



FORENSICS V2 LAB SERIES

Lab 18: Page File Analysis

Document Version: 2021-01-11

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 Identifying and Extracting the pagefile.sys File	6
2 Getting to Know Bulk Extractor Viewer	16
3 Extracting and Reviewing Data from the pagefile.sys	18

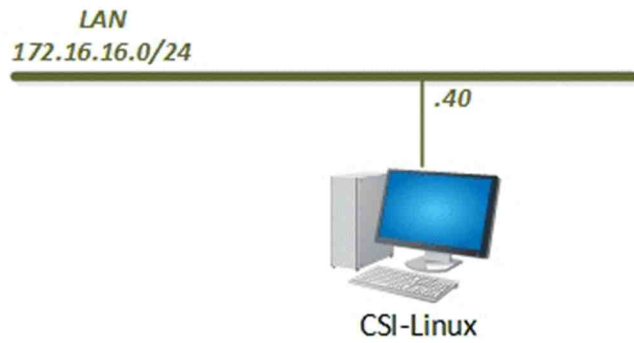
Introduction

The page file stores data that was in memory and can persist even after the computer has lost power. This module will cover what the page file is and how to navigate it to help in an investigation.

Objectives

-) Objectives o Learn what a page file is
-) Learn where to find the page file and how to extract it
-) Learn how to extract useful data from it

Lab Topology



Lab Settings

The information in the table below will be needed in order 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 Identifying and Extracting the pagefile.sys File

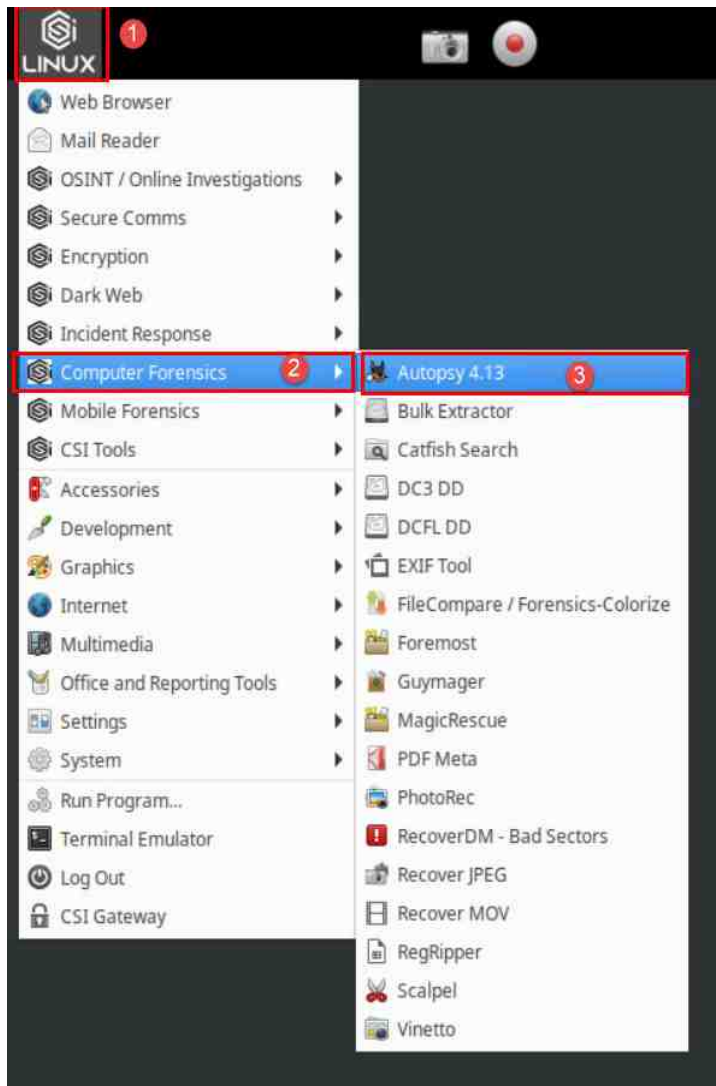
Forensic examiners tell stories about things a user did and saw while they were using a digital device. One of the best ways to get an idea of what the user was seeing, and things that happened in the background, is to review the contents of memory. Unfortunately, memory is volatile which means data within it is not accessible after the computer has been shut down. This is where the page file comes in handy. This file stores data that was in RAM but not currently in use. A user can set the file to be cleared once the computer is shut down, but it is not enabled by default. In this lab, we will identify and extract the file and then review some data within it.

Let's get started by opening Autopsy and loading a FEF.

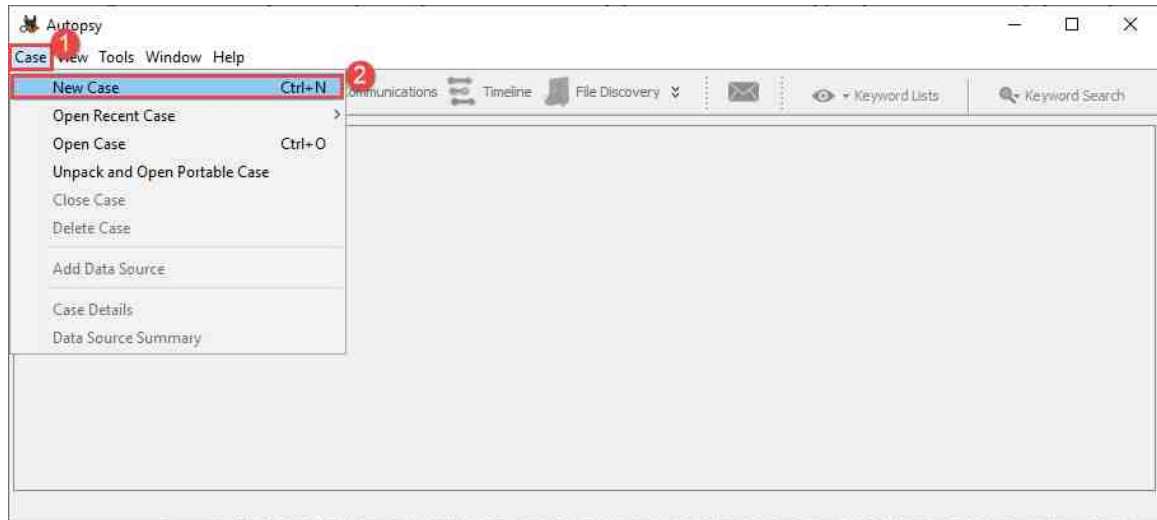
1. To begin, launch the CSI-Linux virtual machine to access the graphical login screen. Log in as `csi` using the password: `csi`



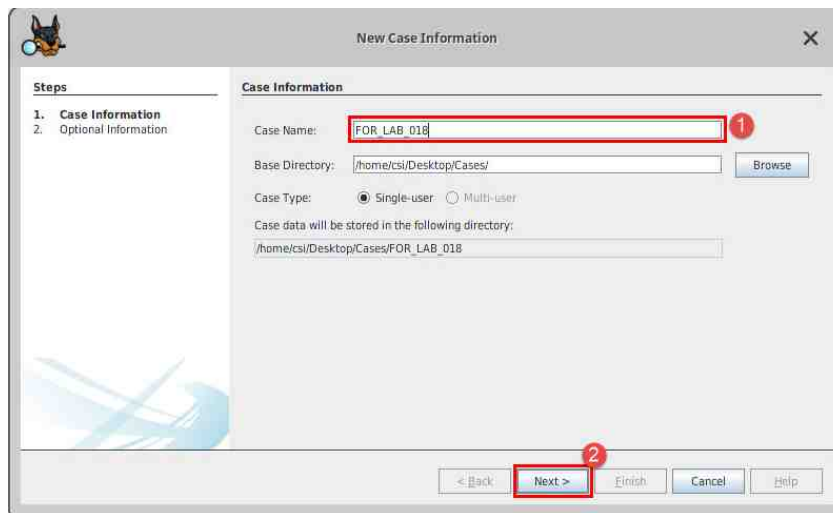
2. Once you are logged into the VM, launch the Autopsy program from the Start menu by navigating to Application Menu (Top left corner) > Computer Forensics > Autopsy 4.13. Alternatively, you can open Autopsy from the taskbar by clicking the Autopsy icon:



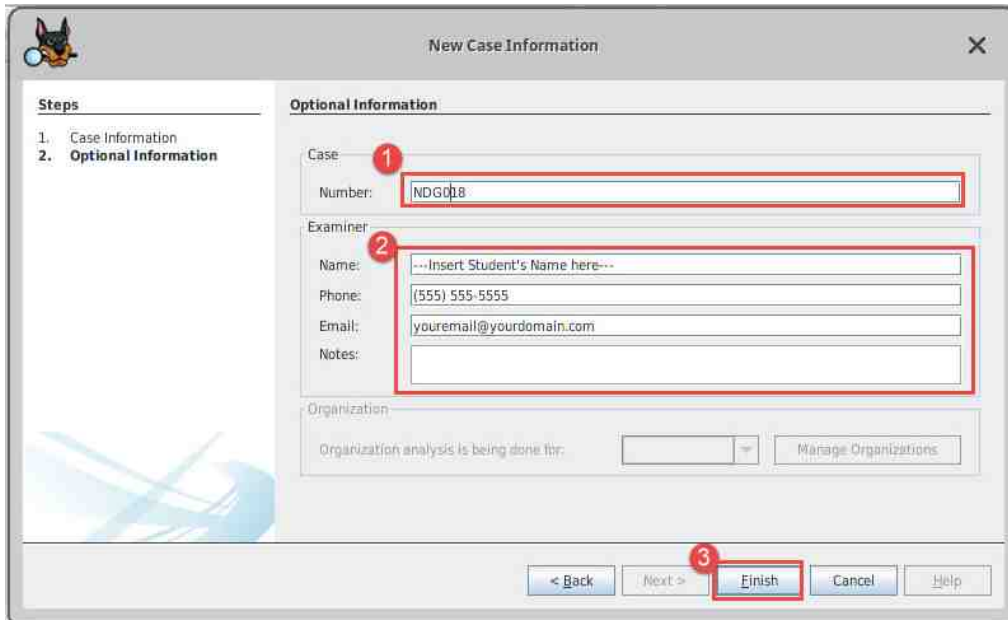
- Since you're already familiar with Autopsy, let's jump right in by creating a new case. In Autopsy, click the New Case option from the Case dropdown menu or press Ctrl + N as highlighted below. This will open the New Case Information window.



