



FORENSICS V2 LAB SERIES

Lab 20: File Hashing and Hash Analysis

Document Version: 2021-01-14

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

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

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

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
1 Exporting a File Hash List with FTK Imager	6
2 File Hashing with Hasher	15
3 Creating and Using a Hash Set	22

Introduction

File hashing is one of the backbones of digital forensics. It helps to verify and validate digital data. This module will teach what hashes are and how to utilize them to ace a digital investigation.

Objectives

-) Learn what hashing is and the different types
-) Understand how to perform file hashing
-) Learn how to create hash sets and compare them in order to identify known and unknown files

Lab Topology



Lab Settings

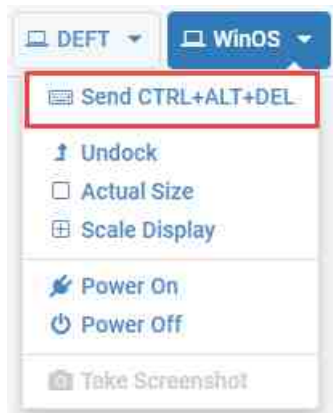
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

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 Exporting a File Hash List with FTK Imager

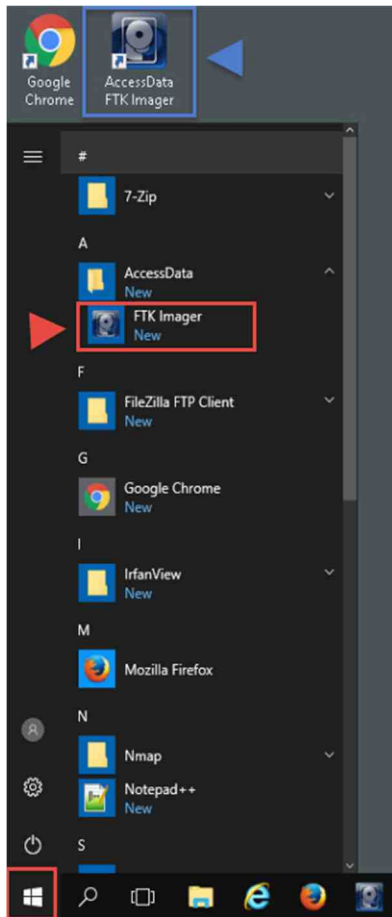
There are many use cases for a file hash list. It could be for compiling a hash set, which is a collection of hash values that are usually related and are designed to highlight or omit certain files from a data set. It could be used for simply proving that the file has not been changed since you hashed it. It could also be used for password cracking as well. In the first 2 exercises, we will do the simple file hash list export for you to see what a hash looks like and see some different types of hashes. The final exercise will be the generation of a hash set and the hash comparison process.

1. To begin, launch the WinOS virtual machine to access the graphical login screen.
 - a. Select Send CTRL+ALT+DEL from the dropdown menu to be prompted with the login screen.

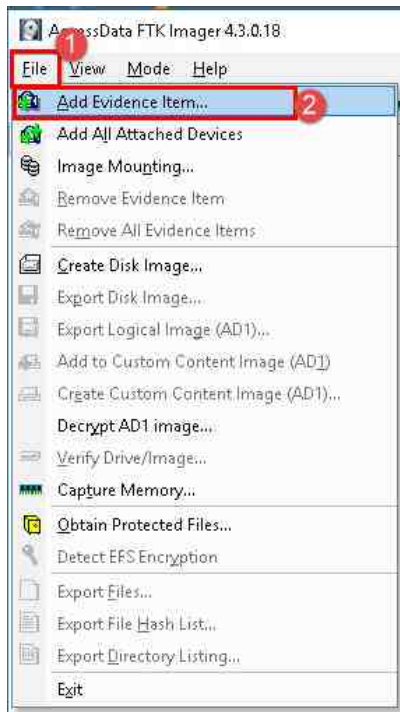


- b. Log in as Administrator using the password: Training\$

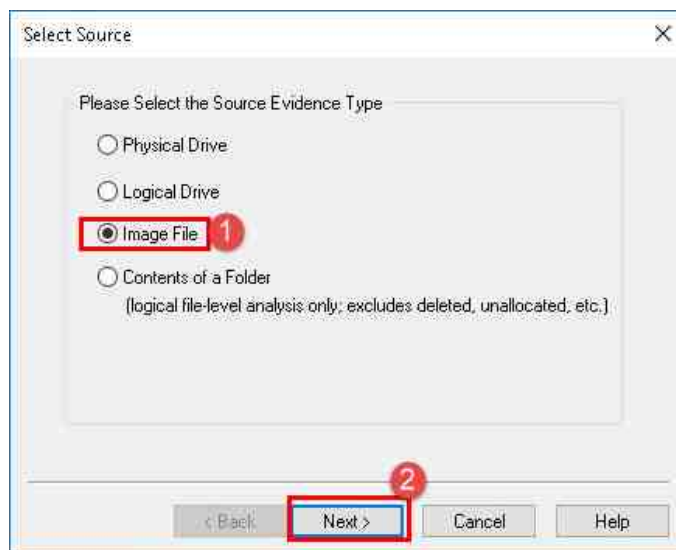
2. In this exercise, we will show you how to use FTK Imager to generate hashes of files from an image.



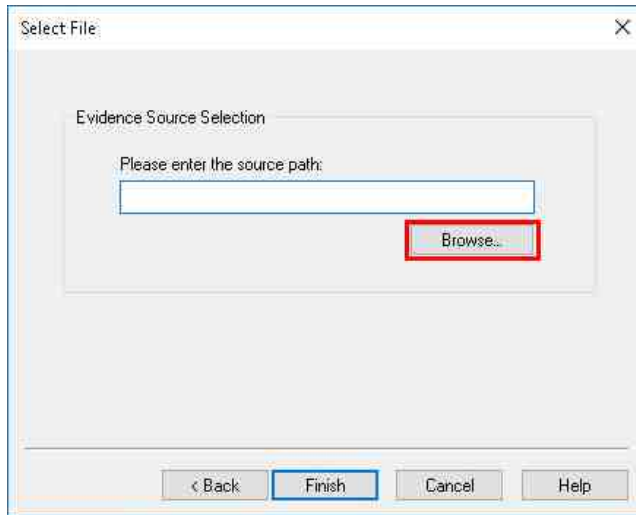
- Once you have FTK Imager open, let us load an FEF. Do this by selecting the options File > Add Evidence Item, which will open the Select Source window.



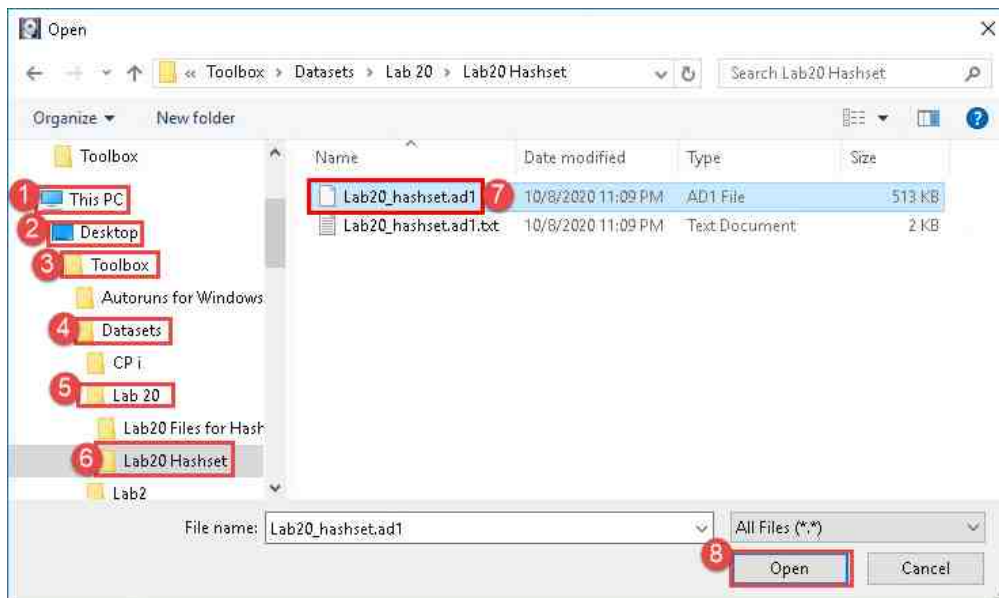
- In the Select Source window, select the Image File radio button and then select Next to proceed to the Select File window.



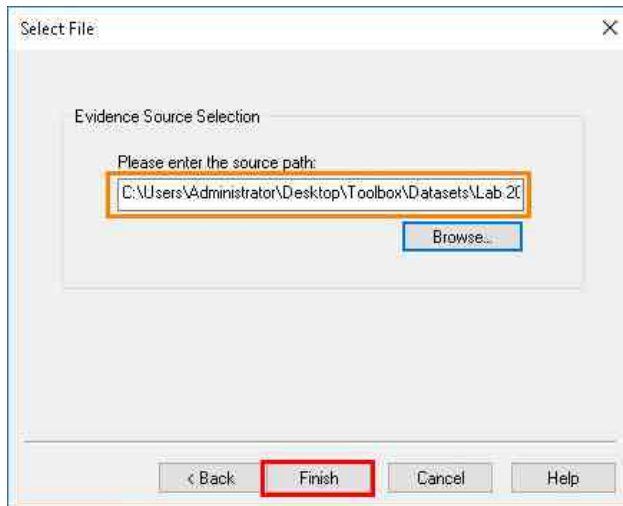
5. In the Select File window, click Browse highlighted in red in the screenshot below. This will open the File Selection window, which will allow you to browse to the appropriate image file.



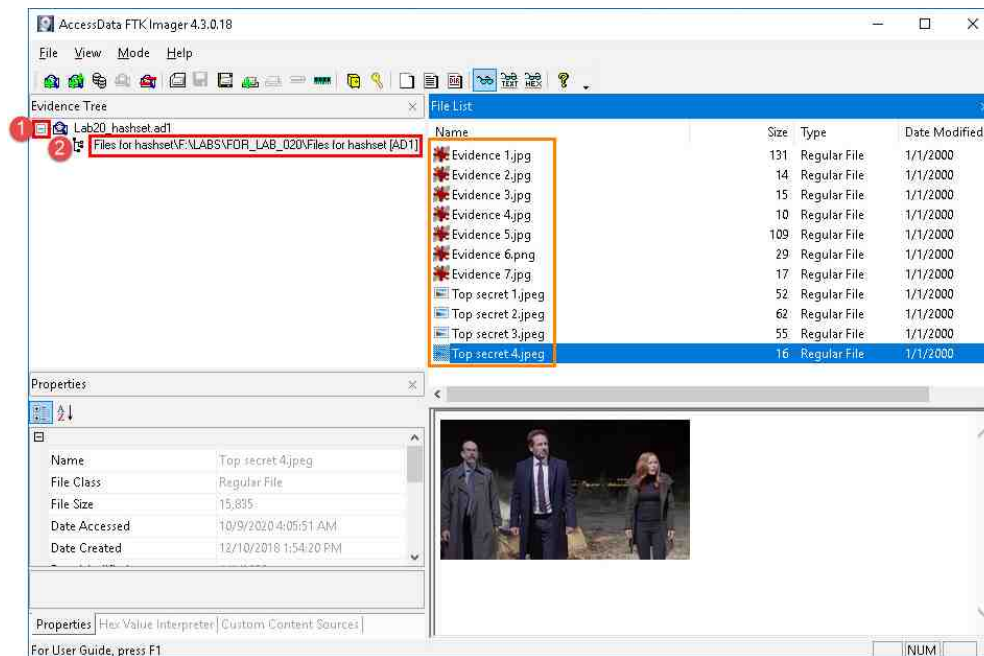
6. Browse to This PC > Desktop and double-click the folder Toolbox > Datasets > Lab20 > Lab20 Hashset. This will open the folder revealing a logical image called Lab20_hashset.ad1 as seen in items 1 - 6. Select the file called Lab20_hashset.ad1 and click the Open button as highlighted at items 7 and 8 below. This will take you back to the Select file window.



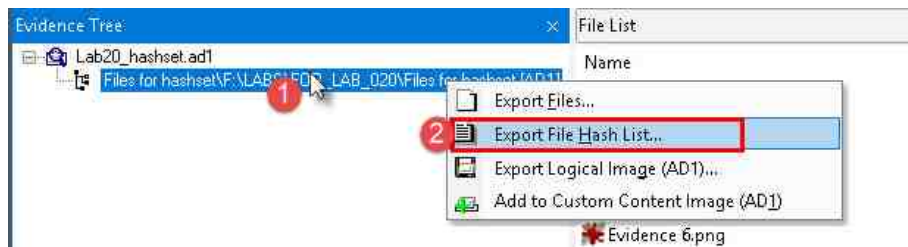
- In the Select File window, verify that the path of the selected file matches the one highlighted in the screenshot below. Once you have verified, click the Finish button at the bottom of the window highlighted below. This will take you to the main GUI, where the image will be loaded in the Evidence Tree pane.



