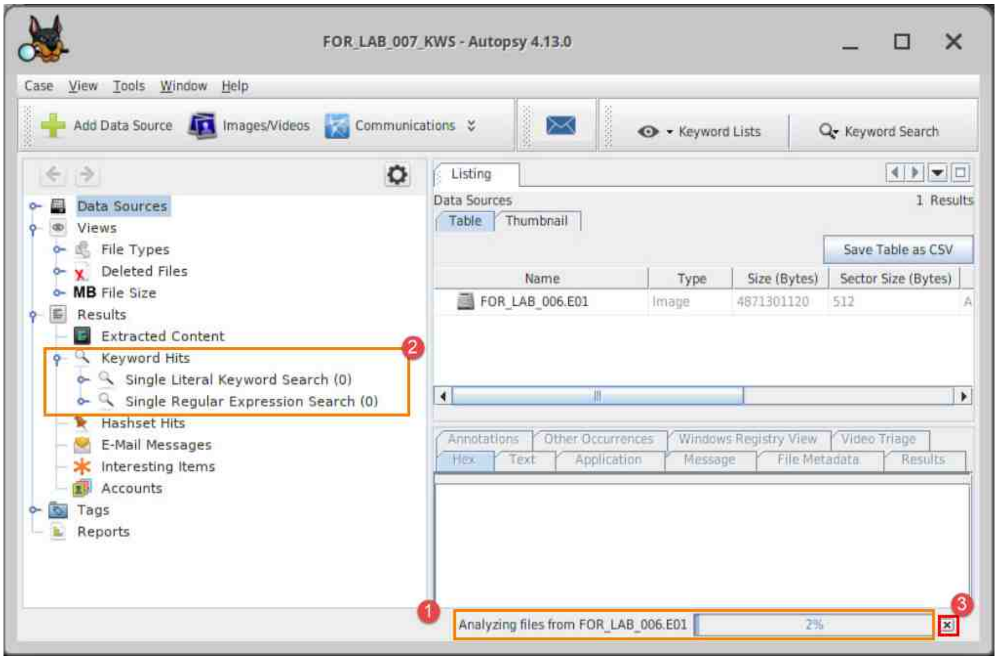
> **STOP** Again, ensure to uncheck the default keyword search lists before proceeding to the next step.

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



Data source has been added to the local database. Files are being analyzed.

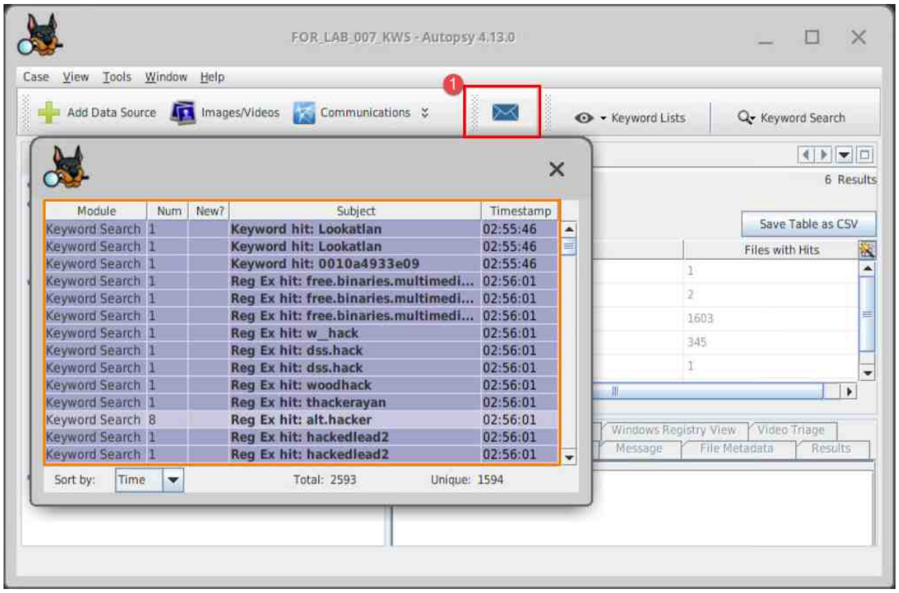
24. You will now be taken to the Autopsy main window. Here the Keyword Search Ingest Module will search the entire FEF; the progress is displayed at the bottom-right corner as seen highlighted at item 1. The decoded results will gradually populate the Keyword Hits section as highlighted at item 2. Processing 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.



Name	Type	Size (Bytes)	Sector Size (Bytes)
FOR_LAB_006.E01	Image	4871301120	512

Analyzing files from FOR_LAB_006.E01 2%

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.