- In the New Case Information window, enter FOR_LAB_018 in the Case Name field. The Base Directory field is used to choose the location of the case folder. Let's leave that default selection and click Next, as highlighted below.

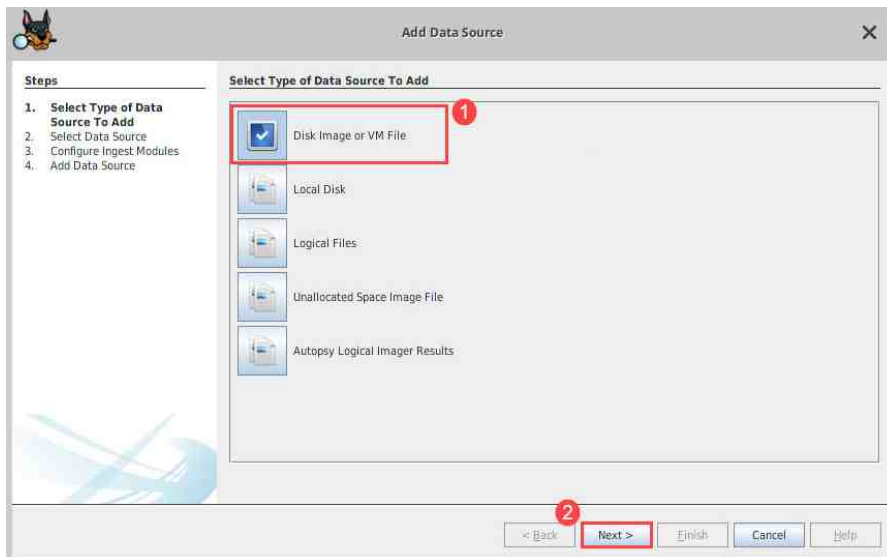


- The next window in the New Case wizard is the Optional information window. Here you can type more information about the case and examiner. Fill in the information as seen in the fields below and then click Finish when you are done. Remember, the Name field highlighted within the examiner section should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



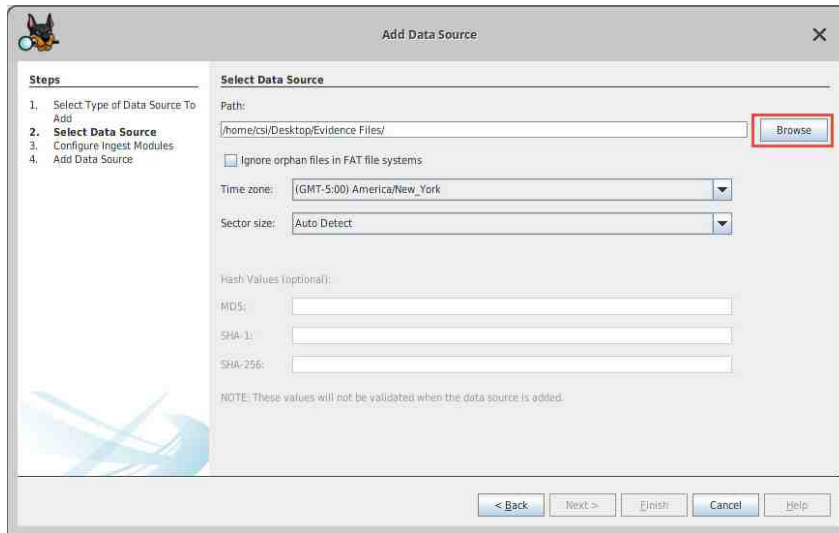
The "New Case Information" window is shown. It has a "Steps" pane on the left with "1. Case Information" and "2. Optional Information". The "Optional Information" section contains fields for Case Number (NDG018), Examiner Name (---Insert Student's Name here---), Phone ((555) 555-5555), Email (youremail@yourdomain.com), and Notes. There is also an Organization section with a dropdown and a "Manage Organizations" button. At the bottom, there are buttons for "< Back", "Next >", "Finish", "Cancel", and "Help". Red circles and boxes highlight the Case Number field (1), the Examiner Name field (2), and the "Finish" button (3).

- 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 a Forensic Evidence File (FEF) so let's select Disk Image or VM file and click Next as highlighted below.

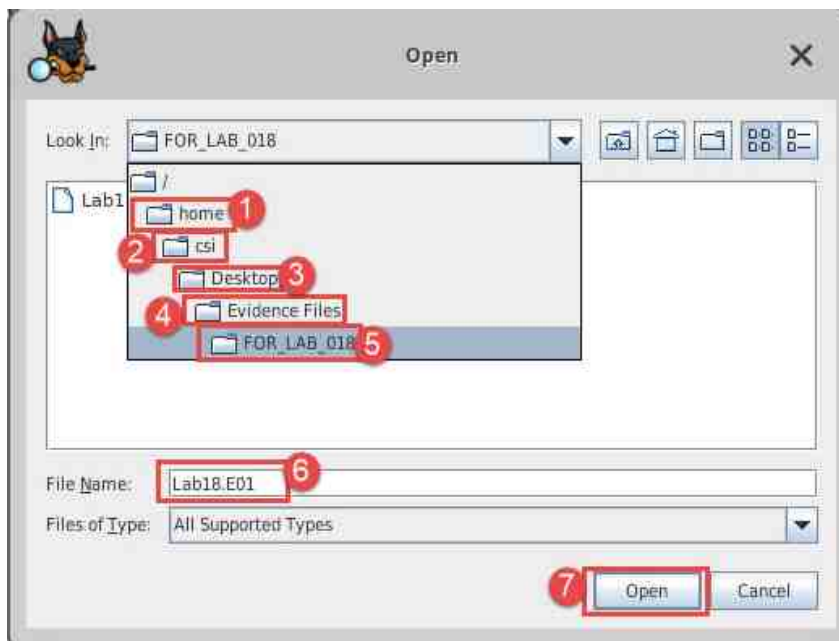


The "Add Data Source" window is shown. It has a "Steps" pane on the left with "1. Select Type of Data Source To Add", "2. Select Data Source", "3. Configure Ingest Modules", and "4. Add Data Source". The "Select Type of Data Source To Add" section contains a list of options: "Disk Image or VM File" (selected with a checkmark), "Local Disk", "Logical Files", "Unallocated Space Image File", and "Autopsy Logical Imager Results". At the bottom, there are buttons for "< Back", "Next >", "Finish", "Cancel", and "Help". Red circles and boxes highlight the "Disk Image or VM File" option (1) and the "Next >" button (2).

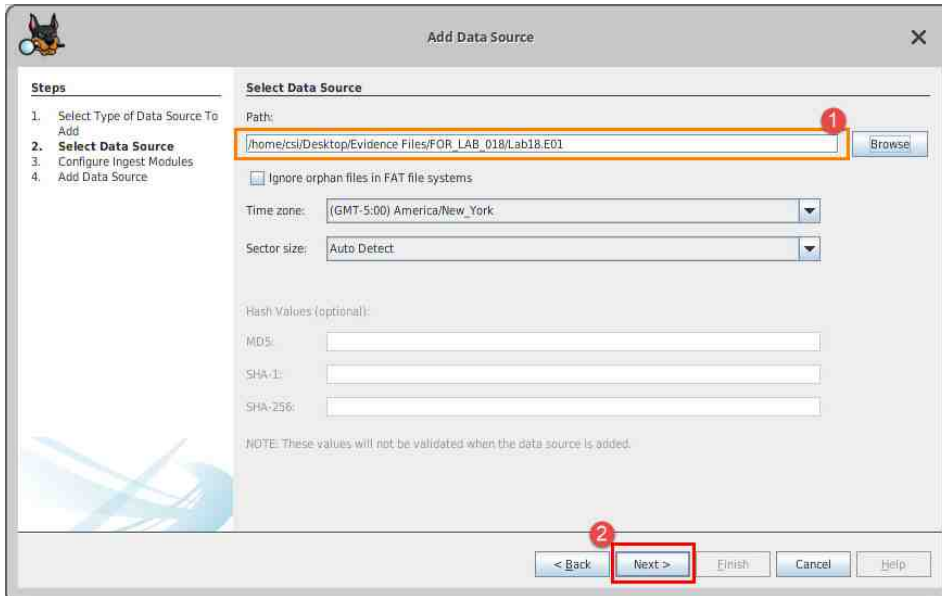
- The next window will allow you to choose the image you want to add to the case. Click the Browse button highlighted below to open the Open window that allows you to browse for the FEF.



- In the Open window, browse to Home > csi > Desktop > Evidence Files > FOR_LAB_018 and click the file called Lab18.E01 and then click Open as highlighted in items 1 – 7 below.



9. 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.

