FTK IMAGER & MINITOOL POWER DATA RECOVERY SOFTWARE VALIDATION REPORT

NOVEMBER 13, 2024

EXAMINER: YAIR RAYO

Table of Contents

Section 1: Executive Summary

1.1 Background

Validating forensic software is vital to ensure the reliability and accuracy of results in digital forensic investigations. Legal courts require forensic tools to produce consistent, defensible outcomes, as unsupported claims of reliability are insufficient. Validation helps identify limitations, potential errors, and systematic issues, indicating that the tool meets the requirements of the inquiry and adheres to industry standards. By testing tools against known datasets and comparing outputs, investigators can confidently rely on their findings in legal and professional contexts,

1.2 Objective

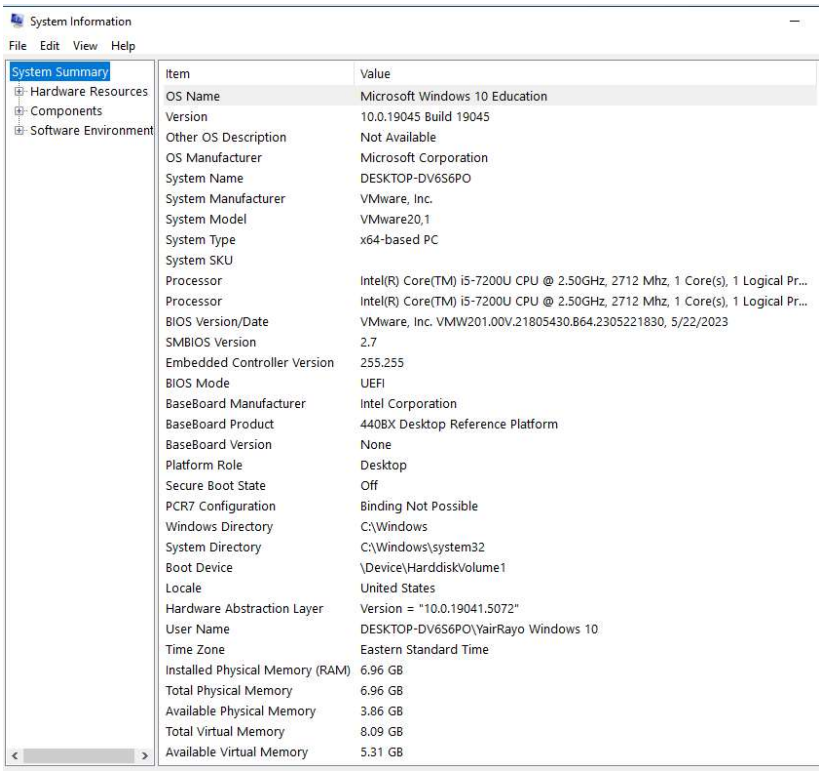
This validation test purpose is to compare the performance of *FTK Imager* (the "known good" tool) with *MiniTool Power Data Recovery* (the "new tool") in recovering 3 deleted files from a USB drive. By analyzing and comparing the results of both tools, we seek to determine if the new tool performs reliably, accurately, and as expected. I will utilize *QuickHash-GUI* to verify the integrity of recovered files through hash comparisons. What is a hash? The simplest explanation is that it is like a unique fingerprint of digital data. The process is documented step-by-step to ensure repeatability using a Windows 10 machine as the host environment.

Section 2: Hardware and Software Setup

2.1 Hardware Used

Host Machine:

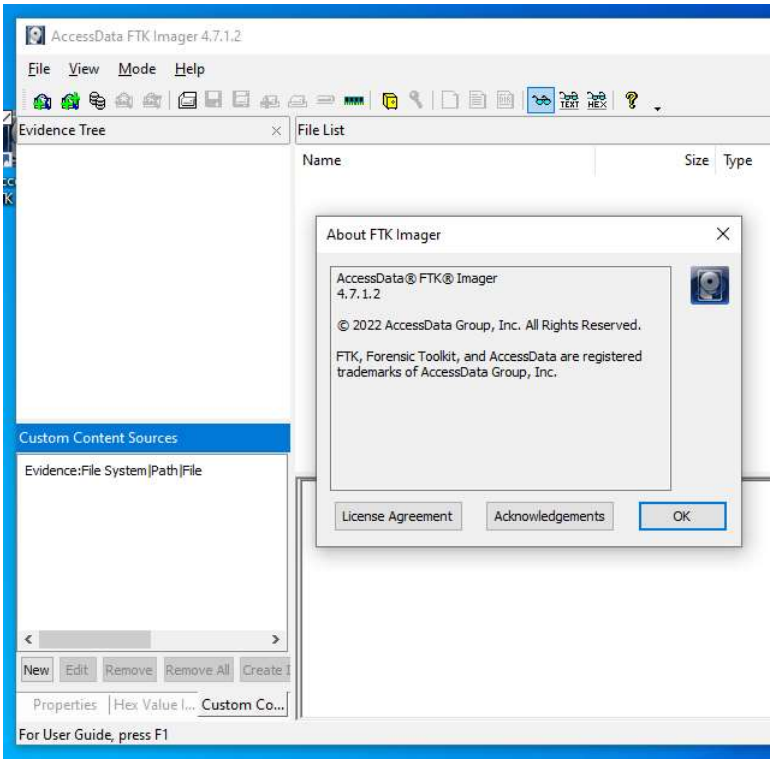
- Windows 10
- Intel® Core™ i5-7200 CPU @ 2.50GHz
- 6.96 RAM (Random Access Memory)
- 64-bit operating system, x64-based processor



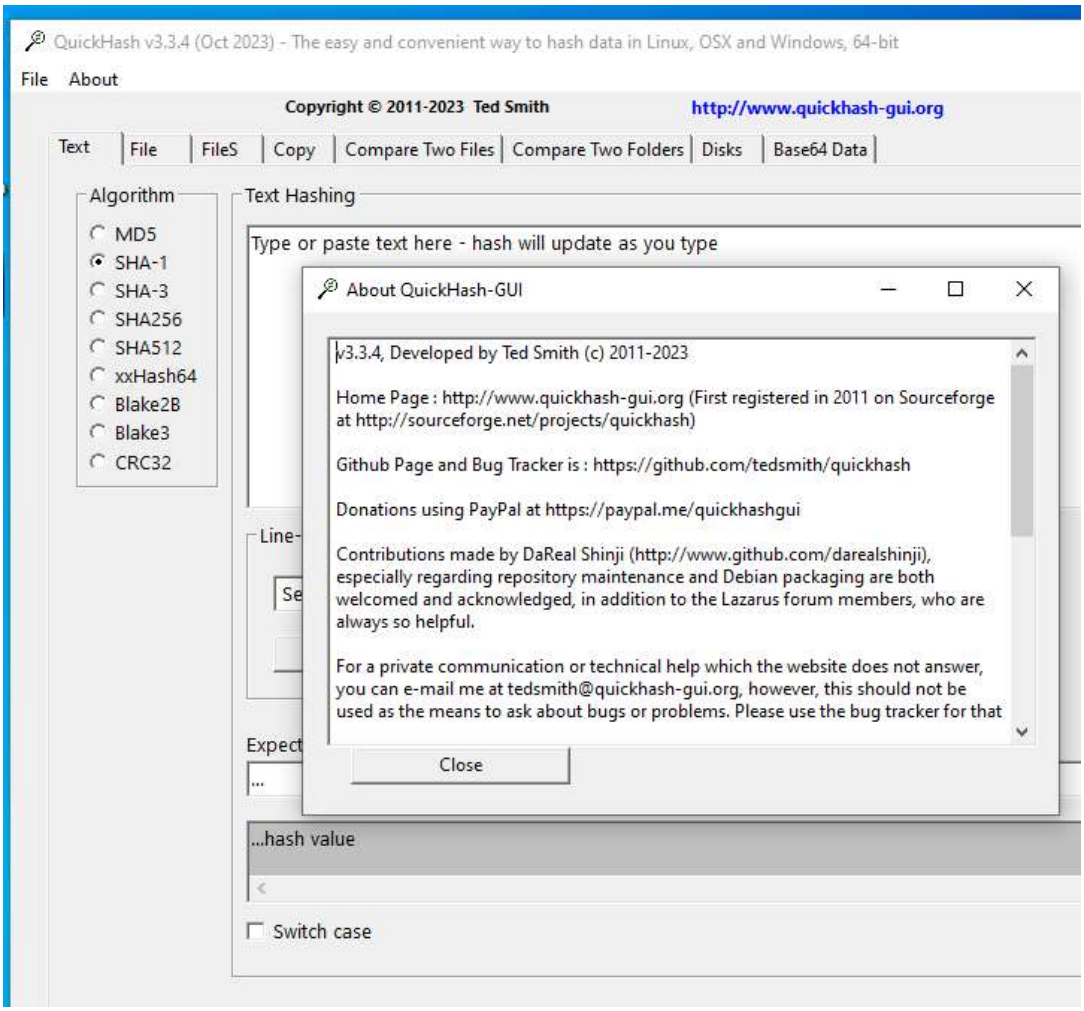
2.2 Software Used

All software used to conduct this examination are open-source.

