



FORENSICS V2 LAB SERIES

Lab 09: Recycle Bin Forensics

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 Parsing the RECYCLER Folder	6
2 Parsing the Recycle.bin Folder	20

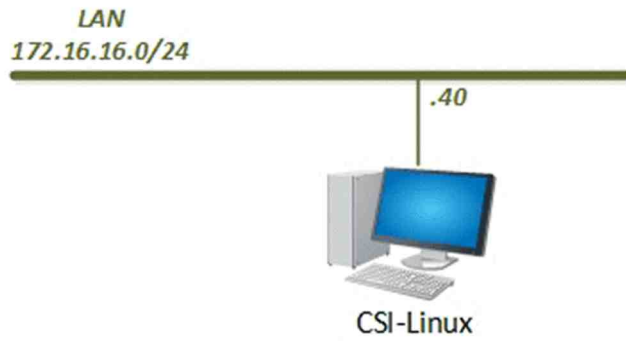
Introduction

The recycle bin is a very popular artifact that stores deleted files. From the user's side, the files are simply there, but from a forensic examiner's perspective, the recycle bin can differentiate who deleted what and provide other information that helps to understand the user's behavior.

Objectives

-) Identify where the recycle bin directory is located on different file systems and operating systems
-) Learn how to identify where the file was deleted from and when
-) Determine how to identify each user's recycle bins

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 Parsing the RECYCLER Folder

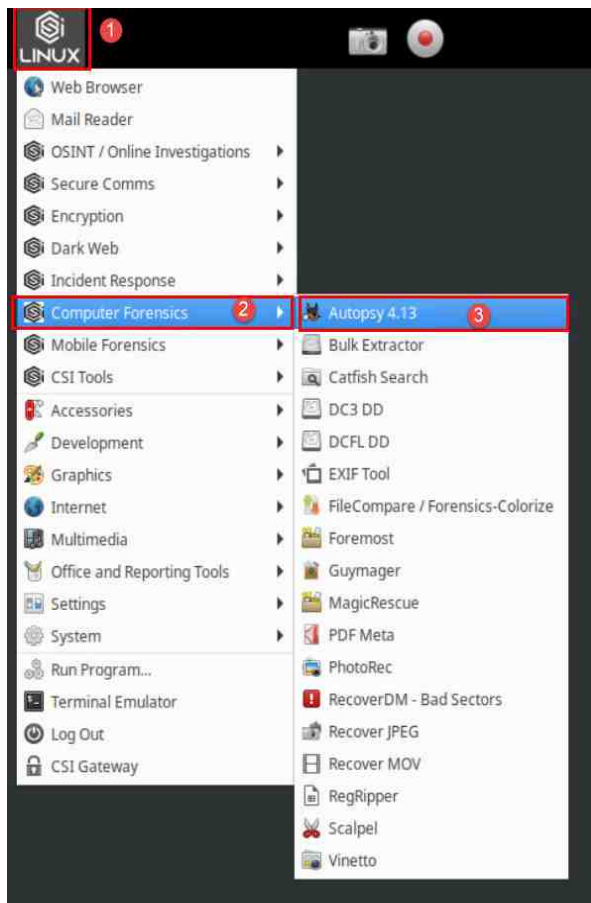
As we mentioned in the introduction, this lab will take you through the artifacts that are stored in the recycle bin. We will teach you how to interpret the files in the recycle bin and learn how to determine things like when they were deleted and where they were deleted from.

Let us get started by opening Autopsy and loading an FEF.

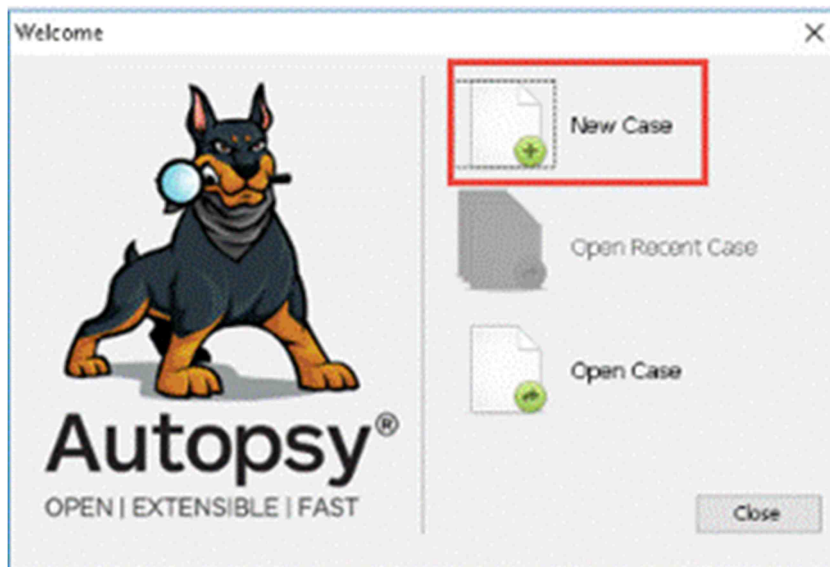
1. To begin, launch the CSI-Linux virtual machine to access the graphical login screen. Log in as `csi` using the password: `csi`



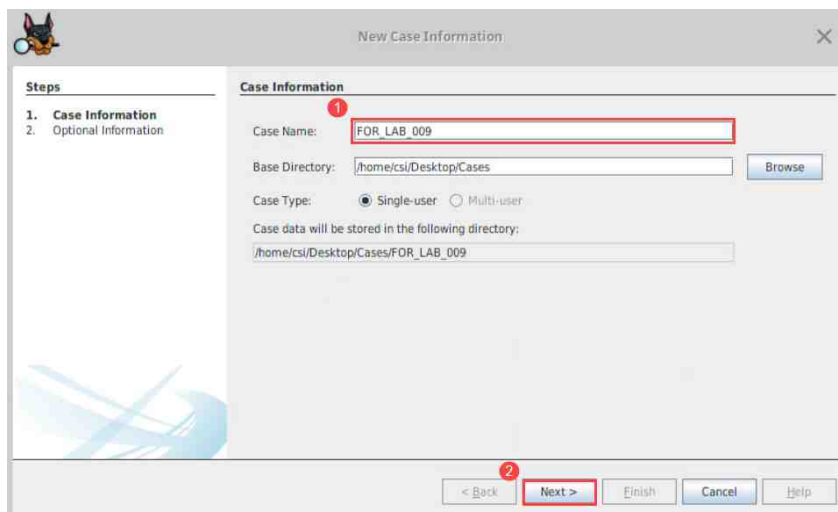
2. Once you are logged into the VM, launch the Autopsy program from the Start menu by navigating to Application Menu (top-left corner) > Computer Forensics > Autopsy 4.13, as shown in items 1, 2, and 3 below. Alternatively, you can open Autopsy from the taskbar by clicking the Autopsy icon:



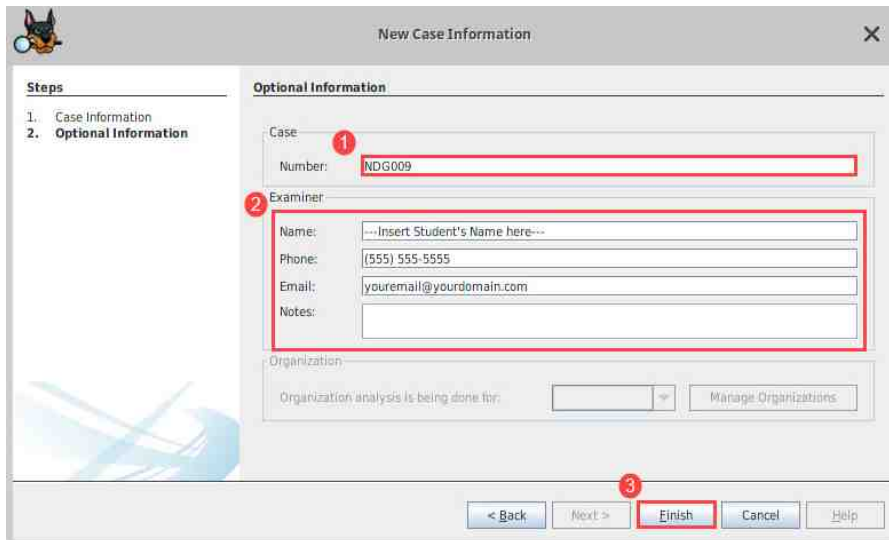
- Since you are already familiar with Autopsy, let us jump right in by creating a new case. At the Welcome window, click New Case as highlighted below. This will open the New Case Information window.



- In the New Case Information window, enter FOR_LAB_009 in the Case Name field, as seen in item 1 below. The Base Directory field is used to choose the location of the case folder. Let us leave the default selection and click Next as highlighted below in item 2.

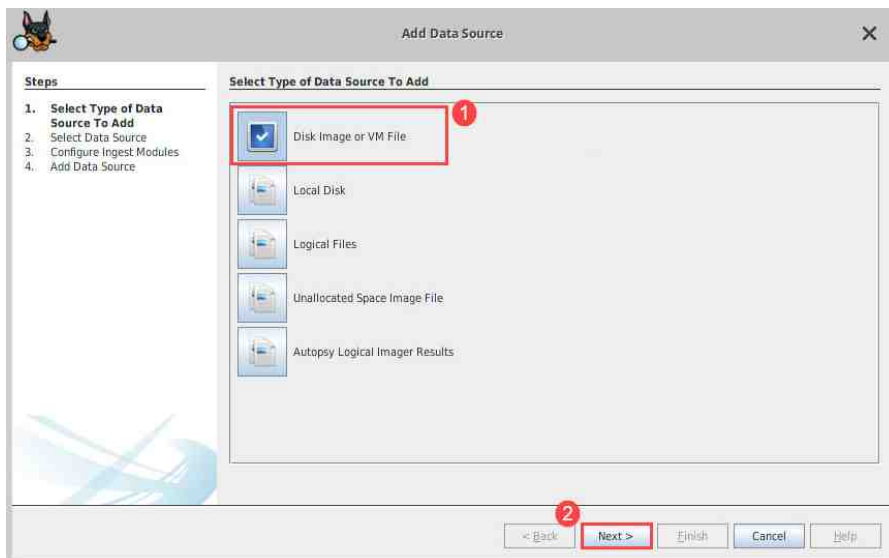


- The next window in the New Case wizard is the Optional Information window. Here you can type more information about the case and examiner. Fill in the information as seen in the fields below, and then click Finish when you are done. Remember, the Name field highlighted within the examiner section should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