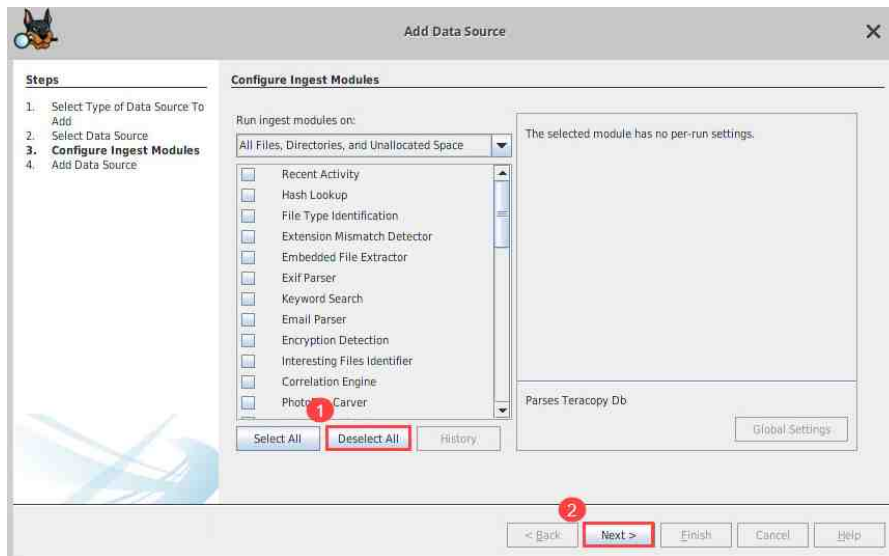


The screenshot shows the 'Add Data Source' dialog box. On the left, a 'Steps' list shows four steps: 1. Select Type of Data Source To Add, 2. **Select Data Source**, 3. Configure Ingest Modules, and 4. Add Data Source. The main area is titled 'Select Data Source'. It contains a 'Path:' label followed by a text field containing the path '/home/csi/Desktop/Evidence Files/FOR_LAB_018/Lab18.E01'. A red box and a red circle with the number 1 highlight this path field. To the right of the path field is a 'Browse...' button. Below the path field is a checkbox labeled 'Ignore orphan files in FAT file systems'. Further down are two dropdown menus: 'Time zone:' set to '(GMT-5:00) America/New_York' and 'Sector size:' set to 'Auto Detect'. Below these are three text fields for 'Hash Values (optional)': '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'. A red box and a red circle with the number 2 highlight the 'Next >' button.

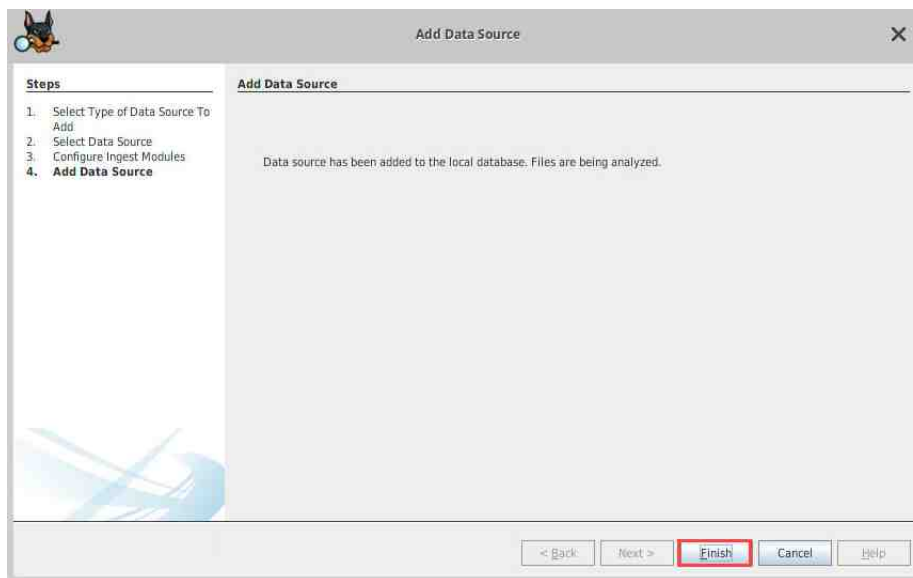


Time zone is an important aspect to any forensic investigation. Feel free to adjust the time zone to match your respective time zone.

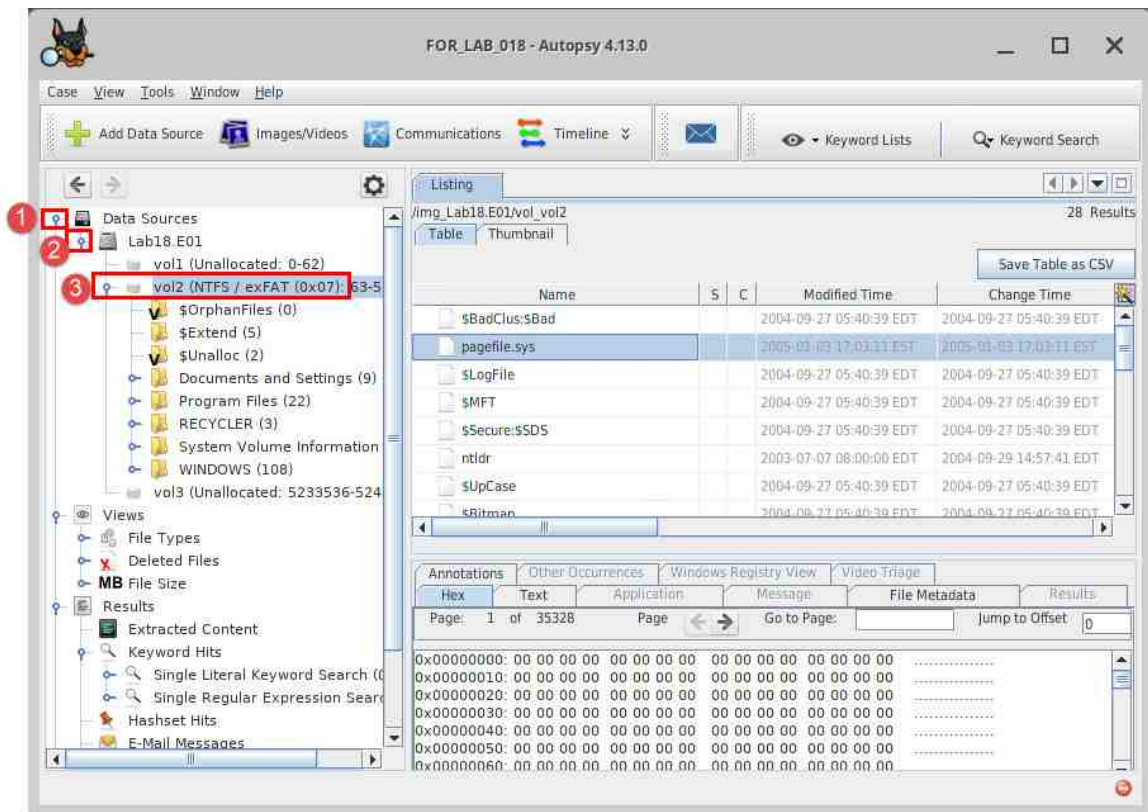
10. You will be taken to the Configure Ingest Modules step of the case creation process. We will not be using an Ingest Module in this exercise, so uncheck any selected Ingest Module by clicking the Deselect All button and then click Next as highlighted in items 1 and 2 below.



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



12. You will now be taken to the Autopsy main window. Here we can navigate the file system and locate the pagefile.sys file. To do this, click the blue pin beside Data sources which will expand and reveal the FEF as seen in item 1 below. Next, click the blue pin beside Lab18.E01 to view the partitions on the drive as seen in item 2 below. The NTFS volume is called vol2 in this FEF, so let's expand it by clicking the blue pin beside it as seen in item 3 below. Within vol2, you are now able to see all the files that make up Microsoft Windows' operating system. The pagefile.sys file is a hidden, system protected file stored in the root directory by default. (This file can be moved to a different location of the user's choice.) Click the volume called vol2 to view its contents in the Listing pane.



Autopsy creates references to the current folder and parent folder within the File List pane.