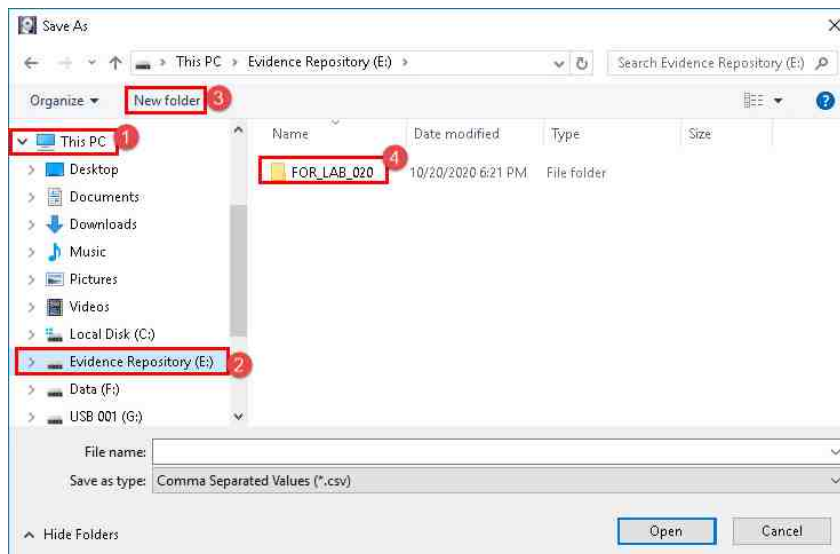
- In the Evidence Tree pane, navigate to Lab20_hashset.ad1 > Files for Lab20_hashset [AD1] by clicking the + sign beside them as seen in items 1 and 2 below. Once there, you can look at the files in the File List pane. Click on each of these files to get familiar with the content.



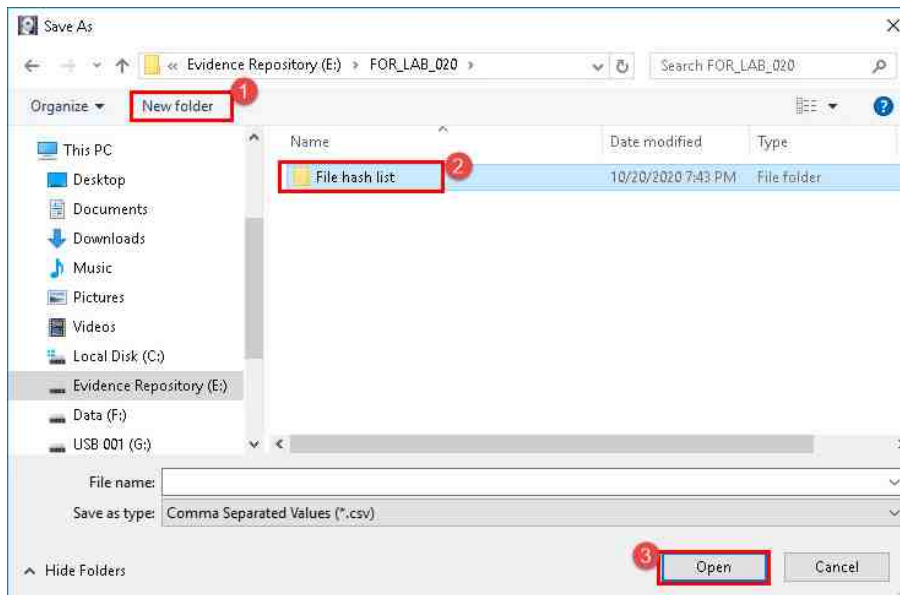
9. Now let us export a file hash list and look at it. This is very simple to do with FTK Imager. To begin, right-click on Files for hashset\F:\LABS\FOR_LAB_020\Files for hashset [AD1], as seen in item 1 below, then click Export File Hash List as seen in item 2 below.



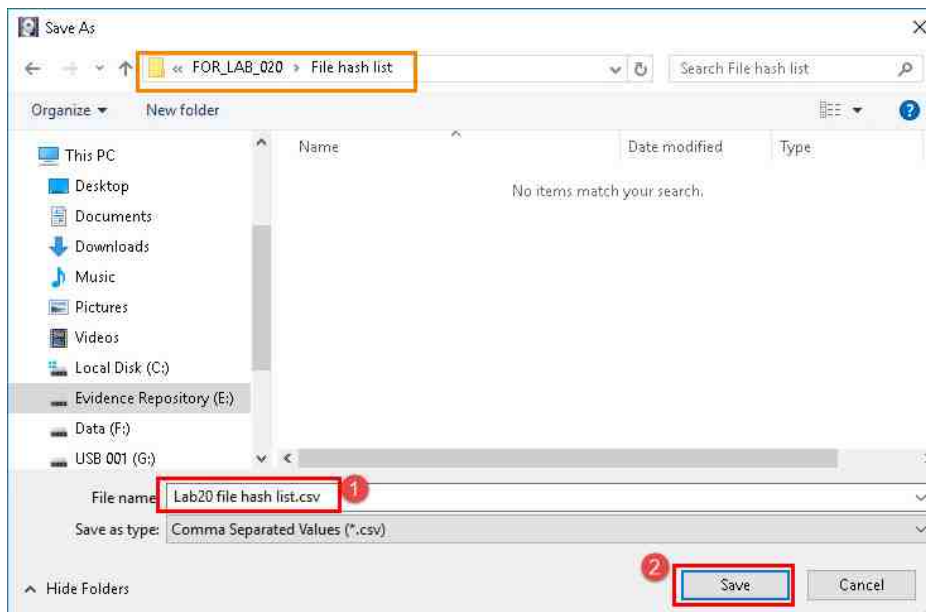
10. The Save As window will open. Browse to This PC > Evidence Repository (E:) as seen in items 1 and 2 below. Once there, click New Folder as seen in item 3 and name the folder FOR_LAB_020 as seen in item 4.



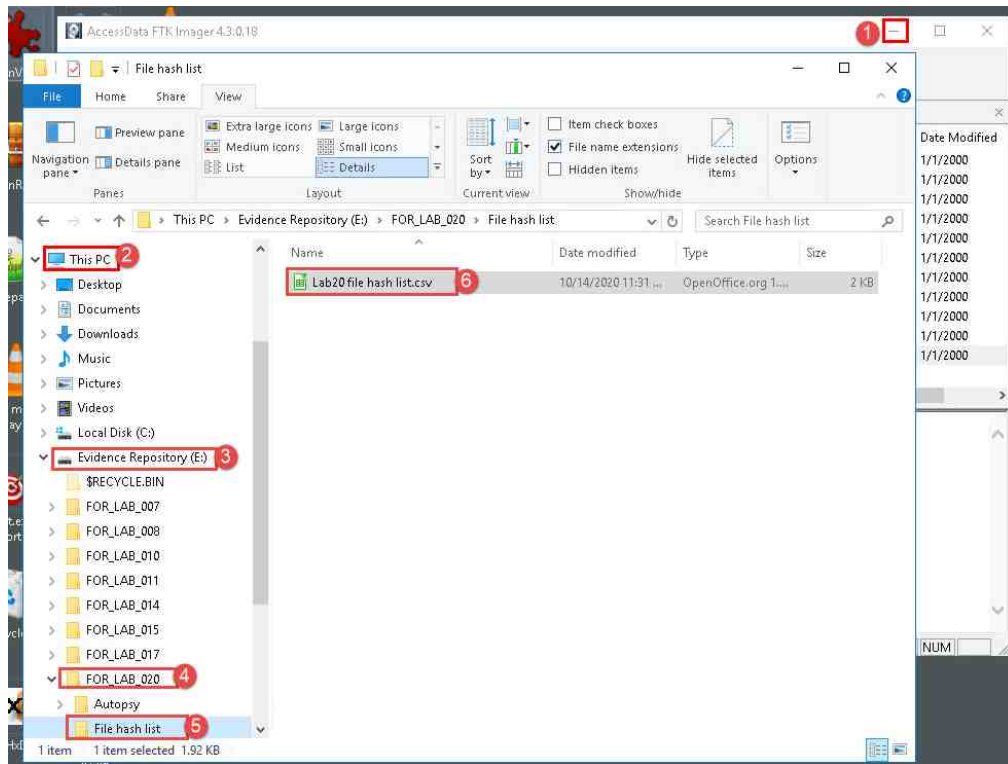
11. Next, double-click the FOR_LAB_020 folder to open it. Click the Create New Folder icon again as seen in item 1 and then name the folder File Hash List and click Open as seen in items 2 and 3 below.



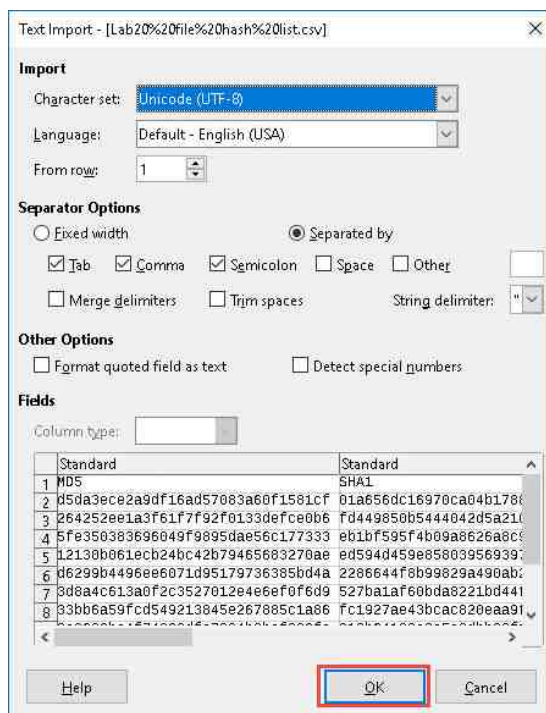
12. Next, double-click the File Hash List folder to open it and then type Lab20 file hash list in the File name field as seen in item 1 below. Once you are done, click Save as seen in item 2. You have successfully exported a hash list of the files in an image. You can do this for a single file or a subset of files. Now let us open the list and look at it.



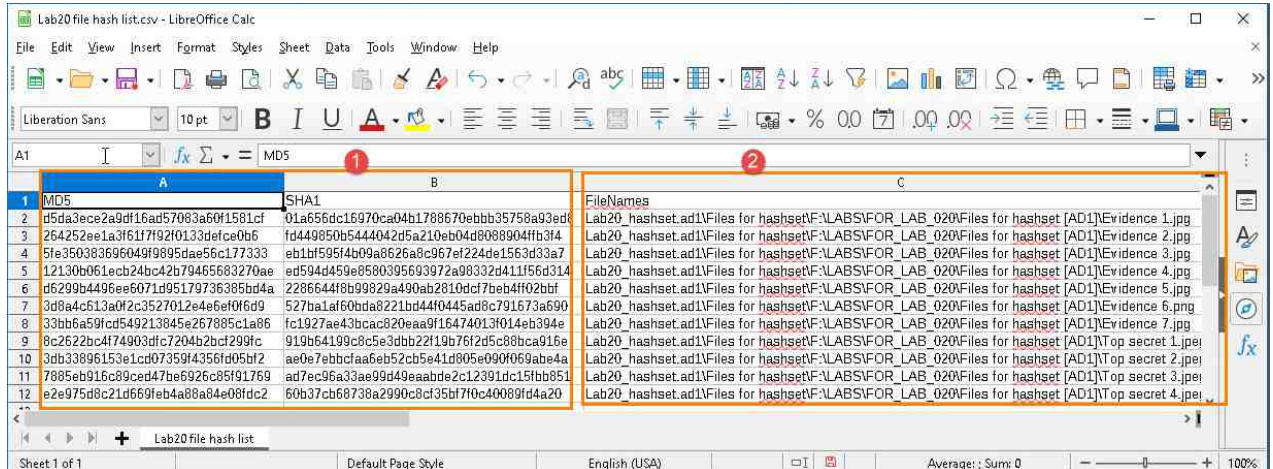
13. Minimize FTK Imager as seen in item 1 and open File Explorer. In File Explorer, navigate to This PC > Evidence Files > FOR_LAB_020 > File Hash List as seen in items 2, 3, 4 and 5. Once there, double-click the file called Lab20 file hash list to open it, as seen in item 6 below.



14. You might be prompted by a Text Import window. Leave everything as default and click OK.



15. In the File hash list, you will see 3 columns and data within each row. This tool uses 2 types of hashes, MD5 (Message Digest – 5) and SHA1 (Secure Hash Algorithm-1) seen in item 1. These are old hash algorithms that are very popular but are not the most secure. For the purposes of hash analysis, it can be used as the likelihood that 2 files can have the same hash is still extremely low. The 3rd column seen in item 2 contains the names and source path of the files.