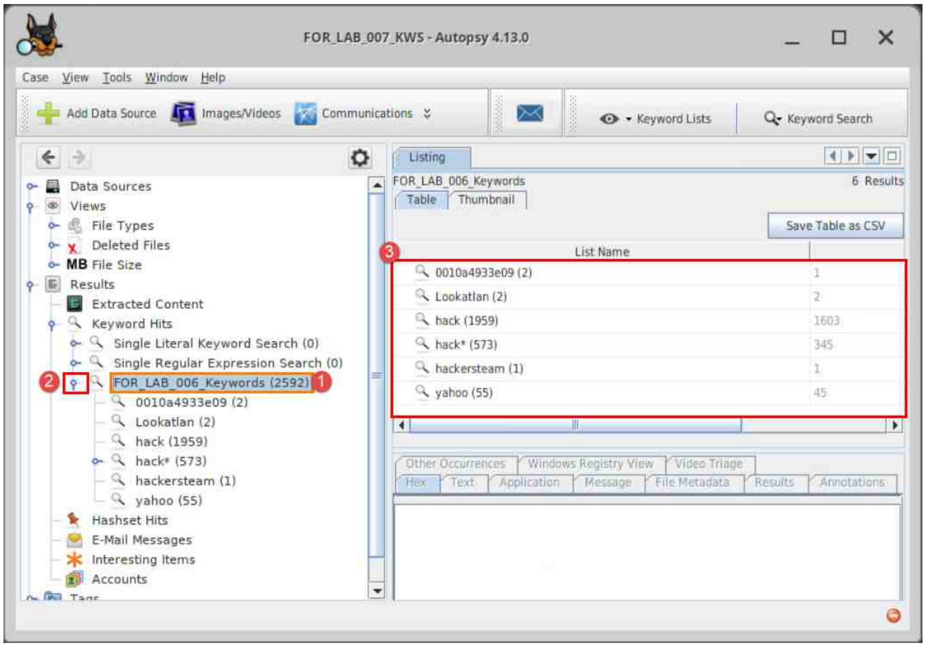


Module	Num	New?	Subject	Timestamp
Keyword Search	1		Keyword hit: Lookatlan	02:55:46
Keyword Search	1		Keyword hit: Lookatlan	02:55:46
Keyword Search	1		Keyword hit: 0010a4933e09	02:55:46
Keyword Search	1		Reg Ex hit: free.binaries.multimedi...	02:56:01
Keyword Search	1		Reg Ex hit: free.binaries.multimedi...	02:56:01
Keyword Search	1		Reg Ex hit: free.binaries.multimedi...	02:56:01
Keyword Search	1		Reg Ex hit: w_hack	02:56:01
Keyword Search	1		Reg Ex hit: dss.hack	02:56:01
Keyword Search	1		Reg Ex hit: dss.hack	02:56:01
Keyword Search	1		Reg Ex hit: woodhack	02:56:01
Keyword Search	1		Reg Ex hit: thackerayan	02:56:01
Keyword Search	8		Reg Ex hit: alt.hacker	02:56:01
Keyword Search	1		Reg Ex hit: hackedlead2	02:56:01
Keyword Search	1		Reg Ex hit: hackedlead2	02:56:01

Sort by: Time   Total: 2593   Unique: 1594

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%.

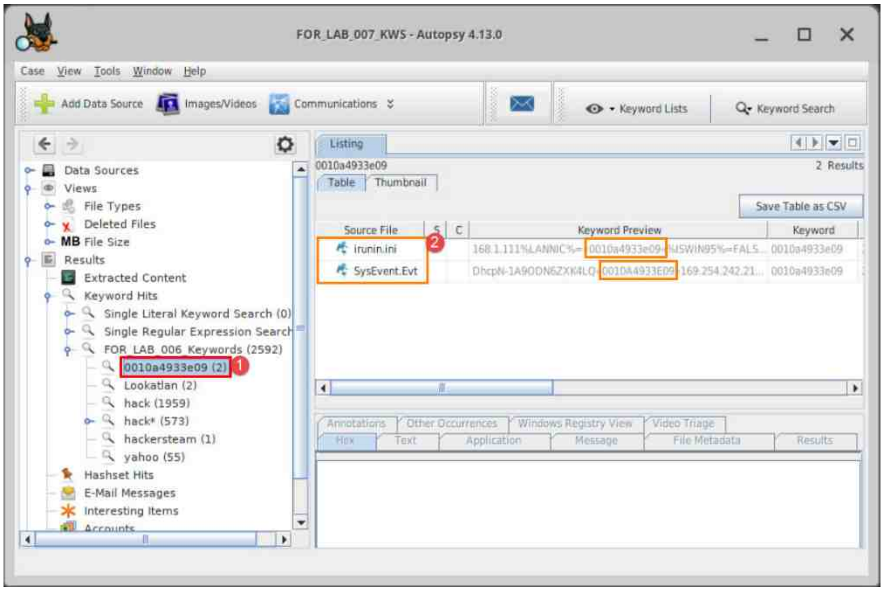
26. The search results are shown in the Keyword Hits section highlighted as item 1 below. The blue pin in item 2 below indicates that there is a subdirectory within the associated list item. Click the blue pin beside the list item called FOR_LAB_006_Keywords, highlighted as item 2, to reveal the results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