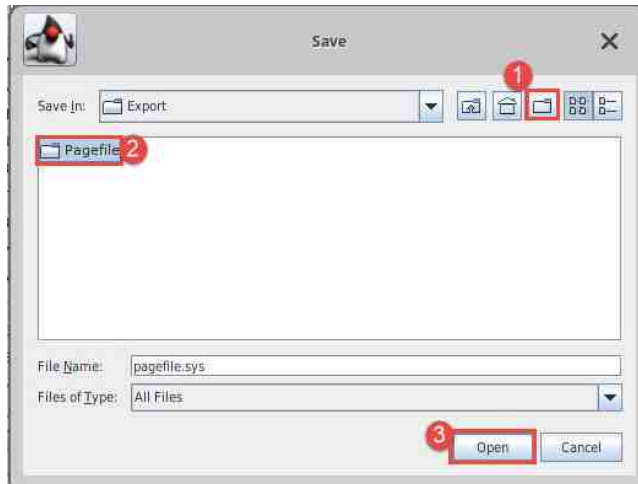
13. Now locate the file called pagefile.sys in the Listing pane, as seen in item 1 below. Look at the size of this file, as seen in item 2. The size displayed in this column is in bytes; when you calculate the size in MB, you will find that this file is 578MB, which is quite big for a standard system file. This is because it aims to be a backup to RAM that requires enough space to be effective. This is good because it also means there is potentially 578MBs worth of data that can be extracted. Let's export this file to look at it in a different tool.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	File
OrphanFiles (0)								
\$Bad			2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2679537664	All
pagefile.sys			2005-01-03 17:03:11 EST	2005-01-03 17:03:11 EST	2005-01-03 17:03:11 EST	2004-09-27 05:40:39 EDT	578817952	All
\$LogFile			2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	15499264	All
\$MFT			2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	13298688	All
\$Secure:\$SDS			2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	301008	All
ntldr			2003-07-07 08:00:00 EDT	2004-09-29 14:57:41 EDT	2004-09-27 05:45:25 EDT	2003-07-07 08:00:00 EDT	233632	All
\$UpCase			2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	131072	All
\$Bitmap			2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	81776	All
NTDETECT.COM			2003-07-07 08:00:00 EDT	2004-09-29 14:57:41 EDT	2004-09-27 05:45:26 EDT	2003-07-07 08:00:00 EDT	47580	All
\$Boot			2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	8192	All
\$MFTMirr			2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	4096	All
\$AttrDef			2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2560	All
System Volume Information			2004-09-29 13:37:33 EDT	2004-09-29 13:37:33 EDT	2005-01-03 17:02:54 EST	2004-09-27 13:46:56 EDT	440	All
\$Extend			2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	2004-09-27 05:40:39 EDT	344	All
RECYCLER			2004-09-30 12:39:31 EDT	2004-09-30 12:39:52 EDT	2004-09-30 12:39:52 EDT	2004-09-30 12:39:31 EDT	328	All
boot.ini			2004-09-27 12:55:13 EDT	2004-09-29 14:57:13 EDT	2004-10-28 12:38:57 EDT	2004-09-27 05:45:36 EDT	194	All
[current folder]			2004-10-27 12:35:57 EDT	2005-01-03 17:03:13 EST	2005-01-03 17:02:53 EST	2004-09-27 05:40:39 EDT	56	All

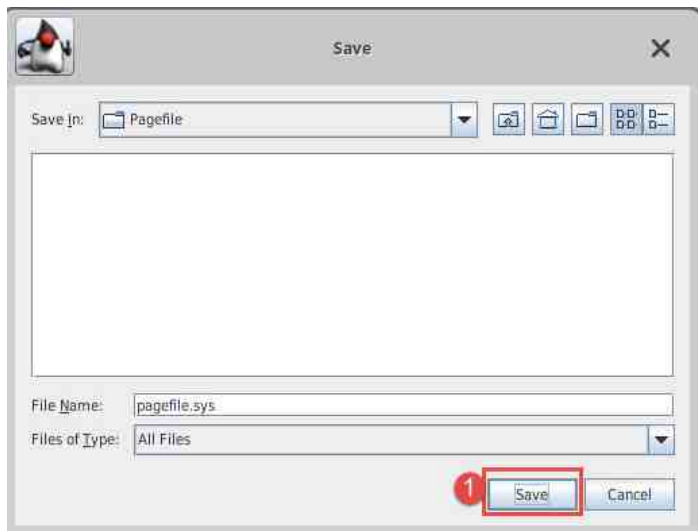
14. Let's begin by right-clicking on the pagefile.sys file, as seen in item 1 below. Once the context menu appears, click the Extract File(s) option, as seen in item 2, to open the Save window.

/img_Lab18.E01_vol_vol2		
Table Thumbnail		
Name	S	Modified Time
\$BadClus:\$Bad		2004-09-27 05:40:39 EDT
pagefile.sys		2005-01-03 17:03:11 EST
\$LogFile		
\$MFT		
\$Secure:\$SDS		
ntldr		
\$UpCase		
\$Bitmap		
NTDETECT.COM		
\$Boot		
\$MFTMirr		2004-09-27 05:40:39 EDT
\$AttrDef		2004-09-27 05:40:39 EDT

15. Once the save window appears, it will default to the Export folder within the Autopsy case folder. Let's create a new folder by clicking the create new folder icon from the toolbar as seen in item 1. Name the folder `Pagefile` as seen in item 2 and then select the Pagefile folder you just created and click Open, as seen in item 3 below.



16. Once inside the Pagefile folder, verify that the File name field has `pagefile.sys` in it, as seen in item 1 and then click Save, as seen in item 2.

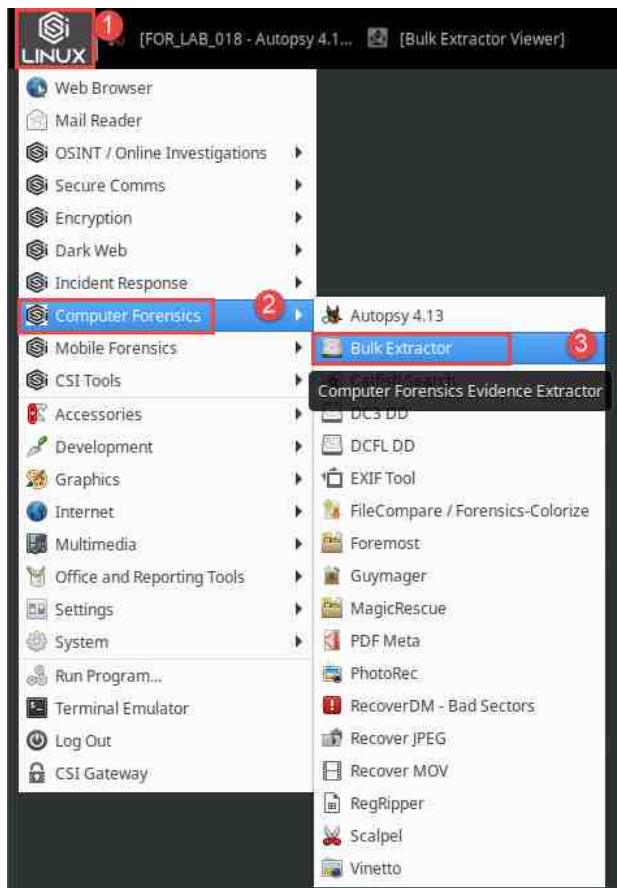


17. Once the export is done, an information window will appear, indicating that the file was extracted. Click OK, as seen below.

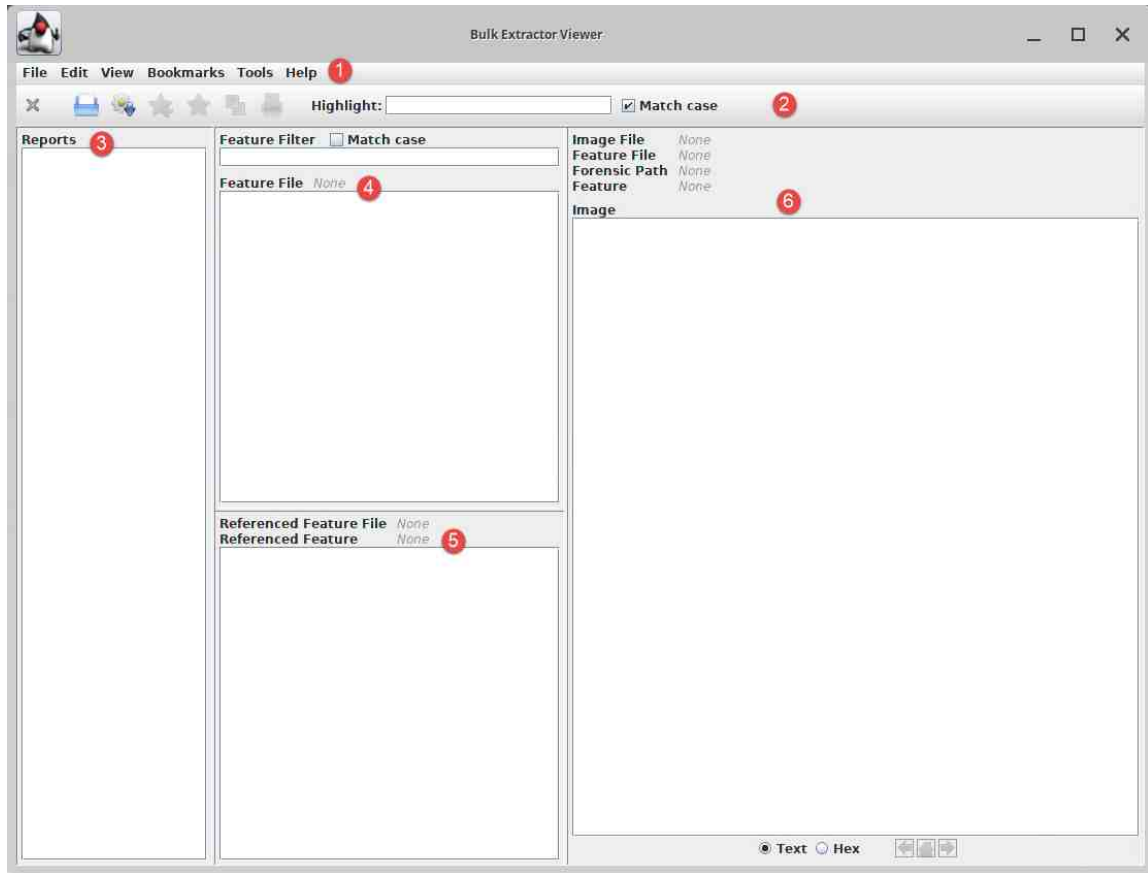


2 Getting to Know Bulk Extractor Viewer

1. Now that we have the pagefile.sys file exported, let's extract some data from it using a handy forensic tool called Bulk Extractor Viewer. This is a tool that extracts useful data from data sources and categorizes them in a single XML report. The first step is to open the Terminal, by navigating to Application Menu > Computer Forensics > Bulk Extractor as seen in items 1, 2, and 3 below. It can also be opened by clicking the Bulk Extractor icon from the dock, as seen in item 3.