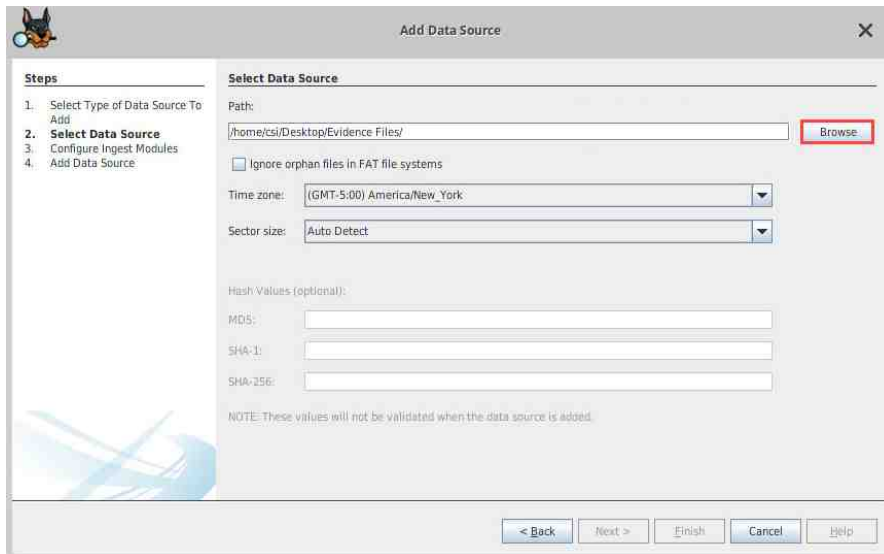
The screenshot shows the 'New Case Information' window. On the left, a 'Steps' pane lists '1. Case Information' and '2. Optional Information'. The main area is titled 'Optional Information'. It contains several input fields: 'Case Number' (with 'NDG009' entered), 'Examiner Name' (with a placeholder '---Insert Student's Name here---'), 'Examiner Phone' (with '(555) 555-5555'), 'Examiner Email' (with 'youremail@yourdomain.com'), and 'Examiner Notes' (empty). Below these is an 'Organization' section with a dropdown menu and a 'Manage Organizations' button. At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish' (highlighted with a red box and a red '3'), 'Cancel', and 'Help'.

- 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 us select Disk Image or VM file and click Next as highlighted below.

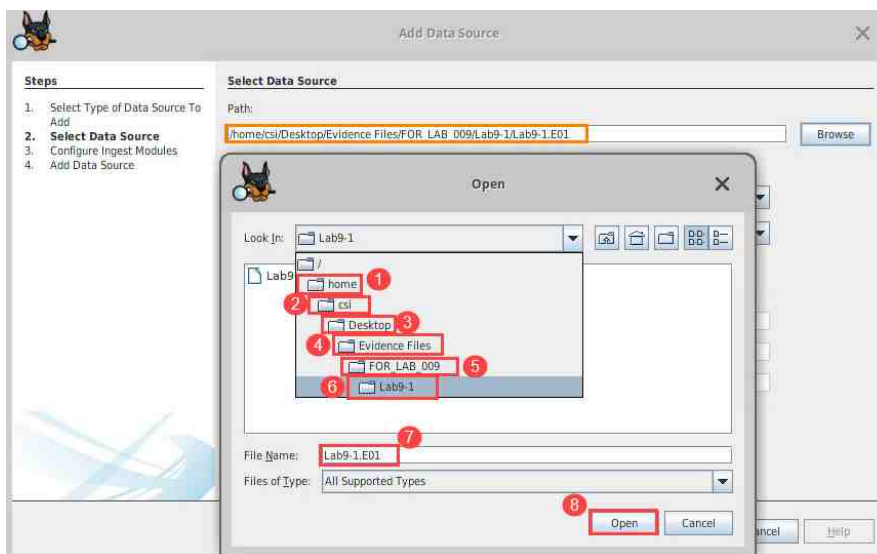


The screenshot shows the 'Add Data Source' window. On the left, a 'Steps' pane lists '1. Select Type of Data Source To Add', '2. Select Data Source', '3. Configure Ingest Modules', and '4. Add Data Source'. The main area is titled 'Select Type of Data Source To Add'. It contains a list of options: 'Disk Image or VM File' (selected with a blue checkmark and highlighted with a red box and a red '1'), 'Local Disk', 'Logical Files', 'Unallocated Space Image File', and 'Autopsy Logical Imager Results'. At the bottom, there are navigation buttons: '< Back', 'Next >' (highlighted with a red box and a red '2'), 'Finish', 'Cancel', and 'Help'.

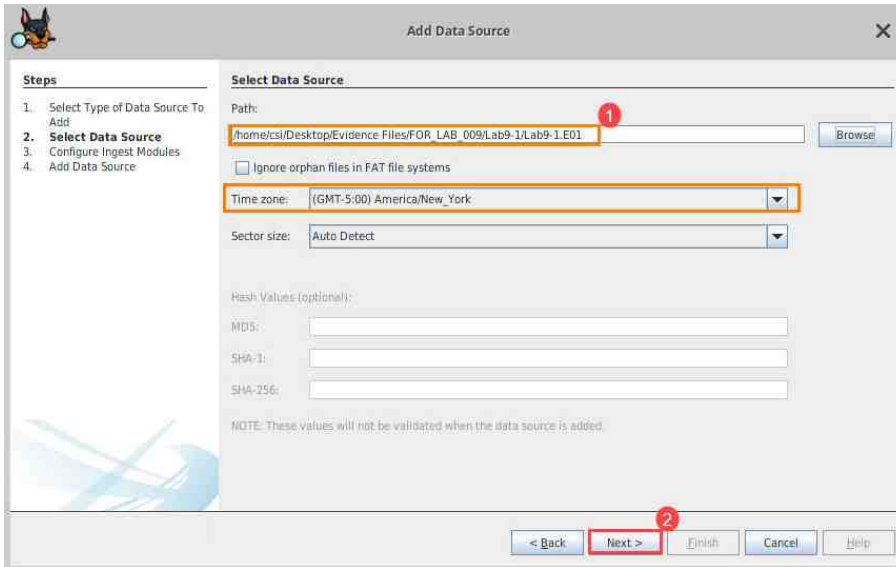
- The next window will allow you to choose the image you want to add to the case. Click the Browse button highlighted below to open the Open window that allows you to browse for the FEF.



- In the Open window, browse to home > csi > Desktop > Evidence Files > FOR_LAB_009 > Lab9-1 and click the file called Lab9-1. E01 and then click Open, as highlighted in steps 1 – 8 below.

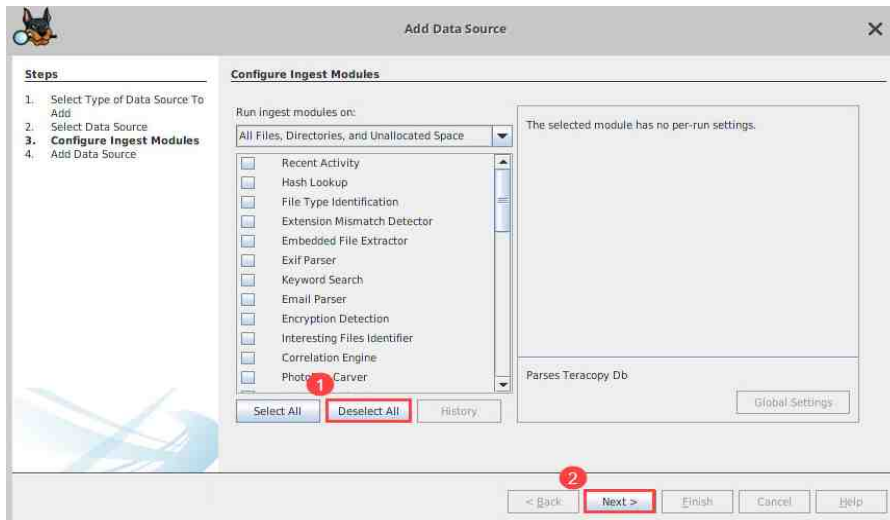


9. The image path will now appear in the Path field highlighted as item 1 below. We will leave the other options as-is for now and click Next, highlighted as item 2 below.

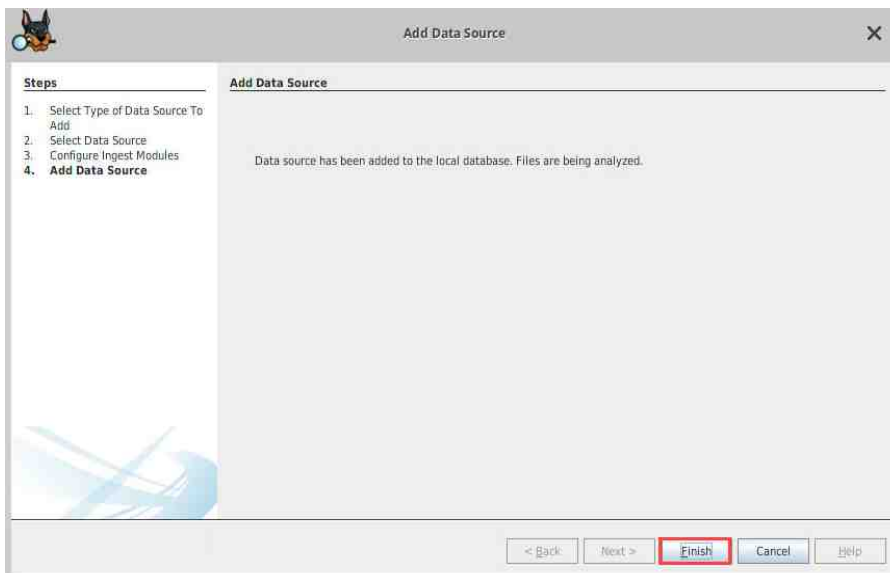


Time zone is an important aspect of any forensic investigation. Feel free to adjust the time zone to match your respective time zones.

