FORENSICS V2 LAB SERIES

Lab 08: Metadata and Link File Analysis

Document Version: 2021-01-14

Contents

Introduction

In digital forensics, corroborative evidence that indicates that a file was accessed is just as important as the file itself. This module focuses on helping you understand what link files are, the different types, and how to extract valuable data from them.

Objectives

- Learn the difference between file system metadata and embedded metadata
- Understand what data link files store and how to extract them
- Learn how to use link file metadata to determine if files were executed and where they were stored

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$

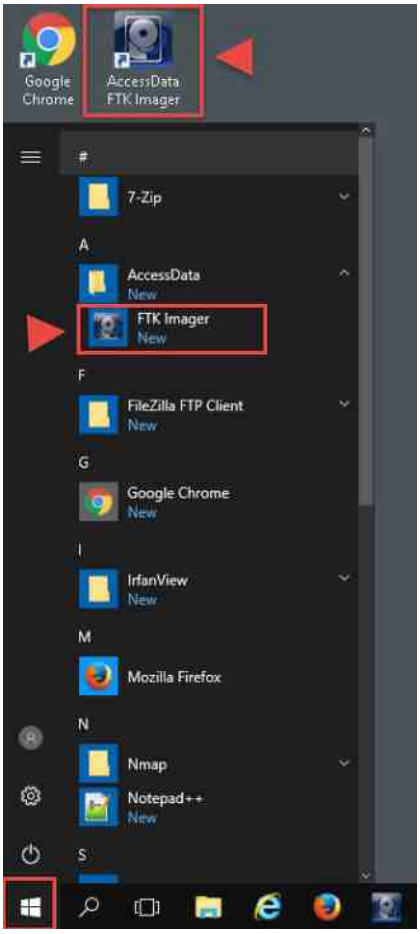
1 Exporting and Analyzing Link Files

Metadata is one of the most delicate but useful pieces of forensic artifact out there. Digital devices constantly record and update data about files, and this data, in turn, can provide information on how a file was created, last modified, and accessed, which drive a file was opened from, and the date and time the file was originally created. Some files have more metadata than others, but all files on a file system will have a record of when they were first placed on the volume, last modified, and possibly last accessed. In this exercise, we will first export and look at some metadata that can be derived from a link (LNK/shortcut) file.

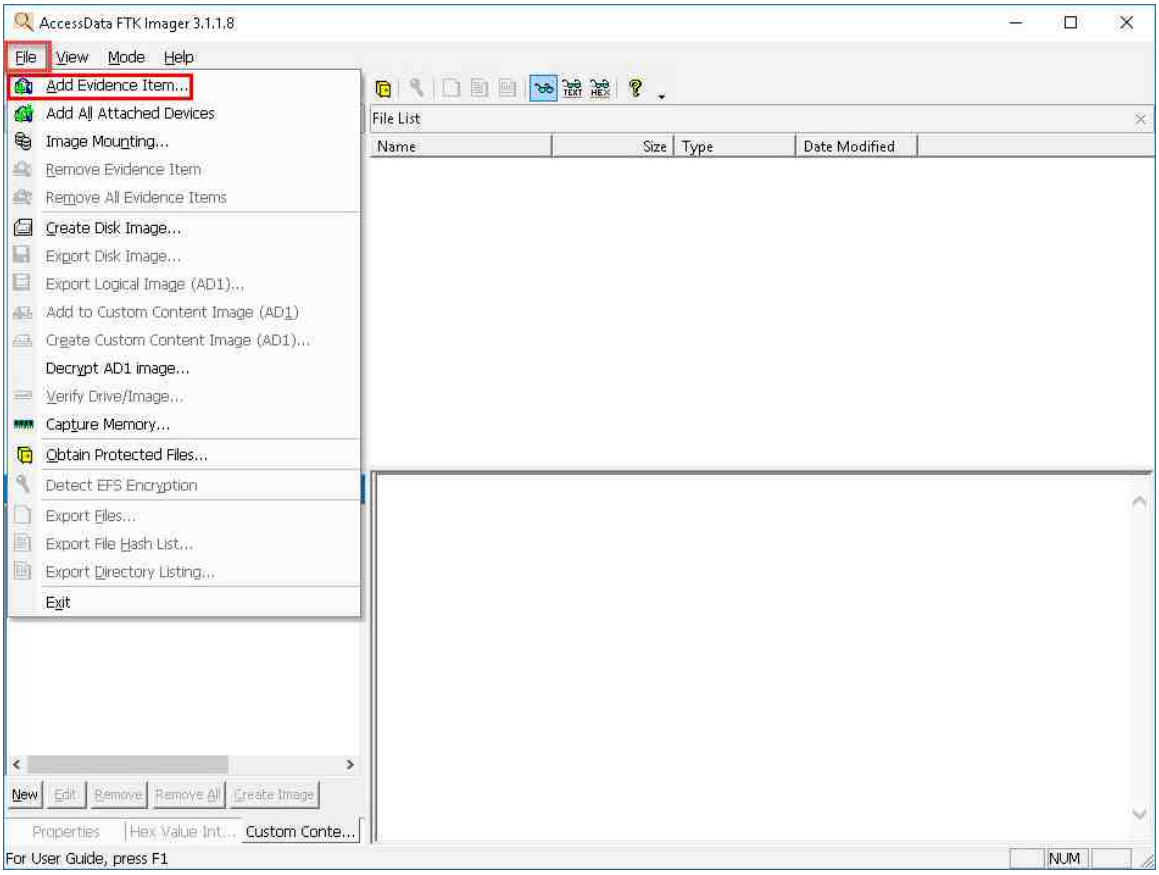
1. To begin, launch the WinOS virtual machine to access the graphical login screen.
   a. Select Send CTRL+ALT+DEL from the dropdown menu to be prompted with the login screen.

   b. Log in as `Administrator` using the password: `Train1ng$`

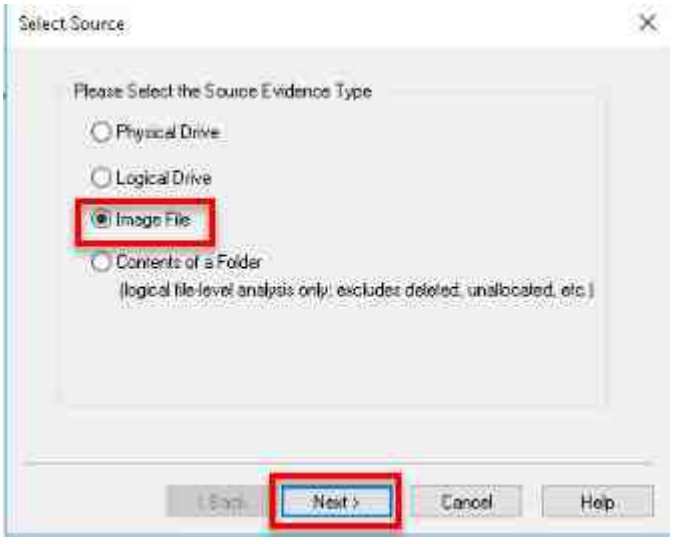
2. Once you are logged into the VM, launch the FTK Imager program from the windows menu by navigating to Start Menu > AccessData > FTK Imager. Alternatively, you can open FTK Imager from the Desktop by clicking the icon called AccessData FTK Imager:



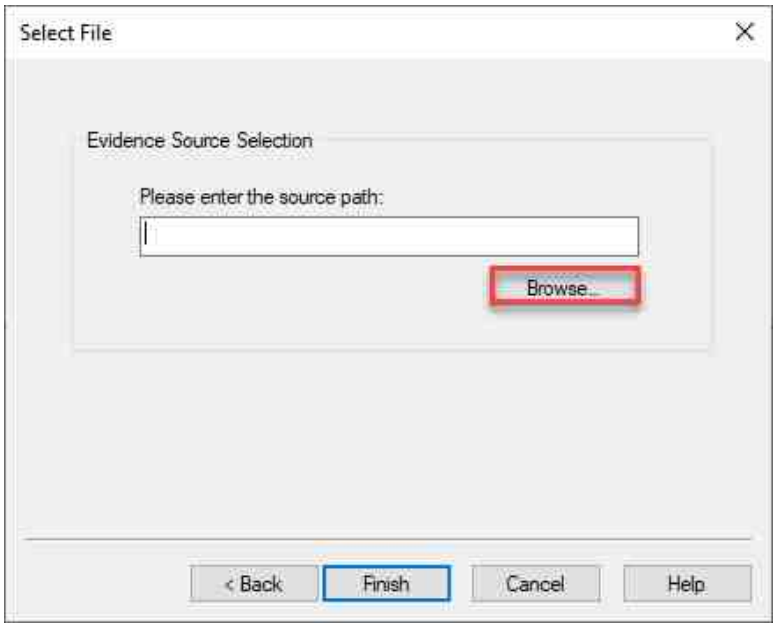
3. You should already be familiar with FTK Imager from our previous labs. In this exercise, we will learn how to navigate to the registry files' locations using some preconfigured Forensic Evidence Files (FEF). Let us begin by loading an FEF. To do this, click the File menu option to open the File dropdown menu, then click the Add Evidence Item option from the dropdown menu. It is the first item on the menu, as highlighted below.



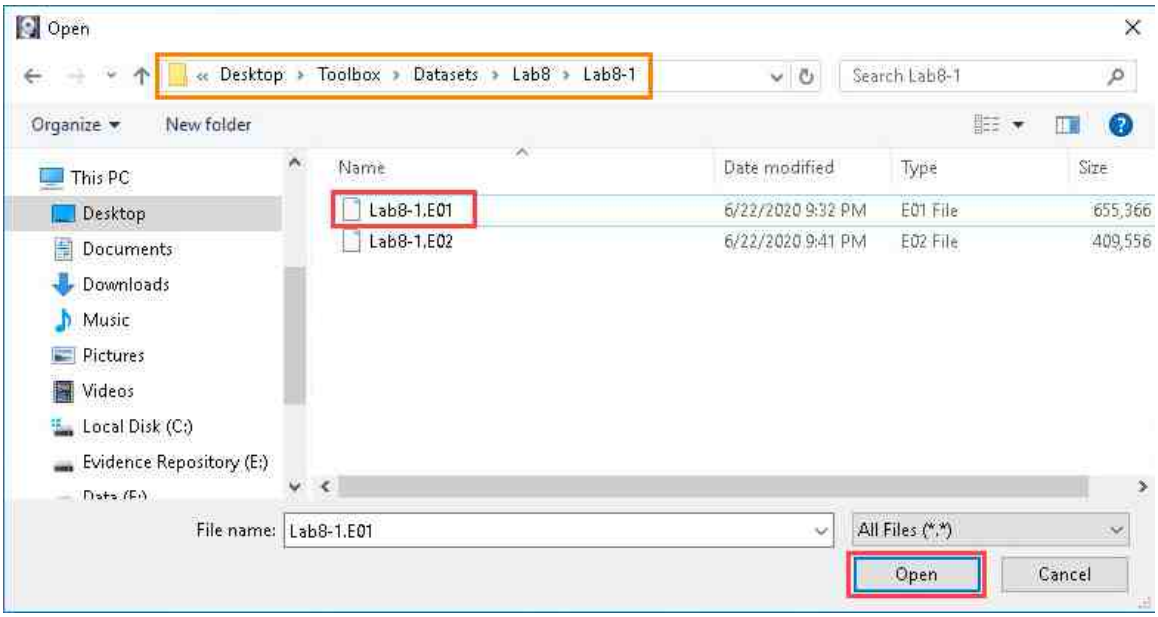
4. You will be brought to the Select Source window. Let us select Image File and click Next as highlighted below.



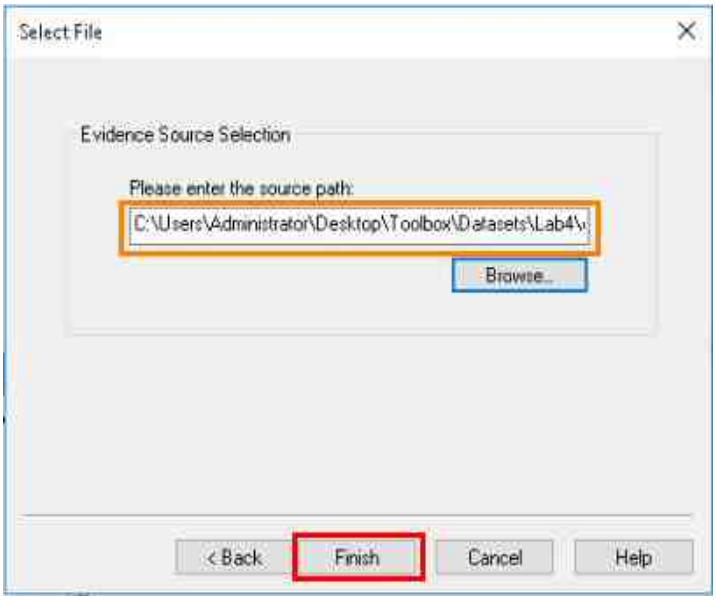
5. In the Select File window, click Browse, highlighted in red in the screenshot below. This will open the Open window, which will allow you to browse to the appropriate FEF.



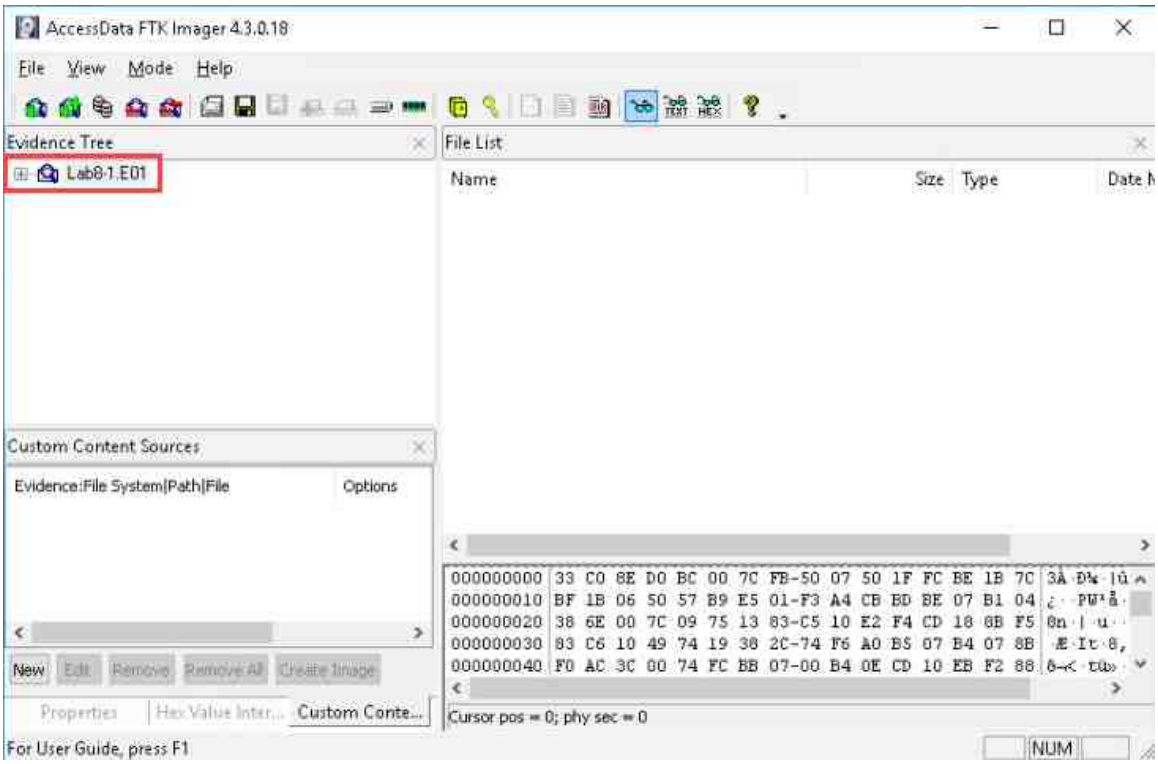
6. You are now at the Open window. Browse to This PC > Desktop Toolbox > Datasets > Lab8 and double-click the folder called Lab8-1. This will open the folder revealing the FEF called Lab8-1.E01. Select the file called Lab8-1.E01 and click the Open button as highlighted below.



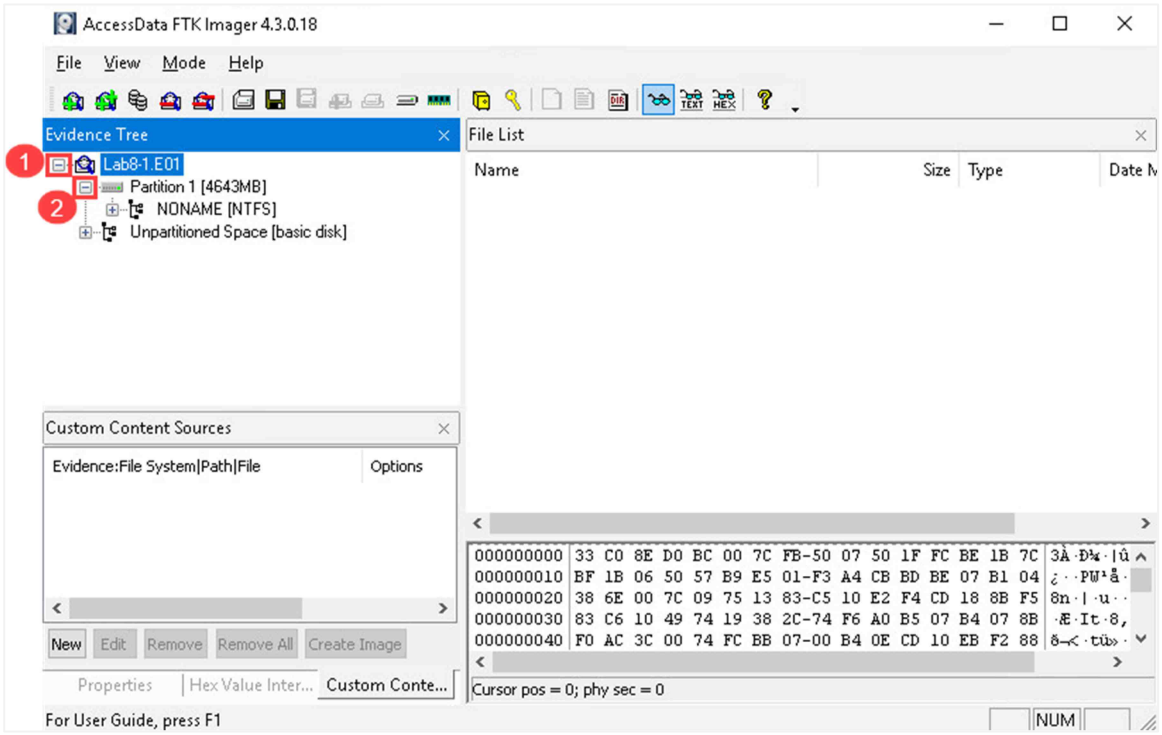
7. Review the source path of the file called Lab8-1.E01. In the Select File window, click Finish, highlighted in red in the screenshot below. This will take you back to FTK Imager's main window.