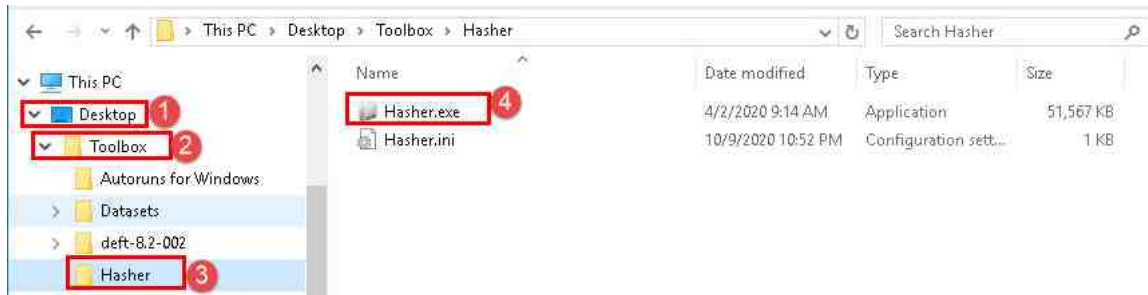
The screenshot shows a LibreOffice Calc spreadsheet titled "Lab20 file hash list.csv". The spreadsheet has three columns: A (MD5), B (SHA1), and C (FileNames). The data is as follows:

	A	B	C
1	MD5	SHA1	FileNames
2	d5da3ece2a9d16ad57083a60f1581cf	01a656dc16970ca04b1788670ebbb35758a93ed6	Lab20_hashset.ad1Files for hashset\F:\LABS\FOR LAB_020Files for hashset (AD1)\Evidence 1.jpg
3	264252ee1a3f617f92f0133defce0b6	fd449850b5444042d5a210eb04d8088904fb3f4	Lab20_hashset.ad1Files for hashset\F:\LABS\FOR LAB_020Files for hashset (AD1)\Evidence 2.jpg
4	5fe350383696049f9895dae56c177333	eb1bf595f4b09a8626a8c967ef224de1563d33a7	Lab20_hashset.ad1Files for hashset\F:\LABS\FOR LAB_020Files for hashset (AD1)\Evidence 3.jpg
5	12130b061ecb24bc42b79465683270ae	ed594d459e8580395693972a98332d411f56d314	Lab20_hashset.ad1Files for hashset\F:\LABS\FOR LAB_020Files for hashset (AD1)\Evidence 4.jpg
6	d6299b4496ee6071d95179736385bd4a	2286644f8b99829a490ab2810dcf7beb4ff02bfb	Lab20_hashset.ad1Files for hashset\F:\LABS\FOR LAB_020Files for hashset (AD1)\Evidence 5.jpg
7	3d8a4c613a0f2c3527012e4e6ef0f6d9	527ba1af60bda8221bd44f0445ad8c791673a690	Lab20_hashset.ad1Files for hashset\F:\LABS\FOR LAB_020Files for hashset (AD1)\Evidence 6.png
8	33bb6a59fcd549213845e267885c1a86	fc1927ae43bcac820eaa9f16474013f014eb394e	Lab20_hashset.ad1Files for hashset\F:\LABS\FOR LAB_020Files for hashset (AD1)\Evidence 7.jpg
9	8c2622bc4f74903dfc7204b2bfc299fc	919b64199c8c5e3dbb22119b76f2d5c88bca916e	Lab20_hashset.ad1Files for hashset\F:\LABS\FOR LAB_020Files for hashset (AD1)\Top secret 1.jpg
10	3db33896153e1cd07359f4356fd05bf2	ae0e7ebbcfaa6eb52cb5e41d805e090f069abe4a	Lab20_hashset.ad1Files for hashset\F:\LABS\FOR LAB_020Files for hashset (AD1)\Top secret 2.jpg
11	7885eb916c9ced47be6926c85f91769	ad7ec96a33ae99d49eaabde2c12391dc15fbb851	Lab20_hashset.ad1Files for hashset\F:\LABS\FOR LAB_020Files for hashset (AD1)\Top secret 3.jpg
12	e2e975d8c21d669feb4a88a84e08fcd2	60b37cb68738a2990c8cf35bf7f0c40089fd4a20	Lab20_hashset.ad1Files for hashset\F:\LABS\FOR LAB_020Files for hashset (AD1)\Top secret 4.jpg

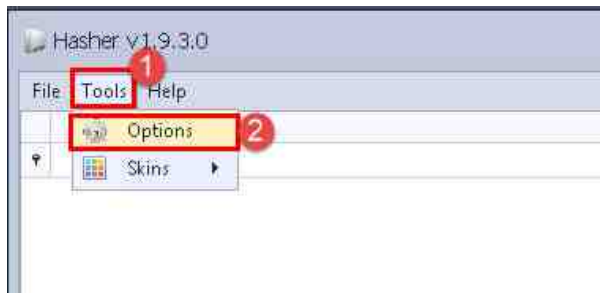
16. Let us use a different tool to hash these files to see other types of hash algorithms.

2 File Hashing with Hasher

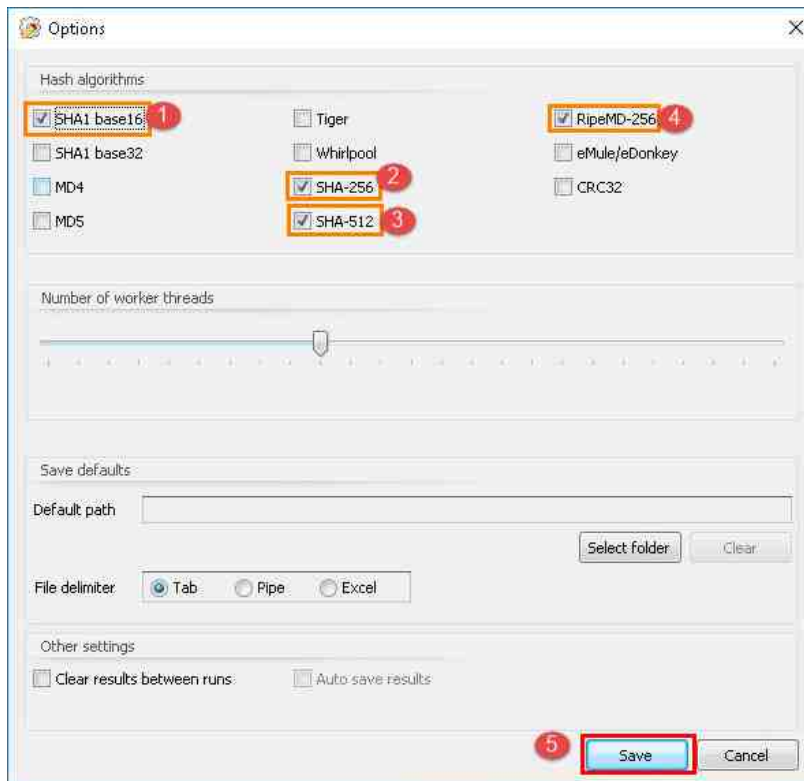
1. This is a quick exercise that can show additional hash values that are more secure and less likely to have collisions. We will be hashing the same files from the logical AD1 file; however, they have already been exported. Let us begin by navigating to Desktop > Toolbox > hasher as seen in items 1, 2, and 3 below. Once there, double-click Hasher.exe to open the program, as seen in item 4.



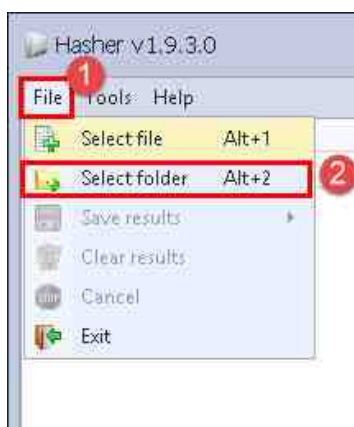
2. Hasher is a small but powerful tool that can hash files or folders using a variety of algorithms. Since it is simple, we will learn as we go. Let us begin by looking at the algorithms that are selected by default. Do this by navigating to Tools > Options, as seen in items 1 and 2 below.



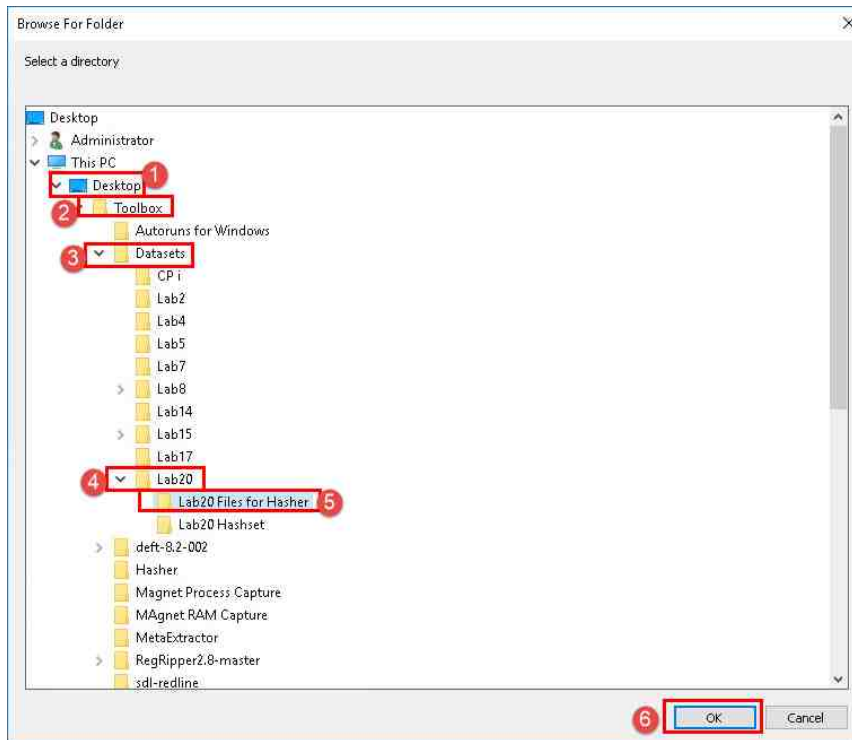
3. In the options menu, there are checkboxes beside SHA-1 Base 16, SHA-256, SHA-512, and RIPEMD-256, as seen in items 1, 2, 3, and 4 below. The other options are hash algorithms as well, but we will only cover these ones. Once you have confirmed the algorithms, click Save as seen in item 5 below.



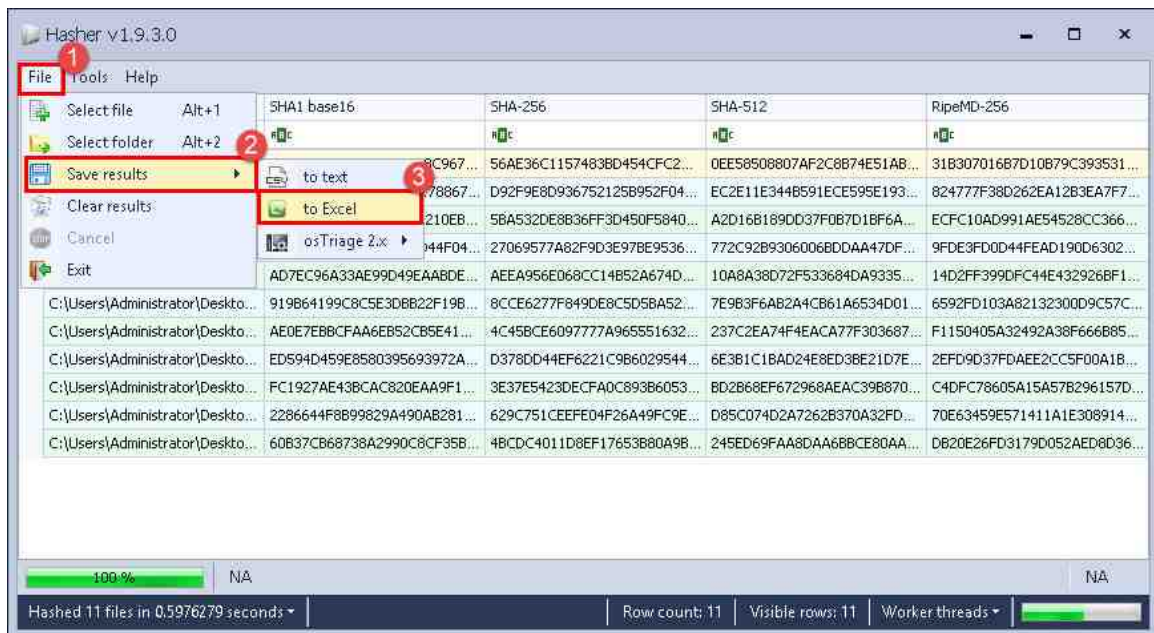
4. Now, let us hash our files. To begin, click File > Select Folder, as seen in items 1 and 2 below. Alternatively, you can use Alt+2. This will open the Browse For Folder window.