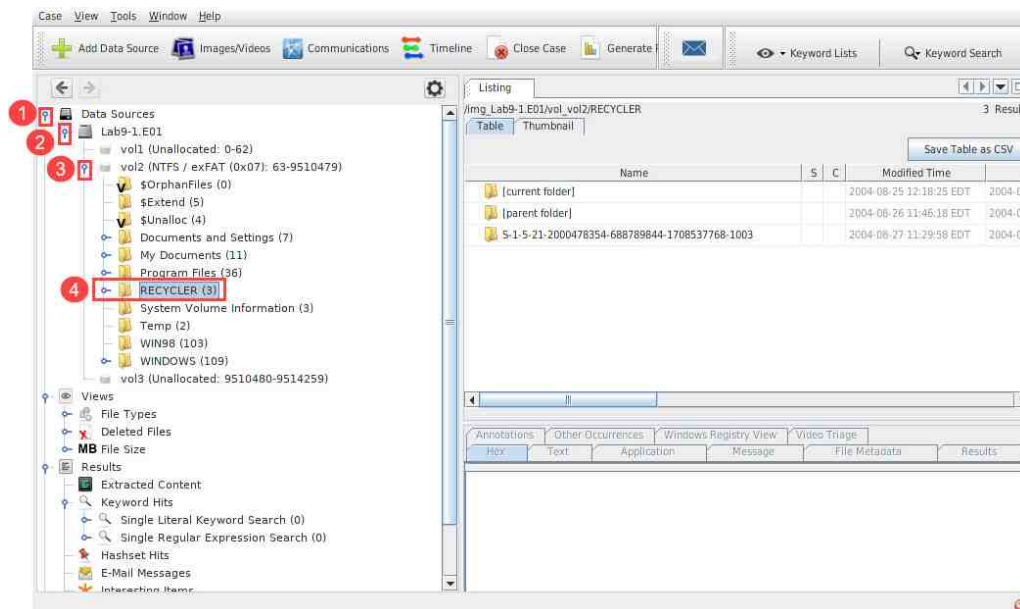
10. You will be taken to the Configure Ingest Modules step of the case creation process. We will not be using an Ingest Module in this exercise, so uncheck any selected Ingest Module by clicking the Deselect All button and then click Next, as highlighted in items 1 and 2 below.



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 RECYCLER folder. 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 Lab9-1.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 us 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 the Microsoft Windows operating system. Based on the folder structure, it is safe to say that this operating system is pre-Windows Vista. We determine this by paying attention to the Documents and Settings folder that contains the user profiles. In Windows Vista and later, the user profiles are stored in a folder called Users. Another folder that can be used to determine the operating system's age is the RECYCLER folder. This folder is our target, and it contains deleted files that were sent to the recycle bin (recycled). Like the Users folder, the RECYCLER folder was renamed to Recycle.bin in Windows Vista and later. Let us click the RECYCLER folder to see its contents, as seen in item 4 below.



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

13. Now that you are in the RECYCLER folder, you can see that there is 1 main folder inside the directory, as highlighted below. This folder stores recycled files for each user. The name of the folder is used to identify the user and is called a Security Identifier or SID. The SID is unique and will never be recycled even after the associated user is deleted. The SID can be broken down to provide details that uniquely identifies a computer as well as its user. The following table provides a breakdown of the SID seen below.

[current folder]	2004-08-25 12:18:25 EDT	2004-08
[parent folder]	2004-08-26 11:46:18 EDT	2004-08
5-1-5-21-2000478354-688789844-1708537768-1003	2004-08-27 11:29:58 EDT	2004-08

S
1
5
21-2000478354-688789844-1708537768
1003

S	This character is an identifier that indicates that the value is an SID. It is always S.
1	This character denotes the revision level of the SID specification and is normally 1.
5	This character is called the Identifier Authority Value and defines the authority that created the SID. This value is normally 5.
21-2000478354-688789844-1708537768	This value is the domain or Local Computer Identifier and is used to uniquely identify the computer that created this identifier.
1003	This is the Relative Identifier (or RID) and is used to identify the user of the computer. RIDs come in 2 main types. The first is the RID that is created automatically by the system, and is always in the 500 range. Some examples are System Administrator, which is RID 500, and Guest, which is RID 501. The second type of RID is the one for user accounts that are created by the user or certain programs; these users' RIDs will always be 1000 or higher. If a user account is deleted and a new one created, the RID will not be recycled. This is a good way to determine if previous user accounts existed on a computer. In this instance, the RID 1003 indicates that this is the 4 th non-system user account.

14. The RID for a user account can be found by decoding the contents of the SAM file. In this exercise, we will not be decoding this file, but the screenshot below is the RegRipper report of the SAM file for this computer, for your reference. The highlighted portion contains the username and the RID, beside the name, in square brackets.

```

Username      : Administrator [500]
Full Name     :
User Comment  : Built-in account for administering the computer/domain
Account Type  : Default Admin User

Username      : Guest [501]
Full Name     :
User Comment  : Built-in account for guest access to the computer/domain
Account Type  : Default Guest Acct

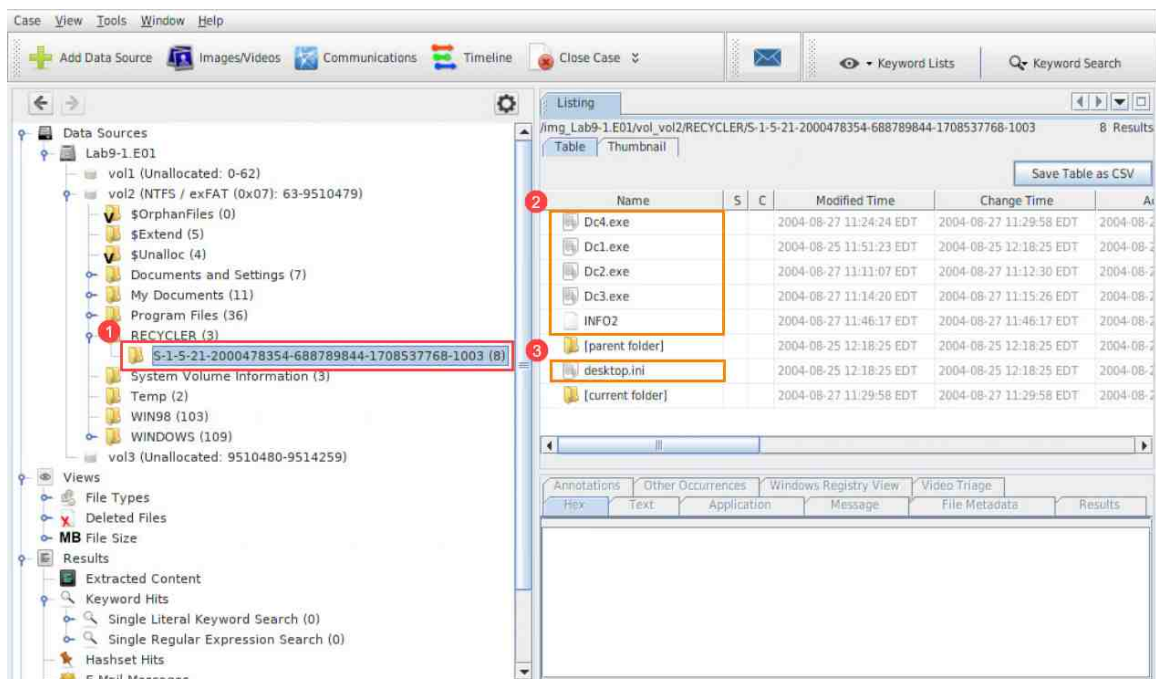
Username      : HelpAssistant [1000]
Full Name     : Remote Desktop Help Assistant Account
User Comment  : Account for Providing Remote Assistance
Account Type  : Custom Limited Acct

Username      : SUPPORT_388945a0 [1002]
Full Name     : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US
User Comment  : This is a vendor's account for the Help and Support Service
Account Type  : Custom Limited Acct

Username      : Mr. Evil [1003]
Full Name     :
User Comment  :
Account Type  : Default Admin User

```

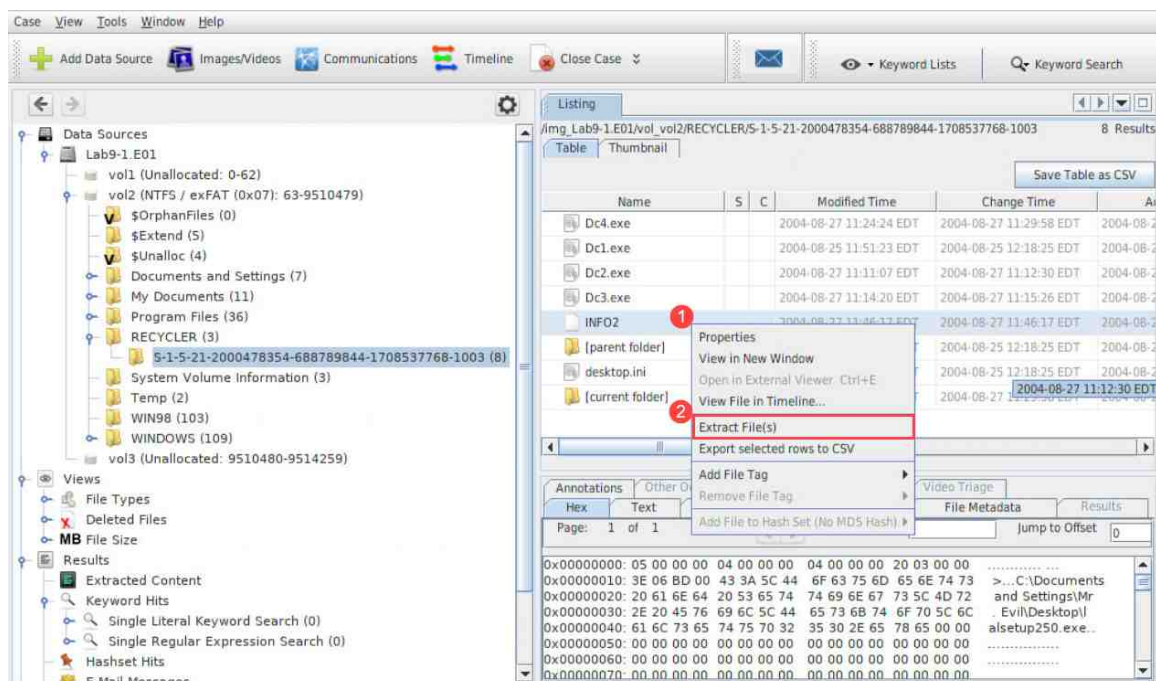
15. Now that we know that this folder is associated with the user account called Mr. Evil, we can associate anything we find there with that user. Let us look in the recycle bin for Mr. Evil by clicking the folder called S-1-5-21-2000478354-688789844-1708537768-1003 as seen in item 1 below. As you can see in the list pane, there are 6 files in this folder (and the 2 folders created by Autopsy that we will ignore in this exercise). The 6 files are highlighted as items 2 and 3 below.