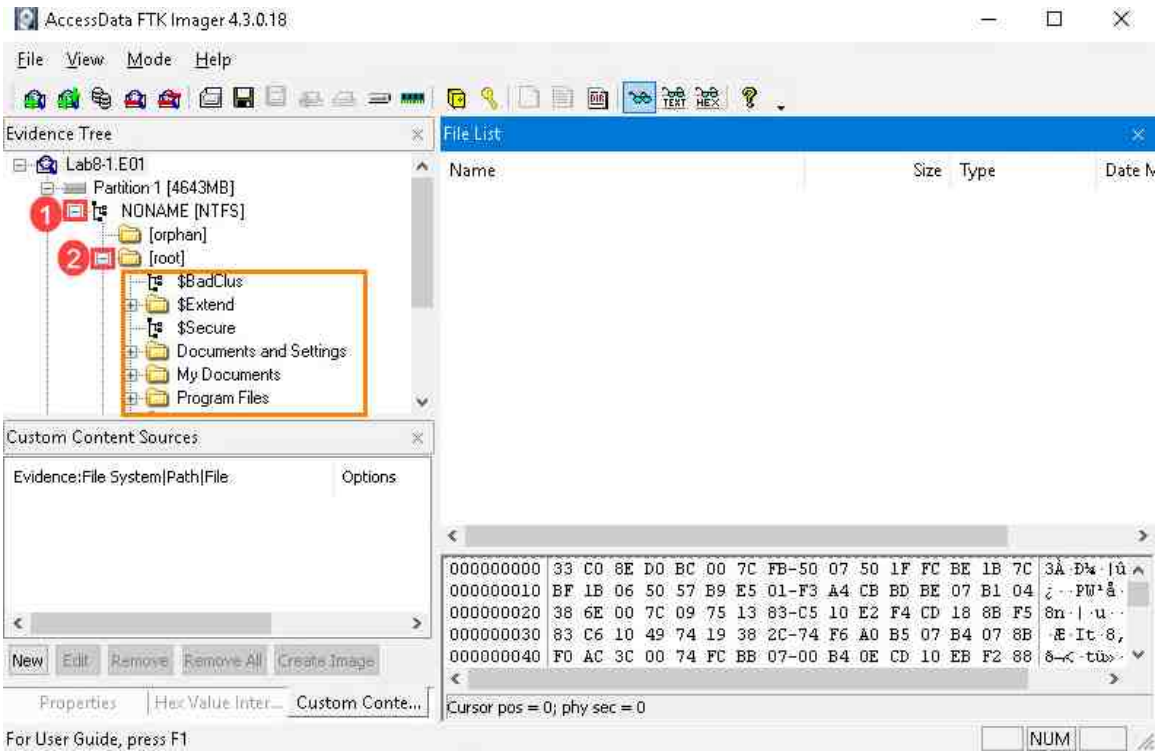
8. If you did everything correctly, you will now be back at FTK Imager's main window with Lab8-1.E01 listed under the Evidence Tree pane. From the Evidence Tree pane, click the tree item Lab8-1.E01 highlighted below. This will select the image you are going to peruse.



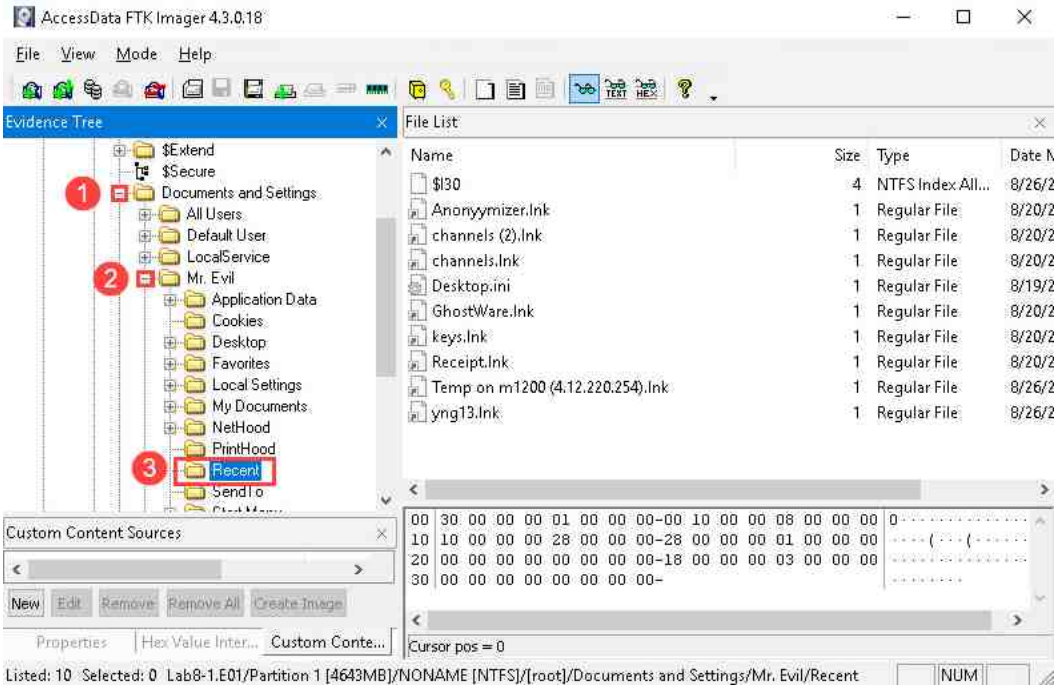
9. We will now browse the FEF and view its contents. To begin, click the + sign beside the hard drive you added called Lab8-1.E01, as seen in item 1 below. This will expand the tree and display the partition on the drive. Now that you can see the partition, let us learn how to identify the recent files shortcut folder for the main user on this computer. Begin by clicking the + sign beside Partition 1 [4643MB], as seen in item 2 below.



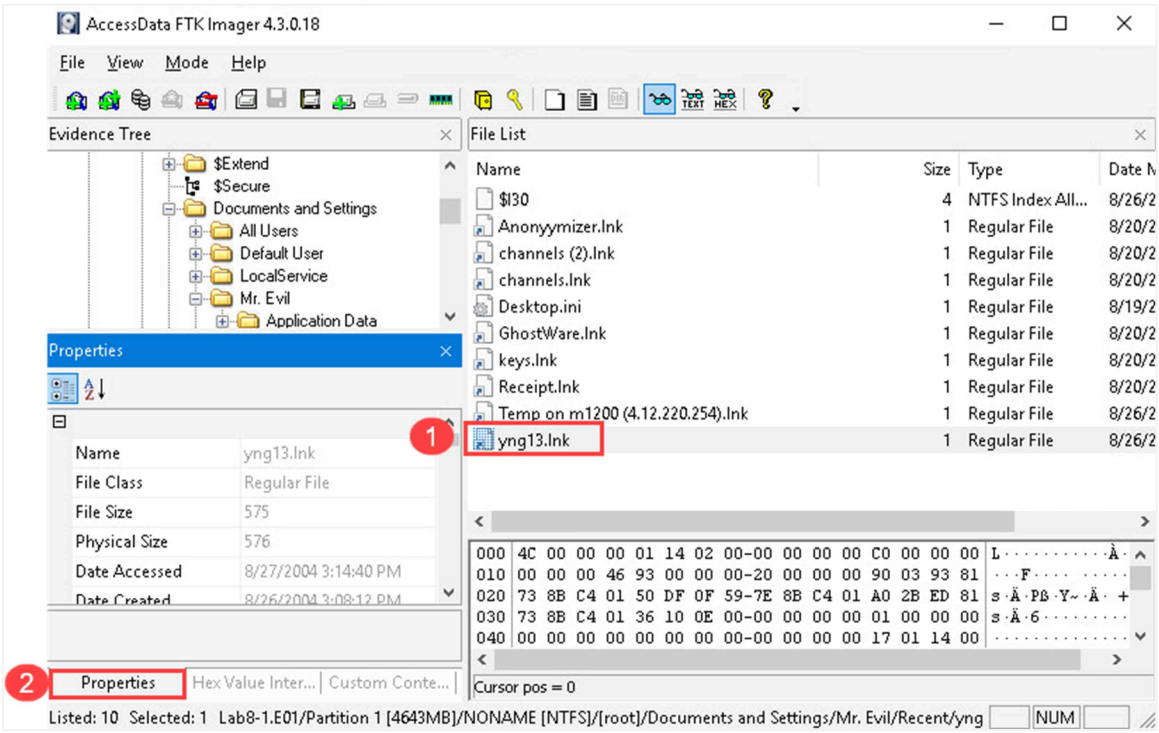
10. You will now see the file system that is being used on the partition. Let us expand the partition by clicking the + beside NONAME [NTFS] as seen in item 1 below. This will reveal three folders; let us expand the folder called root by clicking the + sign beside it, as seen in item 2 below.



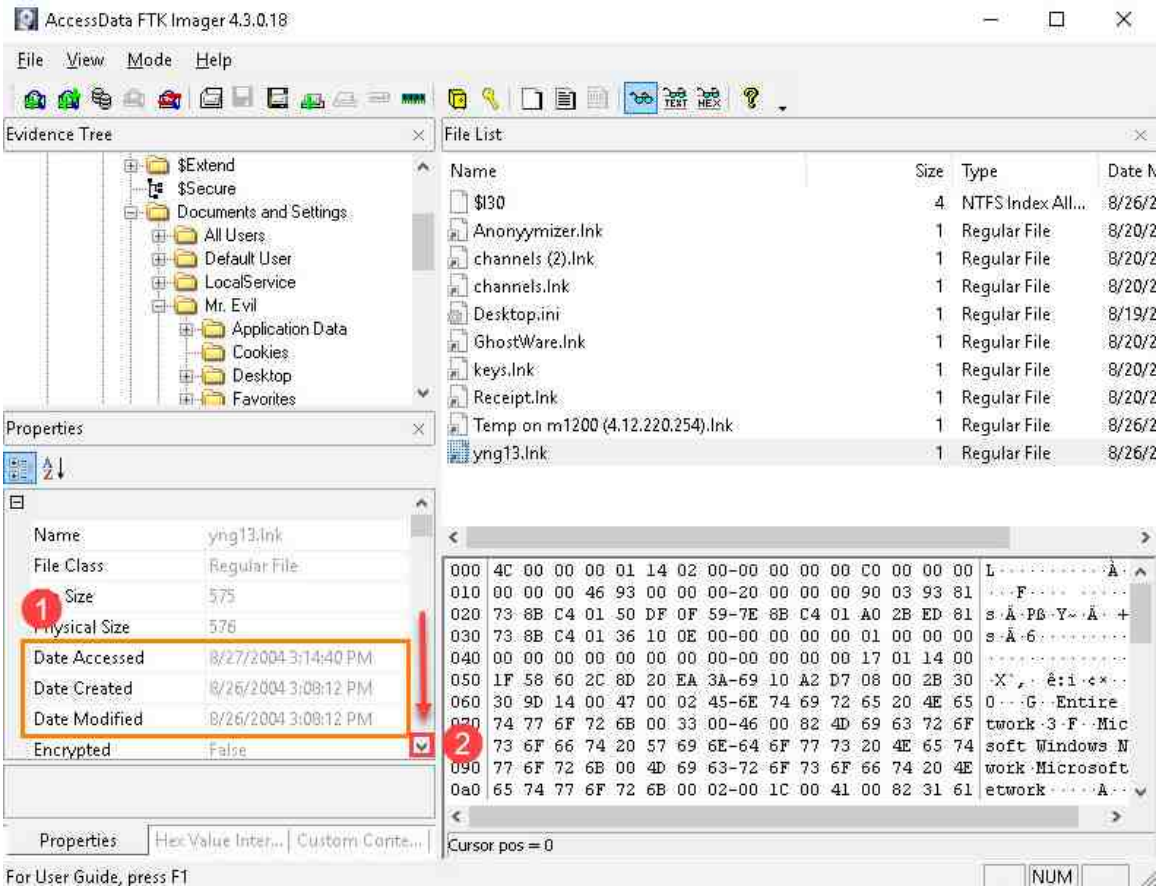
11. As we learned in the previous labs, the user folders for Microsoft Windows can be found in the root folder under the name Documents and Settings (Windows XP and earlier) or Users (Windows Vista and later). Let us head to the Recent folder for the user called Mr. Evil located at Documents and Settings > Mr. Evil > Recent. Do this by clicking the plus beside each of the folders, as seen in items 1, 2, and 3 below.



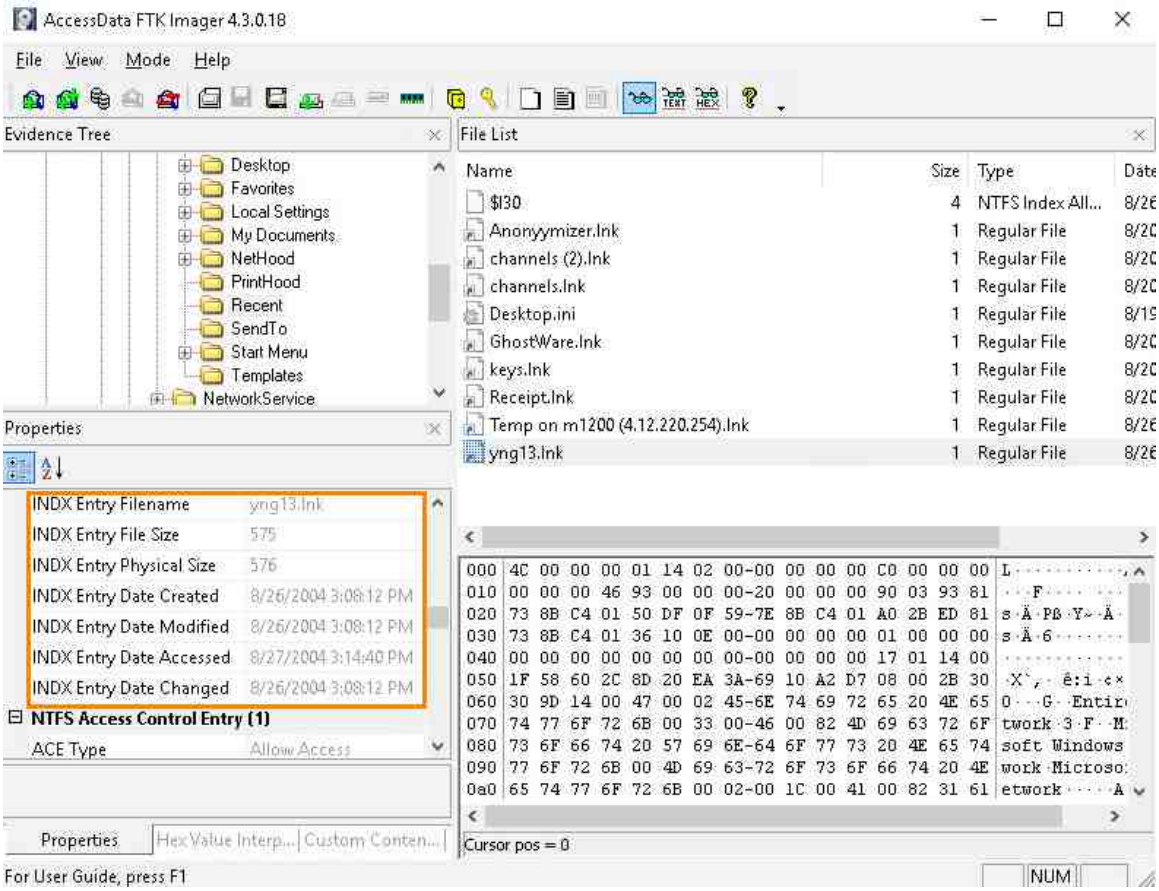
12. Once you get to the location, you will see several files that have the .lnk extension. These are link files or shortcut files and are simply references to other files that are normally located elsewhere. The Recent folder is one that is designed by Microsoft Windows to make it easier for users to see the last set of files they accessed. As a result, this folder doubles as a gold mine for forensic artifacts. Let us look at the file system metadata for one of the link files. As highlighted in item 1 below, click on the file called yng13.lnk in the File List window and then click the Properties tab in the Properties pane highlighted as item 2 below. The Properties tab will reveal the metadata that FTK Imager automatically parsed.



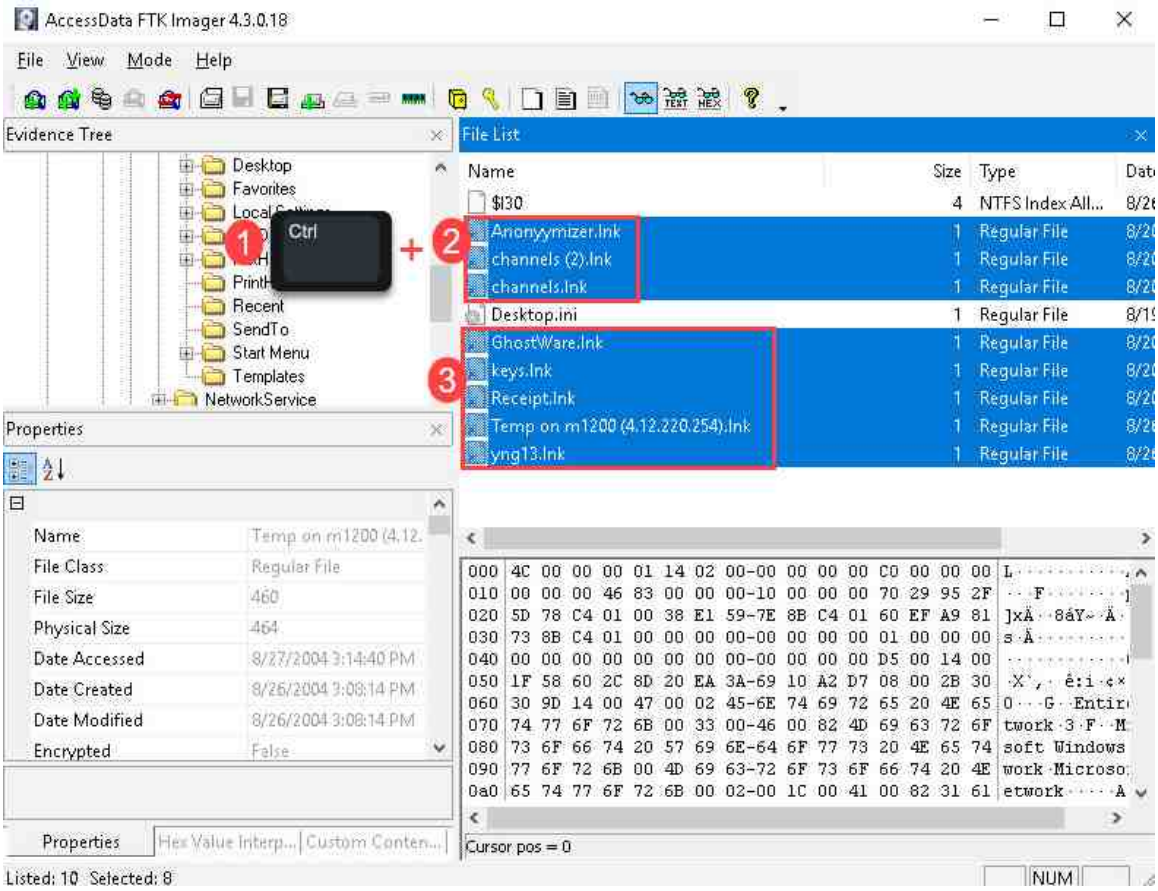
13. Look at the metadata for this file. As highlighted in item 1 below, this file was created on this volume and last modified on 8/26/2004 at 3:08:12 PM. It was last accessed on the following day, 8/27/2004, at 3:14:40 PM. This metadata is the same data that you will see when you right-click on any file and click Properties from Windows File Explorer. If you scroll down in the Properties window by clicking the arrow highlighted as item 2 (or using the mouse wheel), you will see more file system metadata about the file. You will see things such as the file owner's name; the Security Identifier and Relative Identifier; the modified, accessed, and created dates in the MFT; and who has access to view the file.