List Name	
0010a4933e09 (2)	1
Lookatlan (2)	2
hack (1959)	1603
hack* (573)	345
hackersteam (1)	1
yahoo (55)	45

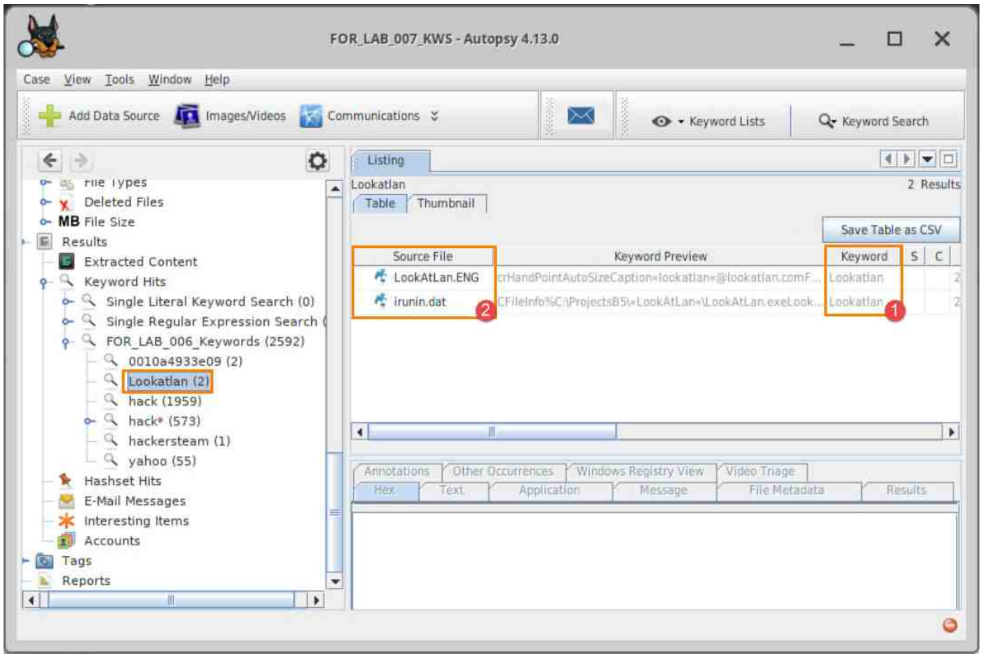
Expand all sub-directories to view the full directory tree pane.

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.



Source File	S	C	Keyword Preview	Keyword
irunin.ini			168.1.111%LANNIC%=0010a4933e09%ISWIN95%=FALS...	0010a4933e09
SysEvent.Evt			DhcpN-1A9ODN6ZXK4LQ-0010A4933E09-169.254.242.21...	0010a4933e09

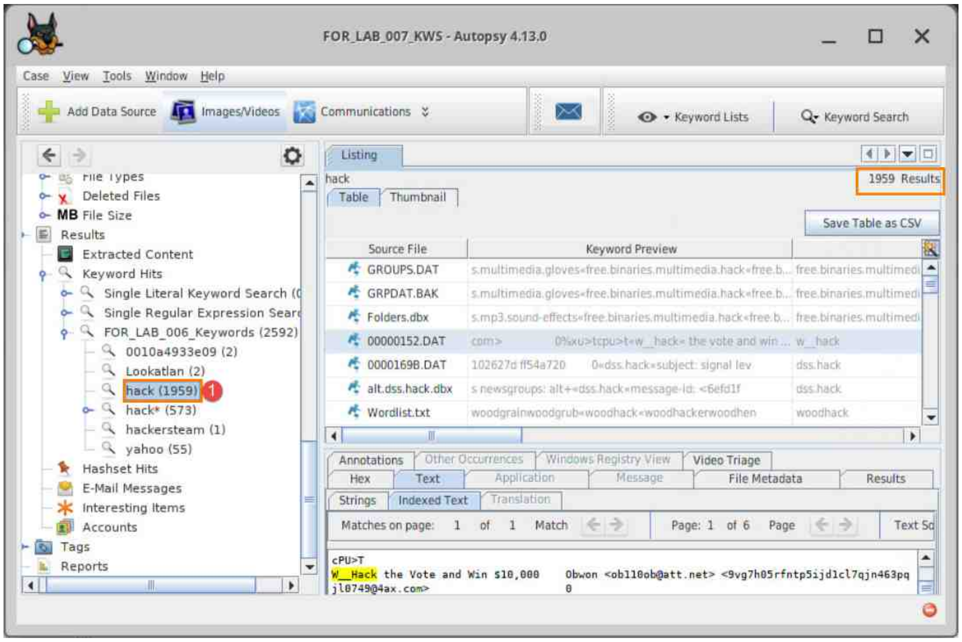
28. If you look at the keyword column highlighted as item 1 below, you will see the search term used to find each result. The result highlighted as item 2 is the Exact Match. This search term only identified the exact term lookatlan. If there were any special characters within the search term, then the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