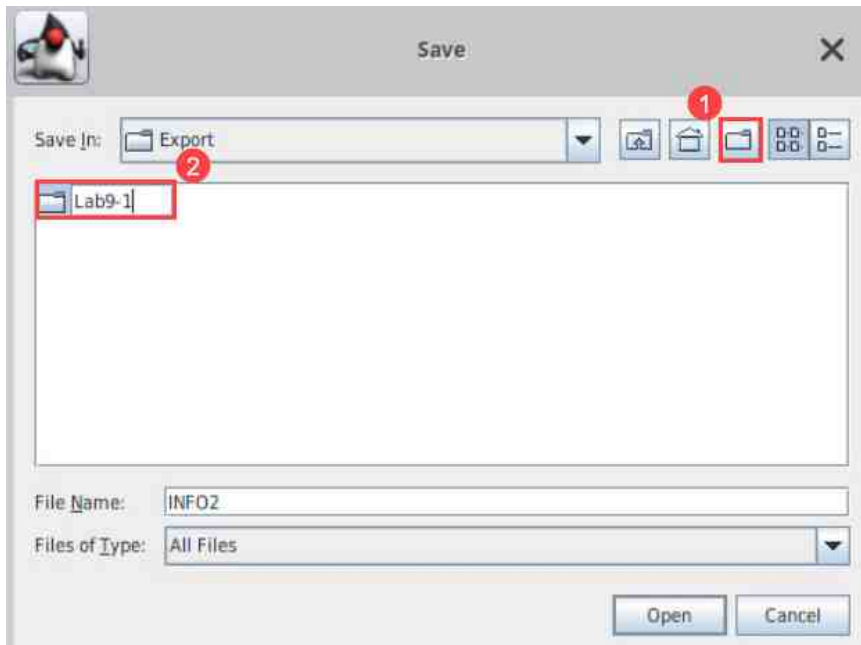
16. Out of the 6 files found in the recycler folder for the Mr. Evil account, the 2 called INFO2 and desktop.ini are system files, while the other 4 are deleted files. When a file is deleted in Windows XP and older operating systems, the file is renamed and moved to this folder. The name of the file can tell what drive the file was deleted from and the order that files were deleted in. The first character indicates that a file was deleted and will always be D. The next character will tell the drive letter that the file was deleted from. The final character is the sequential order that the file was deleted in. For example, the file highlighted below is called Dc1.exe. This means it was the first file that was deleted and that it was deleted from the C drive.

Name	S	C	Modified Time
Dc4.exe			2004-08-27 11:24:24 EDT
Dc1.exe			2004-08-25 11:51:23 EDT
Dc2.exe			2004-08-27 11:11:07 EDT
Dc3.exe			2004-08-27 11:14:20 EDT
INFO2			2004-08-27 11:46:17 EDT
[parent folder]			2004-08-25 12:18:25 EDT
desktop.ini			2004-08-25 12:18:25 EDT
[current folder]			2004-08-27 11:29:58 EDT

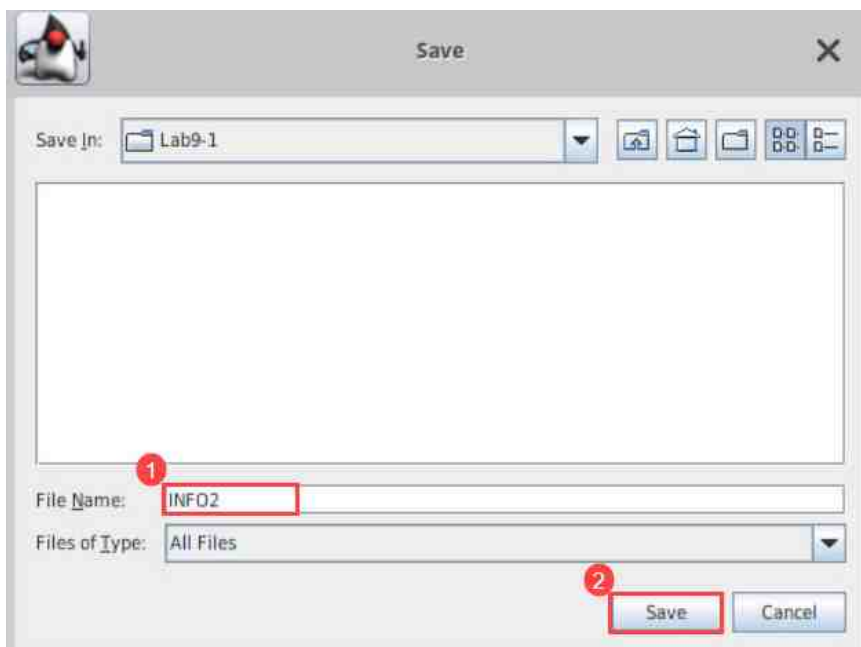
17. The file called desktop.ini is a system file that stores metadata about the File Explorer windows and will not be touched in this exercise. The file that we really need is the INFO2 file. This is a system file that creates an index of the files that are deleted. In this exercise, we will export this file and use a command line tool called Rifiuti to parse the data. Let us begin by right-clicking on the INFO2 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.



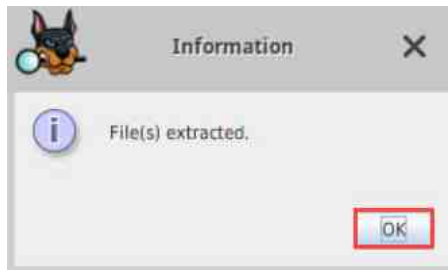
18. Once the Save window appears, it will default to the Export folder within the Autopsy case folder. Let us create a new folder by clicking the create new folder icon from the toolbar as seen in item 1. Name the folder Lab9-1 as seen in item 2, and then double-click the Lab9-1 folder you just created to open it.



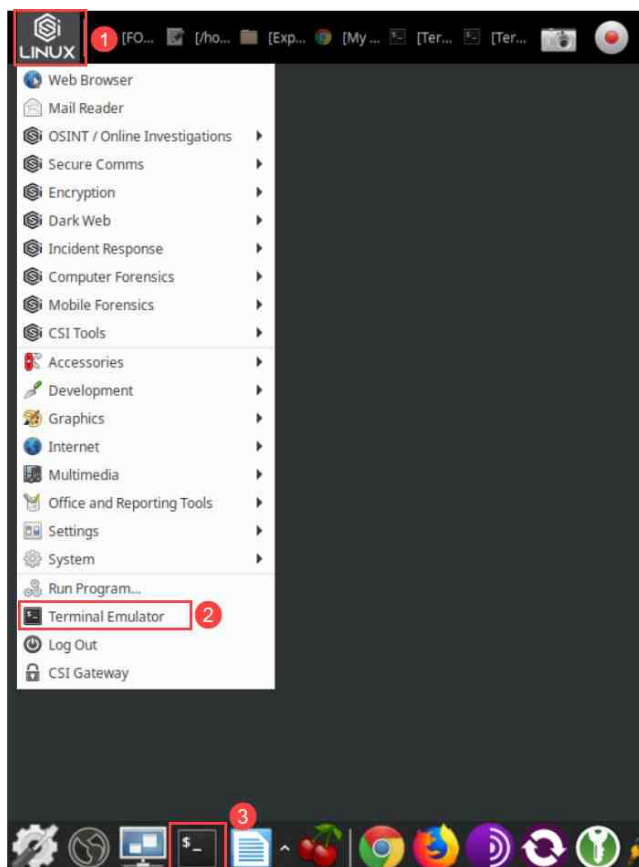
19. Once inside the Lab9-1 folder, verify that the File Name field has INFO2 in it, as seen in item 1, and then click Save as seen in item 2.



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



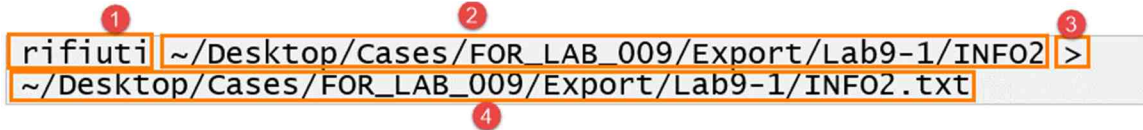
21. Now that we have the INFO2 file exported, let us extract it using the handy forensic tool that was mentioned in step 17 above - Rifiuti. This command line tool is very simple to use, so let us jump right into it. First, minimize the Autopsy window by clicking the _ sign in the top-right corner. The next step is to open the Terminal, by navigating to the Application Menu and then clicking Terminal Emulator, as seen in items 1 and 2 below. It can also be opened by clicking the Terminal Emulator icon from the dock, as seen in item 3.



22. Once the Terminal window appears, type the following command. Once you have verified that the command is correct, press Enter to parse the INFO2 file.

```
ri fi uti ~/Desktop/Cases/FOR_LAB_009/Export/Lab9-1/INFO2 >  
~/Desktop/Cases/FOR_LAB_009/Export/Lab9-1/INFO2.txt
```

23. A breakdown of this command can be seen in the table below.



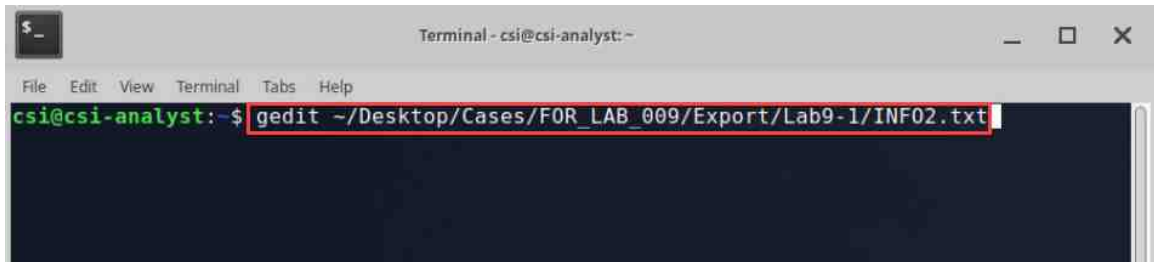
1	The text referenced as item 1 is the name of the program
2	Item 2 is the path of the INFO2 file that will be parsed
3	Item 3 is the command that outputs the parsed data to the provided file
4	Item 4 is the path for the file that will store the extracted data



Linux commands are case-sensitive. Pay attention to capitalizations and double-check the command you typed if you receive an error.

24. If you did everything correctly, then the file called INFO2.txt will be created. Now let us look at this file. Let us use another command line program called gedit to open this file. Gedit works by typing `gedit` and the file path, as seen in the following command. Once you have verified that the command is typed correctly, press Enter.

```
gedit ~/Desktop/Cases/FOR_LAB_009/Export/Lab9-1/INFO2.txt
```



25. Gedit will open the file as seen below. The file is structured by columns. As you can see in item 1 below, the first column is the index number, and this corresponds with the sequential number of the files found in the RECYCLER folder. The next column, highlighted as item 2, is the deleted time and tells the date and time that the file was deleted. The next column, highlighted as item 3, is the drive number and gives the physical drive number that the file was deleted from. The next column, seen in item 4, is the original path of the file. This data tells where the file was stored before it was deleted. Finally, the numbers that are to the right of the path give each file's size in bytes.