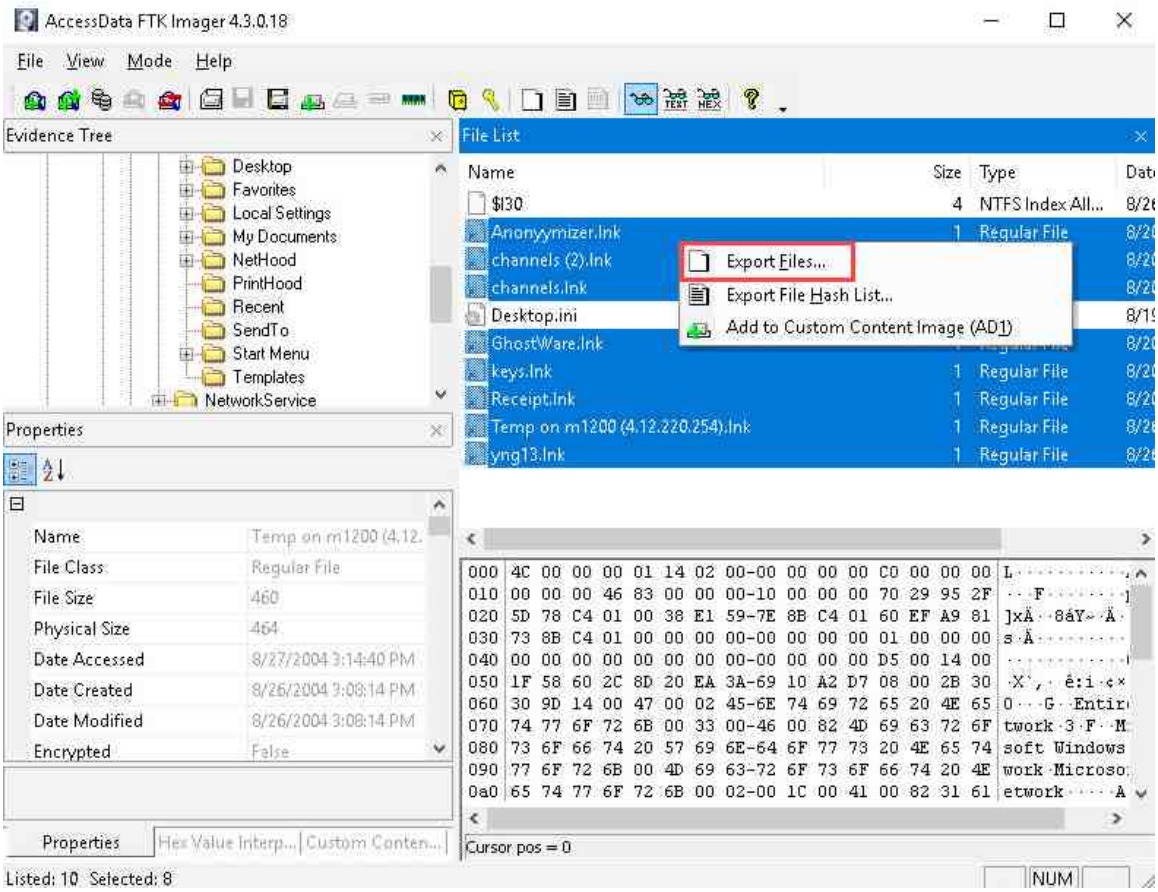
14. An interesting type of metadata to note is the one taken from $I30 files. These are files that are found on NTFS volumes and contain an index of file attributes. These attributes are often like the entries in the MFT and can provide accurate creation, access, and modified dates and times. As highlighted in the screenshot below, the entries that begin with the term INDX are attributes taken from the index.



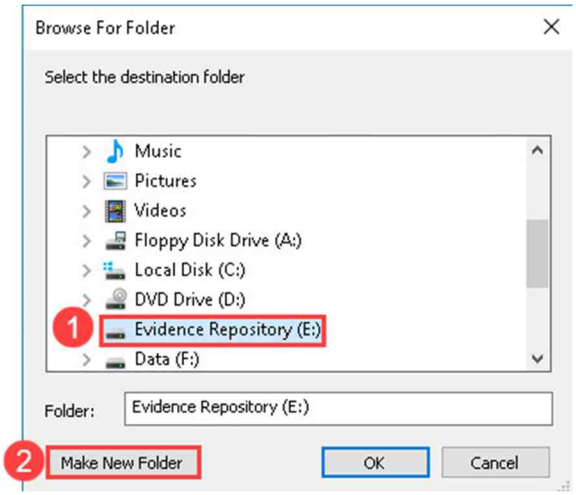
15. There is still some more information to be garnered from link files, though. We are going to use a tool called Lnk Analyzer to extract and view this data. First, we must export the link files that we want to review. To do this, highlight all the link files by holding the Ctrl key and left-clicking on each of them. An example can be seen in items 1, 2, and 3 below.



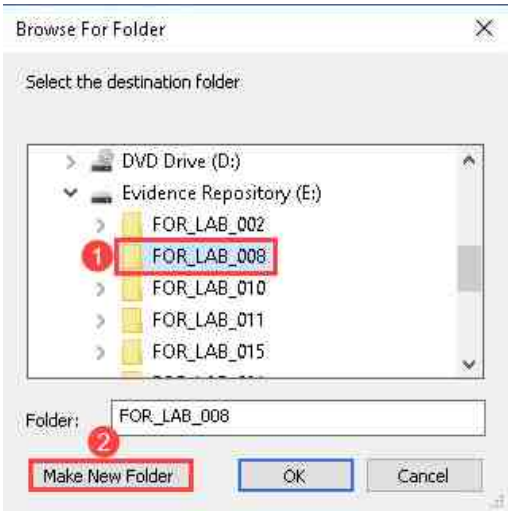
16. Now that they are selected, let us export them. To do this, right-click on one of the highlighted files and select the Export Files... option from the context menu that appears as highlighted below. This will bring up the Browse For Folder window.



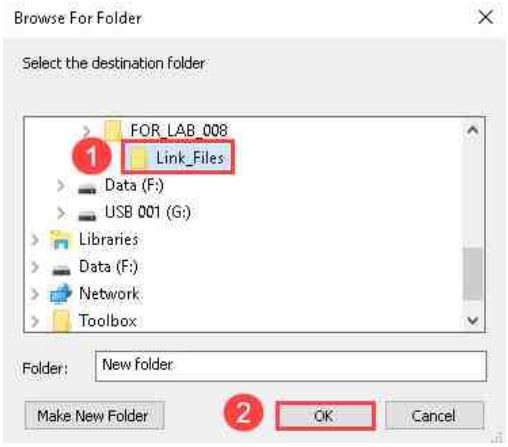
17. In the Browse For Folder window, navigate to the (E:) drive labeled Evidence Repository and click the Make New Folder button.



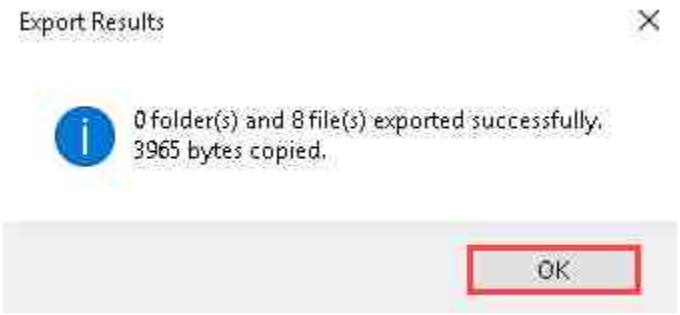
18. Name the folder `FOR_LAB_008` and create another folder within it by clicking on the folder you just created and then clicking the Make New Folder button again.



19. Name this new folder `Link_Files` and then click OK as seen in items 1 and 2 below. This will export the selected link files to the specified folder for further analysis.



20. Now that you have exported the link files, the Export Results window will appear. Click the OK button to close the window. We will now use Lnk Examiner (LNK file previewer) to parse more data from these link files.



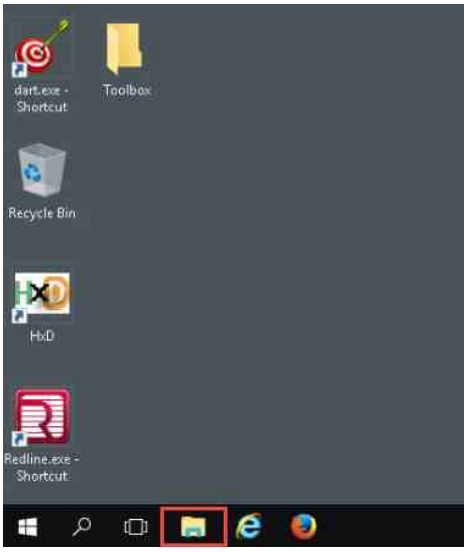
Each export performed will prompt a confirmation. Simply click OK to continue.

21. We will now move on to the next exercise.

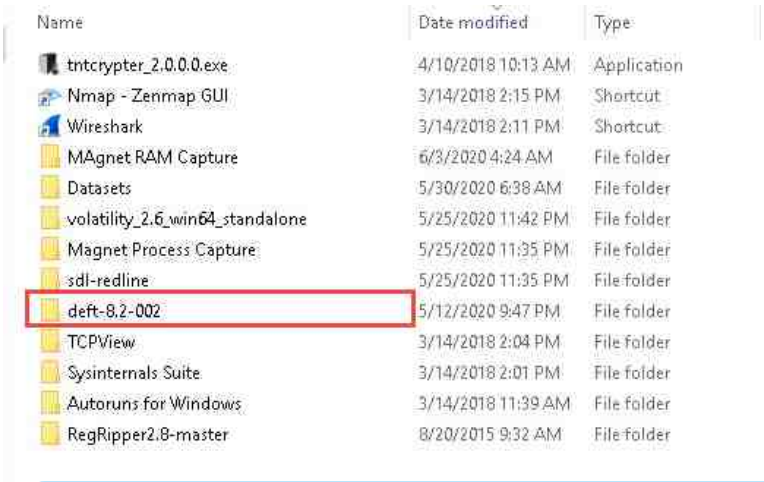
2 Getting to Know Lnk Examiner

Lnk Examiner / Lnk file previewer is a handy, lightweight tool that extracts additional information from link files and provides the output in an easy-to-use table view. This tool can be found in the Digital Advanced Response Toolkit (DART) that comes with the DEFT forensics operating system and live boot CD.

1. Let us get DART open first. To do this, open Windows File Explorer by clicking the folder icon on the taskbar as highlighted below.

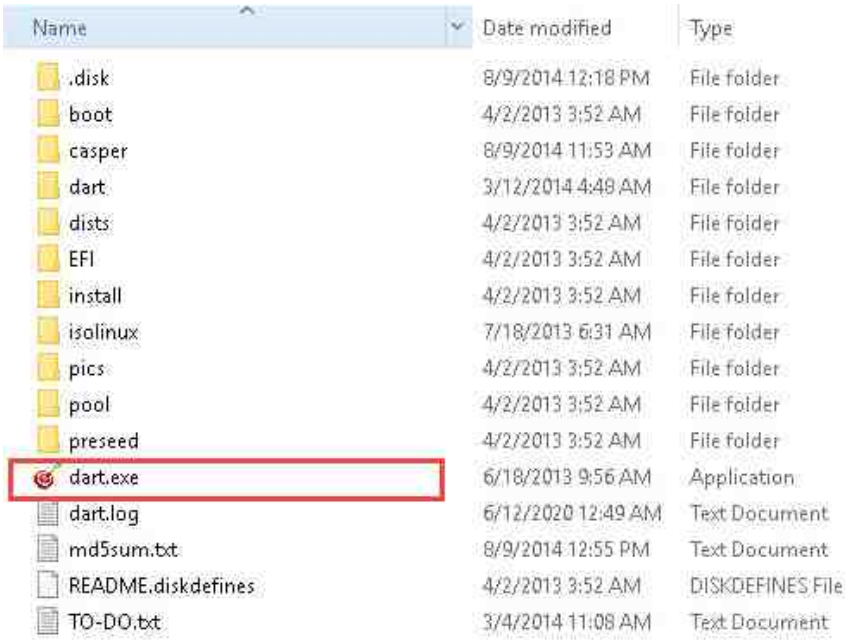


2. Within File Explorer, browse to This PC > Desktop > Toolbox, then double-click the folder called deft-8.2-002, highlighted below. This will allow you to view its contents as if you inserted a removable disk into the computer:

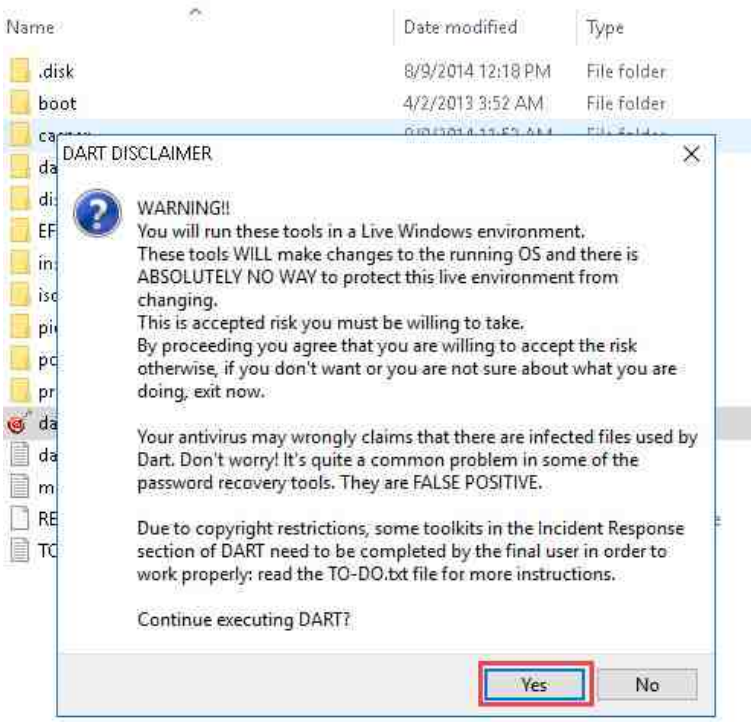


It is important to note that the tools contained within DEFT can be reported as False Positives in antivirus programs. When practicing in the real-world environment, be sure to disable antivirus solutions to prevent them from complicating the capture process.

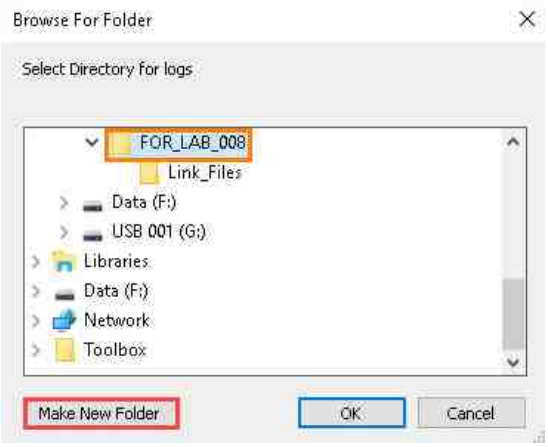
3. Once the folder is opened, you will see the following folder structure appear; double-click the dart.exe icon highlighted below.



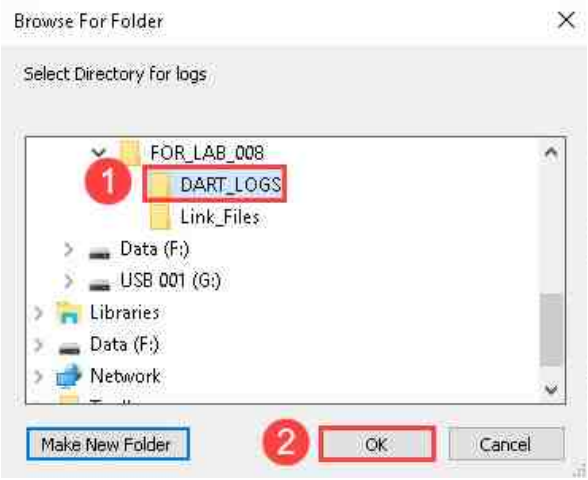
4. Upon launch, DART will display the DART DISCLAIMER window. Read it carefully to understand the risk that is taken when performing an analysis on a computer that is booted into its operating system. It will also provide details about common issues. Click the Yes button as highlighted below to continue.



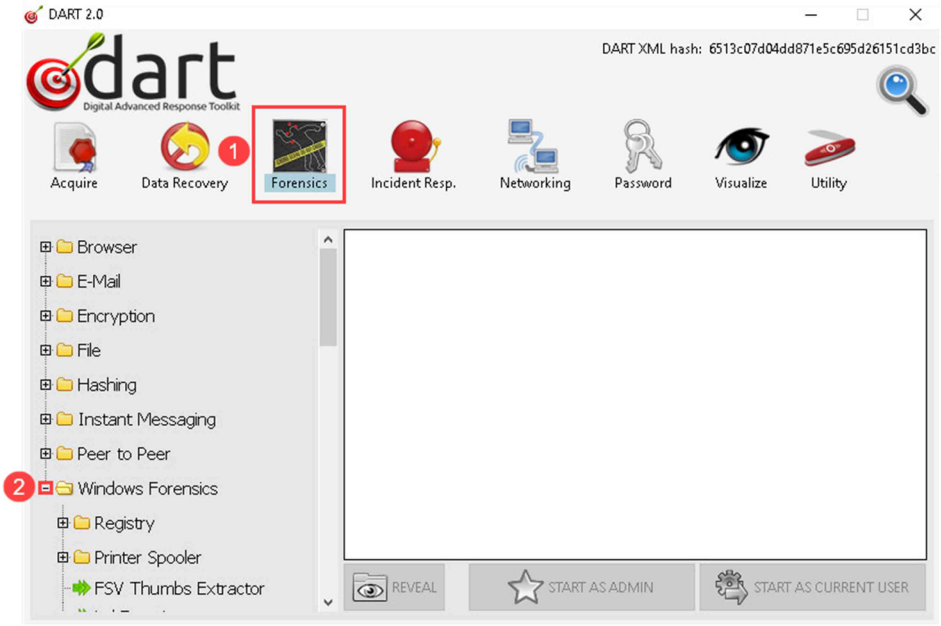
5. The next window that will appear is the Browse For Folder window. As you know, DART creates a log of actions taken while using it, and it requires a path to store the log file. Let us make a new folder in the FOR_LAB_008 folder we created earlier. To do this, browse to Evidence Repository (E:) > FOR_LAB_008 as seen below and click Make New Folder:



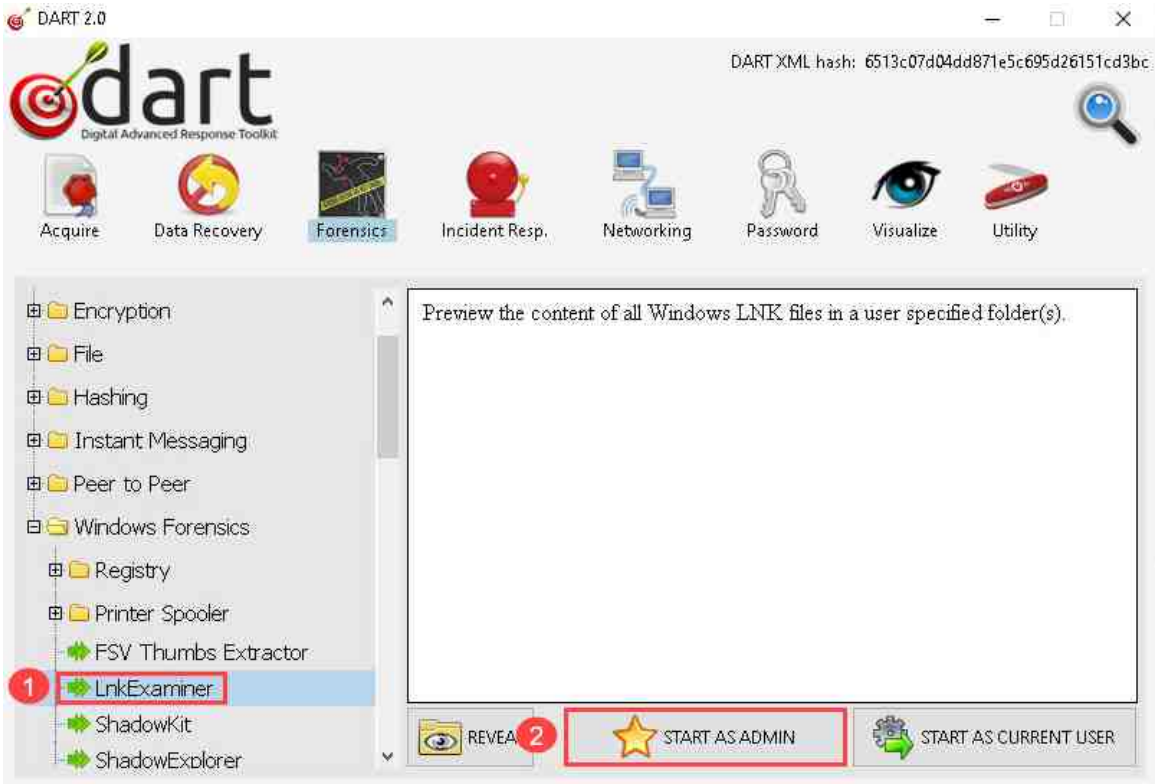
6. Let us name the new folder DART_LOGS and then click OK as highlighted below. You will now be presented with the DART 2.0 home page.