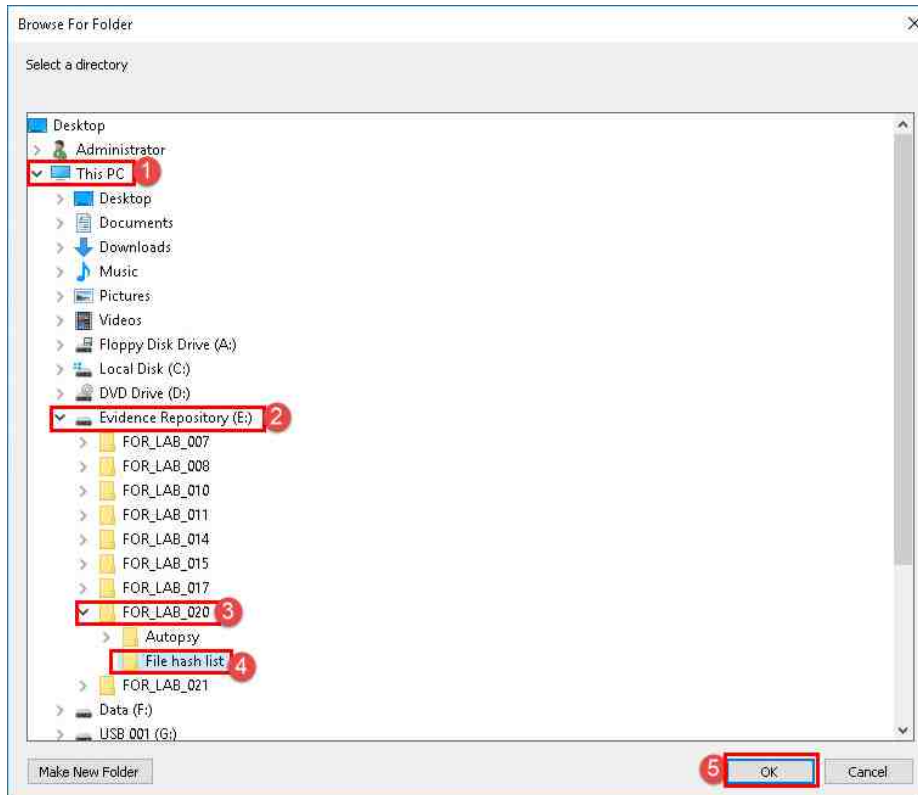
- In the Browse For Folder window, navigate to Desktop > Toolbox > Datasets > Lab20 > Lab20 Files for Hasher and click Ok as seen in items 1, 2, 3, 4, 5, and 6 below.



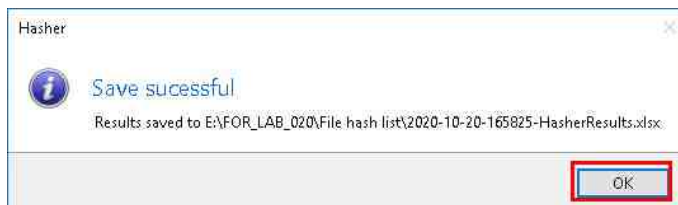
- You will see the hashes populate Hasher's main GUI. Let us export the results by navigating to File > Save results > To Excel as seen in items 1, 2, and 3 below.



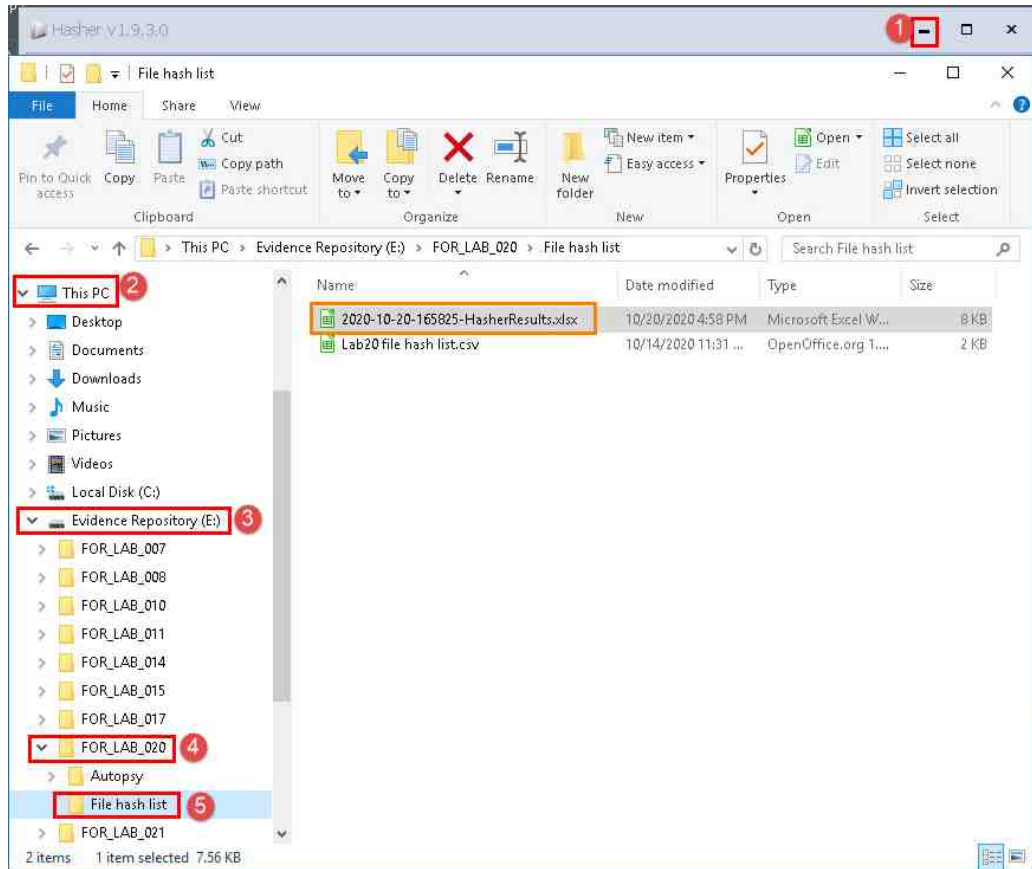
- The Browse For Folder window will open. Navigate to ThisPC > Evidence Repository (E:) > FOR_LAB_020 > File hash list and click OK as seen in items 1, 2, 3, 4, and 5 below.



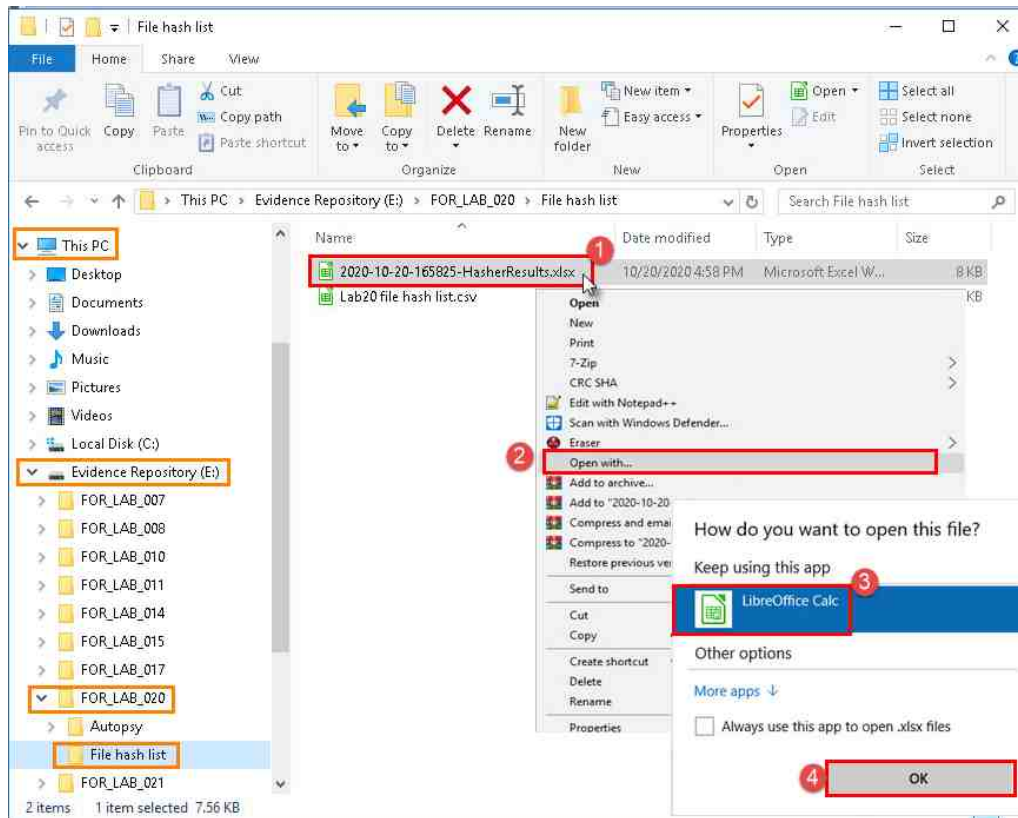
- A prompt will appear that says Save successful. Click OK.



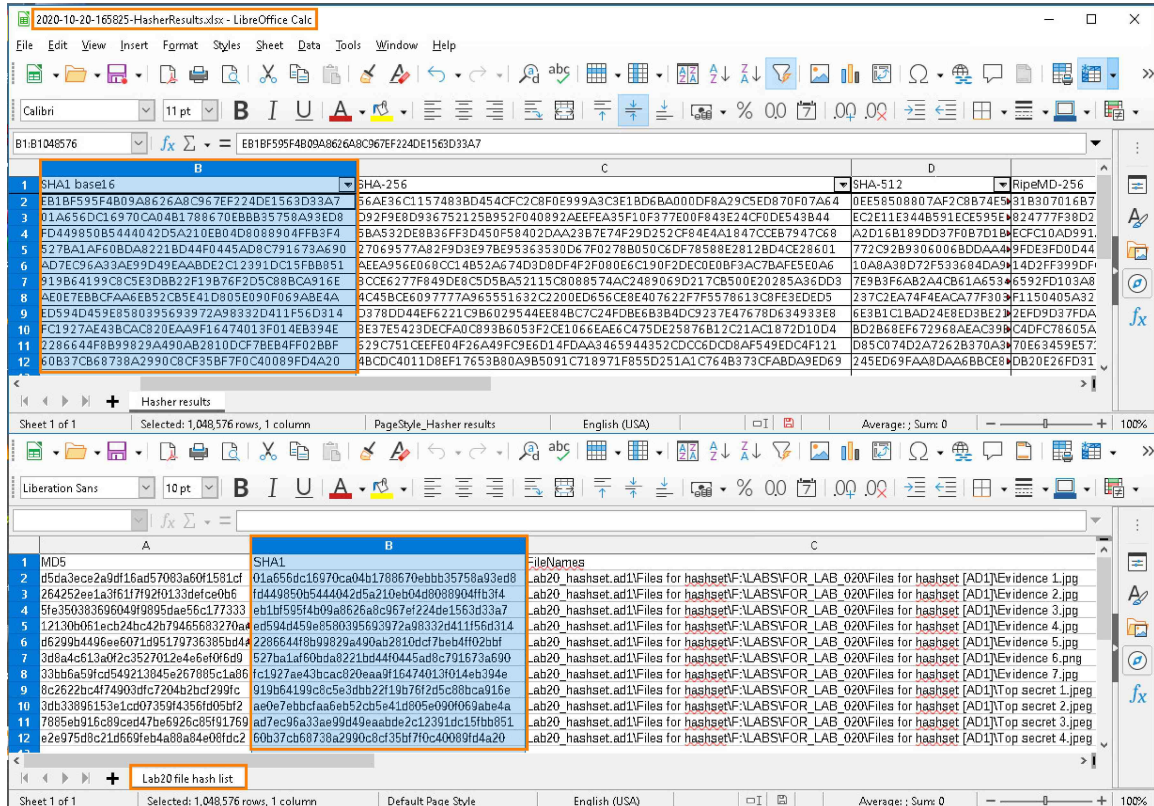
9. Now minimize Hasher as seen in item 1 and open File Explorer. In File Explorer, navigate to ThisPC > Evidence Repository (E:) > FOR_LAB_020 > File Hash List as seen in items 2, 3, 4, and 5 below.



10. Once there, right-click the file called *-HasherResults.xlsx, select open with..., LibreOffice, and then click OK as seen in items 1, 2, 3, and 4 below.



11. When the file opens, you will see the similar columns and row structure that you saw in the previous file hash list. Compare the results from this output and the ones that you did using FTK Imager.