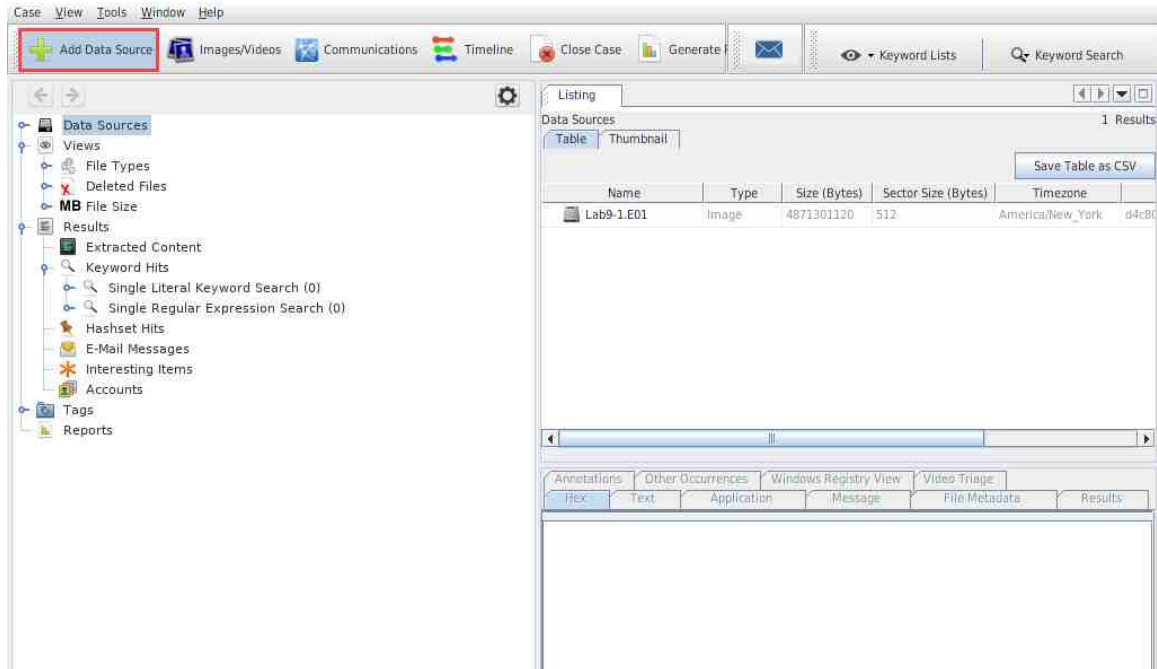
INFO2.txt					
INFO2 File: /home/csi/Desktop/Cases/FOR_LAB_009/Export/Lab9-1/INFO2					
INDEX	DELETED TIME	DRIVE NUMBER	PATH	SIZE	
1	08/25/2004 12:18:25	2	C:\Documents and Settings\Mr. Evil\Desktop\lalsetup250.exe	2160128	
2	08/27/2004 11:12:30	2	C:\Documents and Settings\Mr. Evil\Desktop\netstumblerinstaller_0_4_0.exe	1325056	
3	08/27/2004 11:15:26	2	C:\Documents and Settings\Mr. Evil\Desktop\WinPcap_3_01_a.exe	442880	
4	08/27/2004 11:29:58	2	C:\Documents and Settings\Mr. Evil\Desktop\ethereal-setup-0.10.6.exe	8460800	

26. As you can see from the parsed data, we learned the name of the 4 deleted files we saw in the RECYCLER. We also learned when they were deleted and where from. This information is extremely useful, especially when associated with the specific user that did the deleting. We will now look at the Recycle.bin folder found on newer Windows operating systems.

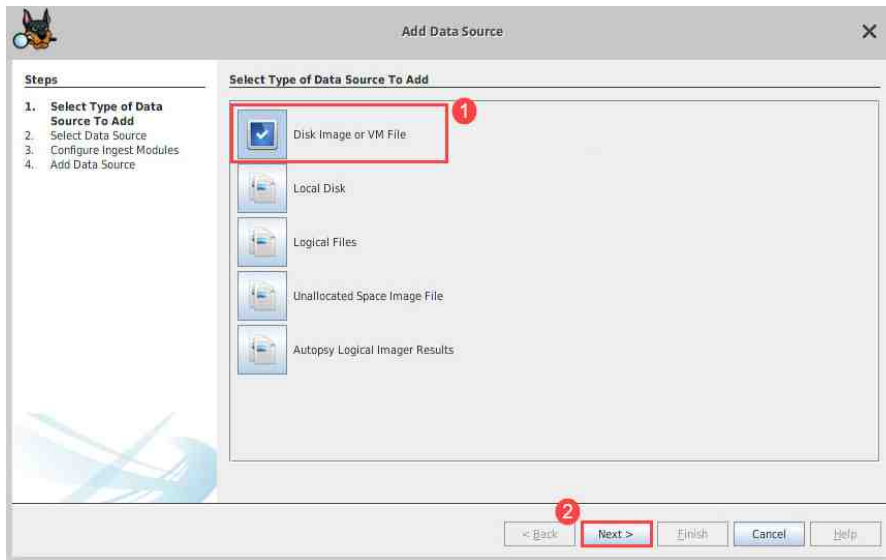
2 Parsing the Recycle.bin Folder

As we mentioned earlier, the newer Microsoft Windows operating systems handle indexing a little differently. Let us look at the recycle bin artifacts for a Windows 10 operating system.

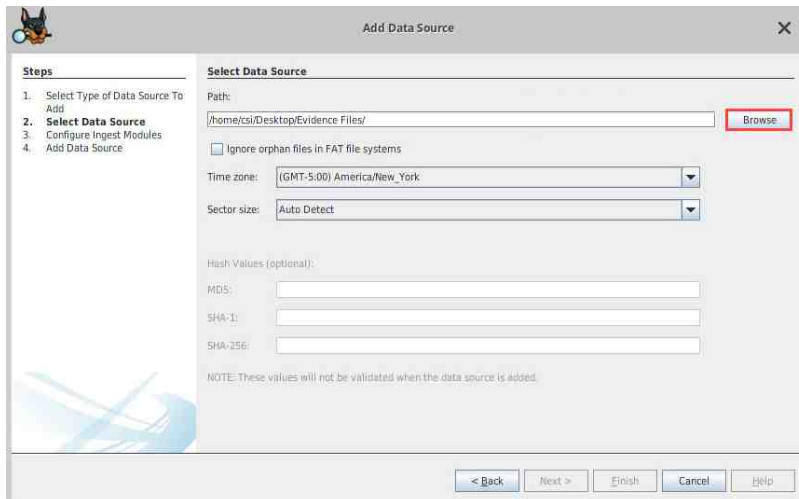
1. Let us begin by adding the Windows 10 FEF to Autopsy. Restore Autopsy by clicking the Autopsy icon on the taskbar. Once the Autopsy window is restored, click the Add Data Source button as seen below. This will reopen the Add Data Source window.



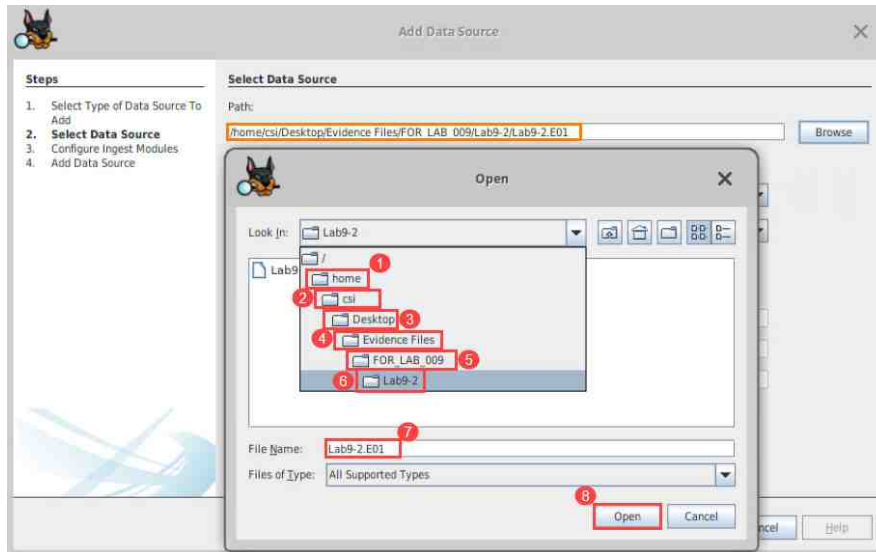
2. In the Add Data Source window, select Disk Image or VM file and click Next as highlighted below.



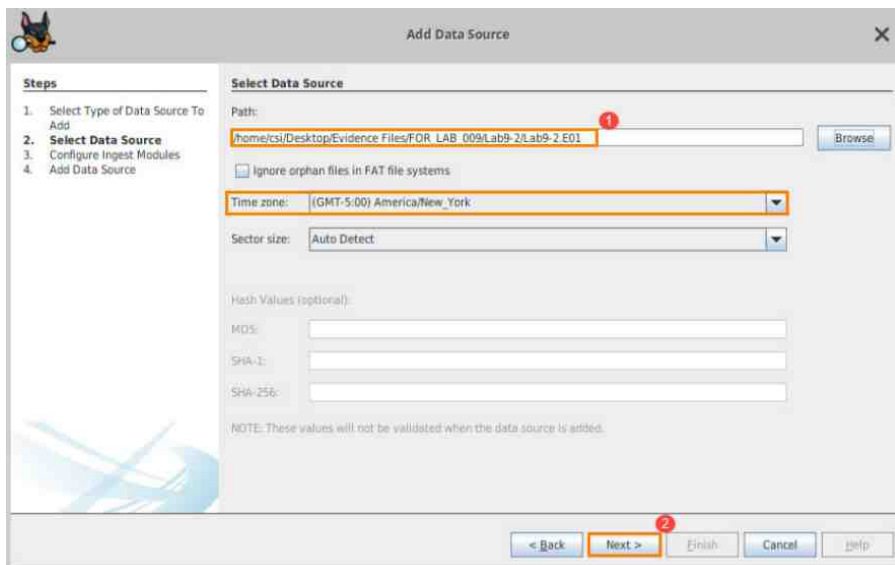
3. In the next window, click the Browse button highlighted below to open the Open window that allows you to browse for the FEF.



4. In the Open window, browse to home > csi > Desktop > Evidence Files > FOR_LAB_009 > Lab9-2 and click the file called Lab9-2.E01 and then click Open as highlighted in items 1 – 8 below.