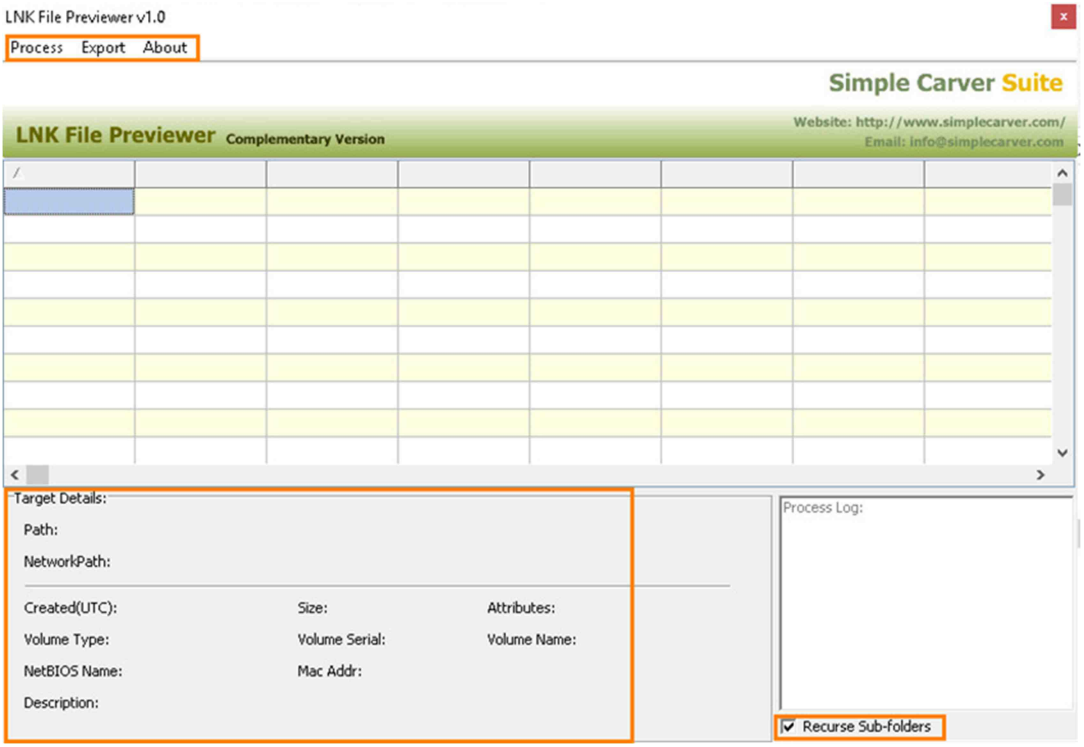
7. The DART main window will appear. Let us access Lnk Examiner / Lnk File Previewer by clicking the Forensics category and then clicking the + sign beside the Windows Forensics folder as highlighted in items 1 and 2 below.



8. You will find the program Lnk Examiner in the root of the Windows folder (right below FSV Thumbs Extractor). Click Lnk Examiner as highlighted in item 1 below. As usual, a description of the tool will appear in the right pane. Click START AS ADMIN as highlighted in item 2 below to run the program.



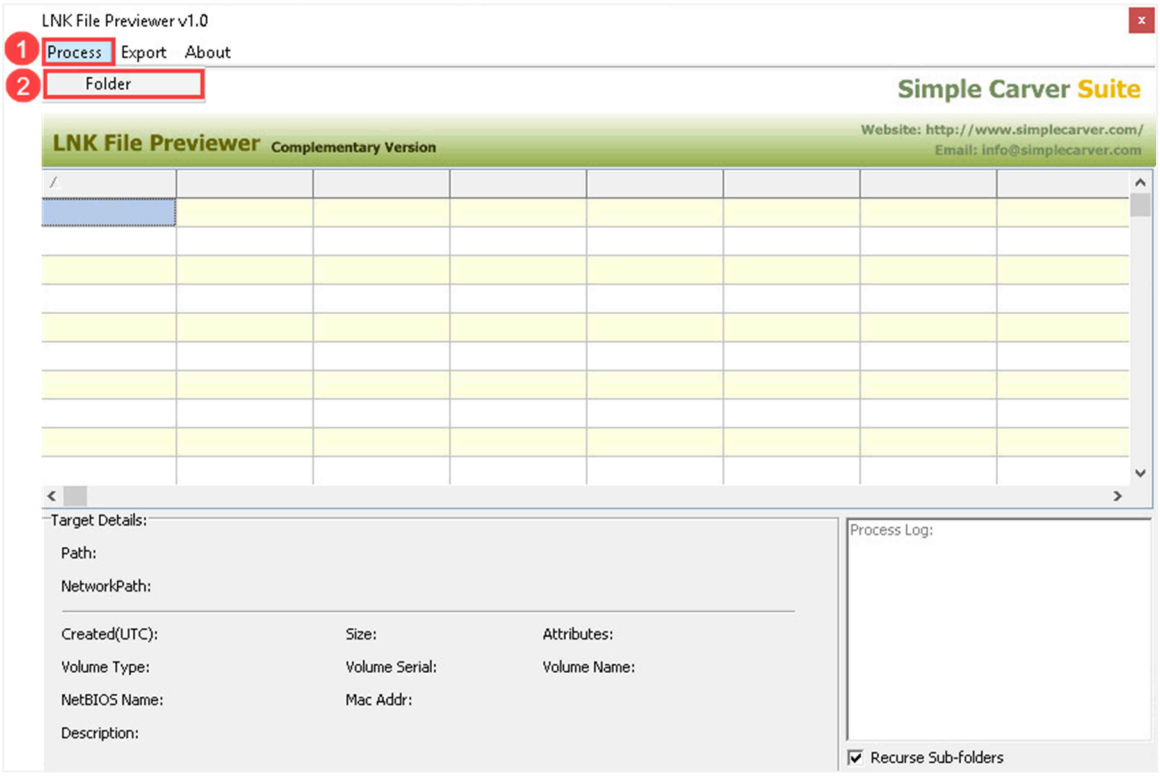
9. LnkExaminer / Lnk File Previewer will open, revealing the main window as seen below. The table below the following screenshot provides a summary of the options that we will be using for this exercise.
10. Lnk Examiner allows you to add a folder that contains link files. The software will then extract the data and present the data in the main window highlighted below.



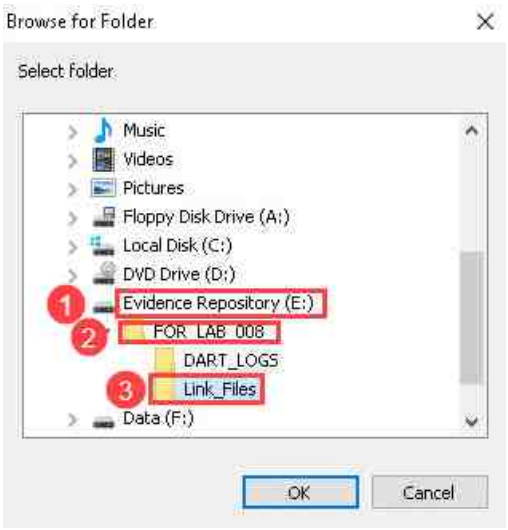
Process	The Process menu option allows you to select the folder that contains the Lnk Files
Export	The Export menu option allows you to export the extracted data to a CSV file
Recurse Sub-Folders checkbox	The Recurse Sub-folders checkbox allows you to choose whether Lnk Examiner should add the contents of sub-folders within the selected folders as well
Target Details Pane	The Target Details pane allows you to view the extracted data for a selected file
Process Log Pane	The Process Log pane allows you to view logs about the volume of files that were processed

3 Extracting Data from Link Files with Lnk Examiner

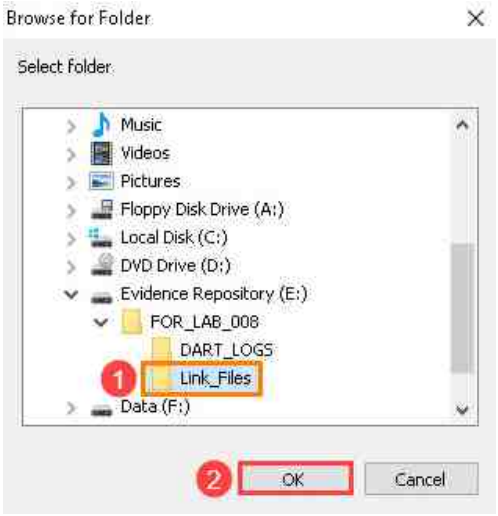
1. Let us use Lnk Examiner to review the files we extracted earlier. Lnk Examiner should still be open; if it is not, reopen it and click Process from the menu bar and then click Folder as highlighted in items 1 and 2 below.



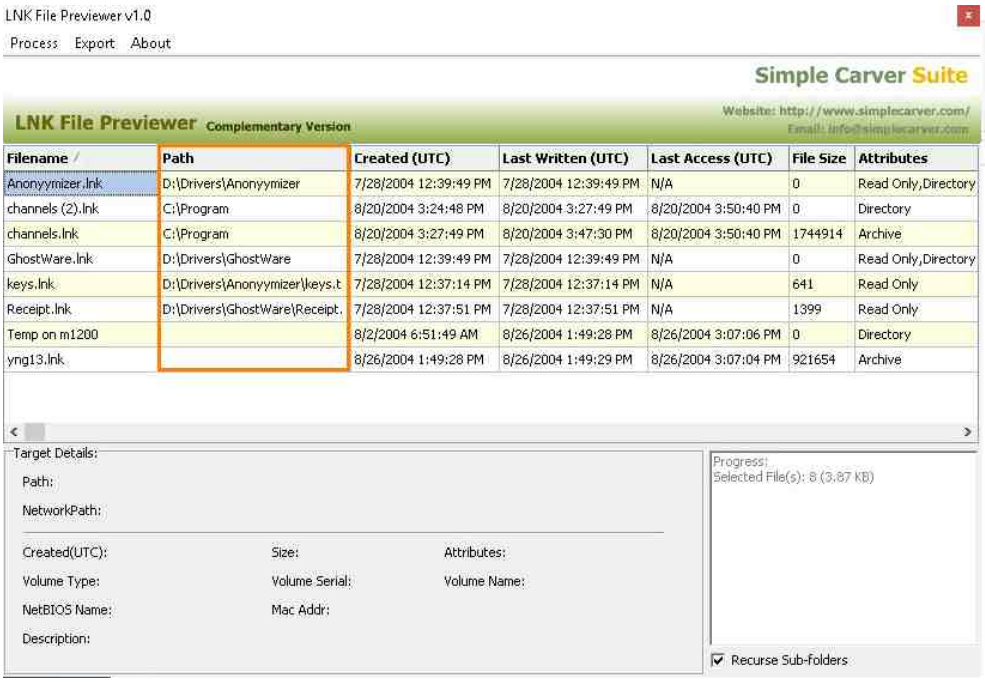
2. This will open the Browse for Folder window. Browse to the folder you created called Link_Files by navigating to Evidence Repository (E:) > FOR_LAB_008 > Link_Files as highlighted in items 1, 2, and 3 below.



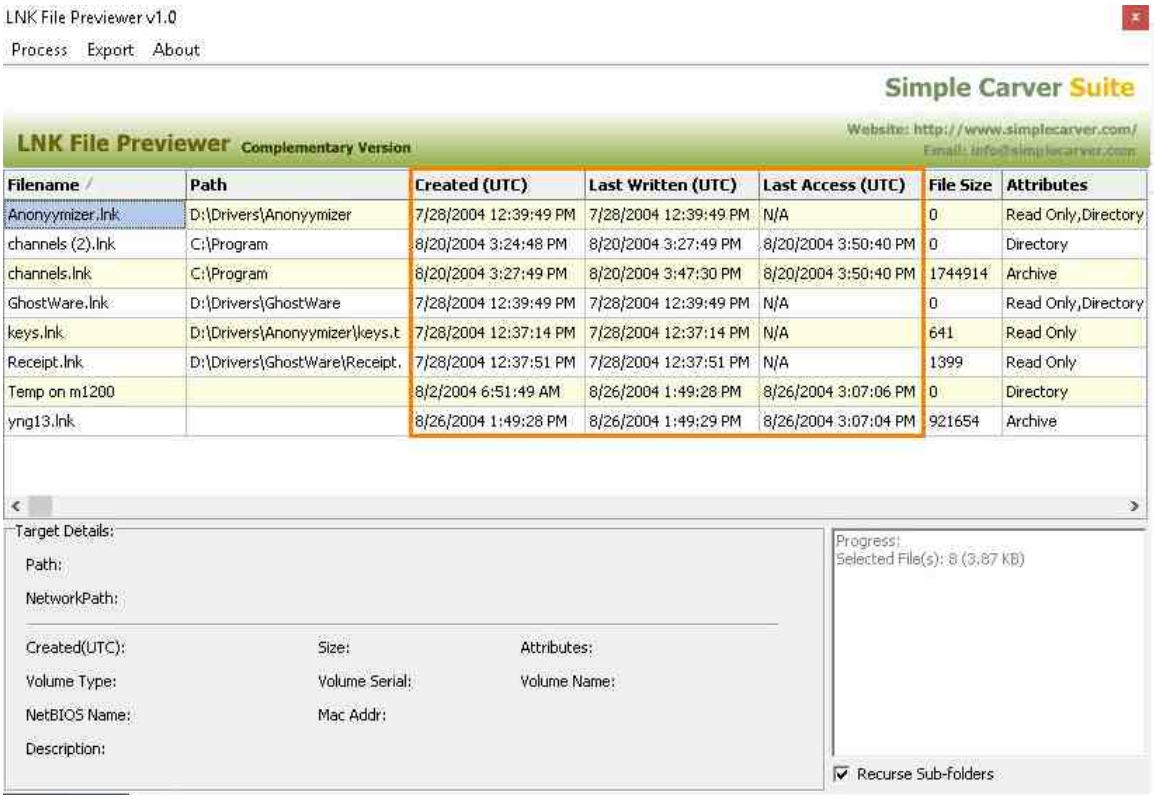
3. Now verify that the folder called Link_Files is selected and then click OK as seen in items 1 and 2 below. This will immediately add and process the files within the Link_Files folder.



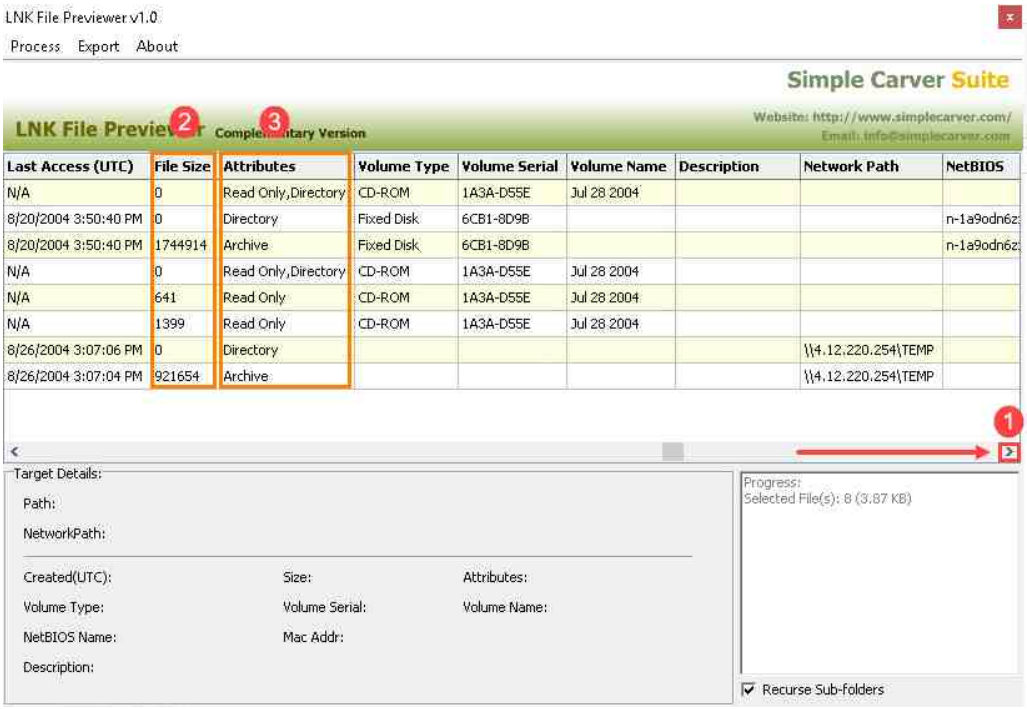
4. As you can see in the main window, the table becomes populated with the names and metadata for the files we extracted earlier. The column called Path contains the paths to the file that each link file references. As you can see, there are 2 files that do not have a path. We will get to these later. For now, you can see that the other files were accessed from 2 main volumes called drives C and D.