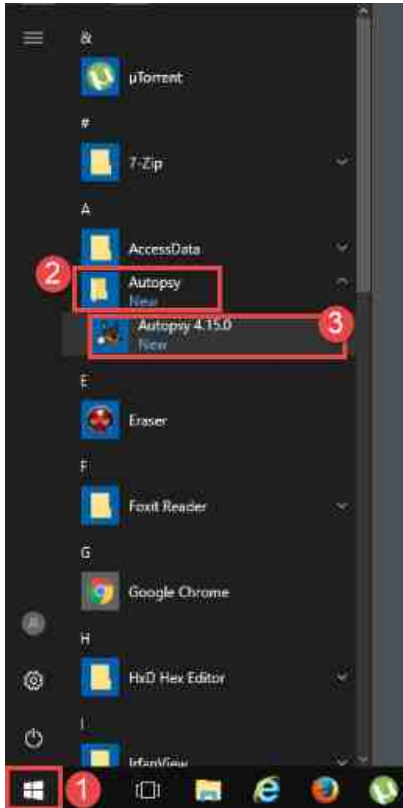
The screenshot shows two sheets of data in LibreOffice Calc. The top sheet, titled "Hasher results", has columns for SHA1, SHA-256, SHA-512, and RipeMD-256. The bottom sheet, titled "Lab20 file hash list", has columns for MD5, SHA1, and FileNames. Both sheets contain a list of file hashes and their corresponding file names.

MD5	SHA1	FileNames
d5da3ece2a9df16ad57083a60f1581cf	01a656dc16970ca04b1788670ebbb35758a03ed8	ab20_hashset.ad1Files for hashsetF:\LABS\FOR_LAB_020Files for hashset
264252e1a3f1617f92f0133defce0b6	fd449850b5444042d5a210eb04d8098904fb3f4	ab20_hashset.ad1Files for hashsetF:\LABS\FOR_LAB_020Files for hashset
5fe350383696049f9895dae56c177333	eb1bf595f4b09a626a8c967ef224de1563d33a7	ab20_hashset.ad1Files for hashsetF:\LABS\FOR_LAB_020Files for hashset
12130b061ecb24bc42b79465683270a4	ed594d459e8580395693972a98332d411f5bd31a	ab20_hashset.ad1Files for hashsetF:\LABS\FOR_LAB_020Files for hashset
6d290b4496ee6071d95179736385bd44	2286644f8b99829a490ab2810dcf7beb4f02dbf	ab20_hashset.ad1Files for hashsetF:\LABS\FOR_LAB_020Files for hashset
3d8a4c613a0f2c3527012e4e6e0f6d0	527ba1af60bda8221bd44f0445ad8c71673a690	ab20_hashset.ad1Files for hashsetF:\LABS\FOR_LAB_020Files for hashset
33bb6a59fcd549213845e267885c1a06	fc1927ae43bcac820eaa9f16474013f014eb394e	ab20_hashset.ad1Files for hashsetF:\LABS\FOR_LAB_020Files for hashset
8c2622bc4f74903dfc7204b2bdcf299fc	919b64199c8c5e3dbb22f19b76f2d5c88bca916e	ab20_hashset.ad1Files for hashsetF:\LABS\FOR_LAB_020Files for hashset
3db33896153e1cd0f7359f4356fd05bf2	ae0e7ebcfcaae5eb52cb5e41d805e09069ab4e4a	ab20_hashset.ad1Files for hashsetF:\LABS\FOR_LAB_020Files for hashset
17885eb916c8ced47be6926c85f91769	ad7ec96a33ae99d49eaabde2c12391dc15fbb851	ab20_hashset.ad1Files for hashsetF:\LABS\FOR_LAB_020Files for hashset
e2e975dc821d669feb4a88a8a0e0fde2	60b37cb68738a2990c8cf35bf70c40089fd4a20	ab20_hashset.ad1Files for hashsetF:\LABS\FOR_LAB_020Files for hashset

12. Once you are done, we will move on to creating and using hash sets.

3 Creating and Using a Hash Set

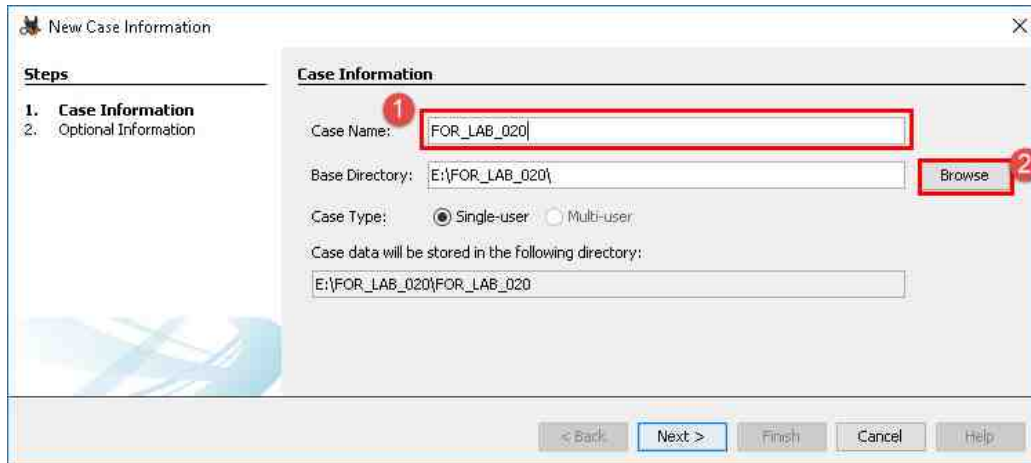
1. In this exercise, we are going to use Autopsy to create a hash set using the files we worked with in the previous exercises. To begin, launch the Autopsy program from the windows menu by navigating to Start Menu > Autopsy > Autopsy 4.15.0. Alternatively, you can open Autopsy from the Desktop by clicking the icon called Autopsy 4.15.0.



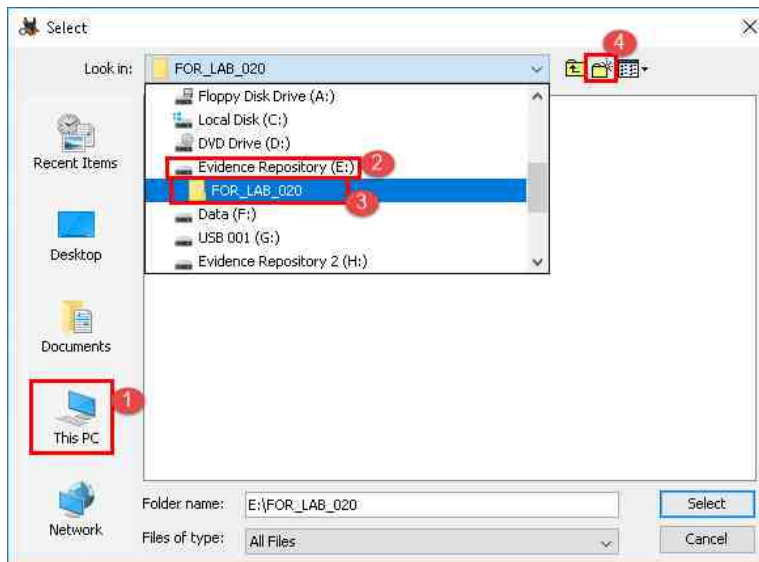
2. The Welcome screen will appear; click the New Case option as highlighted below. This will open the New Case Information window.



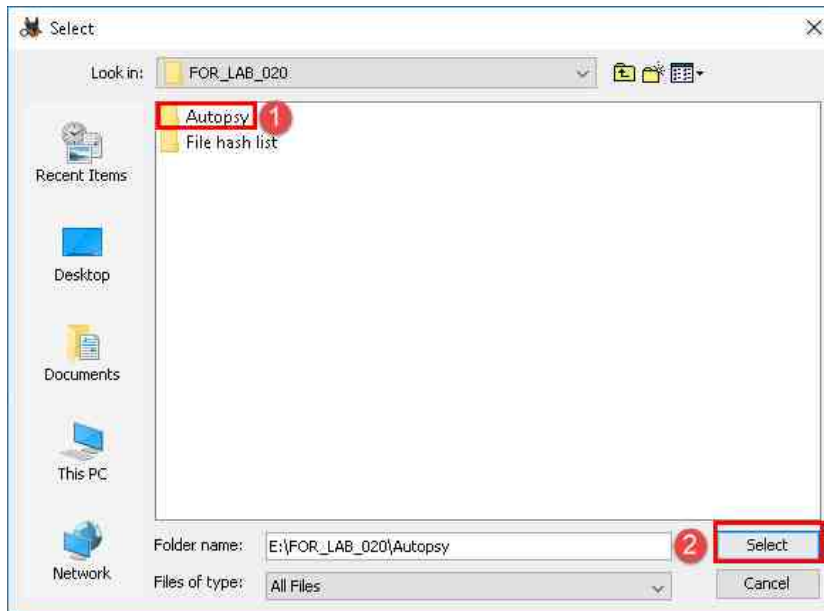
3. In the New Case Information window, enter FOR_LAB_020 in the Case Name field. The Base Directory field is used to choose the location of the case folder. Click Browse to select a location for the case, as seen in item 2.



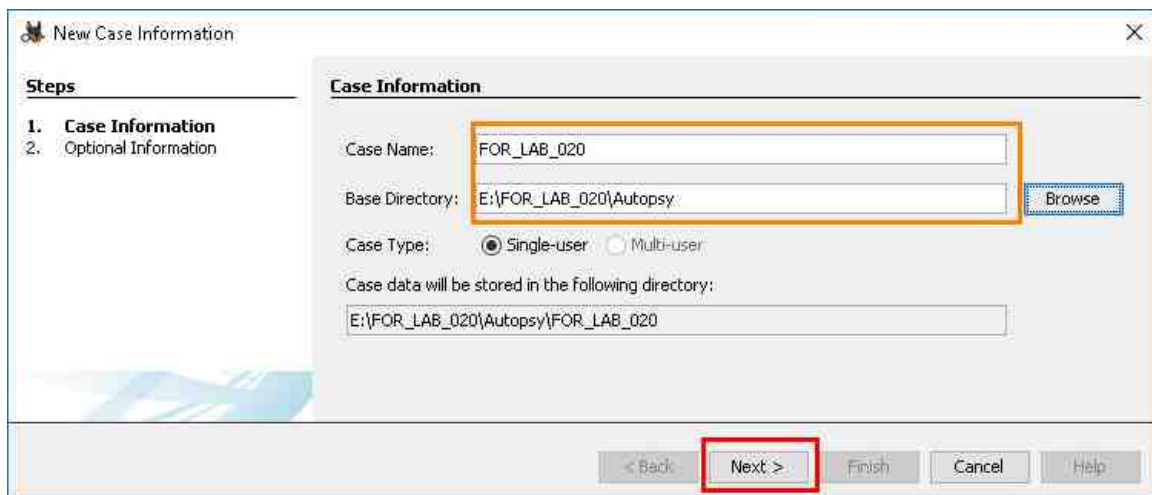
4. The Select window will appear. Navigate to This PC > Evidence Repository (E:) > FOR_LAB_020 as seen in items 1, 2, and 3. Once there, click the Create New Folder icon to create a new folder, as seen in item 4.



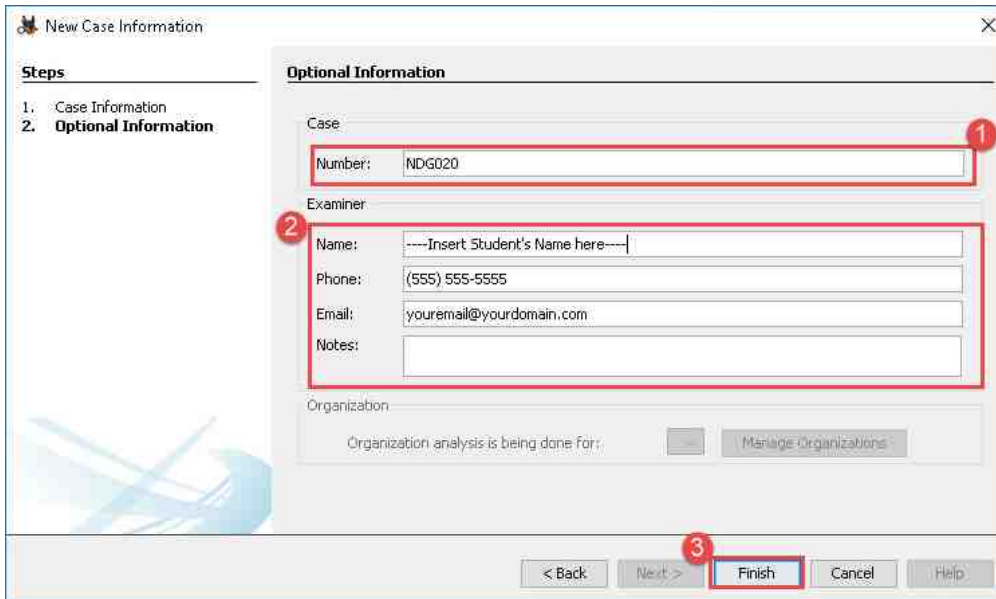
- Next, name the folder Autopsy as seen in item 1, then click Select as seen in item 2 below to use this folder as the case directory.