Lookatlan 2 Results

Source File	Keyword Preview	Keyword	S	C
LookAtLan.ENG	crHandPointAutoSizeCaption«lookatlan«@lookatlan.comF...	Lookatlan		
irunin.dat	CFileInfo%C:\ProjectsB5\«LookAtLan«\LookAtLan.exeLook...	Lookatlan		

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.

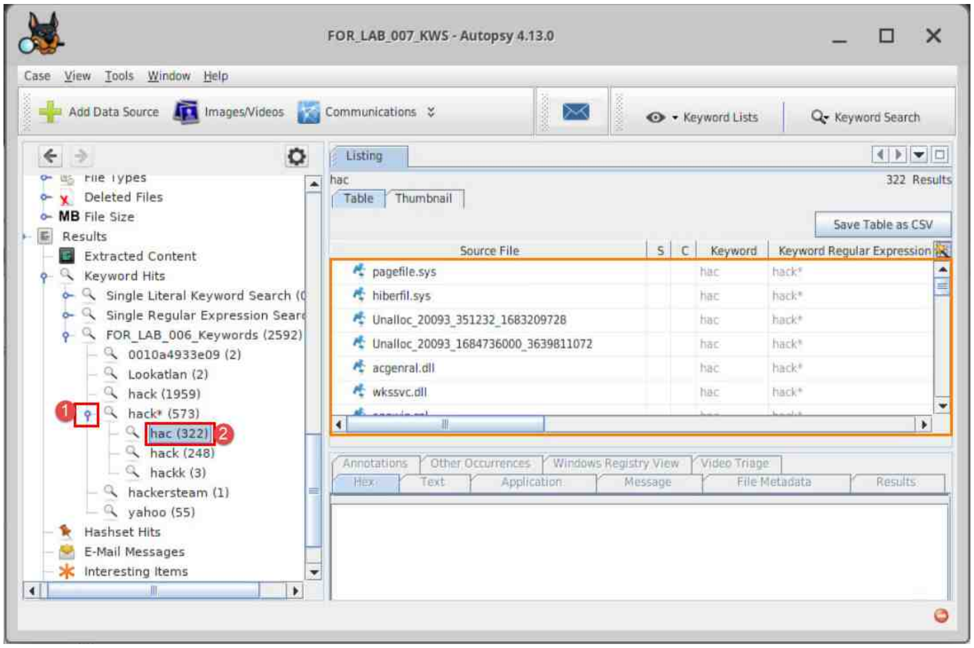


hack 1959 Results

Source File	Keyword Preview	
GROUPS.DAT	s.multimedia.gloves«free.binaries.multimedia.hack«free.b...	free.binaries.multimedi
GRPDAT.BAK	s.multimedia.gloves«free.binaries.multimedia.hack«free.b...	free.binaries.multimedi
Folders.dbx	s.mp3.sound-effects«free.binaries.multimedia.hack«free.b...	free.binaries.multimedi
00000152.DAT	com> 0%xu>tcpu>t«w__hack« the vote and win ...	w__hack
0000169B.DAT	102627d ff54a720 0«dss.hack«subject: signal lev	dss.hack
alt.dss.hack.dbx	s.newsgroups: alt+«dss.hack«message-id: <6efd1f	dss.hack
Wordlist.txt	woodgrainwoodgrub«woodhack«woodhackerwoodhen	woodhack