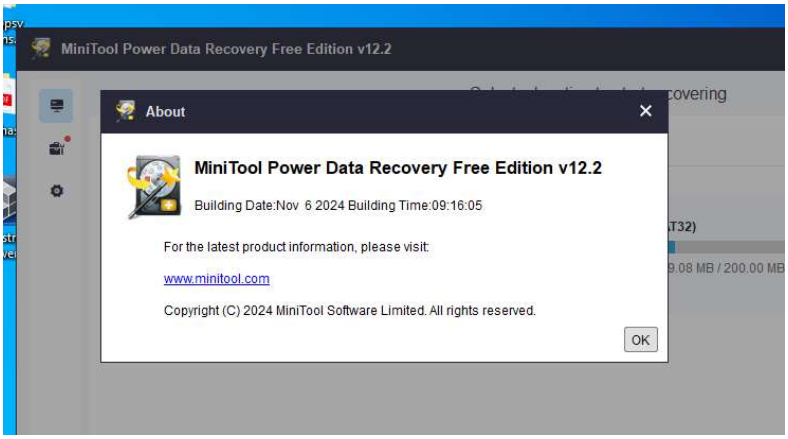
- AccessData Forensic Toolkit Imager (FTK Imager) v4.7.1.2



- Quickhash-GUI v3.3.4 for Windows



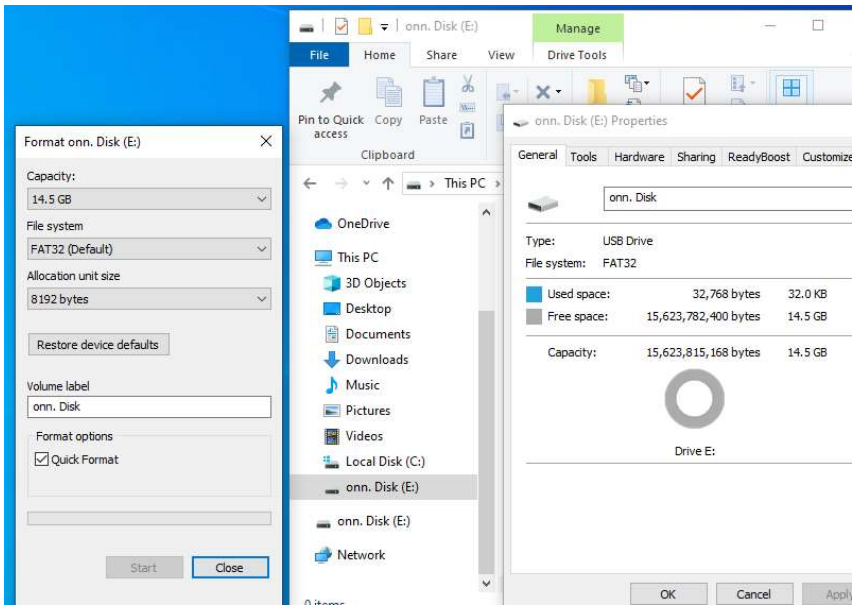
- MiniTool® Data Recovery v12.2 for Windows



2.3 Prepare Dataset and Storage

Use a Universal Serial Bus (USB) drive to store the test datasets. For my validation test, this is what I used:

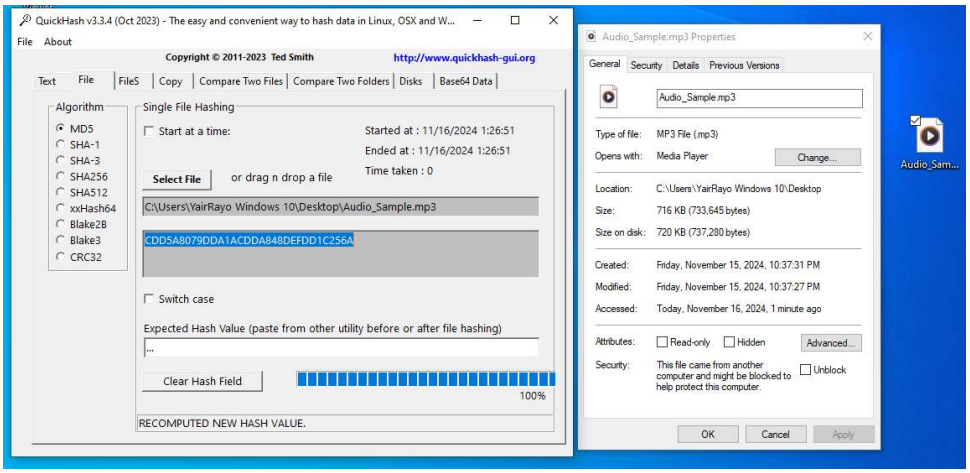
- Brand: onn.
- Capacity: 16 GB, with 14.5 GB of free space
- Model: 100140020
- Weight: 0.02 Pounds
- Dimensions (L x W x H): 2.36 x 0.87 x 0.44 inches
- File system: FAT32