- You will be taken back to the Case Information window. Verify that all the paths and names are correct, and then click Next as highlighted below.



7. 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.

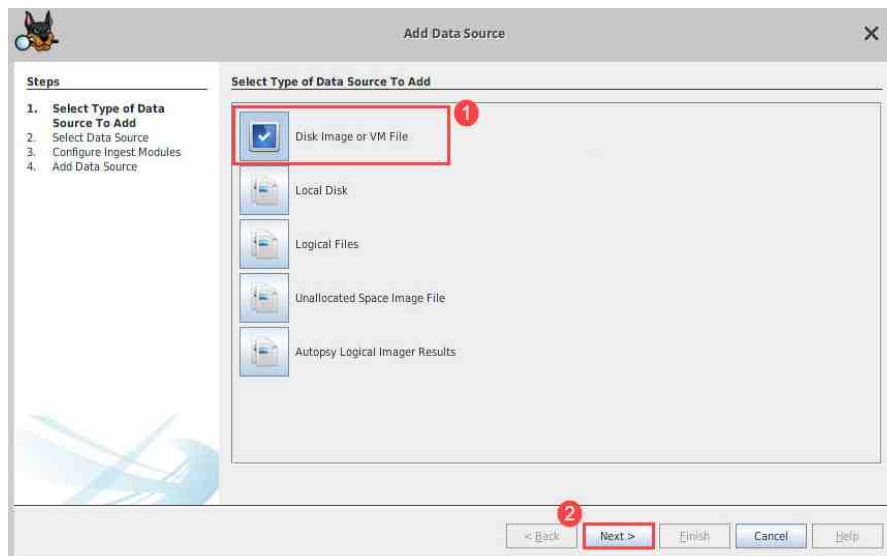


The screenshot shows the 'New Case Information' window with the 'Optional Information' tab selected. The 'Steps' pane on the left shows '1. Case Information' and '2. Optional Information'. The main area contains the following fields:

- Case:** Number: NDG020 (highlighted with a red box and a red circle with the number 1).
- Examiner:** Name: ----Insert Student's Name here---- (highlighted with a red box and a red circle with the number 2). Other fields include Phone: (555) 555-5555, Email: youremail@yourdomain.com, and Notes: (empty).
- Organization:** Organization analysis is being done for: (empty) and Manage Organizations (button).

At the bottom, there are buttons: < Back, Next >, Finish (highlighted with a red box and a red circle with the number 3), Cancel, and Help.

8. 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.

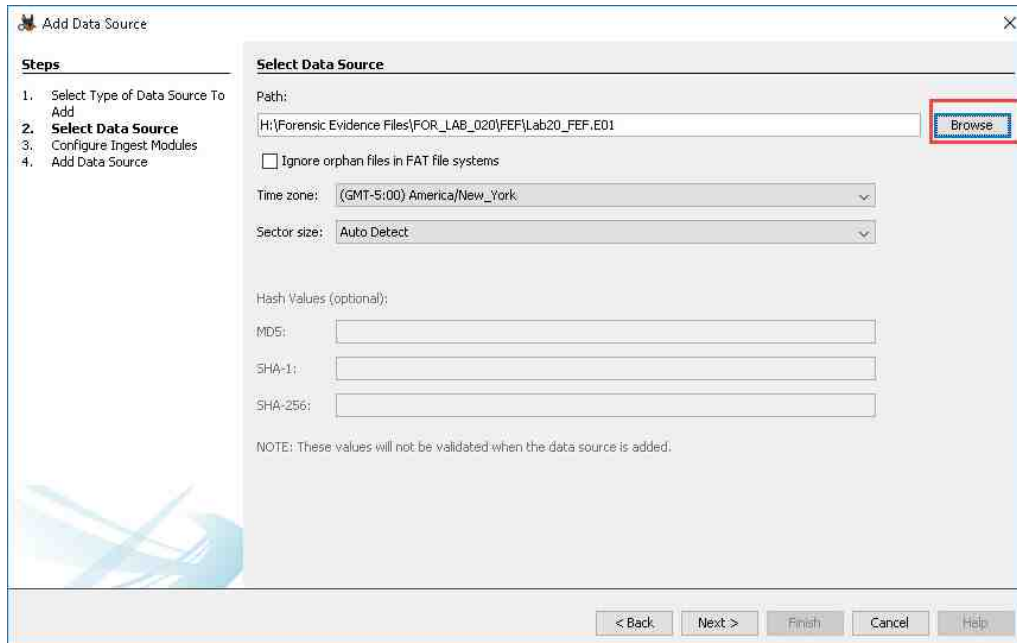


The screenshot shows the 'Add Data Source' window. The 'Steps' pane on the left shows '1. Select Type of Data Source To Add', '2. Select Data Source', '3. Configure Ingest Modules', and '4. Add Data Source'. The main area is titled 'Select Type of Data Source To Add' and contains a list of options:

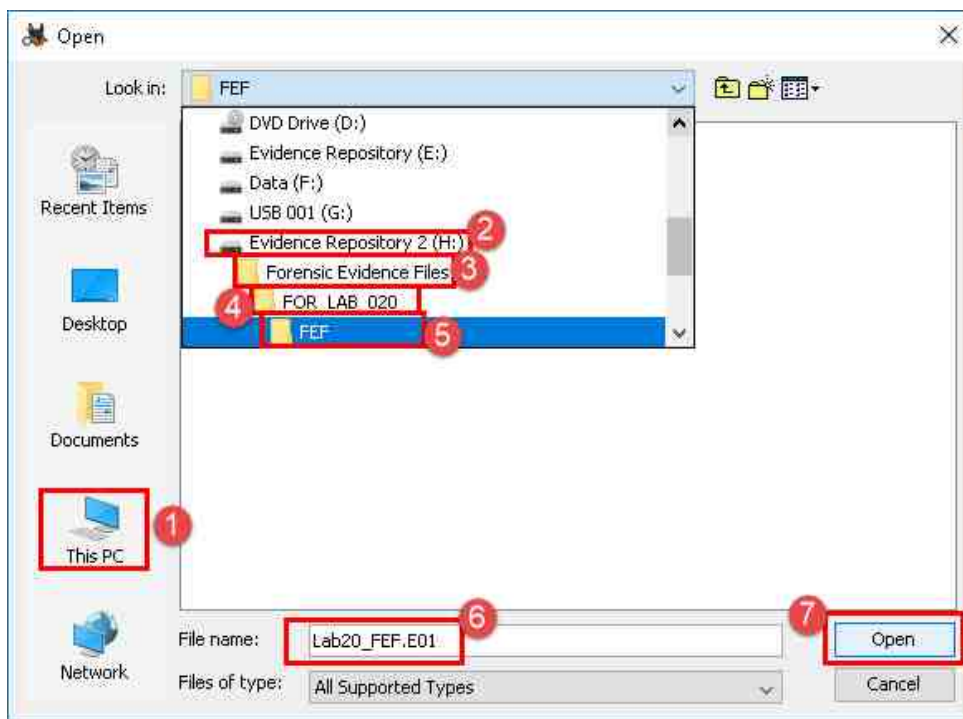
- ☒ Disk Image or VM File (highlighted with a red box and a red circle with the number 1)
- ☐ Local Disk
- ☐ Logical Files
- ☐ Unallocated Space Image File
- ☐ Autopsy Logical Imager Results

At the bottom, there are buttons: < Back, Next > (highlighted with a red box and a red circle with the number 2), Finish, Cancel, and Help.

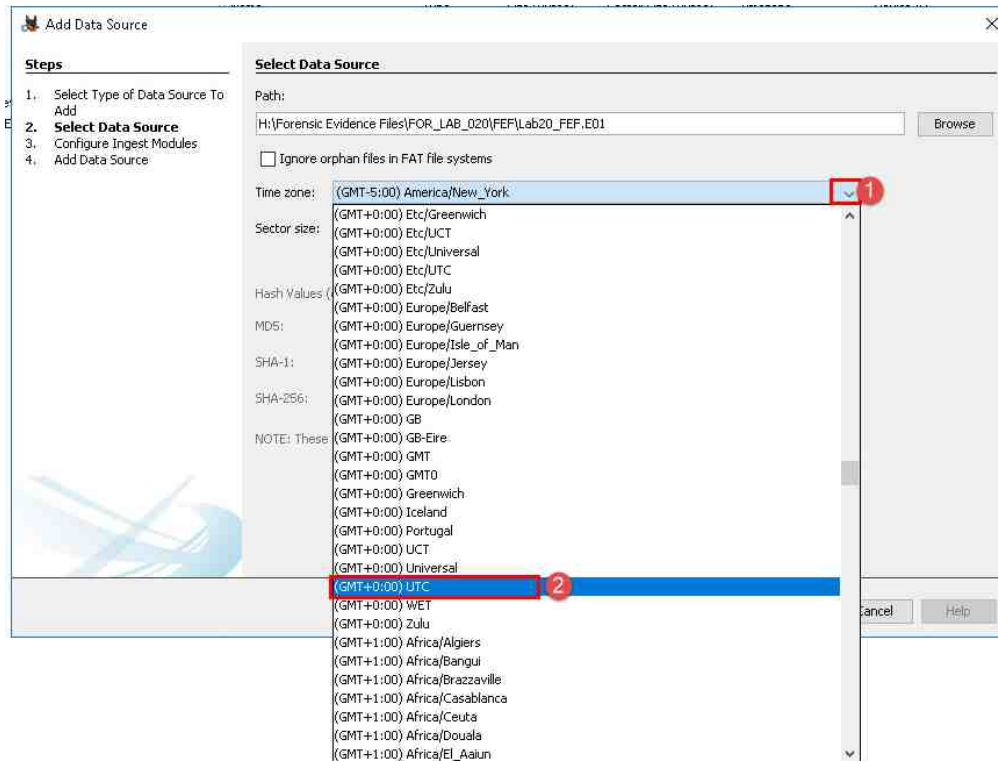
9. The next window will allow you to choose the image you want to add to the case. Click the Browse button highlighted below to open the Open window that allows you to browse for the FEF.



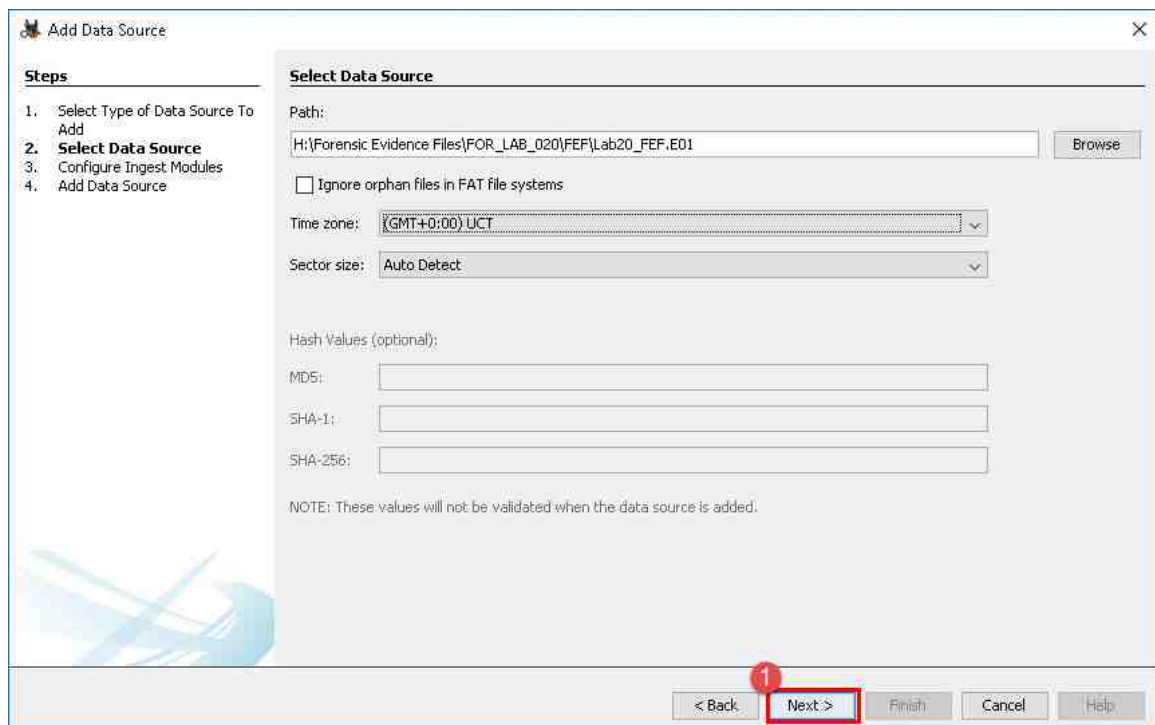
10. In the Open window, browse to ThisPC > Evidence Repository 2 (H:) > Forensic Evidence Files > FOR_LAB_020 > FEF and click the file called Lab20_FEF.E01 and then click Open as highlighted in steps 1 – 7 below.