- The Bulk Extractor GUI will appear. It has several panes that serve varying purposes. The table below the following screenshot will provide details about the functions of the main features we'll be using.

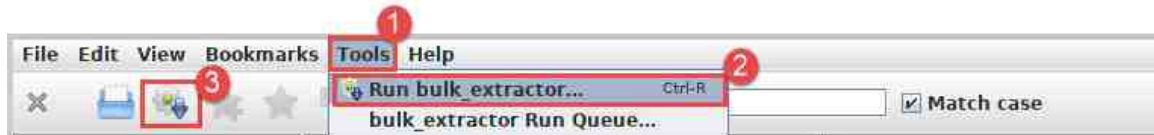


1	Menu Bar	This menu bar contains some familiar options and that are unique to Bulk Extractor Viewer. There are options that allow you to open saved reports, create new reports, change views and copy data, etc.
2	Toolbar	This toolbar contains options that allow you to create, open, bookmark, copy, print, and search data.
3	Reports	This pane lists the different reports that have been generated and has a tree-structure.
4	Feature File	This pane displays the contents of reports that have been selected in the Reports pane.
5	Referenced Feature File	This pane lists data that is viewed in a histogram format in the Feature File pane.
6	File Content	This pane displays the contents of the file that the data was found and takes you to the specific location that the data was found.

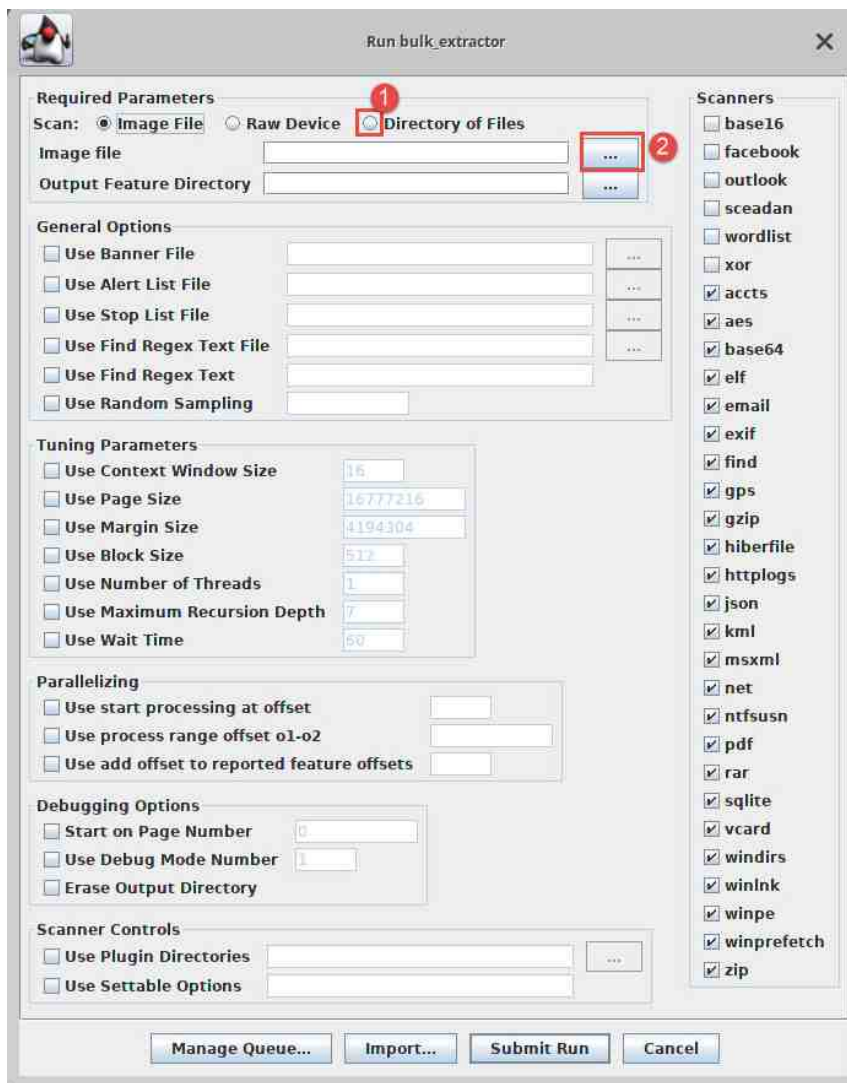
3 Extracting and Reviewing Data from the pagefile.sys

Now that we are a little more familiar with Bulk Extractor Viewer, we can go ahead and extract the data from the pagefile.sys file we exported earlier.

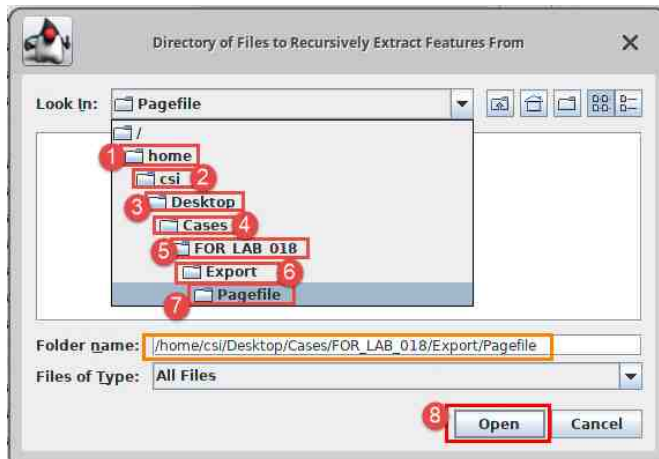
1. Bulk Extractor Viewer should still be open; if not, reopen it and click Tools > Run bulk_extractor... as seen in items 1 and 2 below. Alternatively, you can click the gear icon from the toolbar seen in item 3 below.



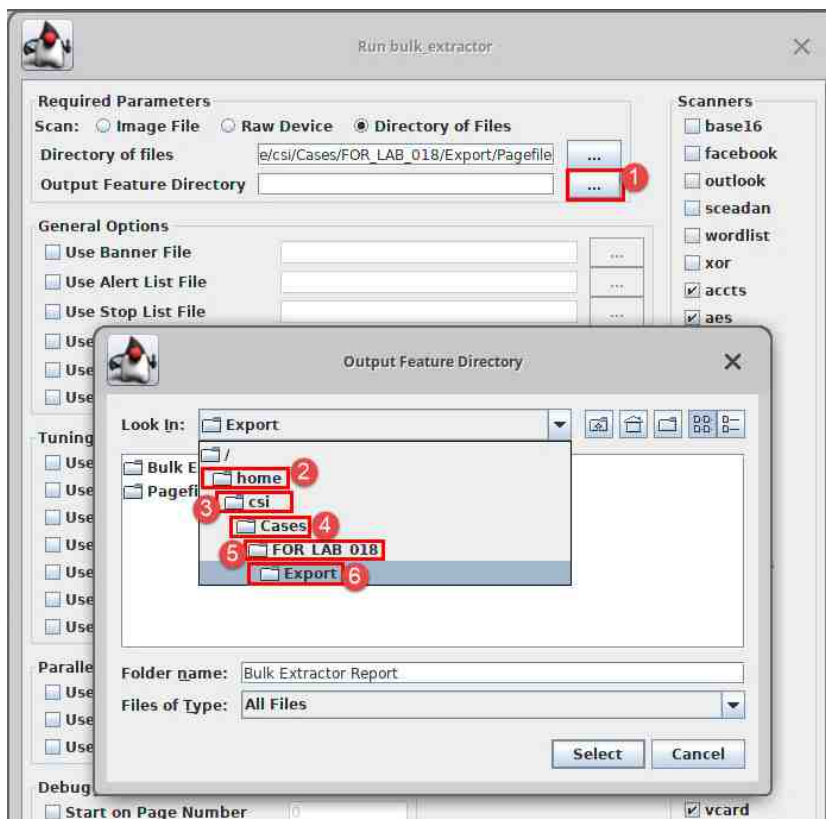
2. The Run bulk_extractor window will appear. There are many different options that can help you refine your search, but we will leave everything as default for now. Select the radio button beside Directory of Files, as seen in item 1 and then click the browse (...) button seen in item 2 below.



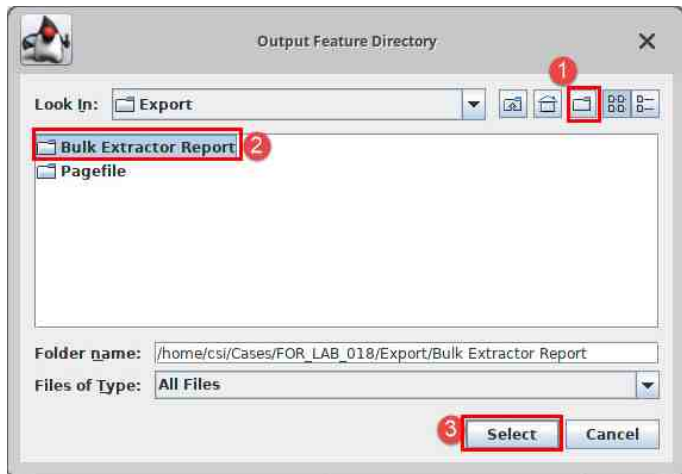
- The Directory of Files to Recursively Extract Features From window will appear. Navigate to Home > csi > Cases > FOR_LAB_018 > Export > Pagefile, as seen in items 1 - 7 below. Once there, click Open as seen in item 8 below.