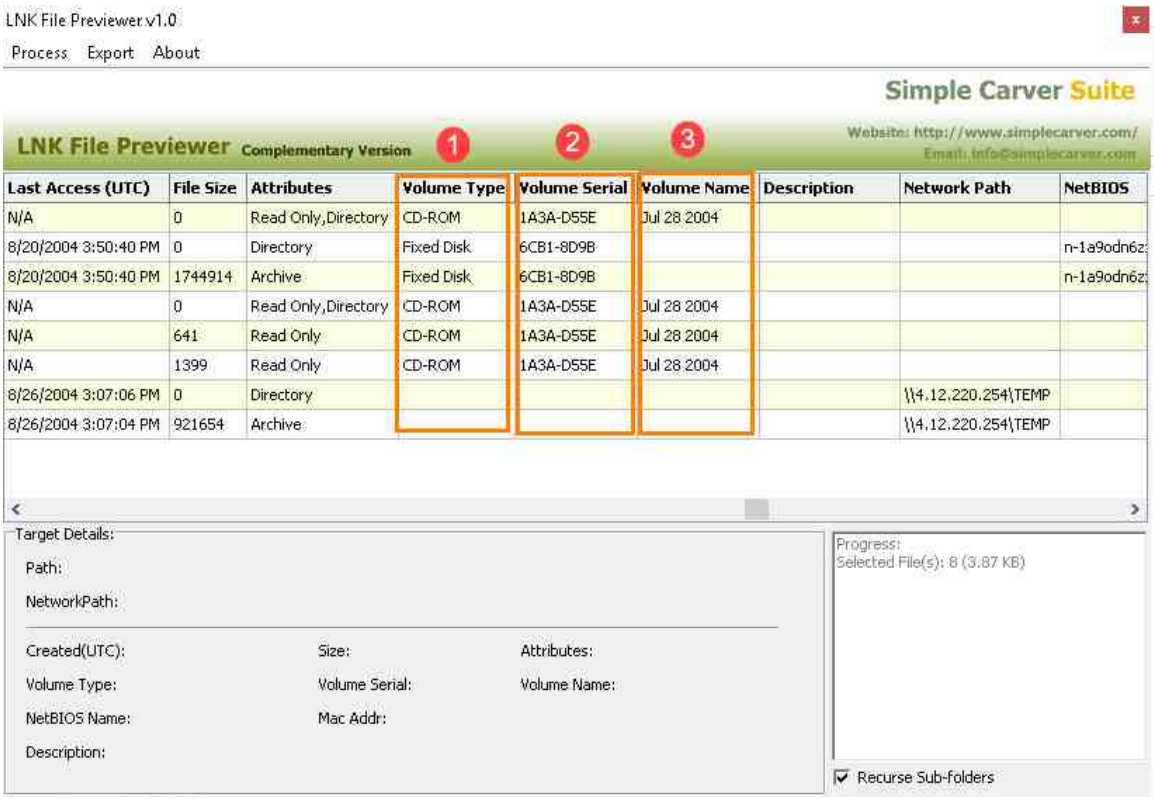
5. To the right of the path column is the metadata associated with the creation, last modification, and last access dates and times for the file that the shortcut references. This metadata is extracted from the index attributes that are stored in $I30 files and can be used to learn more about the file that is referenced by the link file.



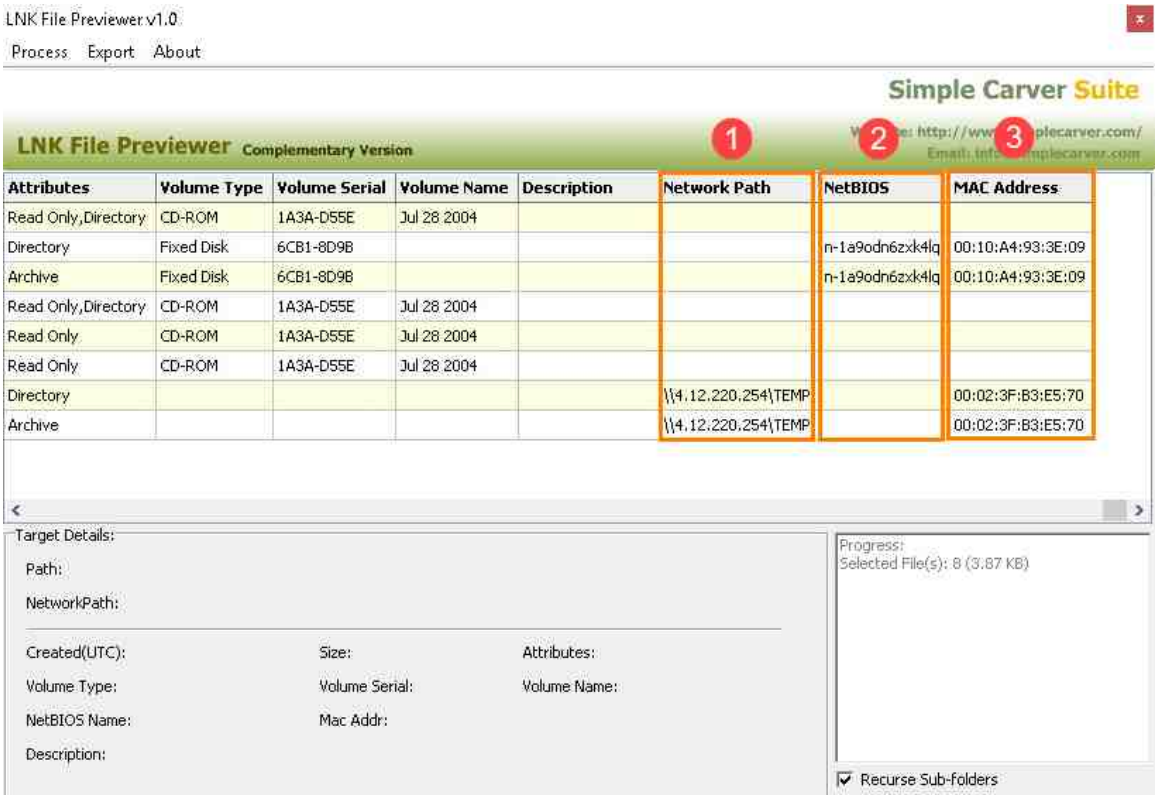
6. Let us scroll further right and see what other information is there. To scroll, click the arrow button on the horizontal scroll bar as seen in item 1 below. As you can see, the File Size column indicates the size of the referenced file, as seen in item 2, while the Attributes column indicates what type of item the shortcut references. In this list, highlighted as item 3, there are 4 directories, 2 archive files, and 2 read-only files referenced by these shortcuts.



7. The next 3 columns describe the location of the referenced file. The Volume Type column, seen in item 1 below, lists the type of volume that the referenced item is stored on. As you can see in item 1, there are 4 files/folders that reside on a CD-ROM while 2 reside on a fixed disk (internal storage drive). There are also 2 blank entries, which we will discuss later. The next column is called Volume serial number, and this provides the volume serial number for the volume that the file resides on. The volume serial number is highlighted in item 2 below. There is no question as to the importance of this data since it can tell exactly what volume a file resides on, simply because it was opened on the workstation at one point. The final column seen in item 3 is Volume Name and this gets populated if the volume is given a name. As you can see, the CD-ROM that was inserted into the computer has Jul 28, 2004 as the volume name.

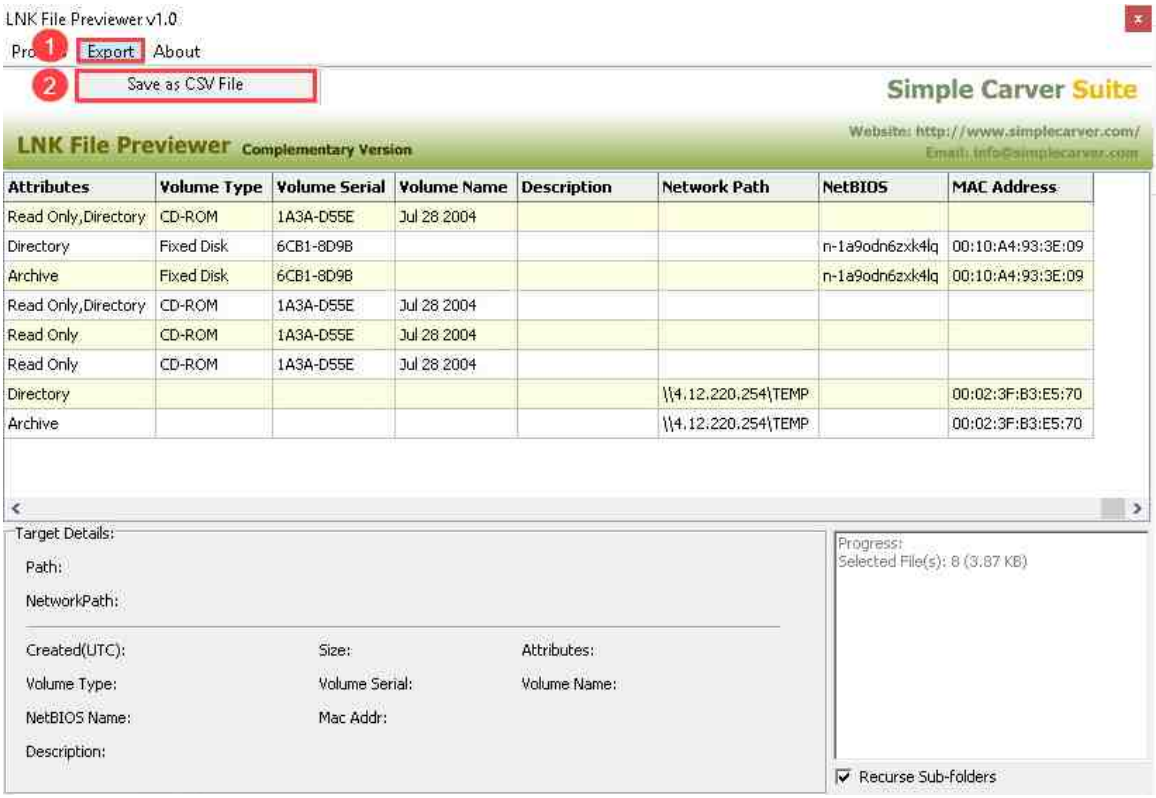


8. Now let us look at the last three columns. The first one, highlighted in item 1, is Network Path, and it gets populated if the file/folder was opened from a network location. As you can see in item 1, there are 2 items that were accessed from the network path \\4.12.220.254\TEMP. This is important data as it can tell the exact IP and directory of the device that was connected. It also explains why there was no volume type, name, and serial number for these 2 files. The next column, highlighted in item 2, is NetBIOS, which gives the computername/NetBIOS name of the computer that the file/folder resides on. The last column, seen in item 3, is MAC Address, and this gives the MAC address of the computer that the file resides on if it was run from a computer.



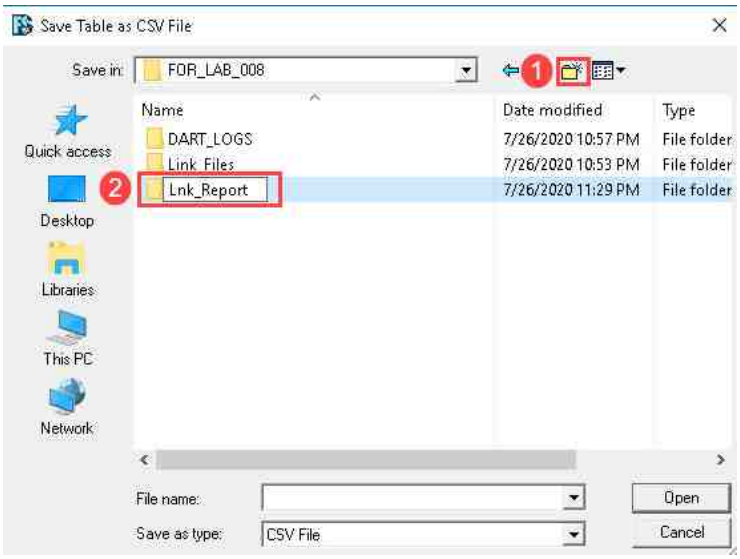
You can click each item in the list to view each link file's metadata in the Target Details area.

9. It is amazing how much data can be found in a shortcut. In most examinations, the examiner will prefer to retain a copy of the parsed data, so let us learn how to export the data in a CSV file. This application makes it extremely easy to do this. Simply click Save as CSV File in the Export dropdown menu on the menu bar as highlighted in items 1 and 2 below. The Save as CSV File window will appear.

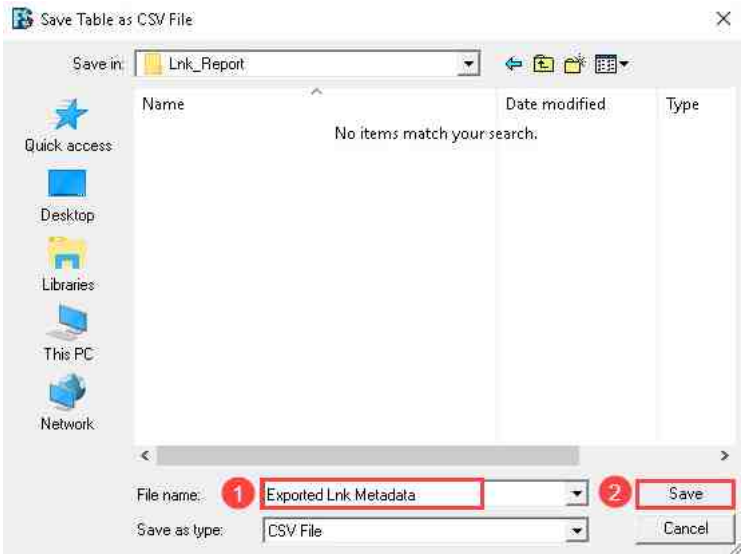


The Save as CSV File option will save the entire table as a CSV file so you don't have to worry about selecting each entry.

10. In the Save as CSV File window, browse to the folder we created earlier called FOR_LAB_008 by navigating to This PC > Evidence Repository (E:) > FOR_LAB_008. Once there, create a new folder by clicking the new folder toolbar icon as highlighted in item 1 below and name the new folder `Lnk_Report` as seen in item 2 below.



11. Double-click the Lnk_Report folder you just created to open it. Once inside the folder, type `Exported Lnk Metadata` in the File name field and then click Save as highlighted in items 1 and 2 below.

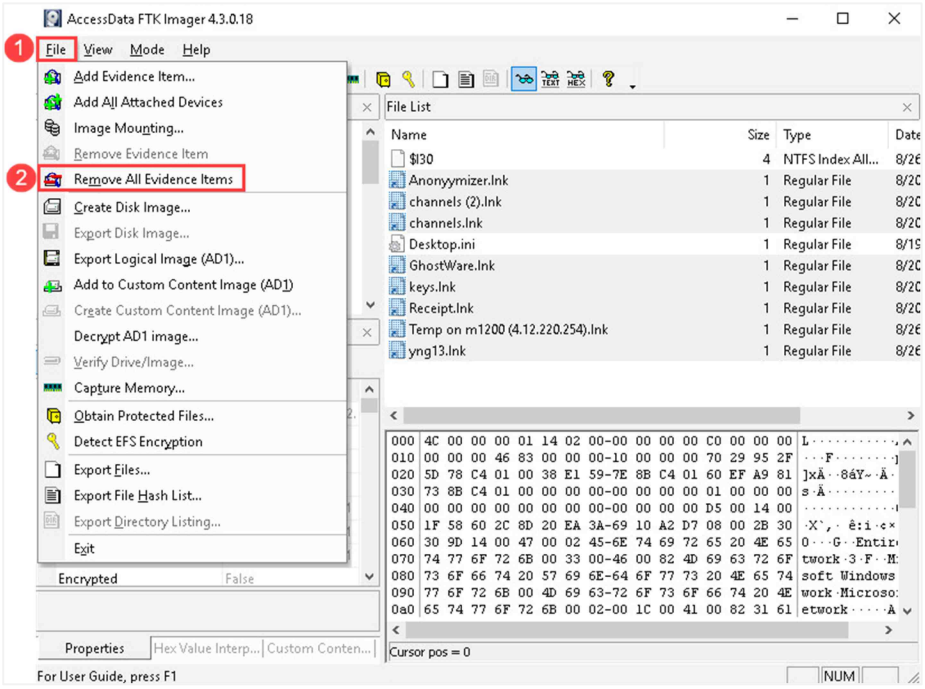


12. Now that you have that data saved, you can always go back and look at the contents to further your investigations. We are now going to look at some other types of metadata in some common document files. Before continuing, close LNK File Previewer by clicking the X at the top-right corner of the window.

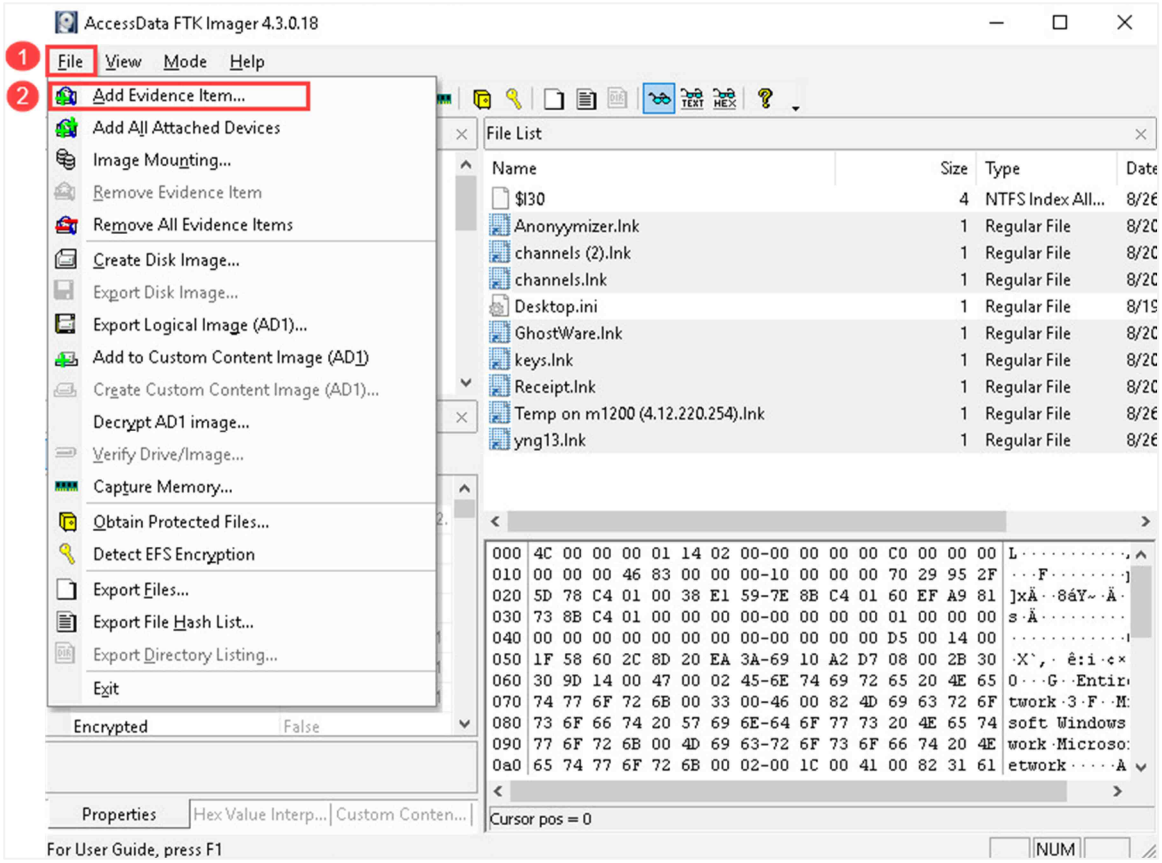
4 Exporting and Analyzing Regular Files

In this exercise, we will look at some more types of metadata stored in common document files found on digital devices.