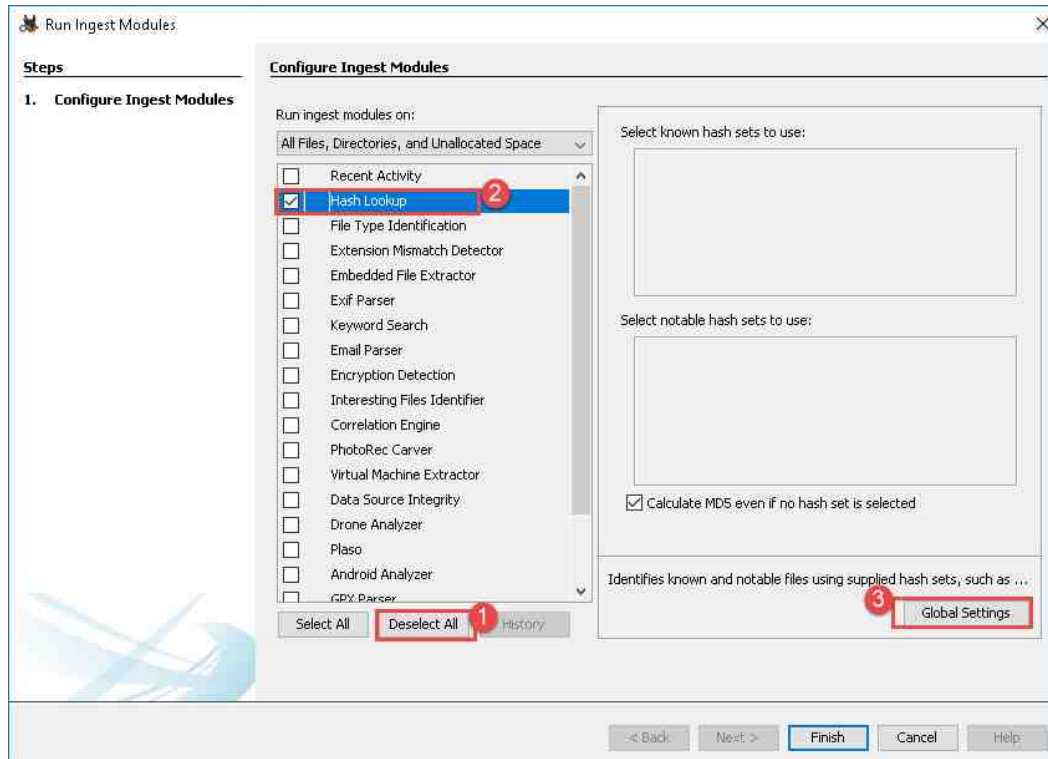
11. The image path will now appear in the Path field highlighted as item 1 below. Next, change the Time Zone to (GMT+0:00) UTC from the dropdown menu as seen in item 2.



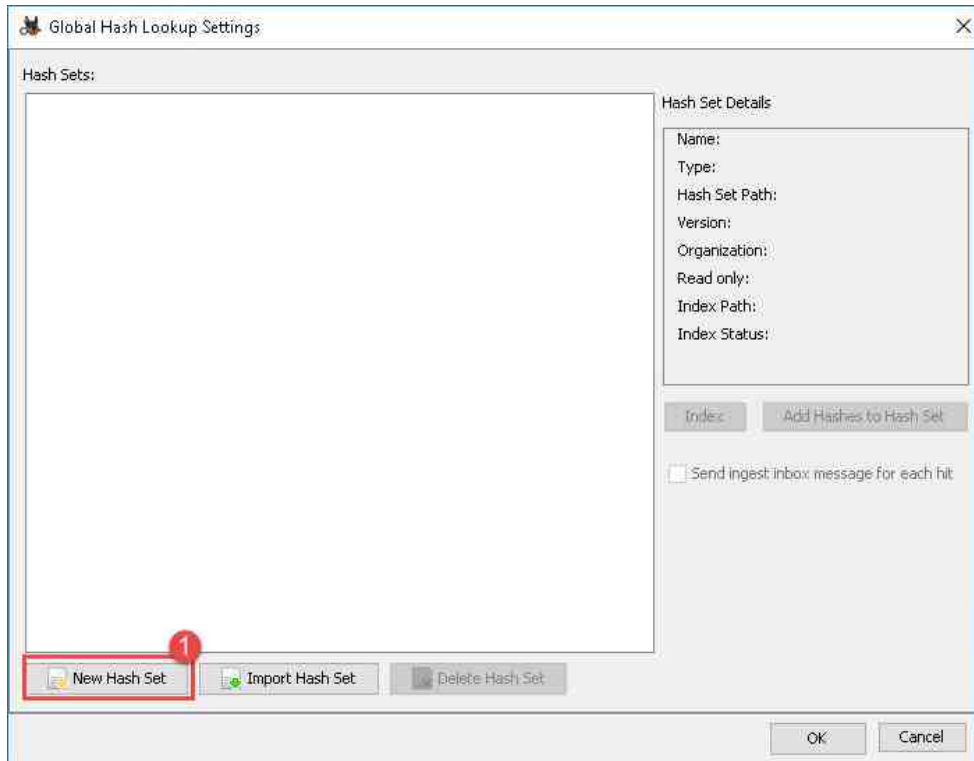
12. We will leave the other options as-is for now and click Next highlighted as item 1 below.



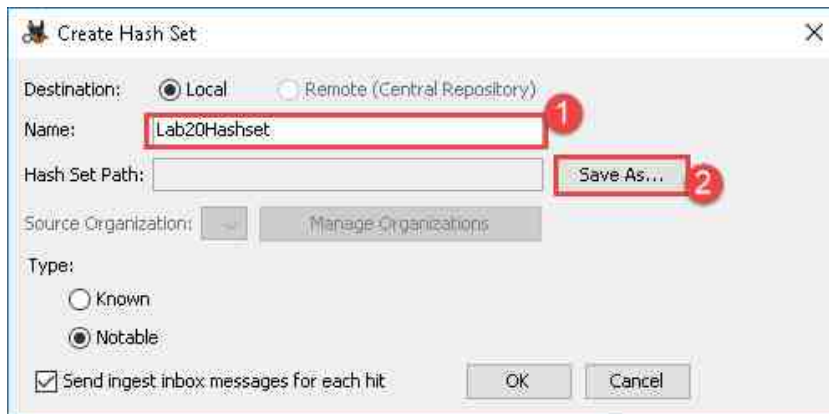
13. You will be taken to the Configure Ingest Modules step of the case creation process. We will be using the Hash Lookup Ingest Module in this exercise, so uncheck any selected Ingest Module by clicking the Deselect All button and then click the checkbox beside Hash Lookup as seen in items 1 and 2 below. This Ingest Module requires some setup so let us click the Global Settings option seen in item 3 below.



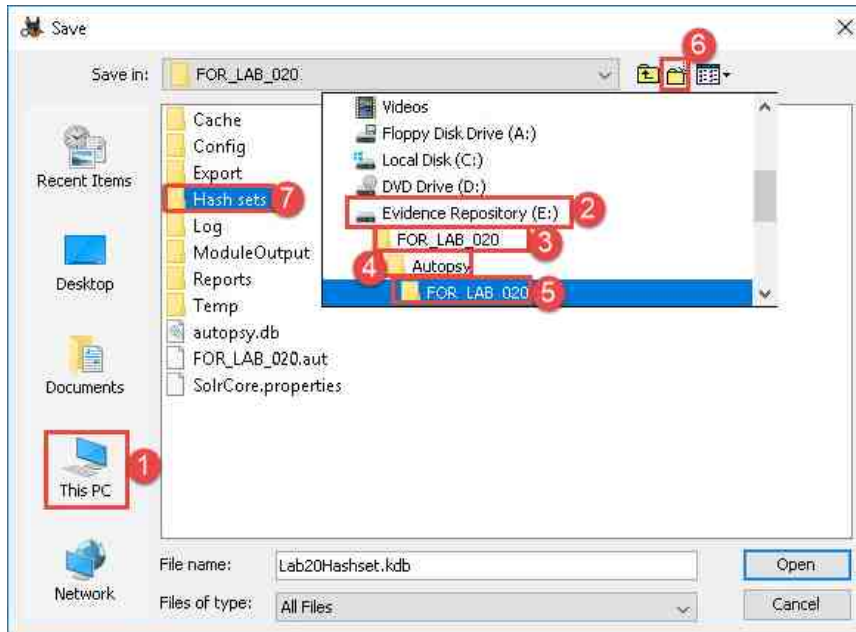
14. The Global Hash Lookup Settings window will appear. This window lists all the hash sets that are added to Autopsy. Click New Hash Set as seen in item 1 to create a new one.



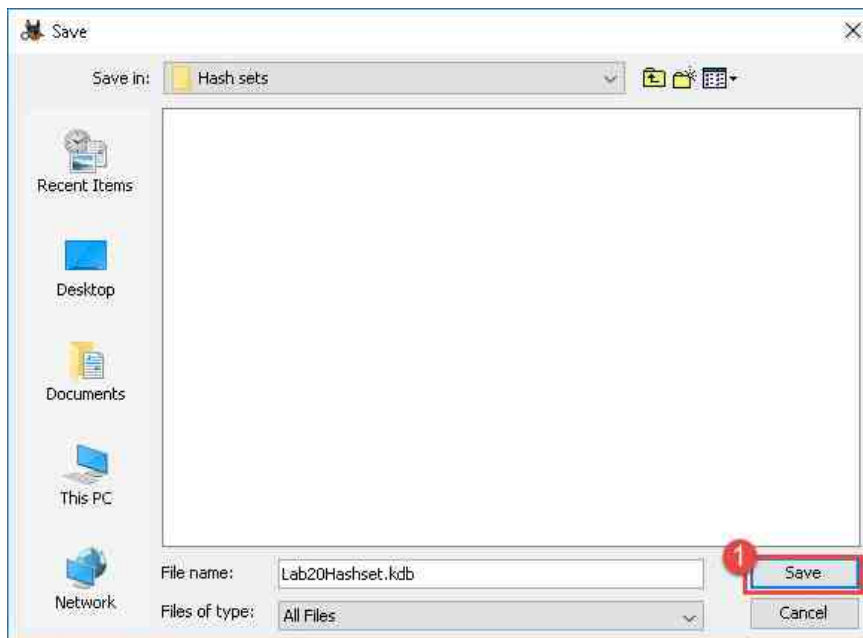
15. The Create Hash Set window will appear. In the Name field, type Lab20Hashset as seen in item 1. Next, we need to choose a location to store the hash set. To do this, click Save As seen in item 2 below.



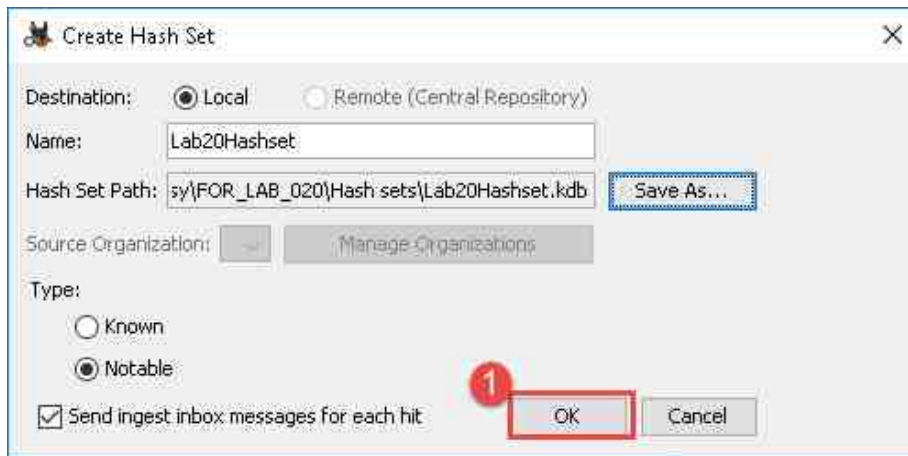
16. The Save window will appear. Navigate to ThisPC > Evidence Repository (E:) > FOR_LAB_020 > Autopsy > FOR_LAB_020 and then click the Create New Folder icon as seen in items 1,2,3,4,5, and 6 below. Name this folder Hash sets as seen in item 7.