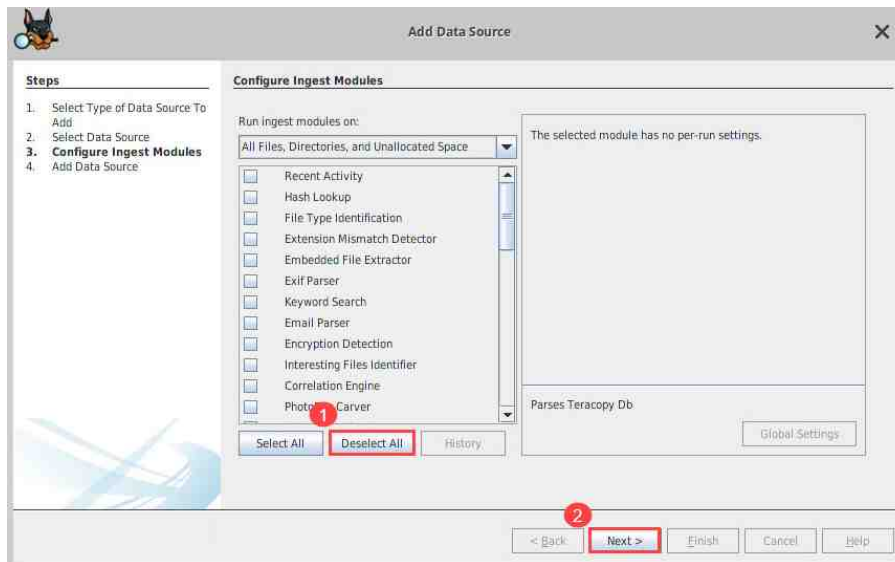


5. The image path will now appear in the Path field, highlighted as item 1 below. We will leave the other options as-is for now and click Next, highlighted as item 2 below.

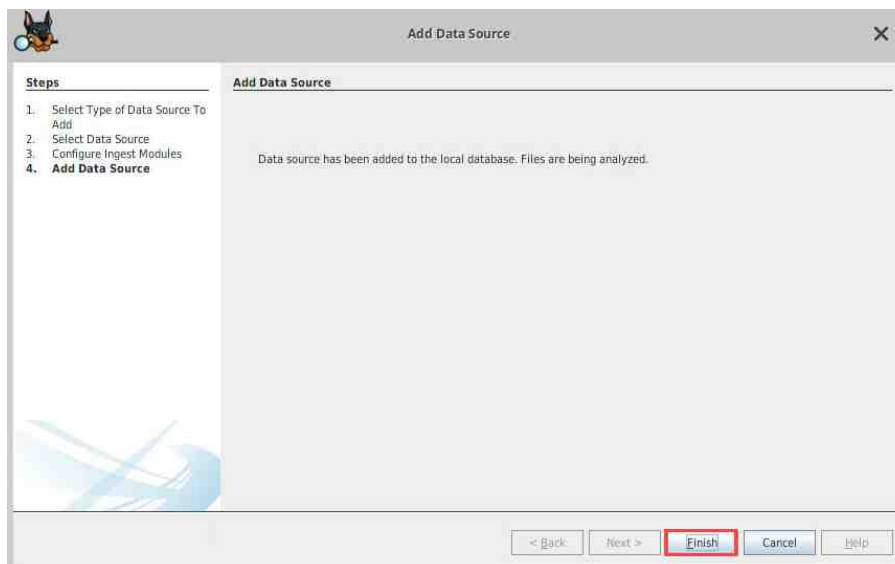


Time zone is an important aspect of any forensic investigation. Feel free to adjust the time zone to match your respective time zones.

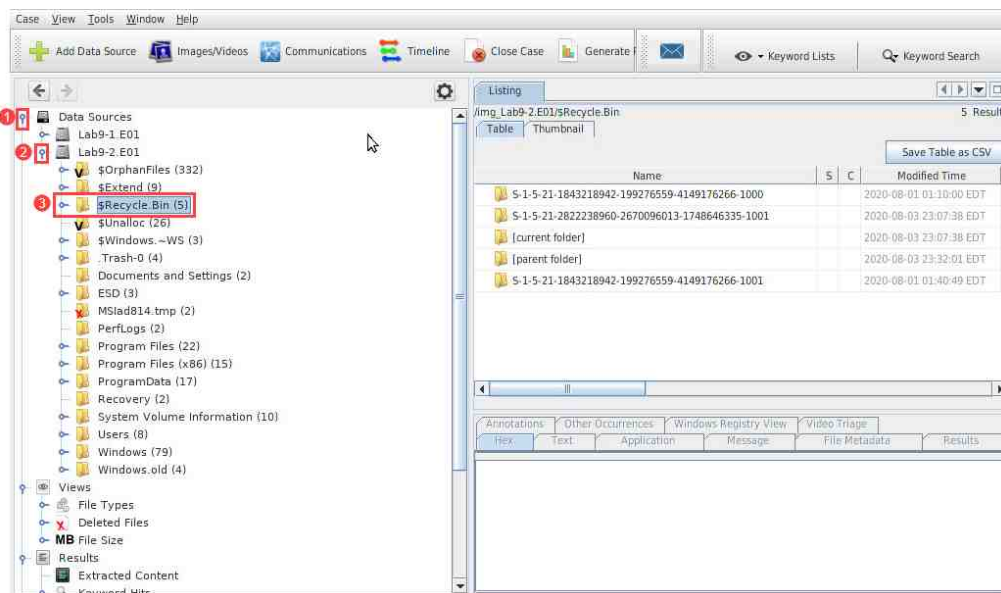
6. You will be taken to the Configure Ingest Modules step of the case creation process. In this exercise, we will not be using an Ingest Module, so uncheck any selected Ingest Module by clicking the Deselect All button and then click Next as highlighted in items 1 and 2 below.



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

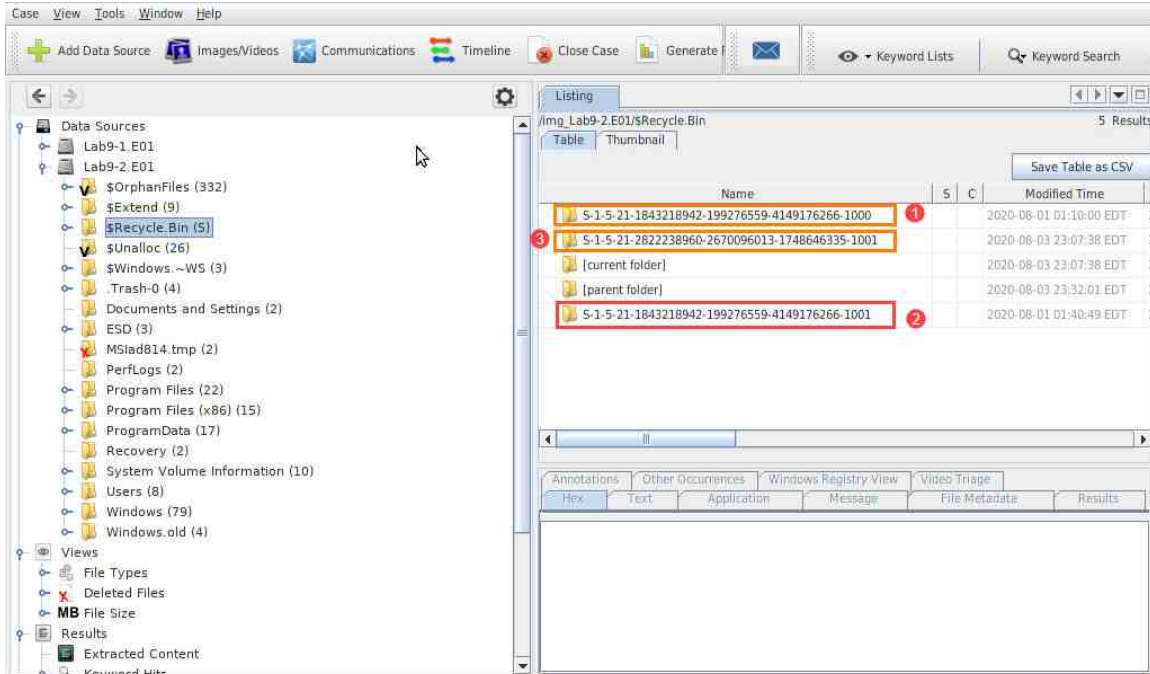


8. You will now be taken back to the Autopsy main window. Here we can navigate the file system and locate the \$Recycle.bin folder. Let us do this by clicking the blue pin beside Data Sources, which will expand and reveal the FEF as seen in item 1 below. Next, click the blue pin beside Lab9-2.E01 to view all the files that make up the Microsoft Windows operating system. Based on the folder structure, it is safe to say that this operating system is post-Windows XP. As with the previous FEF, we can determine this by paying attention to the folder called Users. In Windows XP and older operating systems, the user profiles are stored in a folder called Documents and Settings. The Documents and Settings folder still exists in recent versions and is used for compatibility purposes. As we mentioned in the previous exercise, the \$Recycle.bin folder is the name given to the Recycle Bin folder in Windows Vista and later. Let us click the \$Recycle.bin folder to see its contents, as seen in item 3 below.



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

9. Now that you are in the \$Recycle.bin folder, you can see that there are 3 folders that have SIDs as names. The SIDs highlighted as items 1 and 2 below are from the same computer. You can determine this because they have the same Local Computer Identifier value that comes before the RID. The SID seen in item 3 is from a different computer. This is the only way multiple RIDs can be on the same computer. Since the RIDs are all 1000 or higher, we know that the computer had 3 non-system user accounts interact with the volume at some point in time. In this exercise, we will only look at the folder called S-1-5-21-1843218942-199276559-4149176266-1001. Let us do this by double-clicking the folder as seen in item 2 below.