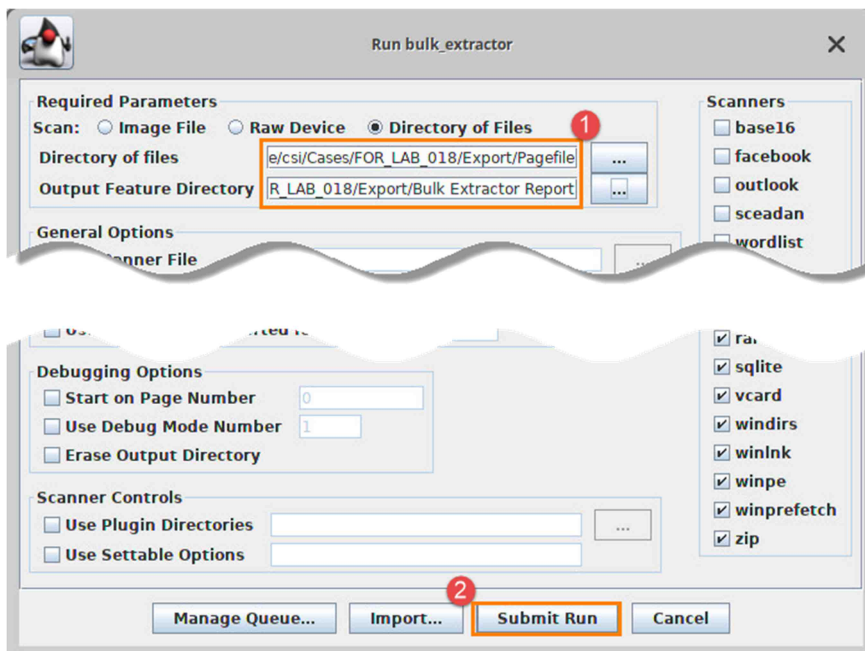
- You will be taken back to the Run bulk_extractor window. Let's set an output directory now to store the extracted data. Click the browse (...) button seen in item 1 below to open the Output Feature Directory window. Navigate to the path Home > csi > Cases > FOR_LAB_018 > Export as seen in items 2-6 below.



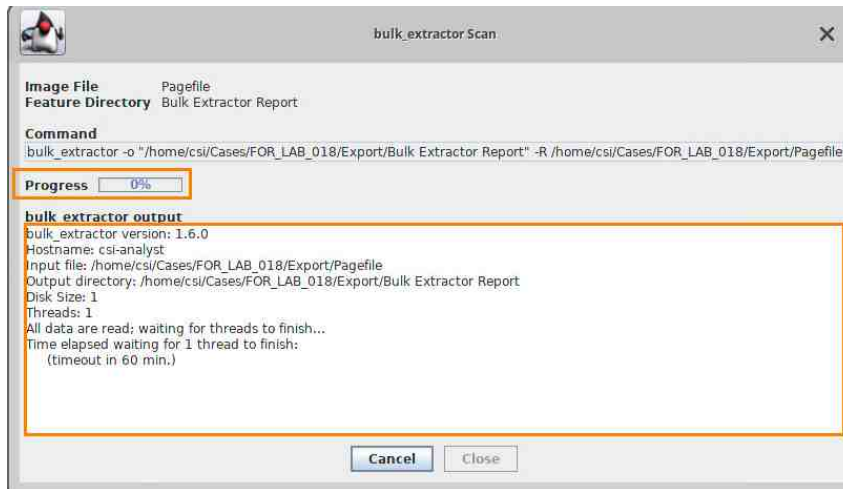
- Now select the Create New Folder button, as seen in item 1. Name the new folder Bulk Extractor Report and click Select as seen in items 2 and 3 below.



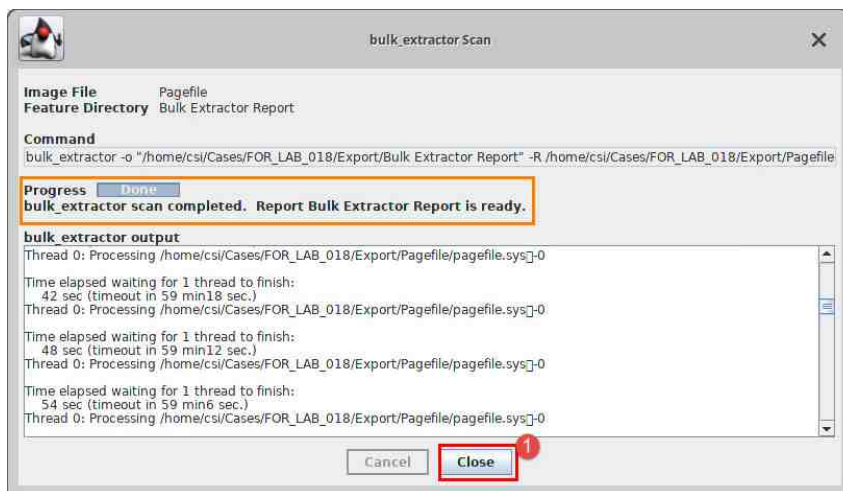
- Now verify that the paths are correct in both the Directory of files and Output Feature Directory fields, as seen in item 1 below. If the paths are correct, click Submit Run as seen in item 2 below. This will start the processing.



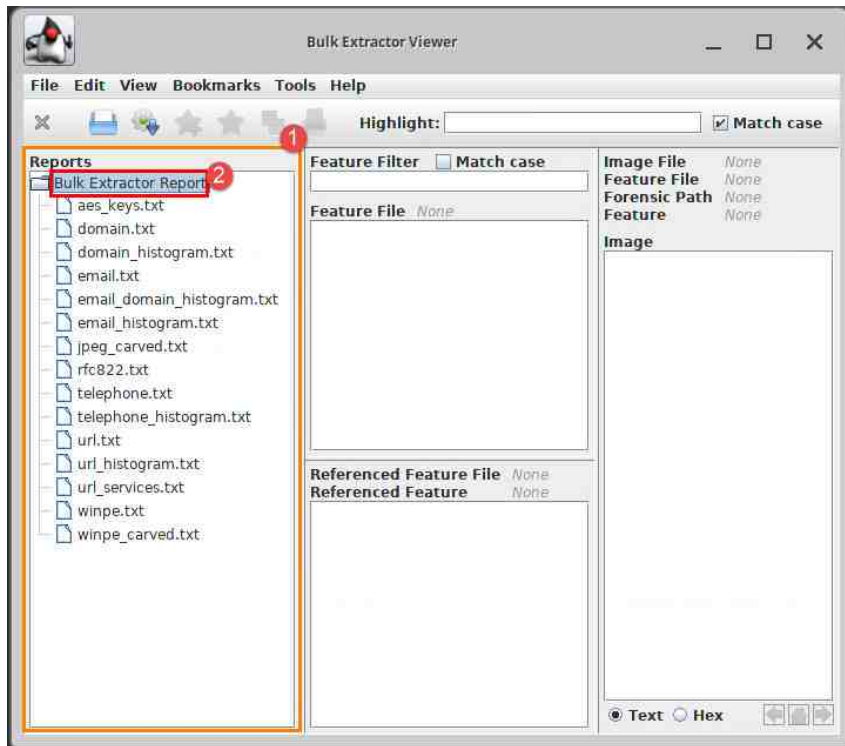
- The window below, called bulk_extractor Scan will appear, and it will provide progress reports as the scan goes.



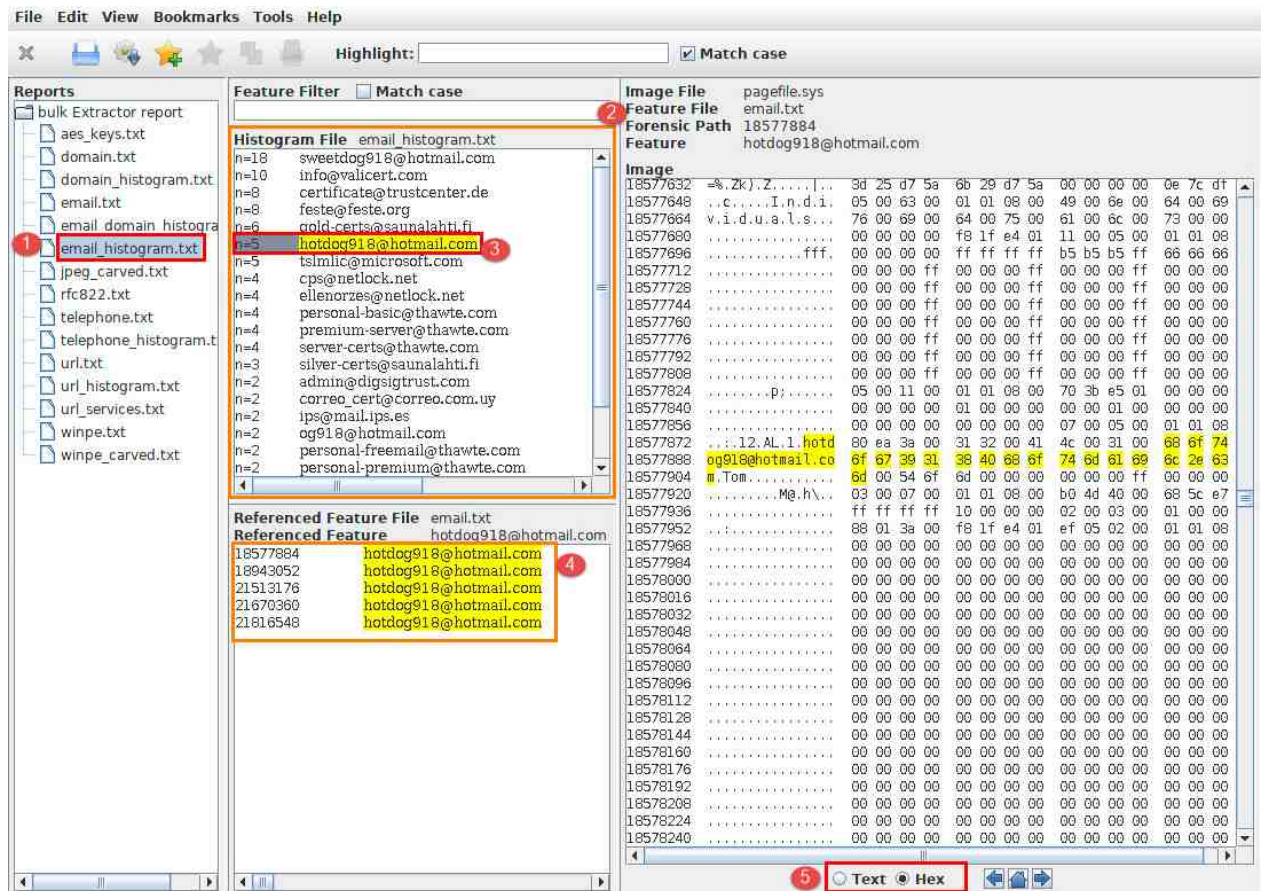
- Once the scan is done, the bulk_extractor Scan window will indicate it; click close as seen in item 1 below. You will be taken back to the main Bulk Extractor Viewer window.