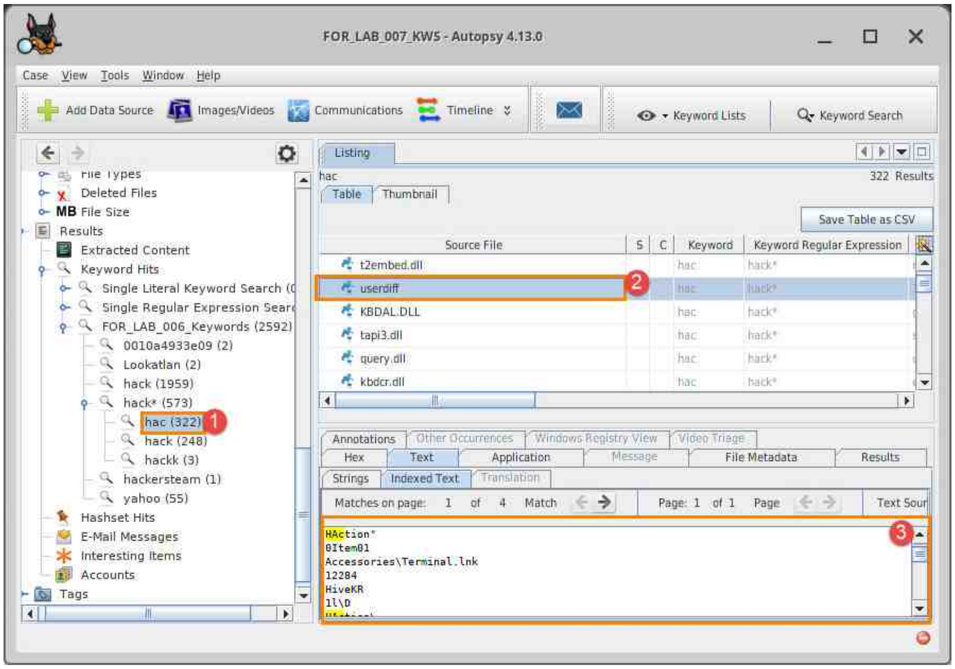
```
cPU>T
W__Hack the Vote and Win $10,000    Obwon <ob110ob@att.net> <9vg7h05rfntp5ijd1cl7qjn463pq
jl0749@4ax.com>                     0
```

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.



Source File	S	C	Keyword	Keyword Regular Expression
pagefile.sys			hac	hack*
hiberfil.sys			hac	hack*
Unalloc_20093_351232_1683209728			hac	hack*
Unalloc_20093_1684736000_3639811072			hac	hack*
acgenral.dll			hac	hack*
wkssvc.dll			hac	hack*

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.

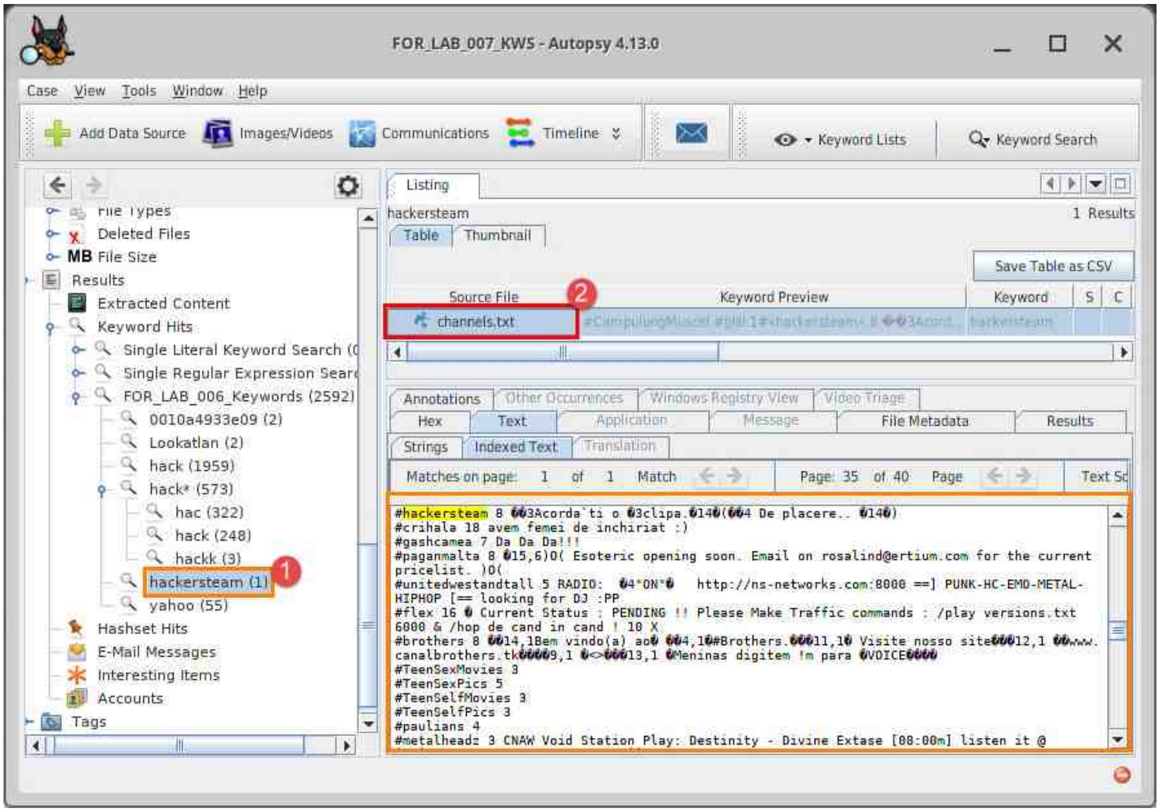


Source File	S	C	Keyword	Keyword Regular Expression
t2embed.dll			hac	hack*
userdiff			hac	hack*
KBDAL.DLL			hac	hack*
tapi3.dll			hac	hack*
query.dll			hac	hack*
kbdcr.dll			hac	hack*

```
HAction"
0Item01
Accessories\Terminal.lnk
12284
HiveKR
1l\D
```

> 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.