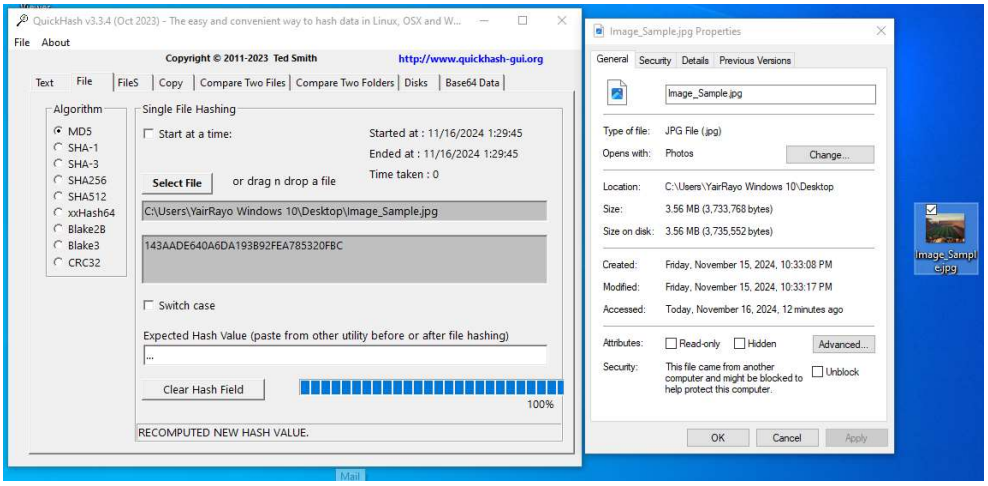
*To find details and format options for a drive in Windows, go to File Explorer, hover over the USB drive, left click on the USB drive, and select 'Properties'/'Format' to find this data.

Use 3 files as datasets. To find the properties data of a file on Windows, hover over the file, right click, and select 'properties'. To hash each file, open Quickhash-GUI, select 'File' from the options, select 'MD5' from the 'Algorithm' option, and drag/drop the desired file within the 'Select File' button. At this point, Quickhash-GUI will automatically generate the hash value within the window visible above the 'Switch Case' button. In my test, I used the following:

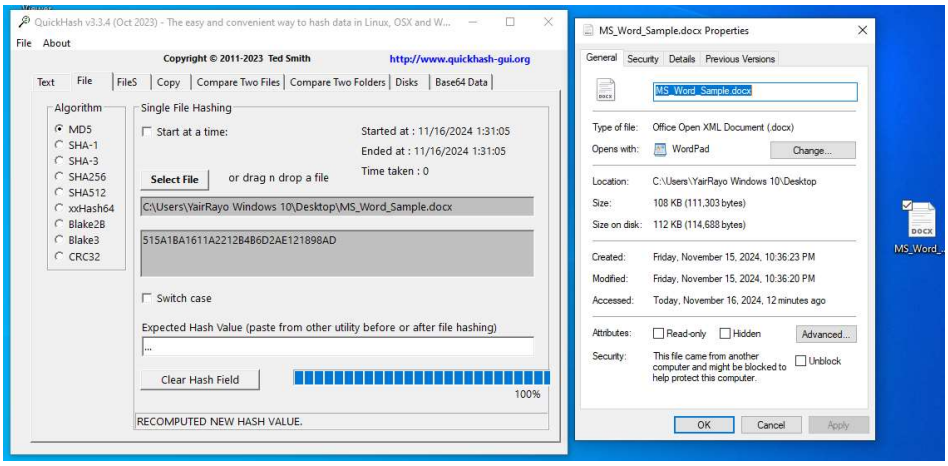
- One file called: Audio_Sample.mp3
  - Size on disk: 720 KB (737,280 bytes)
  - Type: MP3 File (.mp3)
  - MD5 hash: CDD5A8079DDA1ACDDA848DEFDD1C256A