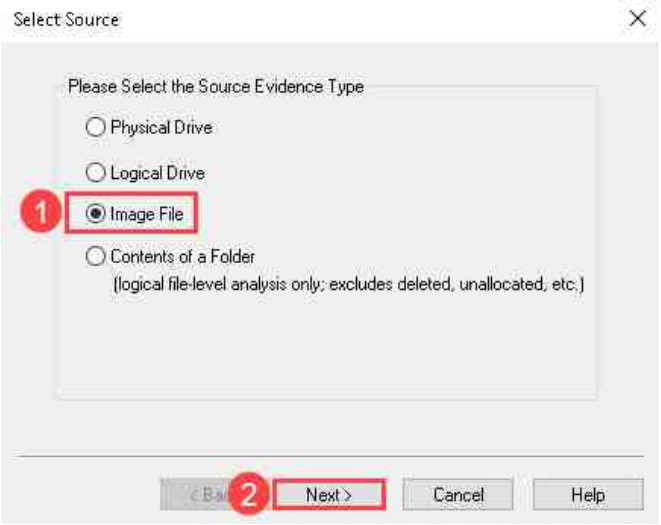
1. You should still have FTK Imager open; if not, reopen it and click the File menu option to open the File dropdown menu, then click the Remove All Evidence Items option from the dropdown menu as seen in items 1 and 2. This will remove the loaded FEF and will make it easier for us to navigate the new FEF we will be loading.



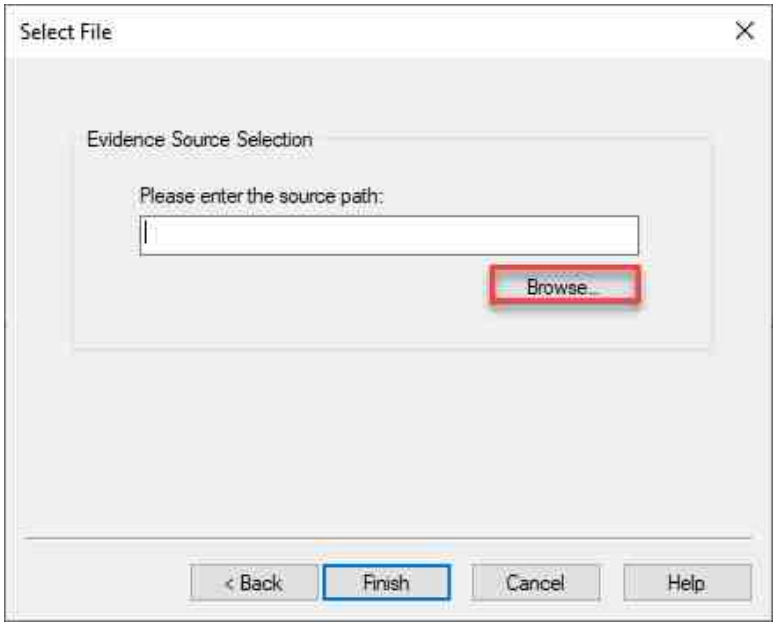
2. Once the previous FEF has been removed, click the File dropdown menu again and click the Add Evidence Item... option from the list as seen in items 1 and 2.



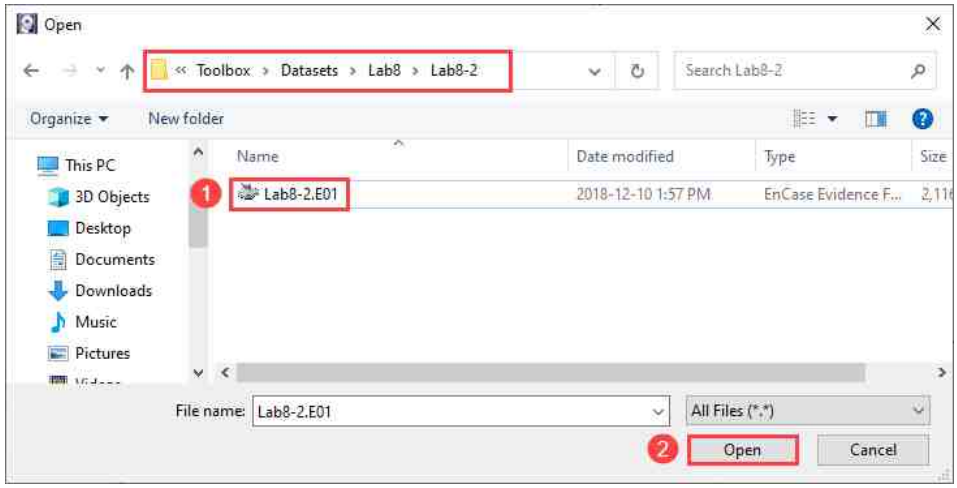
3. You will be brought to the Select Source window. Let us select Image File and click Next as highlighted in items 1 and 2:



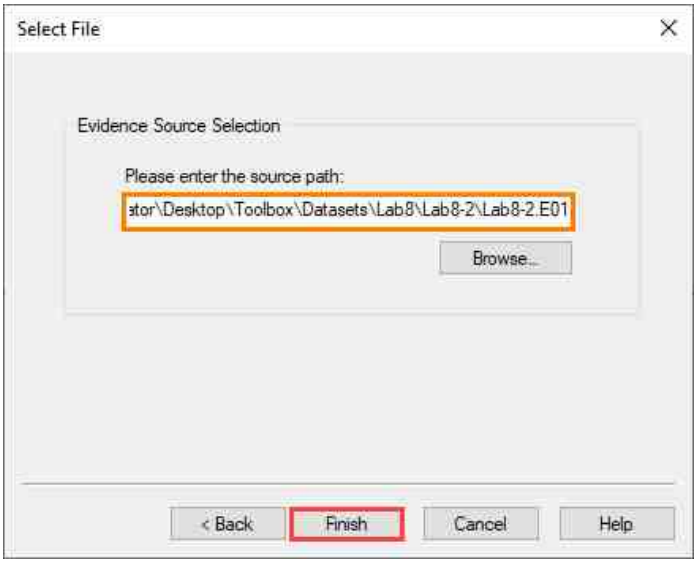
4. In the Select File window, click Browse, highlighted in red in the screenshot below. This will allow you to browse to the appropriate FEF.



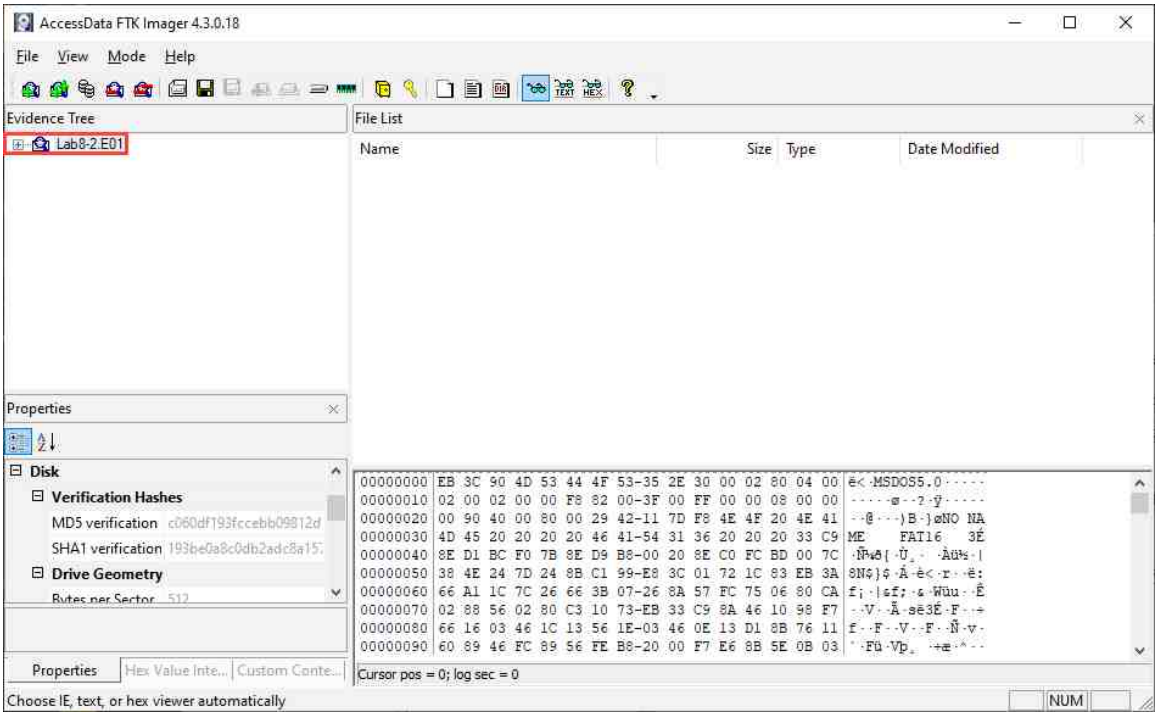
5. Now browse to This PC > Desktop > Toolbox > Datasets > Lab8 and double-click the folder called Lab8-2. This will open the folder revealing the FEF called Lab8-2.E01. Select the file called Lab8-2.E01 and click the Open button as highlighted in items 1 and 2 below.



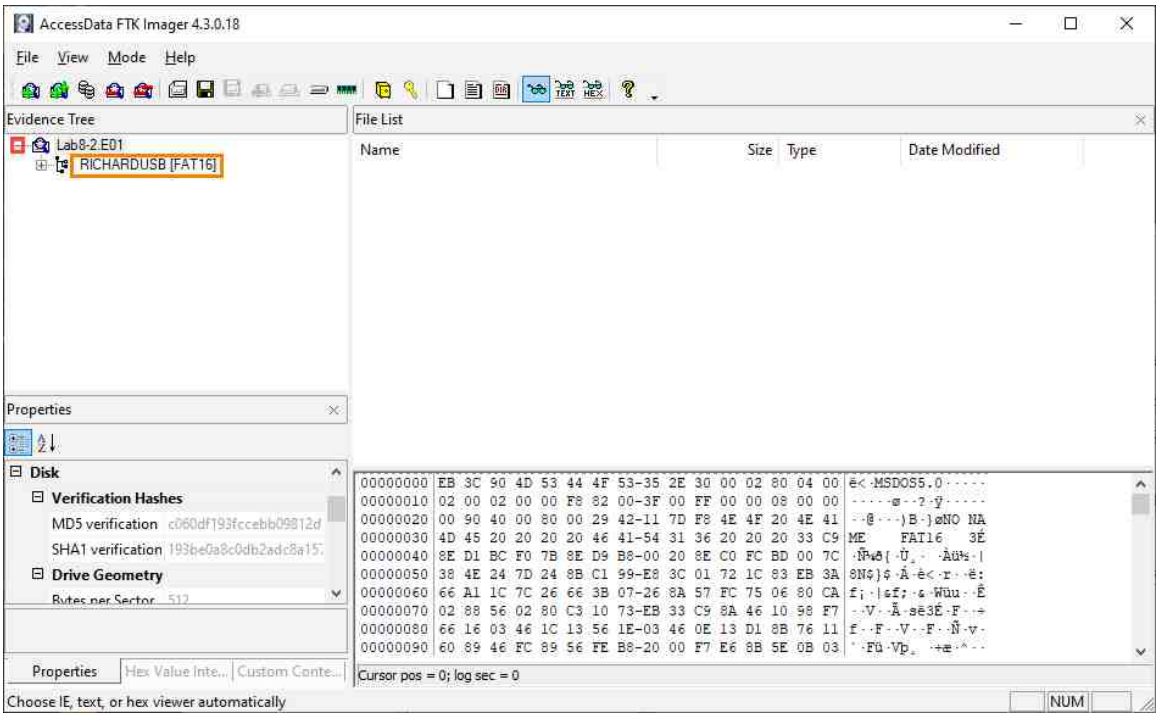
6. Review the source path of the file called Lab8-2.E01. In the Select File window, click Finish, highlighted in the screenshot below. This will take you back to the FTK Imager's main window.



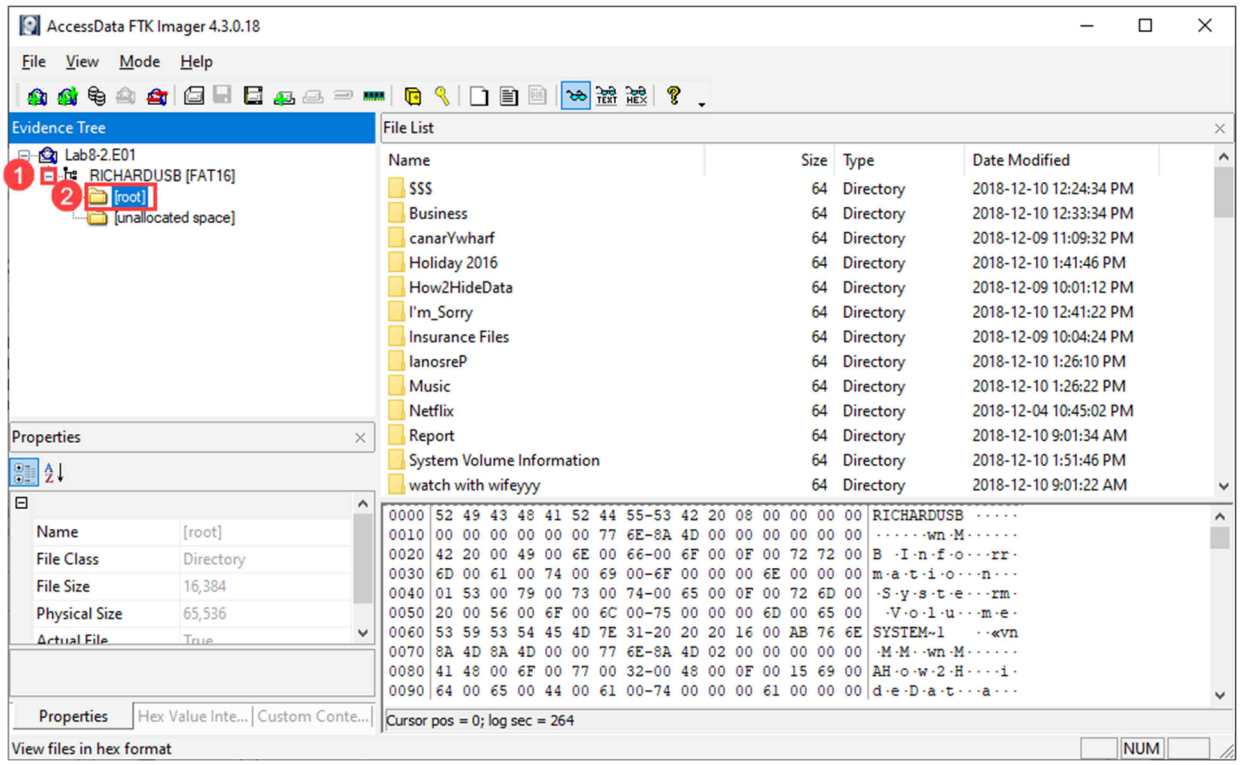
7. If you did everything correctly, you will now be back at FTK Imager's main window with Lab8-2.E01 listed under the Evidence Tree pane. From the Evidence Tree pane, click the tree item Lab8-2.E01, highlighted below. This will select the image you are going to peruse.



8. We will now browse the FEF and view its contents. To begin, click the + sign beside the hard drive you added called Lab8-2.E01, as seen below. This will expand the tree and display the file system on the drive.



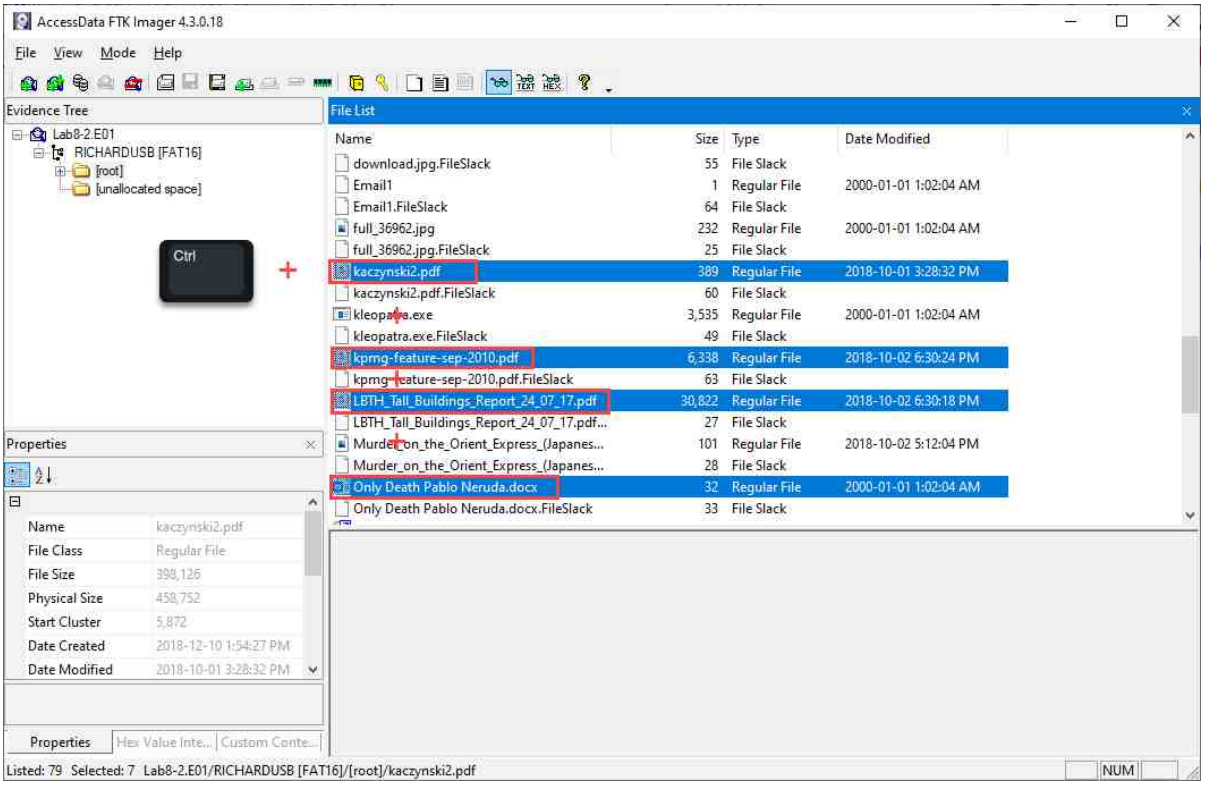
9. Let us expand the volume by clicking the + beside RICHARDUSB [FAT16] as seen in item 1. This will reveal two folders; let us click on the folder called root, as seen in item 2, and look at the files inside it.