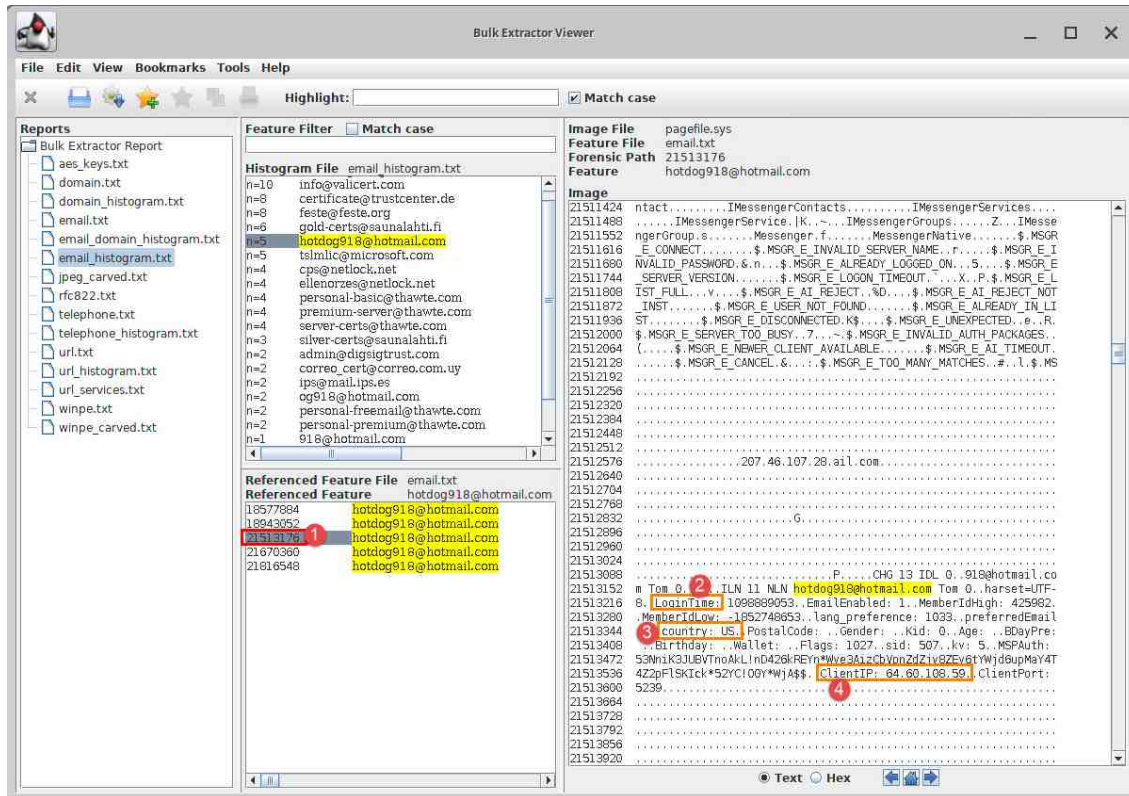
9. You will see Bulk extractor report appear in the Reports pane, as seen in item 1. Let's look at some of the data it parsed. Click the folder called Bulk extractor report and it will expand to reveal several files that have a .txt extension, as seen in item 2. These files contain the data we extracted. Since the tool used automated parsers, it may recover false positives, so you should always verify by closely reviewing the result and its source. Bulk Extractor makes that easy.



10. The different reports listed have familiar names. Let us look at a few of them. Click `email_histogram.txt` to start, as seen in item 1 below. The email histogram will populate the pane to the right of the Reports pane. This provides a count of all the email addresses found in the page file and can be seen to the left of the email addresses as seen in item 2. This is a great way to determine if an email address was used on the computer and how regularly. Let us click on the one with the highest count, `hotdog918@hotmail.com` as seen in item 3 below. All occurrences of this email address will appear in the Referenced Feature File window as seen in item 4. Bulk Extractor allows you to view the data in Text or Hex view as highlighted at item 5. Feel free to alternate between to observe how each are represented.



11. Let us take a closer look at one of these occurrences. Click the entry located at 21513176, as seen in item 1 below. This will reveal the location of this email address in the pagefile.sys file in the view pane. Take a close look at the data around this file. It contains data that you would find in an internet user profile. You can see a LoginTime in item 2, which is saved in epoch time. In item 3 is the country which we can see is US. In item 4 you can see a ClientIP and Port. As you can see, this information can be very detailed.



The screenshot shows the Bulk Extractor Viewer interface. The left pane displays a tree of reports, with 'email_histogram.txt' selected. The middle pane shows the histogram data, listing email addresses and their counts. The right pane shows the raw data from the pagefile.sys file, with the entry at offset 21513176 highlighted.

Feature Filter ☐ Match case

Histogram File email_histogram.txt

Count	Email Address
n=10	info@valicert.com
n=8	certificate@trustcenter.de
n=8	feste@feste.org
n=6	gold-certs@saunalahti.fi
n=5	hotdog918@hotmail.com
n=5	tsimic@microsoft.com
n=4	cps@netlock.net
n=4	ellenorzes@netlock.net
n=4	personal-basic@thawte.com
n=4	premium-server@thawte.com
n=4	server-certs@thawte.com
n=3	silver-certs@saunalahti.fi
n=2	admin@digsigtrust.com
n=2	correo_cert@correo.com.uy
n=2	ips@mail.ips.es
n=2	og918@hotmail.com
n=2	personal-freemail@thawte.com
n=2	personal-premium@thawte.com
n=1	918@hotmail.com

Referenced Feature File email.txt

Referenced Feature hotdog918@hotmail.com

Offset	Feature
18577984	hotdog918@hotmail.com
18943052	hotdog918@hotmail.com
21513176	hotdog918@hotmail.com
21670360	hotdog918@hotmail.com
21816548	hotdog918@hotmail.com