- One file called: Image_Sample.jpg
  - Size on disk: 3.56 MB (3,735,552 bytes)
  - Type: JPG File (.jpg)
  - MD5 hash: 143AADE640A6DA193B92FEA785320FBC

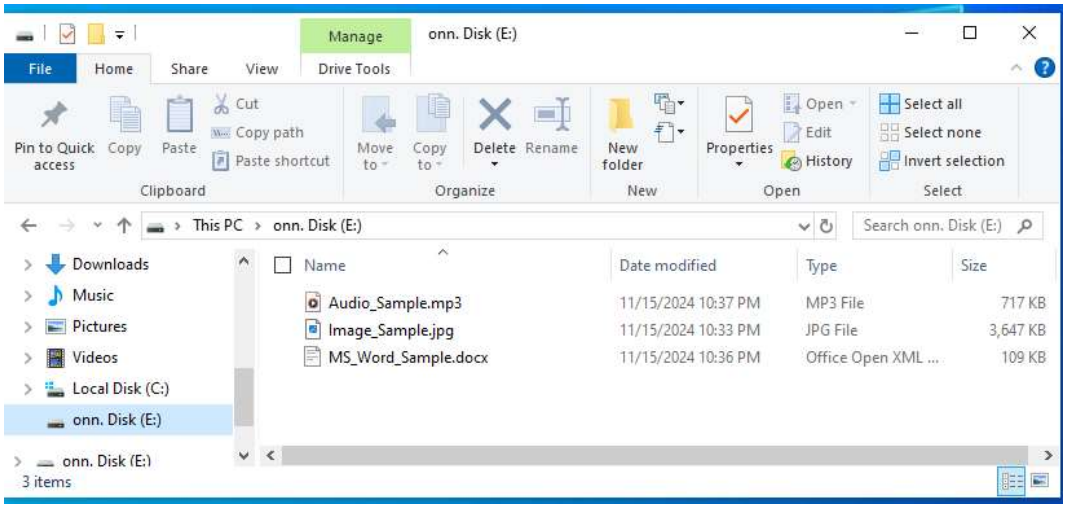


- One file called: MS_Word_Sample.docx
  - Size on disk: 112 KB (114,688 bytes)
  - Type: Office Open XML Document (.docx)
  - MD5 hash: 515A1BA1611A2212B4B6D2AE121898AD

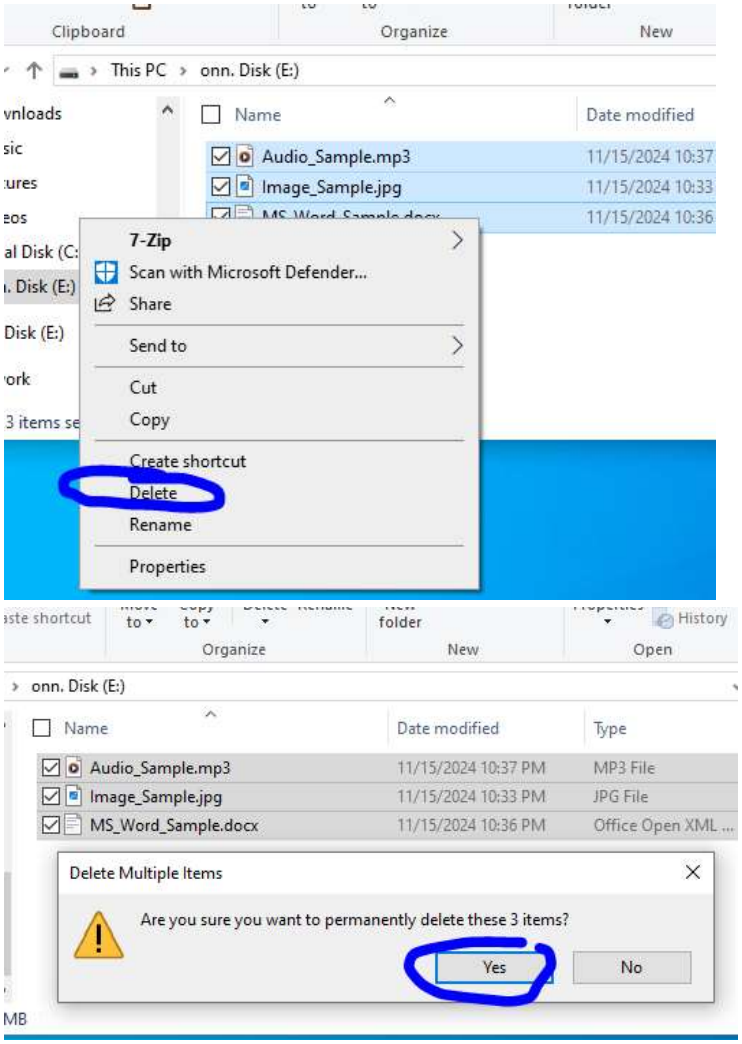


At this point, do the following with the 3 files and the USB drive:

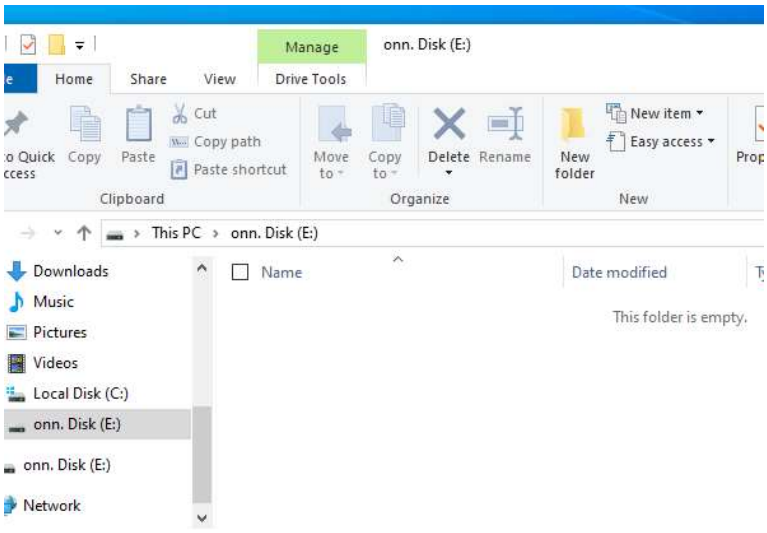
- Cut and paste all 3 sample files (*Audio_Sample.mp3*, *Image_Sample.jpg*, and *MS_Word_Sample.docx*) into the USB drive you are using



- Next, select all 3 files, right click over the selected files, click ‘Delete’. On the next warning ‘Delete Multiple Items’ box, click ‘Yes’



- At this point, you should see an empty USB drive with no apparent content



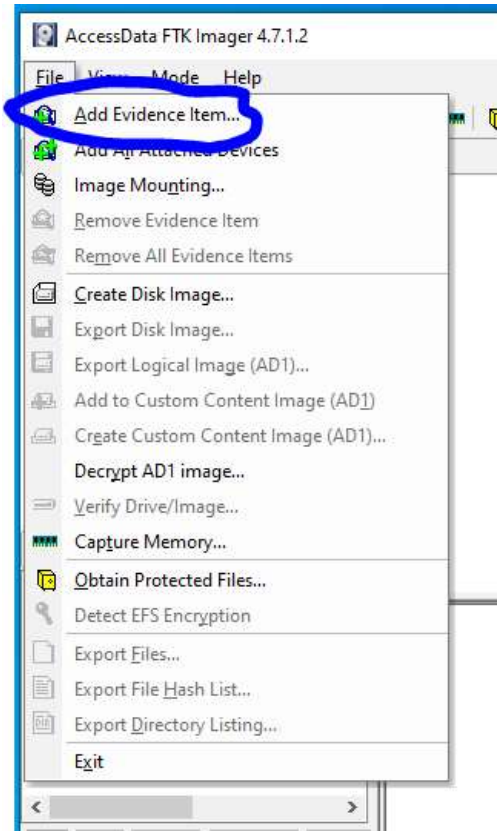
Now we are ready to continue with the actual validation of each software. First, we will perform recovery with *FTK Imager* (known good tool). Second, we will perform recovery with *MiniTool Power Data Recovery* (new tool).