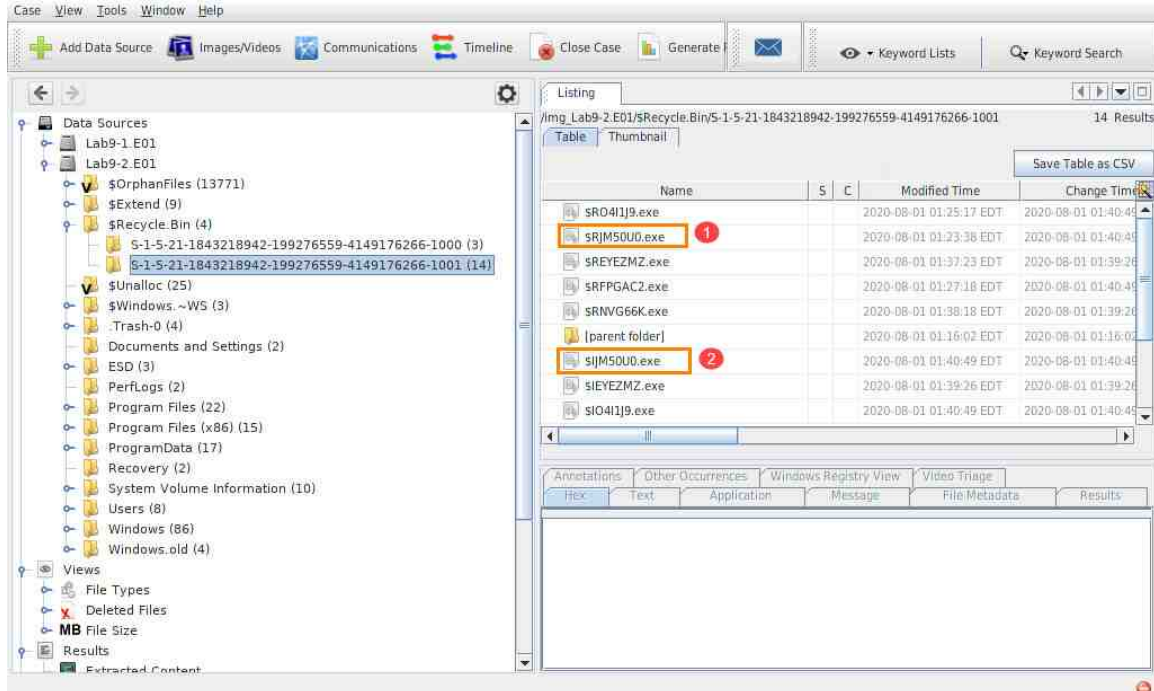


Name	S	C	Modified Time
S-1-5-21-1843218942-199276559-4149176266-1000	1		2020-08-01 01:10:00 EDT
S-1-5-21-2822238960-2670096013-1748646335-1001	3		2020-08-03 23:07:38 EDT
[current folder]			2020-08-03 23:07:38 EDT
[parent folder]			2020-08-03 23:32:01 EDT
S-1-5-21-1843218942-199276559-4149176266-1001	2		2020-08-01 01:40:49 EDT



In practice, always review all the recycle bin folders. We will ignore them in this exercise because there is nothing in them.

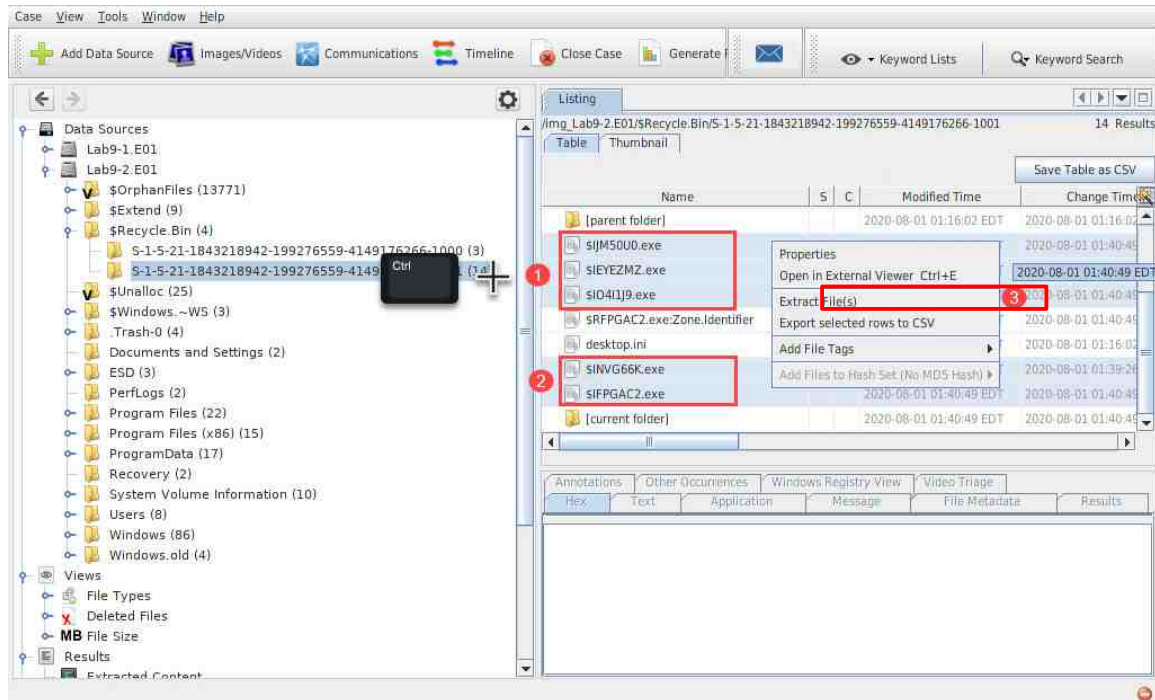
10. The list of deleted files will appear in the Listing pane as seen below. The deleted files in this folder get renamed in a different way than the ones in the RECYCLER folder. As you can see in the Listing pane, the files all start with \$R or \$I. In the Recycle.bin folder, deleted files get renamed with \$R and an alphanumeric value. A file containing metadata for the deleted file is also created and stored in the folder. This deleted file is called the index file and starts with \$I and has the same alphanumeric string as the one that starts with \$R. An example can be seen in items 1 and 2 below. The index file contains similar information to the INFO2 file. Let us export these index files and use Rifiuti to decode them.



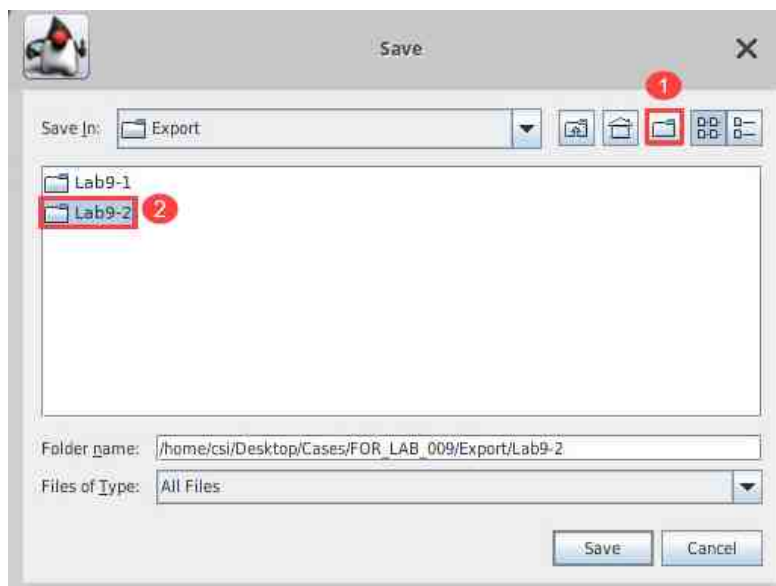
The screenshot shows a forensic tool interface with a sidebar on the left displaying a tree view of data sources. The main pane on the right shows a listing of files in the Recycle Bin. The files are listed in a table with columns for Name, S, C, Modified Time, and Change Time. Two files are highlighted with red circles and numbered 1 and 2.

Name	S	C	Modified Time	Change Time
\$R041J9.exe			2020-08-01 01:25:17 EDT	2020-08-01 01:40:49
\$RJM50U0.exe	1		2020-08-01 01:23:38 EDT	2020-08-01 01:40:49
\$REYEZMZ.exe			2020-08-01 01:37:23 EDT	2020-08-01 01:39:26
\$RFPGAC2.exe			2020-08-01 01:27:18 EDT	2020-08-01 01:40:49
\$RNVG66K.exe			2020-08-01 01:38:18 EDT	2020-08-01 01:39:26
[parent folder]			2020-08-01 01:16:02 EDT	2020-08-01 01:16:02
\$IJM50U0.exe	2		2020-08-01 01:40:49 EDT	2020-08-01 01:40:49
\$IEYEZMZ.exe			2020-08-01 01:39:26 EDT	2020-08-01 01:39:26
\$IO41J9.exe			2020-08-01 01:40:49 EDT	2020-08-01 01:40:49

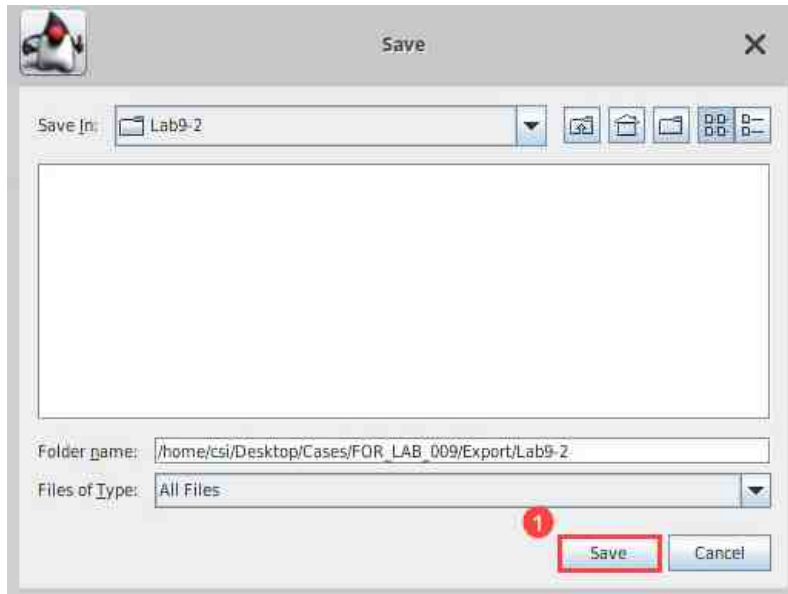
11. Let us begin by exporting all the index files. To do this, hold Ctrl and click on each of the files that begin with \$I, as seen in items 1 and 2 below. When you have selected all the files that start with \$I, right-click on any one of the files and click the Extract File(s) option from the context menu, as seen in item 3 below, to open the Save window.



12. Once the Save window appears, it will default to the Export folder within the Autopsy case folder. Let us create a new folder by clicking the create new folder icon from the toolbar as seen in item 1. Name the folder Lab9-2 as seen in item 2, and then double-click the Lab9-2 folder you just created to open it.