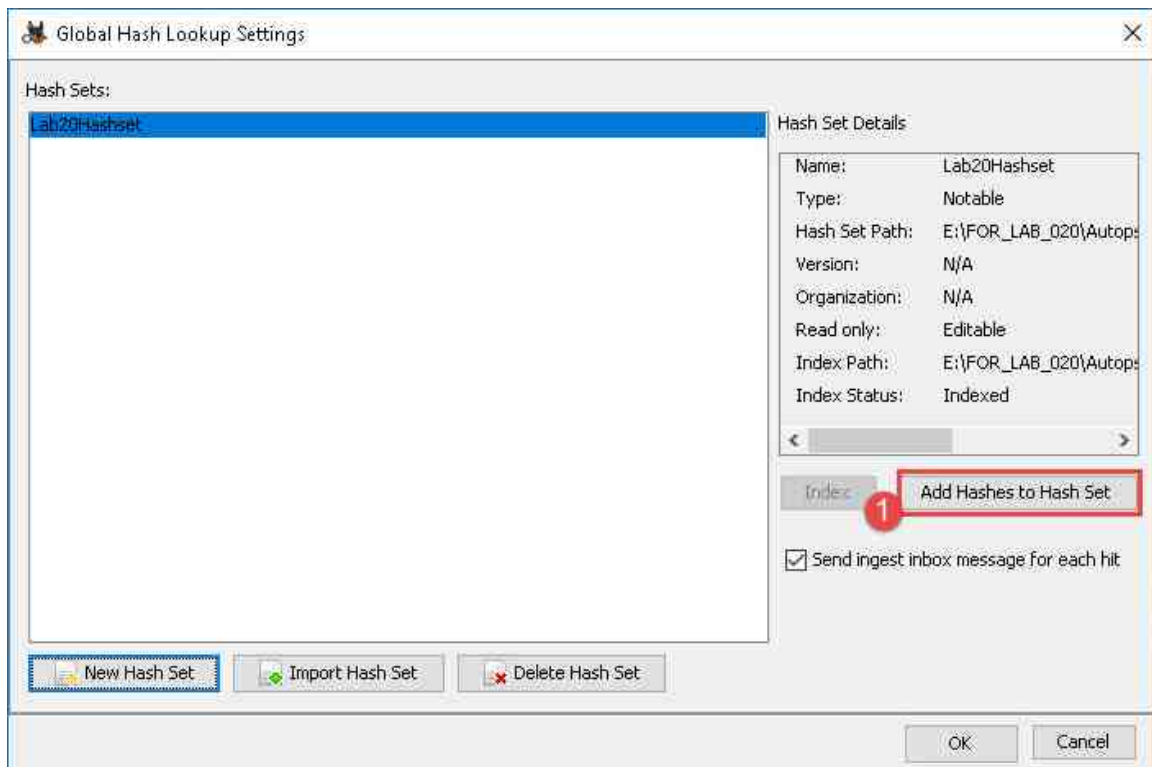
17. Double-click the folder you created called Hash sets to open it, and then click Save as seen in item 1.



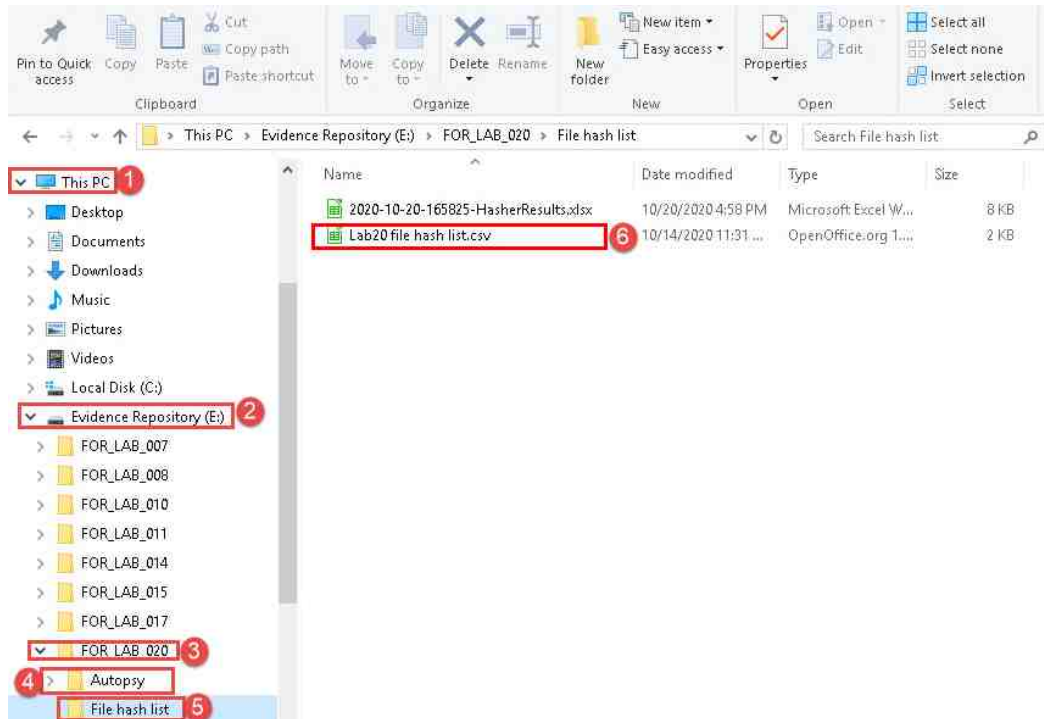
18. You will now be back at the Create Hash Set window. The other options, Known or Notable define what type of hashes this set contains. Known files are ignorable files, while Notable files are files of interest. Let us leave this as Notable and click OK as seen in item 1 below.



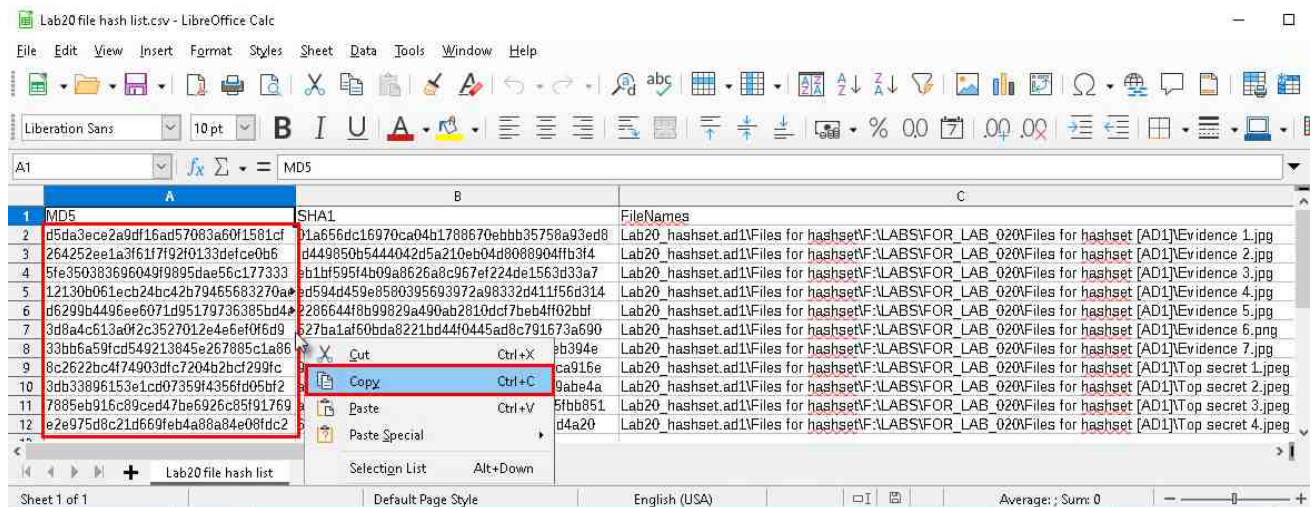
19. Now you will be taken back to the Global Hash Lookup Settings window. Click Add Hashes to Hash Set as seen in item 1 to open a new window that allows us to add the hashes.



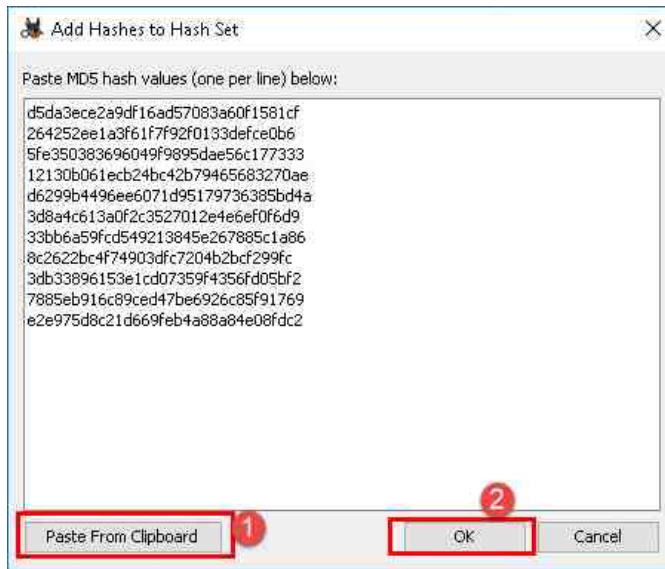
20. The Add Hashes to Hash Set window will appear. It is a simple window that requests MD5 hashes to be added, one per line. Let us add the hashes from one of the lists you created earlier. To do this, open Windows File Explorer and navigate to ThisPC > Evidence Repository (E:) > FOR_LAB_020 > File Hash List and open Lab20 file hash list by double-clicking it.



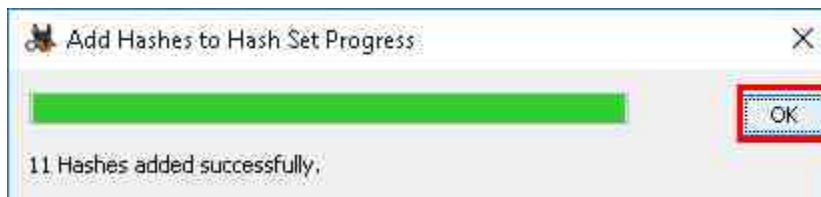
21. Next, highlight all the MD5 hashes, right-click on them and select Copy from the context menu as seen in items 1, 2, and 3 below.



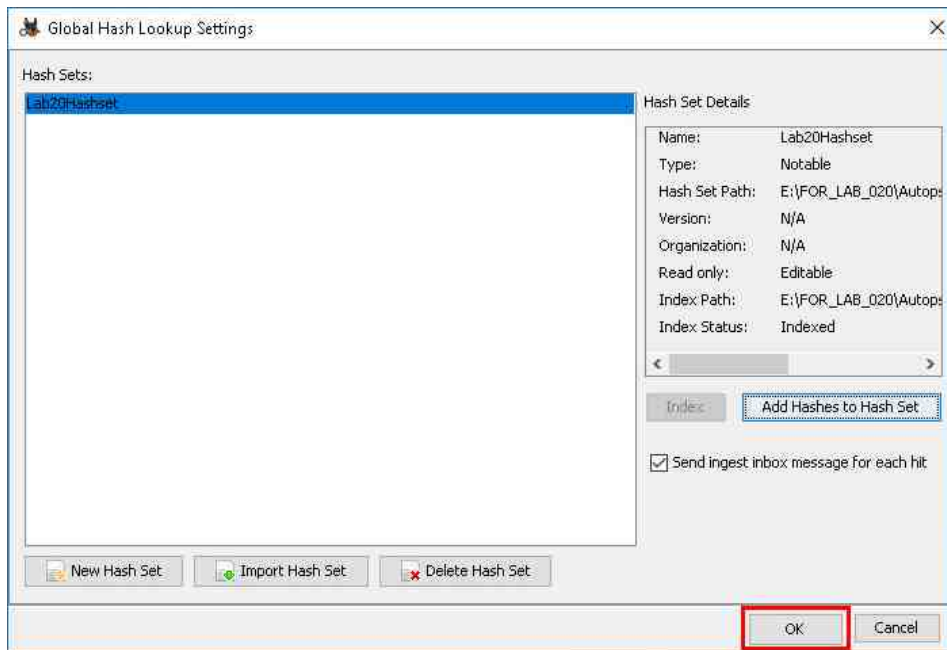
22. Now return to the Add Hashes to Hash Set window and click the Paste From Clipboard button and then click OK as seen in items 1 and 2 below.



23. The Add Hashes to Hash Set Progress window will appear. Click OK.



24. The hash set is now created with the files we saw in the Files for Hasher folder and the Lab20_hashset.ad1 evidence file. If any copies of the hashed file exist on this FEF, the hash set will identify them. Click OK, as seen in item 1, to go back to the Configure Ingest Module window.



25. In the Configure Ingest Module window, double-check your options to make sure they match the ones in the screenshot below, then click Next and then click Finish in the final window as highlighted below.