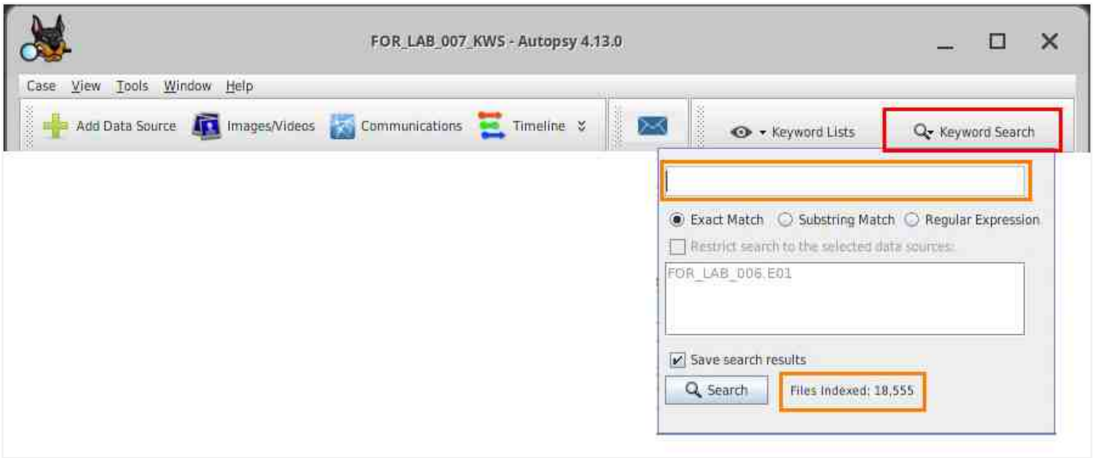
32. Now that we have identified the different types of keywords and the possible results that can be recovered from each, let us look at some ambiguous search terms vs. refined ones. Let us say we wanted to find the term hackersteam. As you saw earlier, the search term hack had over 1000 results. The 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.



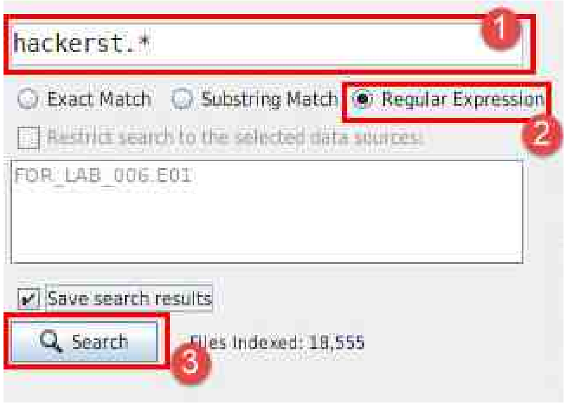
Source File	Keyword Preview	Keyword	S	C
channels.txt	#CampulungMuscel #jill 1#«hackersteam» 8 ��3Acord...	hackersteam		

```
#hackersteam 8 ��3Acorda`ti o �3clipa.�14�(��4 De placere.. �14�)
#crihala 18 avem femei de inchiriat :)
#gashcamea 7 Da Da Da!!!
#paganmalta 8 �15,6)O( Esoteric opening soon. Email on rosalind@ertium.com for the current
pricelist. )O(
#unitedwestandtall 5 RADIO:  �4*ON*�   http://ns-networks.com:8000 ==] PUNK-HC-EMO-METAL-
HIPHOP [== looking for DJ :PP
#flex 16 � Current Status : PENDING !! Please Make Traffic commands : /play versions.txt
6000 & /hop de cand in cand ! 10 X
#brothers 8 ��14,1Bem vindo(a) ao� ��4,1�#Brothers.���11,1� Visite nosso site���12,1 ��www.
canalbrothers.tk����9,1 �<>���13,1 �Meninas digitem !m para �VOICE����
#TeenSexMovies 3
#TeenSexPics 5
#TeenSelfMovies 3
#TeenSelfPics 3
#paulians 4
#metalheadz 3 CNAW Void Station Play: Destinity - Divine Extase [00:00m] listen it @
```

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.