13. Once inside the Lab9-2 folder, click Save as seen in item 1.

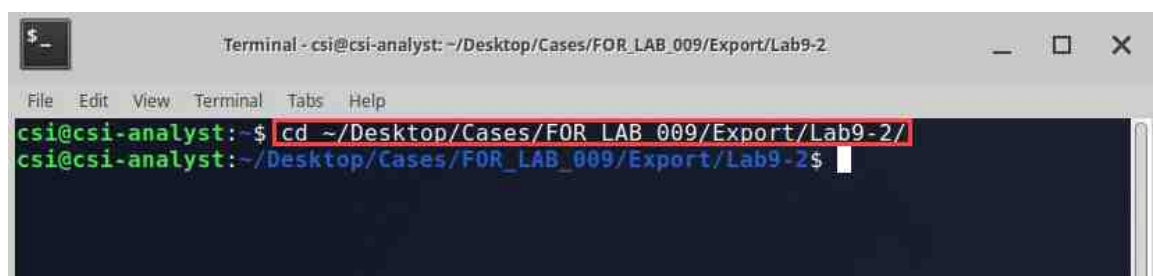


14. Once the export is done, an information window will appear, indicating that the file has been extracted. Click OK as seen below.



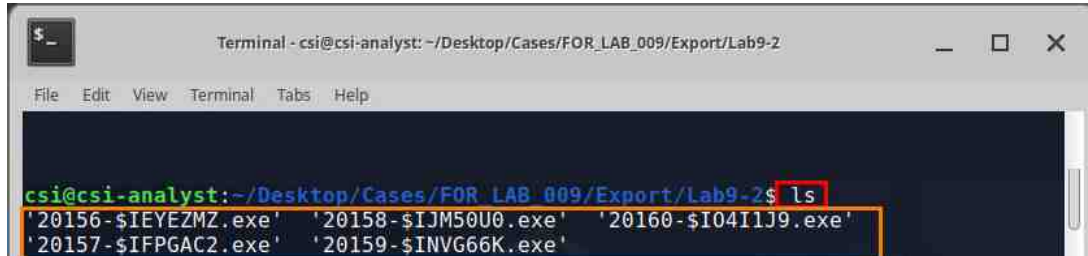
15. With the files extracted, we can use Rifiuti to extract the data from it. In addition to INFO2 files, Rifiuti is programmed to extract data from files that start with the characters \$I. The files we exported just now are \$I files, but when they are exported in bulk, Autopsy renames each file and adds an offset value to the beginning of the filename. This means we will have to rename these files to get them to work with Rifiuti. Let us do this using the terminal. First, we will browse to the path we exported the files to. Open a new terminal window and type the following command.

```
cd ~/Desktop/Cases/FOR_LAB_009/Export/Lab9-2/
```



16. Type `ls` to view the contents of the current directory. This command will list information about the file(s). During the export process, the application may affix a random string of numbers before each `$I` recycle bin file. Using the `ls` command, we can note the string for each and append the command accordingly.

```
ls
```



The string in this screenshot may differ from the string in the environment at the time of this lab. Pay close attention and note the difference then append the command accordingly.

17. We will be renaming the files that we saw when we viewed the folder's contents. Let us begin renaming by typing the command below. We will use the first name on the list, as seen in item 1 below. Once you have typed the command, press Enter.

```
mv 20156-\$I EYEZMZ.exe \$I EYEZMZ.exe
```



The backslash '`\`' in the command is used to remove the whitespace from the name. Simply, start typing the name of the file and press Tab to auto-fill the name.

18. Now that you have renamed one, let us do it for all the files in the directory. Retype the command using the names for each file from the list, as seen in step 16 above.

```
mv 20157-\\$I FPGAC2. exe \\$I FPGAC2. exe
```

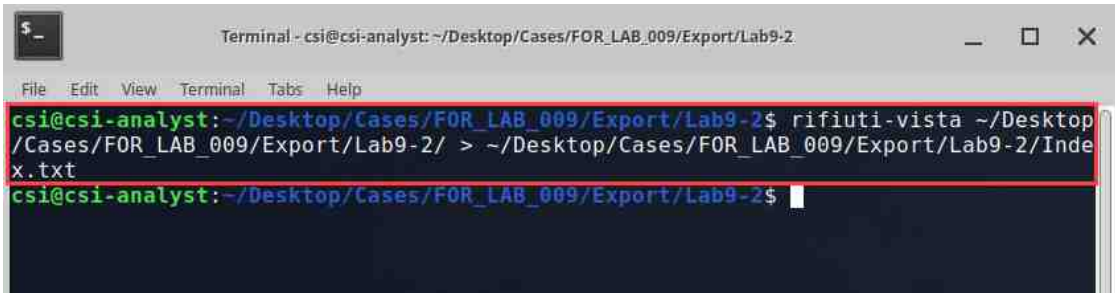
```
mv 20158-\\$I JM50U0. exe \\$I JM50U0. exe
```

```
mv 20159-\\$I NVG66K. exe \\$I NVG66K. exe
```

```
mv 20160-\\$I 04I 1J9. exe \\$I 04I 1J9. exe
```

19. Once you have all the files in the folder renamed, we can begin parsing them with Rifiuti. The command is slightly different in this exercise. Instead of just `ri fi uti`, we will type `ri fi uti -vi sta`. We will also be parsing the folder instead of a specific file. Let us begin by typing the following command and then pressing Enter.

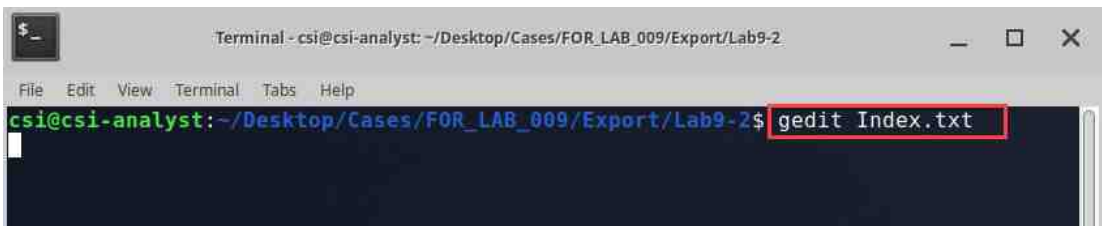
```
ri fi uti -vi sta ~/Desktop/Cases/FOR_LAB_009/Export/Lab9-2/ > ~/Desktop/Cases/FOR_LAB_009/Export/Lab9-2/Index. txt
```



```
Terminal - csi@csi-analyst: ~/Desktop/Cases/FOR_LAB_009/Export/Lab9-2.
File Edit View Terminal Tabs Help
csi@csi-analyst:~/Desktop/Cases/FOR_LAB_009/Export/Lab9-2$ rifiuti-vista ~/Desktop/Cases/FOR_LAB_009/Export/Lab9-2/ > ~/Desktop/Cases/FOR_LAB_009/Export/Lab9-2/Index.txt
csi@csi-analyst:~/Desktop/Cases/FOR_LAB_009/Export/Lab9-2$
```

20. As in the previous exercise, the command we just entered will extract the data from the `$I` index files. Now let us look at the file we just created. Let us use Gedit to open this file. Do this by typing the following command and pressing Enter.

```
gedi t I ndex. txt
```



```
Terminal - csi@csi-analyst: ~/Desktop/Cases/FOR_LAB_009/Export/Lab9-2.
File Edit View Terminal Tabs Help
csi@csi-analyst:~/Desktop/Cases/FOR_LAB_009/Export/Lab9-2$ gedit Index.txt
```

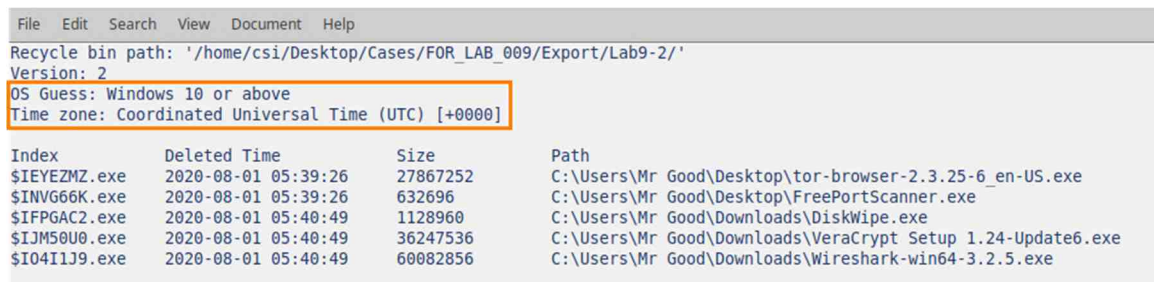

21. Gedit will open the file as seen below. This file is structured just like the one from the previous exercise, except for the drive number column, which is not present in this version.



```
File Edit Search View Document Help
Recycle bin path: '/home/csi/Desktop/Cases/FOR_LAB_009/Export/Lab9-2/'
Version: 2
OS Guess: Windows 10 or above
Time zone: Coordinated Universal Time (UTC) [+0000]

Index Deleted Time Size Path
$IEYEZMZ.exe 2020-08-01 05:39:26 27867252 C:\Users\Mr Good\Desktop\tor-browser-2.3.25-6_en-US.exe
$INV666K.exe 2020-08-01 05:39:26 632696 C:\Users\Mr Good\Desktop\FreePortScanner.exe
$IFPGAC2.exe 2020-08-01 05:40:49 1128960 C:\Users\Mr Good\Downloads\DiskWipe.exe
$IJMS0U0.exe 2020-08-01 05:40:49 36247536 C:\Users\Mr Good\Downloads\VeraCrypt Setup 1.24-Update6.exe
$I04I1J9.exe 2020-08-01 05:40:49 60082856 C:\Users\Mr Good\Downloads\Wireshark-win64-3.2.5.exe
```

22. This report also guesses what operating system the files were taken from and lists the time zone that the dates and times are being presented in.



```
File Edit Search View Document Help
Recycle bin path: '/home/csi/Desktop/Cases/FOR_LAB_009/Export/Lab9-2/'
Version: 2
OS Guess: Windows 10 or above
Time zone: Coordinated Universal Time (UTC) [+0000]

Index Deleted Time Size Path
$IEYEZMZ.exe 2020-08-01 05:39:26 27867252 C:\Users\Mr Good\Desktop\tor-browser-2.3.25-6_en-US.exe
$INV666K.exe 2020-08-01 05:39:26 632696 C:\Users\Mr Good\Desktop\FreePortScanner.exe
$IFPGAC2.exe 2020-08-01 05:40:49 1128960 C:\Users\Mr Good\Downloads\DiskWipe.exe
$IJMS0U0.exe 2020-08-01 05:40:49 36247536 C:\Users\Mr Good\Downloads\VeraCrypt Setup 1.24-Update6.exe
$I04I1J9.exe 2020-08-01 05:40:49 60082856 C:\Users\Mr Good\Downloads\Wireshark-win64-3.2.5.exe
```

23. As you can see from the parsed data, we learned the name of the 5 deleted files we saw in the Recycle.bin folder. We learned when they were deleted and where from as well. These artifacts are priceless in investigations and should never be overlooked.
24. You are now at the end of the lab. Close all the open programs by clicking the X on each one, as seen below.