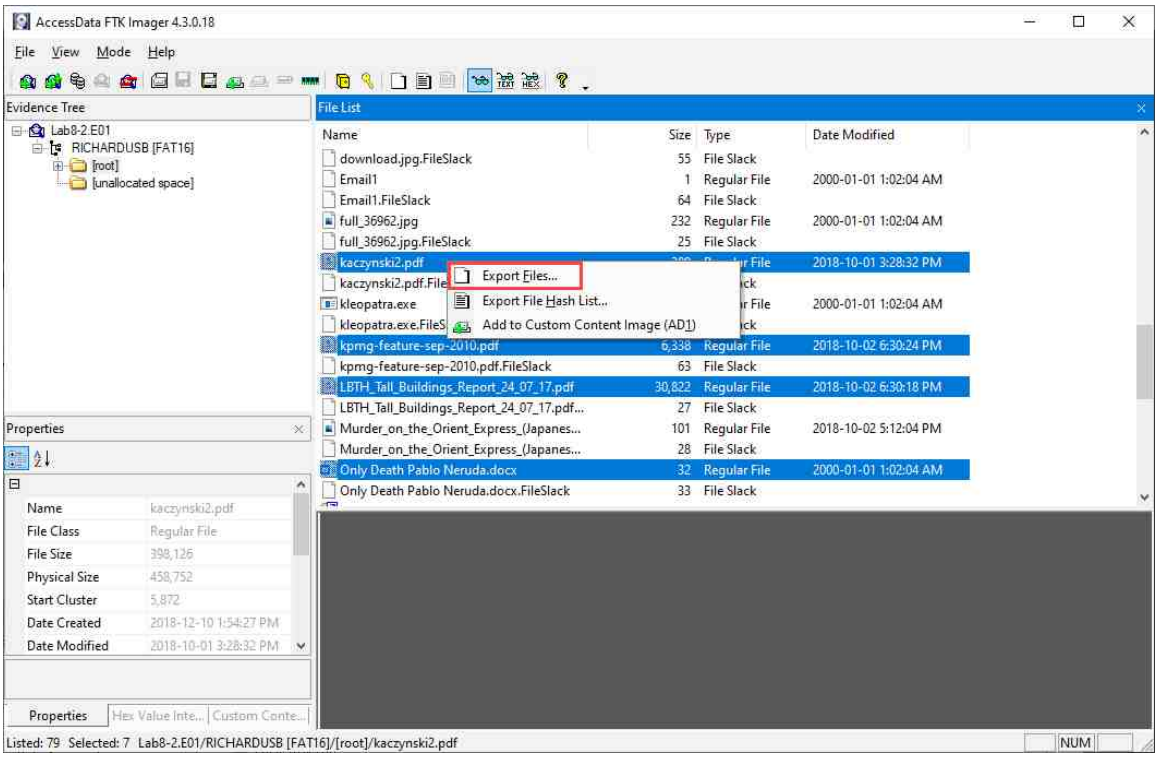
10. You can see all the files and folders from the root directory, in the File List pane. Let us scroll down and select a few files from the list. To do this, hold the Ctrl key and select the files called:

    a. 19861-sc-clients-national.xls
    b. Ar17_en.pdf
    c. Kaczynski2.pdf
    d. Kpmg-feature-sep-2010.pdf
    e. LBTH_Tall_Buildings_Report_24_07_17.pdf
    f. Only Death Pablo Neruda.docs
    g. TuringComputing.pdf

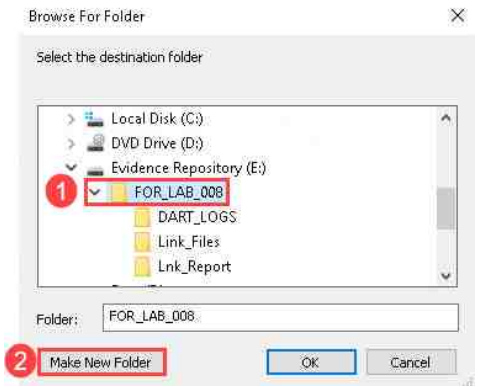
    An example can be seen in the screenshot below.



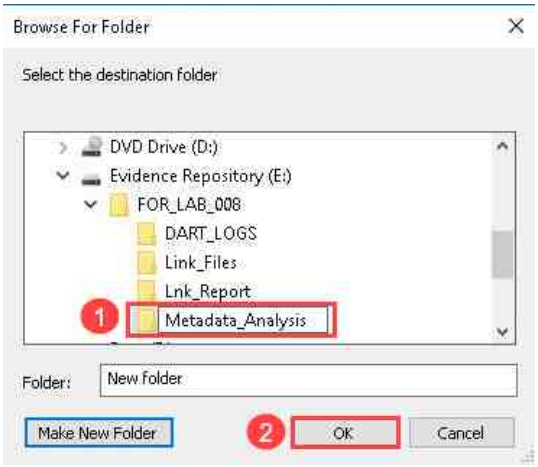
11. Now that they are selected, let us export them. To do this, right-click on one of the highlighted files and select the Export Files... option from the context menu that appears as highlighted below. This will bring up the Browse For Folder window.



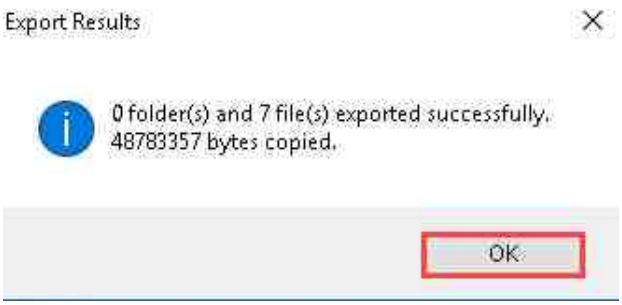
12. In the Browse For Folder window, navigate to the folder you created called FOR_LAB_008 by browsing to the path This PC > Evidence Repository (E:) > FOR_LAB_008 and click the Make New Folder button as seen in items 1 and 2 below.



13. Name the folder `Metadata_Analysis` and then click OK as seen in items 1 and 2 below. This will export the selected files to the specified folder for further analysis.



14. Now that you have exported the files, the Export Results window will appear. Click the OK button to close the window. We will now use MetaExtractor to parse more data from these document files.

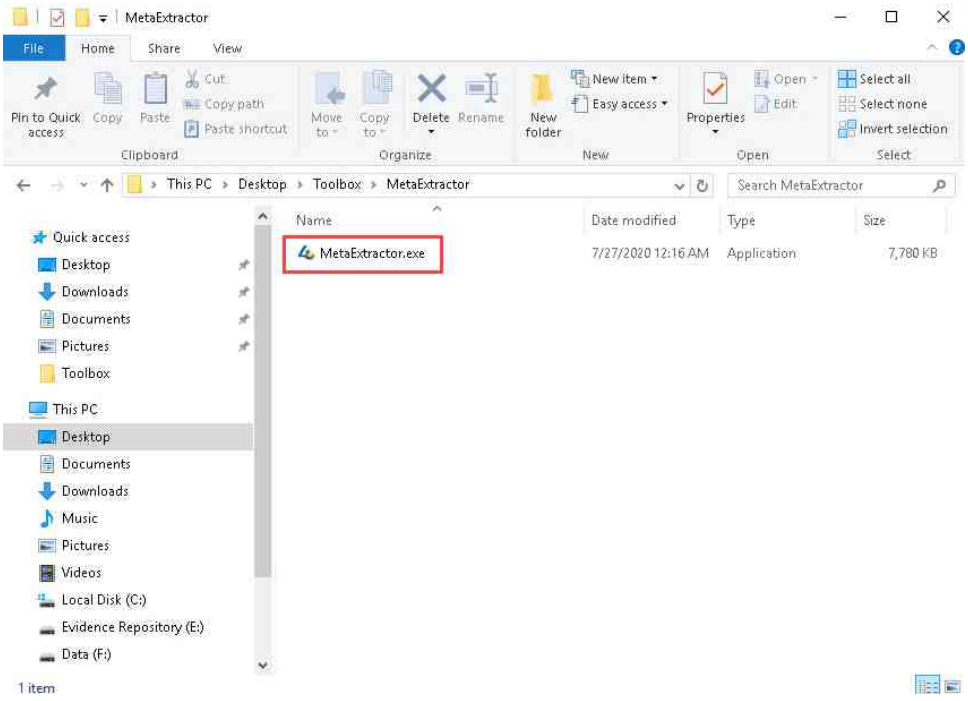


15. Before continuing, close FTK Imager, DART 2.0, and all other open windows by clicking the X at the top-right corner of each window.

5 Getting to Know MetaExtractor

Sometimes, we need to view the internal metadata for multiple files, and a handy tool to get this done is the one known as MetaExtractor created by 4Discovery. This tool is one of the popular forensic tools available for extracting all types of metadata and providing a report of the extracted data. In this lab, we will take you through the common features of this simple but powerful tool.

1. Let us start by opening MetaExtractor. This can be done by opening Windows File Explorer and browsing to This PC > Desktop > Toolbox > MetaExtractor. Once in the MetaExtractor folder, double-click the executable file called MetaExtractor.exe as highlighted below.



2. MetaExtractor will open, revealing the main window as seen below. The table below the following screenshot provides a summary of the options that we will be using for this exercise.

Toolbar Option	Description
Save to CSV	The Save to CSV toolbar option allows the user to export the extracted data to a CSV file
Open File(s)	The Open File(s) option allows the user to choose specific files from which to extract their metadata
Open Folder or Files	The Open Folder or Files option allows the user to choose specific files or a folder from which to extract the metadata

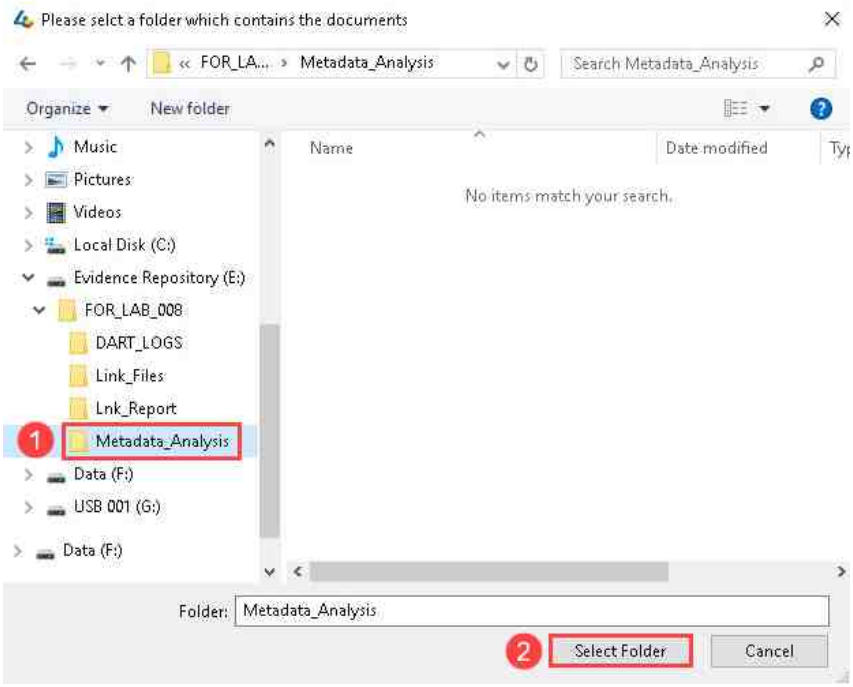
6 Extracting Metadata with MetaExtractor

Now that we know how to use MetaExtractor, let us use it to parse the metadata from the files we just exported. The way MetaExtractor works is simple. Add the file(s) using either the Open File(s) button or the Open Folder or Files button. The software will then extract the data and present the data in the main window, as highlighted below.

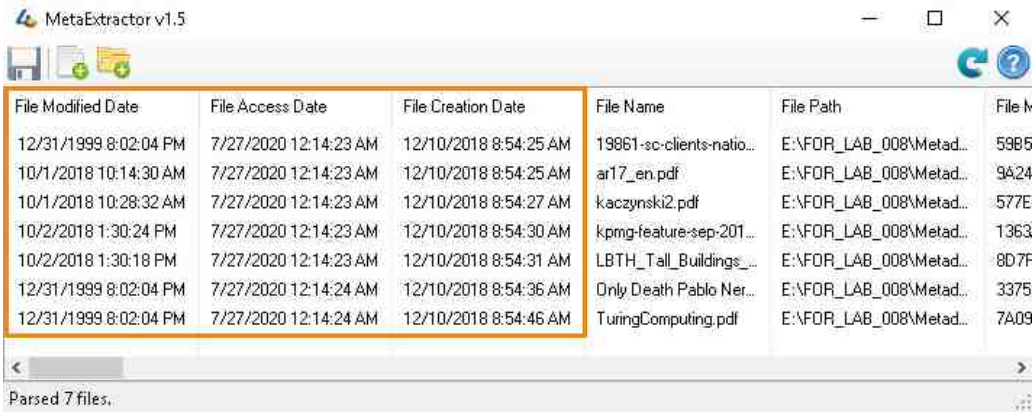
We will now use MetaExtractor on the files we extracted in the last exercise. We will walk you through it below.

1. MetaExtractor should still be open; if not, reopen it and then click the Open Folder toolbar icon as highlighted below.

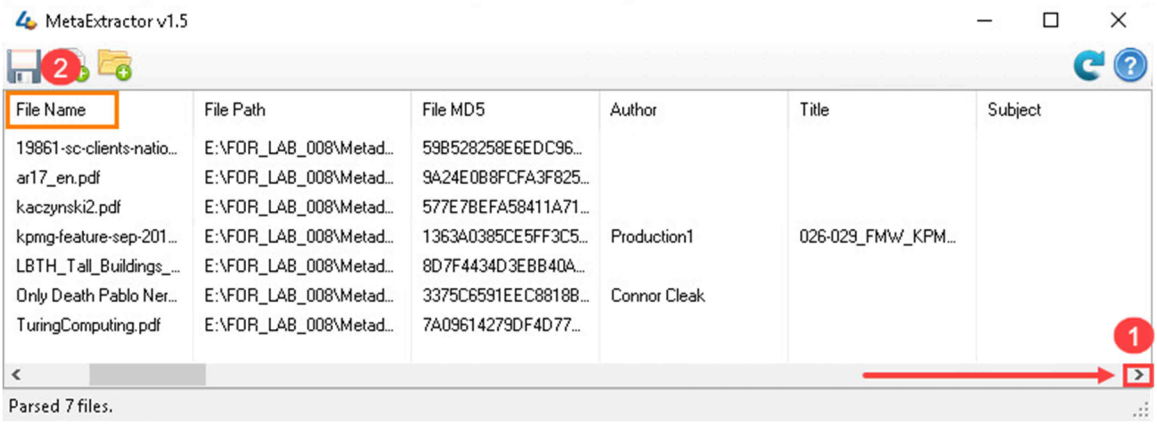
2. The Please select a folder which contains the documents window will appear; let us load the files we exported in the last exercise by browsing to the folder we called Metadata_Analysis. To get there, navigate to This PC > Evidence Repository (E:) > FOR_LAB_008. Once in the FOR_LAB_008 folder, select the folder called Metadata_Analysis by clicking on it and then click the Select Folder button as highlighted in items 1 and 2 below.



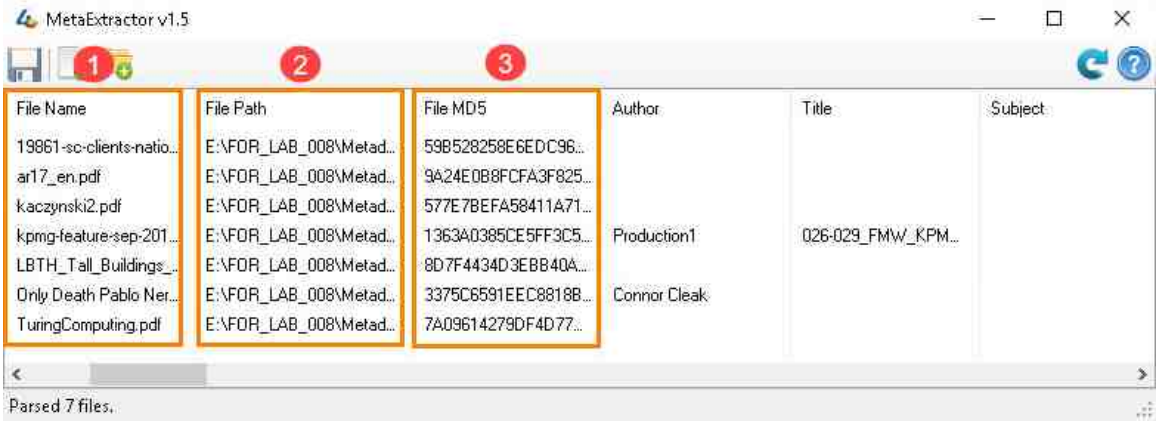
3. Now the results of the metadata parse should populate the main window in MetaExtractor. As you can see, the first three columns provide the file system metadata. An interesting thing to note in the file system metadata is that the modified dates of all the files predate their creation dates. This is an indicator that these files were created on a different device and copied to the volume we extracted them from.



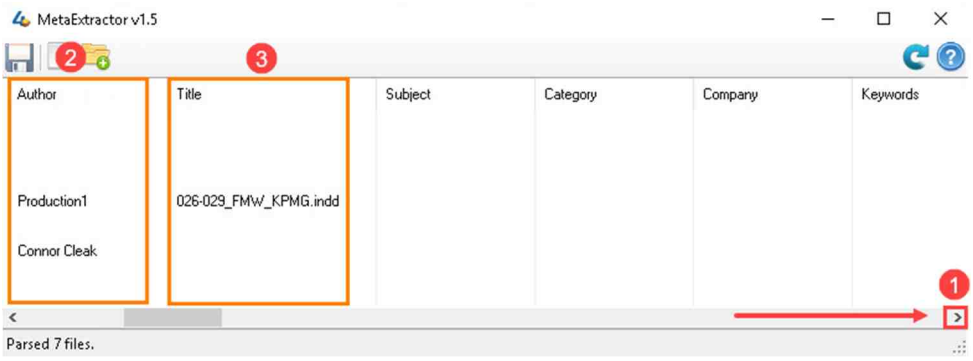
4. Let us move further to the right by clicking the arrow button on the horizontal scroll bar as highlighted below in item 1. Stop scrolling once you get to the File Name column, item 2 below.



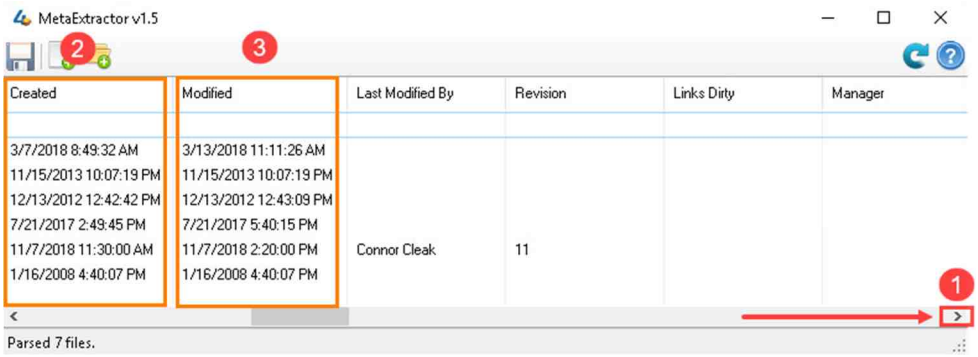
5. The File Name column lists the name of the file while the File Path column, beside it, details the path that the files are currently located at. These are highlighted as items 1 and 2. Please note that the File Path field should not be used if you exported the files, since it will list the path on your workstation/working directory. The File MD5 column, seen in item 3, lists the MD5 hash value for each file and can be used to help determine the uniqueness of a file.