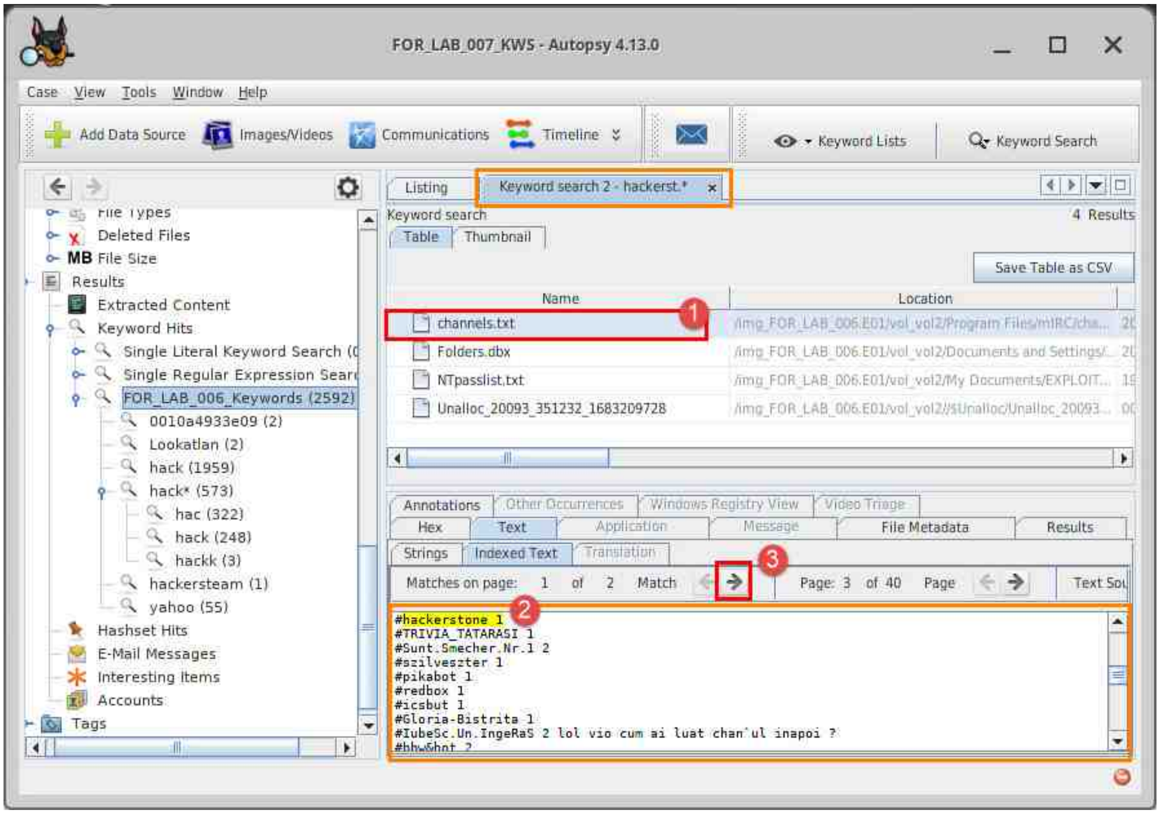

FOR_LAB_007_KWS - Autopsy 4.13.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
Keyword Lists
Keyword Search
○ Exact Match ○ Substring Match ○ Regular Expression
□ Restrict search to the selected data sources:
FOR_LAB_006.E01
☑ Save search results
Search
Files Indexed: 18,555

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.


hackerst.*
1
○ Exact Match ○ Substring Match ● Regular Expression
2
□ Restrict search to the selected data sources:
FOR_LAB_006.E01
☑ Save search results
Search
3
Files Indexed: 18,555

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.

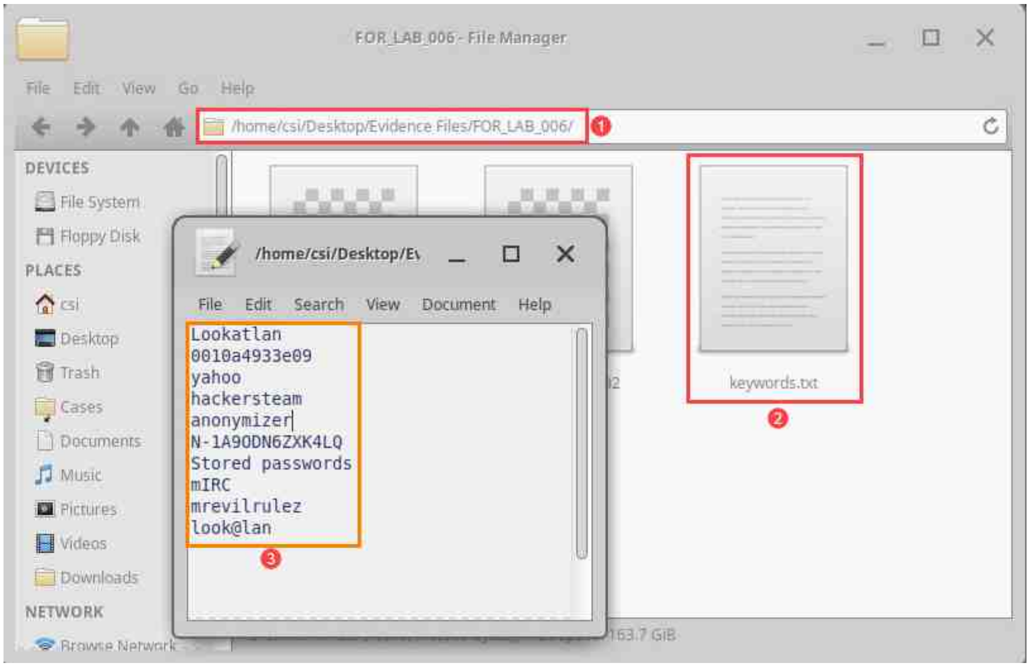
35. The index search should be quick, and the results should increase in comparison to our previous search for the term hackersteam. The Regular Expression term hackerst.* searches for all terms that start with the letters hackerst and will find any occurrence of it regardless of the string that follows 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.