Image File pagefile.sys

Feature Path email.txt

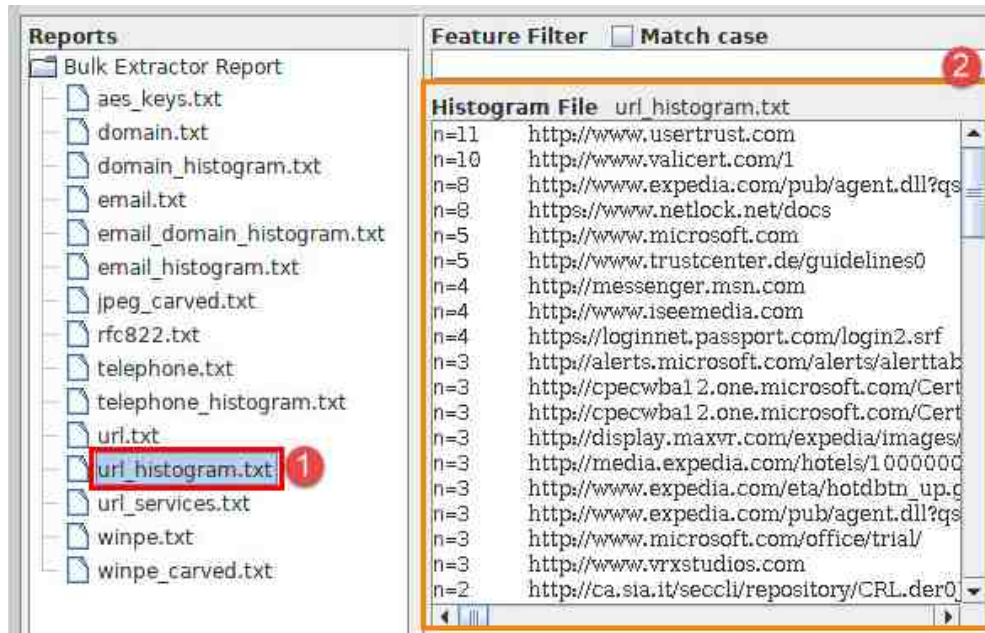
Feature hotdog918@hotmail.com

Image

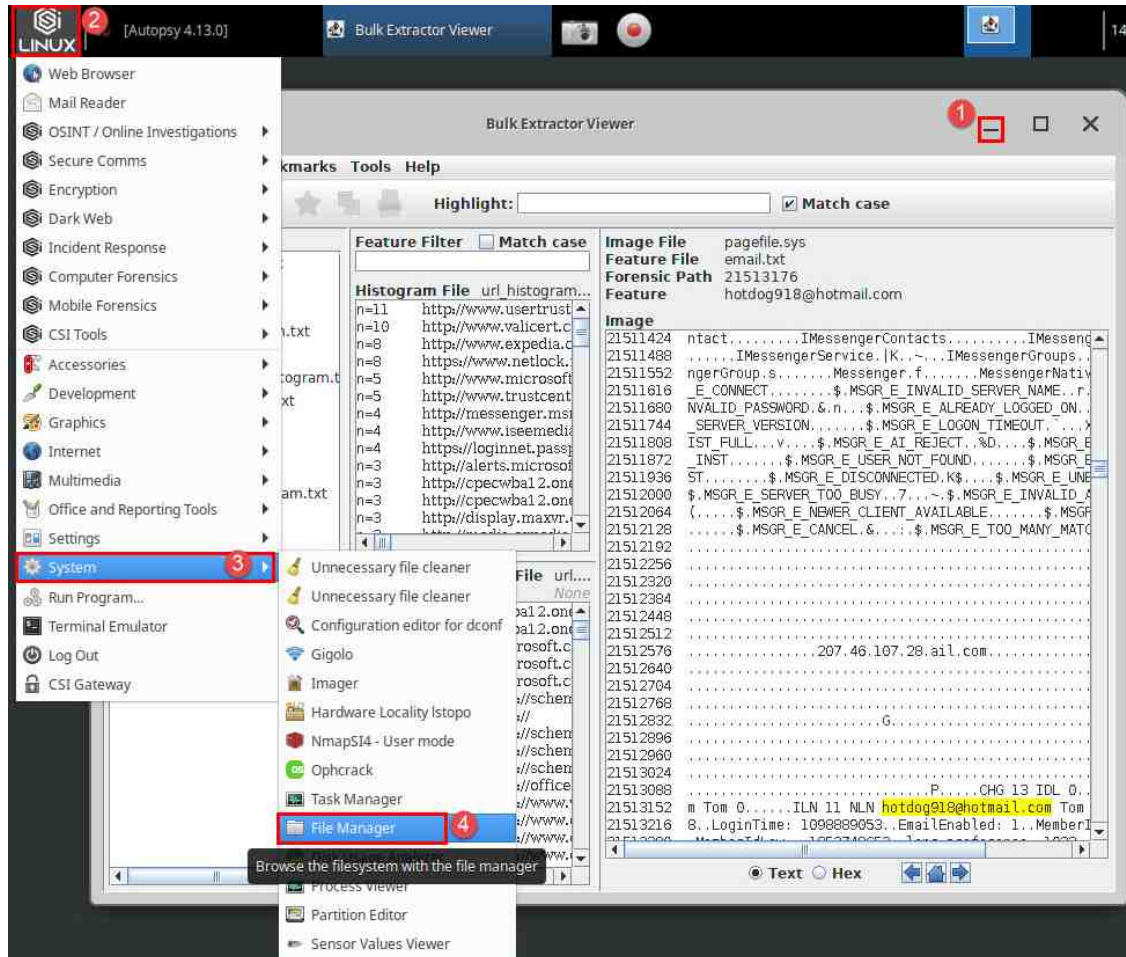
```

21511424 ntact.....IMessengerContacts.....IMessengerServices...
21511488 .....IMessengerService.IK.....IMessengerGroups.....IMesse
21511552 ngerGroup.s.....Messenger.f.....MessengerNative.....$ MSGR
21511616 E.CONNECT.....$ MSGR_E_INVALID_SERVER_NAME.....$ MSGR_E_I
21511680 INVALID_PASSWORD.&n...$ MSGR_E_ALREADY_LOGGED_ON...5...$ MSGR_E
21511744 SERVER_VERSION.....$ MSGR_E_LOGIN_TIMEOUT.....X..P.$ MSGR_E_L
21511808 IST_FULL...V...$ MSGR_E_AI_REJECT.%D...$ MSGR_E_AI_REJECT_NOT
21511872 INST.....$ MSGR_E_USER_NOT_FOUND.....$ MSGR_E_ALREADY_IN LI
21511936 ST.....$ MSGR_E_DISCONNECTED.K$.....$ MSGR_E_UNEXPECTED..0..R.
21512000 $ MSGR_E_SERVER_TOO_BUSY..7...$ MSGR_E_INVALID_AUTH_PACKAGES..
21512064 (.....$ MSGR_E_NEWER_CLIENT_AVAILABLE.....$ MSGR_E_AI_TIMEOUT.
21512128 .....$ MSGR_E_CANCEL.&....$ MSGR_E_TOO_MANY_MATCHES..#..l.$ MS
21512192 .....
21512256 .....
21512320 .....
21512384 .....
21512448 .....
21512512 .....
21512576 .....207.46.107.28:ail.com.....
21512640 .....
21512704 .....
21512768 .....
21512832 .....6.....
21512896 .....
21512960 .....
21513024 .....
21513088 .....P.....CHG 13 TOL 0..818@hotmail.co
21513152 # Tom 0 2 TLN 11 NLN hotdog918@hotmail.com Tom 0..harset=UTF-
21513216 8.LoginTime: 1098869053.EmailEnabled: 1.MemberIdHigh: 425982.
21513280 MemberIdLow: 1652748653.lang_preference: 1033.preferredEmail
21513344 country: US.PostalCode: ..Gender: ..Kid: 0.Age: ..BdayPre:
21513408 ..Birthday: ..Wallet: ..Flags: 1027..sid: 507.kv: 5..MSPAuth:
21513472 53NhK3JUBVTnoAkLind426kREYn*Wre36iczbyonZdZiv8ZEv6tYWjd0upMay4T
21513536 42zpFLSKick*52YC100Y*WjA$$.ClientIP: 64.60.108.59.ClientPort:
21513600 5239.....
21513664 .....
21513728 .....
21513792 .....
21513856 .....
21513920 .....
  
```

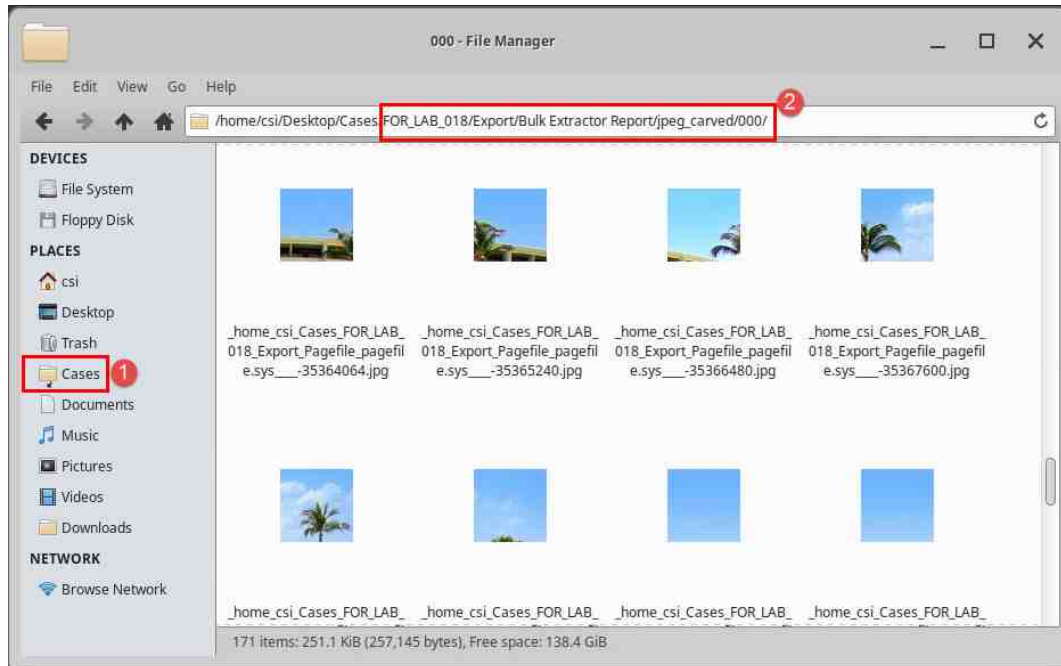

12. Let us look at a different category now. Click the URL Histogram report as seen in item 1 below. The URL histogram will populate the pane to the right of the Reports pane. This provides a count of all the URLs found in the page file and can be seen to the left of the URLs as seen in item 2. This list gives you an idea of the websites visited or accessed by applications on the computer. The histogram also provides an idea of the user's familiarity with the website based on the number of times each URL appears.



13. Let's look at one last set of data from the report. This data is the carved jpeg files that were stored in the page file. It is a great way to see images the user viewed even if they were never downloaded to the computer. We will use the File Manager to view these files instead of viewing them in Bulk Extractor Viewer. To begin, minimize Bulk Extractor Viewer and open the File Manager by clicking the Start Menu > System > File Manager icon on the desktop as seen in items 1, 2, 3, and 4 below.



14. Once there, navigate to Cases > FOR_LAB_018 > Export > Bulk extractor report > jpeg_carved > 000 as seen in items 1 and 2 below. The carved jpg files will appear in the File Manager as seen below. The files that were carved here are small, and some will be partial files, meaning the files will only show a fragment of the image, and then a black area will represent the missing information.



15. The data that was extracted in this exercise will differ in variety and volume, dependent on the size of the page file and the things the user does on the computer. This file is an obvious source of valuable data and should always be included in computer examinations. We are now at the end of this lab. Close all the open programs by clicking the X at the top-right corner of each window.