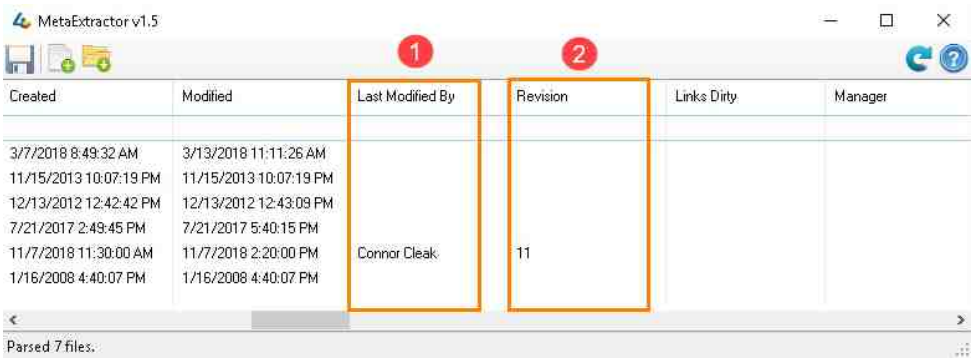
6. Let us scroll further to the right and stop at the column called Author as seen in item 1. The Author metadata, as seen in the column in item 2, is very interesting in that it can contain the name of the user that created the file. This is most often found in Microsoft Office documents but can be found in PDF files and other document types as well. As seen in the Author column below, there were only 2 authors parsed from the 7 files, Production1 and Connor Cleak. The next column, seen in item 3, is called Title and lists the document's title. As you can see in the screenshot below, there is only one document title that was parsed, which is 026-029_FMW_KPMG.indd. Based on the extension .indd in this title, we can deduce that the PDF file called kpmg-feature-sep-2010.pdf was created from a file called 026-029_FMW_KPMG.indd using Adobe InDesign.



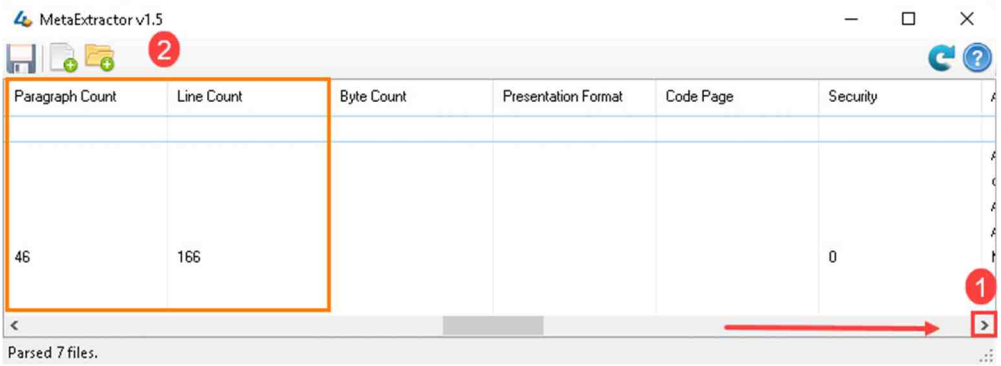
7. Let us keep scrolling to the right until we get to the column called Created, using the arrow icon as seen in item 1. The Created column, as seen in item 2, lists the embedded creation dates of the files. This metadata will tell you when the file was originally created as compared to the file system metadata, which tells you when the file was placed on the volume. Highlighted as item 3 is the Modified column and this metadata is embedded as well. This means it will show the last time the file was saved. If you compare the creation and modified dates in these 2 columns with the file system creation and modified dates, you will see that they are conflicting. In this case, the embedded metadata is more trustworthy and reliable as it is not as easy to manipulate. The difference between the dates and times in these files indicate that there was some manipulation with the computer system dates and times. Hints like these can often make or break a case.



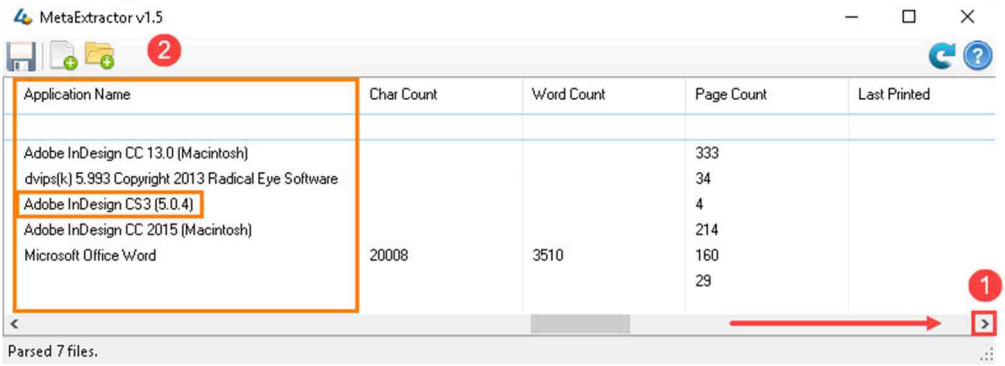
8. Let us look at the Last Modified By column highlighted as item 1 below. This is another type of embedded metadata and gives the name of the user that last modified the file. In this example, the file that was created on November 7, 2018 at 11:30 AM was last saved by a user called Connor Cleak on November 7, 2018 at 2:20 PM. The column to the right of this one, called Revision, as seen in item 2 below, highlights the number of "revisions" that the documents has had; it can be useful in determining a file's authenticity.



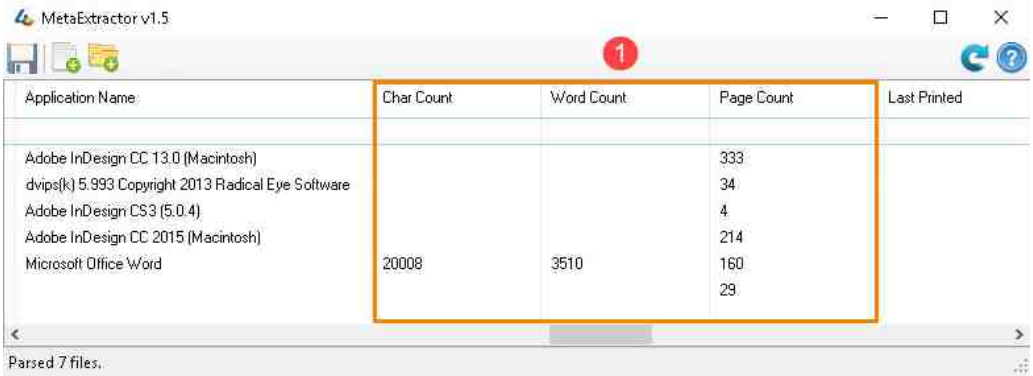
9. Let us scroll further to the right, as highlighted in item 1 below, until we get to the columns called Paragraph Count and Line Count. As seen in item 2 below, these columns list the number of paragraphs and the number of lines within a document.



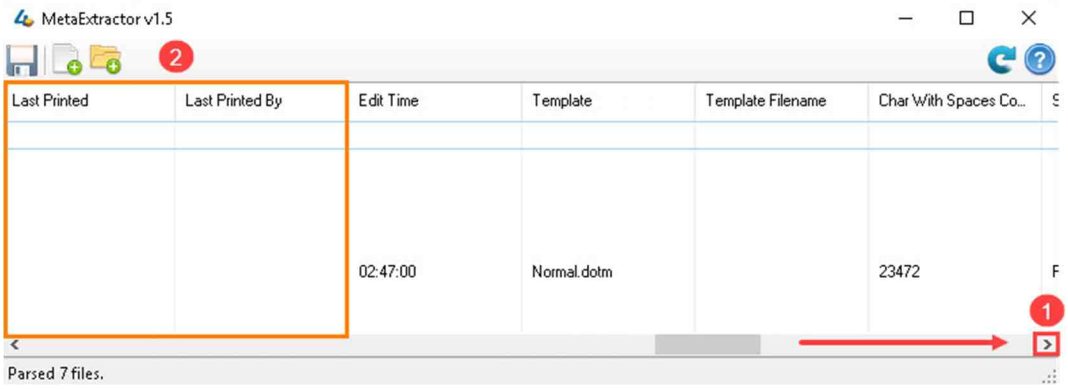
10. Let us scroll once more until we get to the column called Application Name as seen in item 1 below. This column lists the name of the program that last edited the file. As you can see in item 2 below, the PDF file with the value in the Title column (on page 46, step 6, item 3) was indeed created by Adobe InDesign. This is useful information to help trace the origins of files.



11. The next 3 columns to the right are Char Count, Word Count and Page Count as seen in item 1 below. These columns list the number of characters, words, and pages within documents.

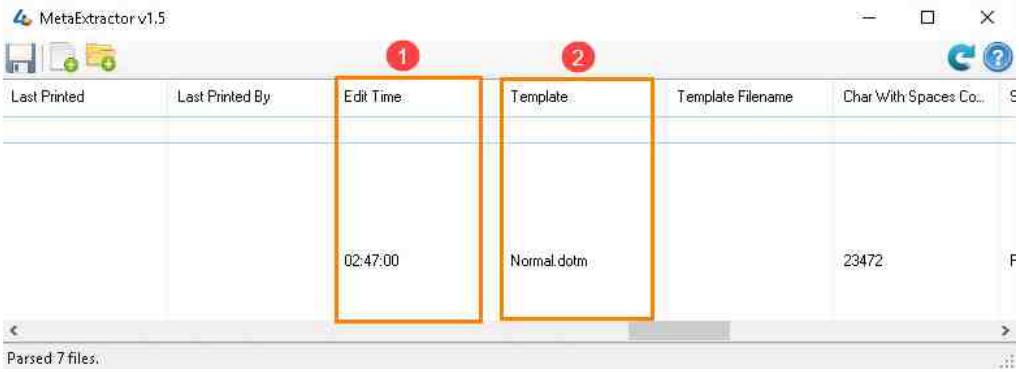


12. Let us scroll to the right once more and stop at the Last Printed column as seen in item 1. If the Last Printed and Last Printed By columns in item 2 were populated, we could learn the last time the document was printed and the name of the user that printed it.



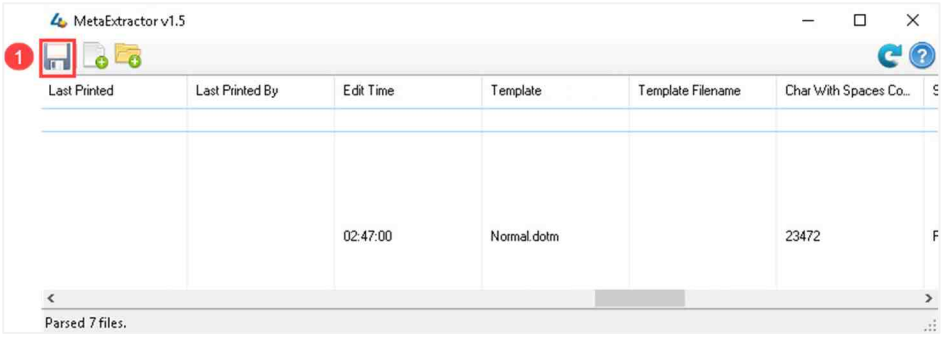
Please Note Even though there is no data there, it does not mean the document was never printed. It simply means that there is no record of it inside.

13. Let us look at a few more columns. The next column, seen in item 1, is called Edit Time and this details the total time the document was open in Edit mode. The next column, seen in item 2, is called Template and it contains metadata that tells us whether the document was created from a template and lists the name of the template.



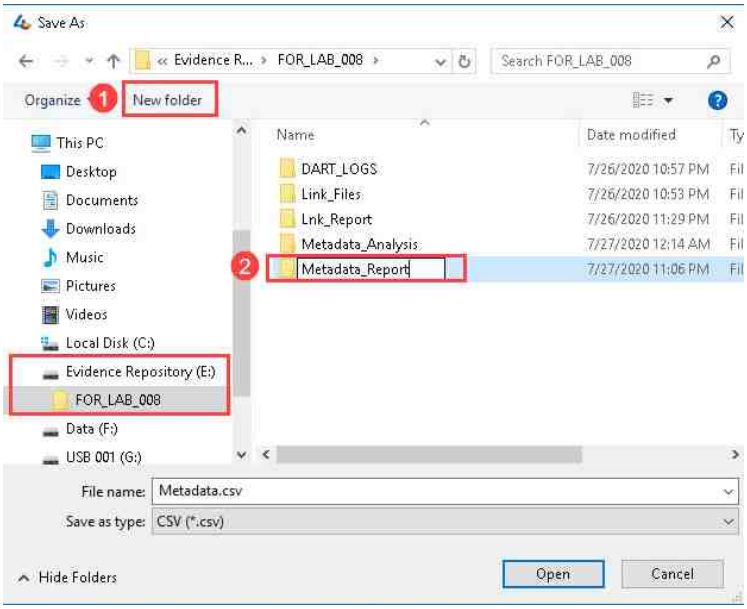
14. There are many other columns that contain valuable data and may apply to different cases and different types of files. Be sure to scroll all the way to the last column to see the different types of metadata you can find. This knowledge will help you form better opinions in your forensic examinations.
15. Some of the metadata may not be extracted by this tool, and as such, you can manually check the files by accessing their properties from within the programs designed to open them. You can also access some metadata by looking at the Details tab in the Windows Properties window. This can be accessed by right-clicking on the file and clicking Properties from the dropdown menu.

16. Now let us save the metadata we have extracted as a CSV file. Click Save to CSV toolbar icon as seen in item 1. The Save As window will appear.

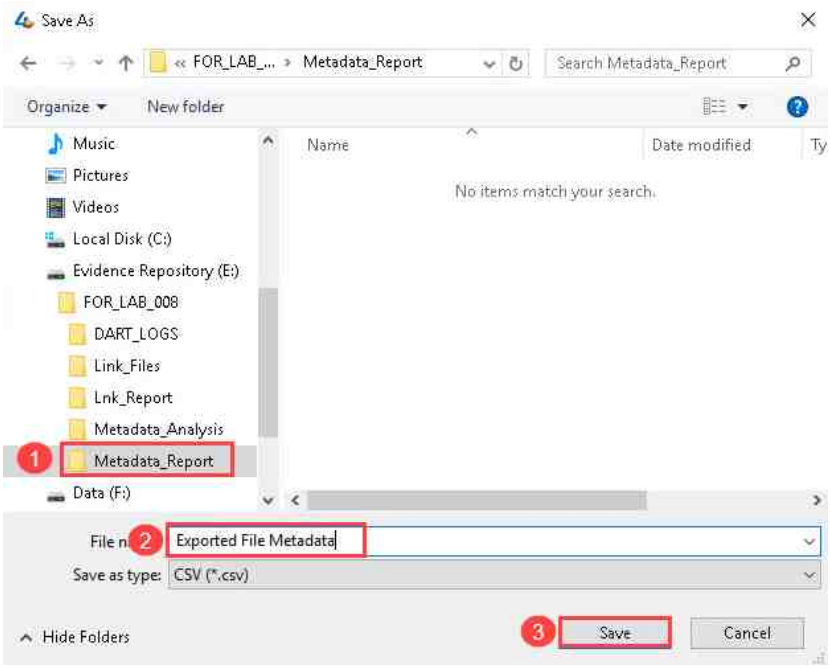


The Save to CSV option will save the entire table as a CSV file so you don't have to worry about selecting each entry.

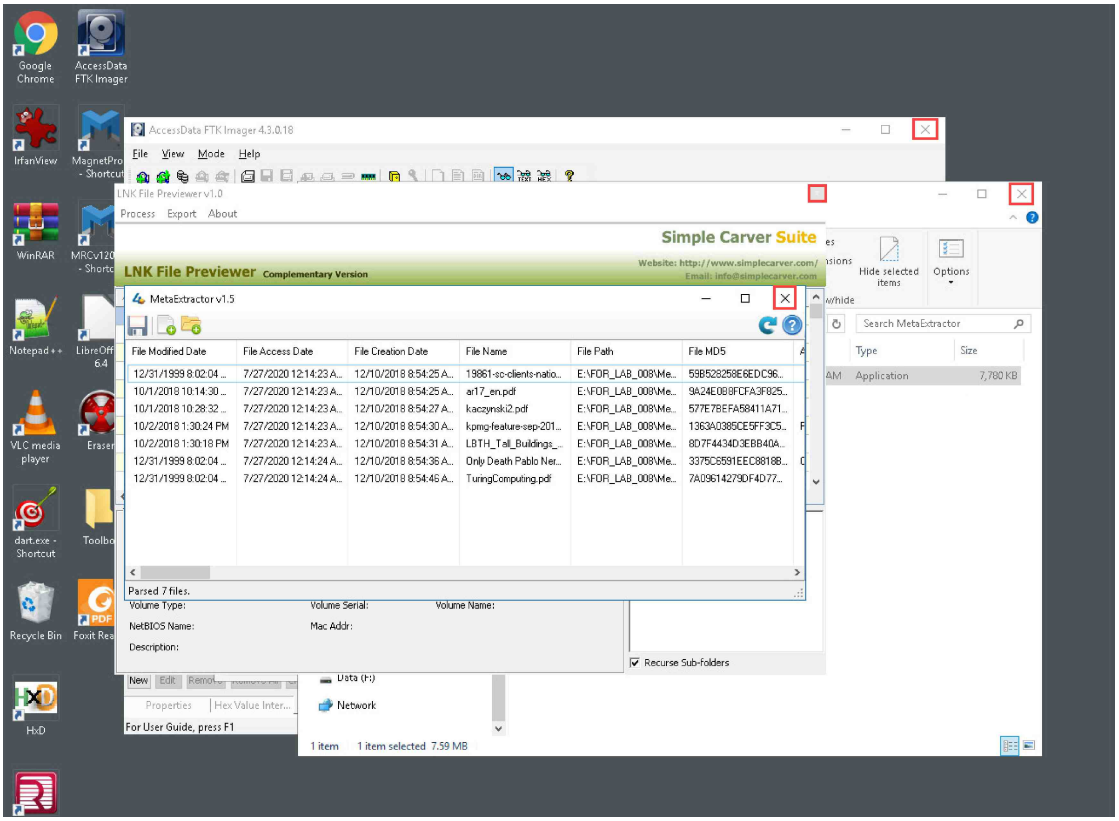
17. In the Save As window, browse to the folder we created earlier called FOR_LAB_008 by navigating to This PC > Evidence Repository (E:) > FOR_LAB_008. Once there, create a new folder by clicking the New folder toolbar icon as highlighted in item 1 below and name the new folder `Metadata_Report` as seen in item 2 below.



18. Click the Metadata_Report folder you just created to open it, as seen in item 1. Once inside the folder, type `Exported File Metadata` in the File Name field and then click Save as highlighted in items 2 and 3 below.



19. Now that you have stored that file, you have completed the exercise and the lab. Now that the exercises are complete, close each open window by clicking the X at the top-right corner of each one.



20. In this lab, you learned how to export and analyze link files and embedded metadata. You were also exposed to the difference between file system metadata and other types of data that are not readily available. This information can often tie up loose ends or find hidden and manipulated data. Hence, understanding where to find it and how to interpret it is extremely valuable.
21. Close the remaining windows by clicking the X at the top-right corner of the windows to complete the lab.