Name	Location
channels.txt	/img_FOR_LAB_006.E01/vol_vol2/Program Files/mIRC/cha...
Folders.dbx	/img_FOR_LAB_006.E01/vol_vol2/Documents and Settings/...
NTpasslist.txt	/img_FOR_LAB_006.E01/vol_vol2/My Documents/EXPLOIT...
Unalloc_20093_351232_1683209728	/img_FOR_LAB_006.E01/vol_vol2/$Unalloc/Unalloc_20093...

```
#hackerstone 1
#TRIVIA_TATARASI 1
#Sunt.Smecher.Nr.1 2
#szilveszter 1
#pikabot 1
#redbox 1
#icsbut 1
#Gloria-Bistrita 1
#IubeSc.Un.IngeRaS 2 lol vio cum ai luat chan'ul inapoi ?
#bhw&hot 2
```

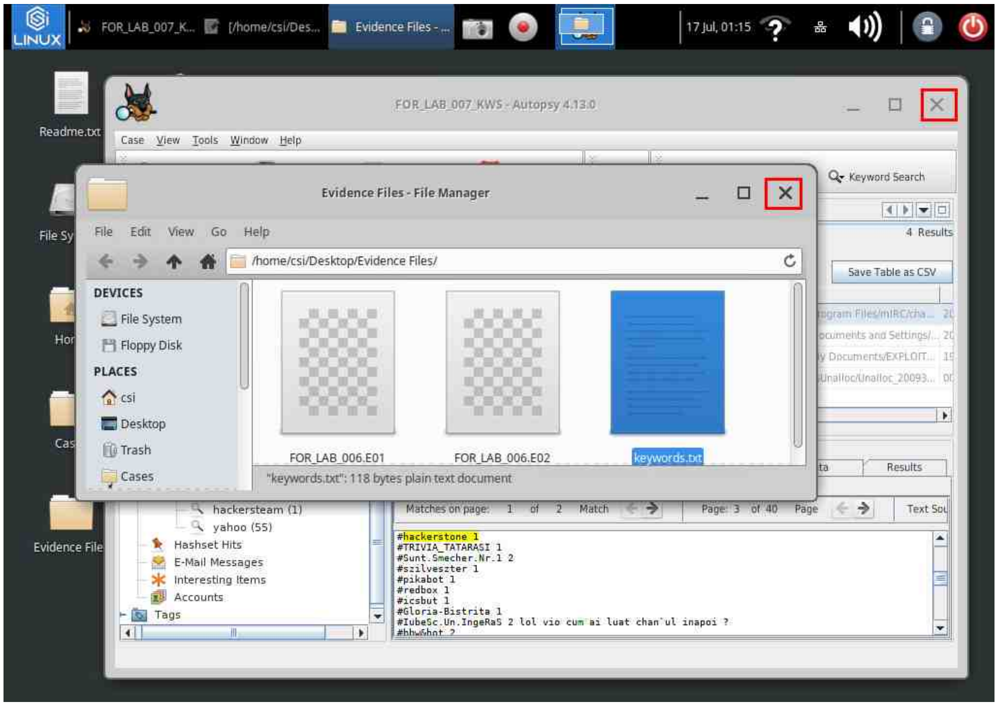
36. There is no limit to the number of keywords that you can search in a case. Navigate to the directory /home/csi/Desktop/Evidence Files/FOR_LAB_006 seen in item 1. There you will find a text file titled keywords.txt seen in item 2. Double-click keywords.txt to open it in Mousepad text editor. The keywords.txt 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.



```
Lookatlan
0010a4933e09
yahoo
hackersteam
anonymizer
N-1A9ODN6ZXK4LQ
Stored passwords
mIRC
mrevilrulez
look@lan
```

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.



```
#hackerstone 1
#TRIVIA_TATARASI 1
#Sunt.Smecher.Nr.1 2
#szilveszter 1
#pikabot 1
#redbox 1
#icsbut 1
#Gloria-Bistrita 1
#IubeSc.Un.IngeRaS 2 lol vio cum ai luat chan`ul inapoi ?
#bhw6hot 2
```

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.