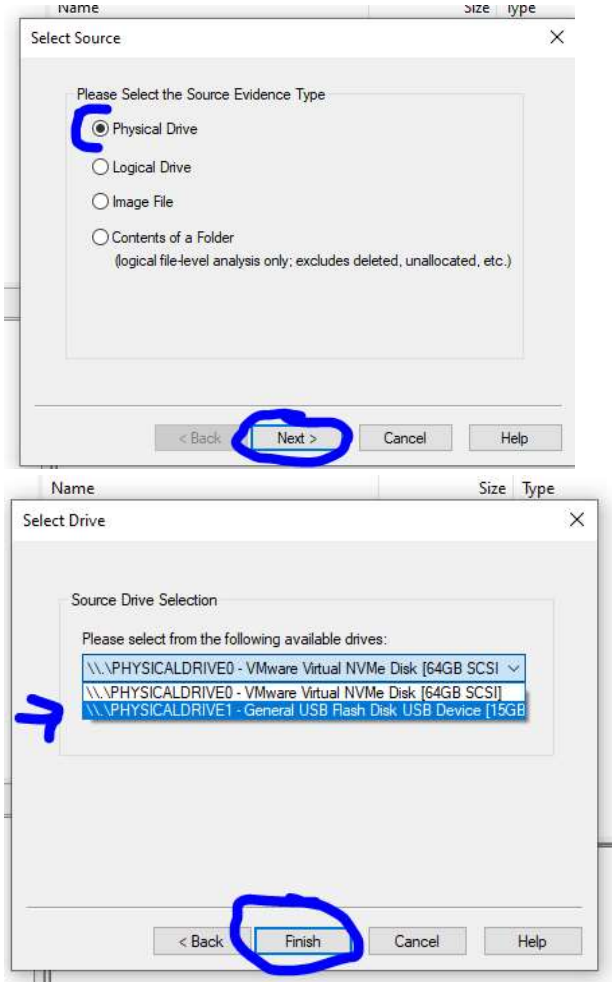
Section 3: Perform Recovery with FTK Imager (Known Good Tool)

3.1 Adding Evidence

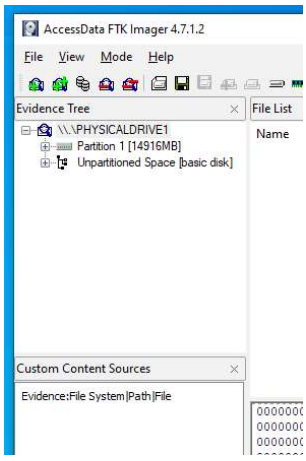
To successfully add your USB drive as evidence, follow these steps in order:

- Open FTK Imager and select *File* > *Add Evidence Item* > Choose *Physical Drive* and click *Next* > From dropdown options, choose your USB Drive and click *Finish*





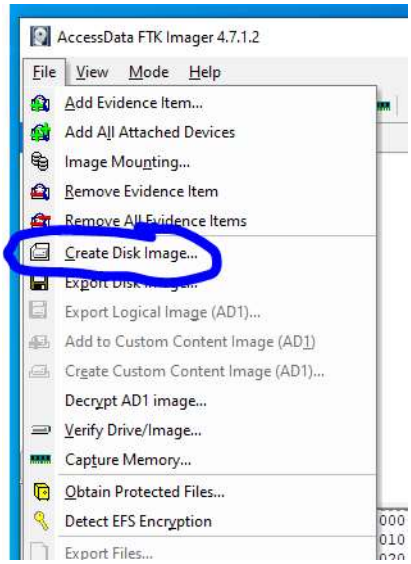
- At this point you will see you USB drive added as an evidence item within the Evidence Tree of FTK Imager. We are now ready to create a disk image of this USB drive:



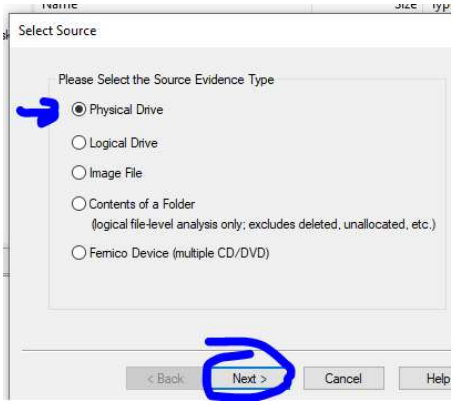
3.2 Create a Disk Image

To generate a disk image of this USB drive, follow the instructions in order:

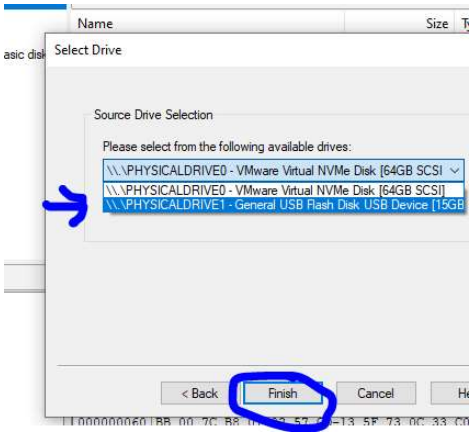
- Go to *File* > *Create Disk Image*



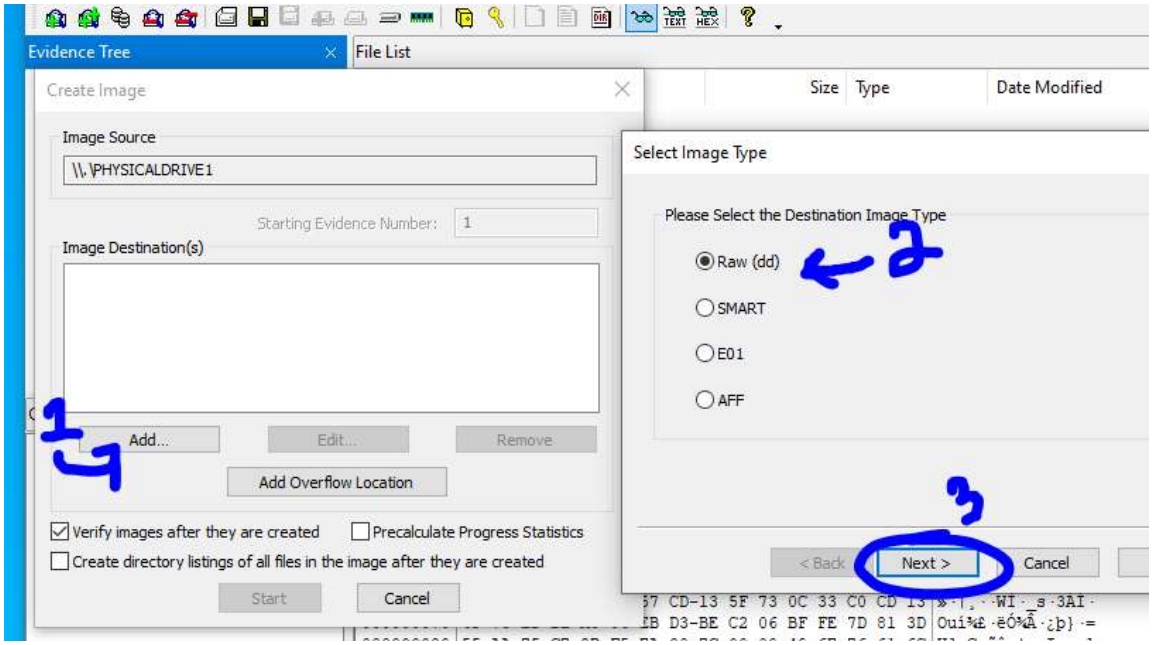
- Choose *Physical Drive* and click *Next*

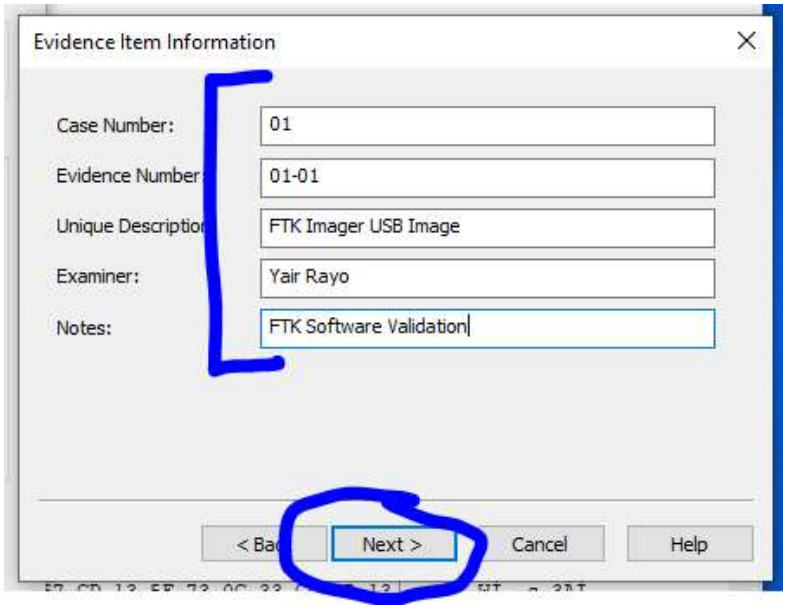


- From the *Select Source window*, go to the drop down menu and select your USB drive

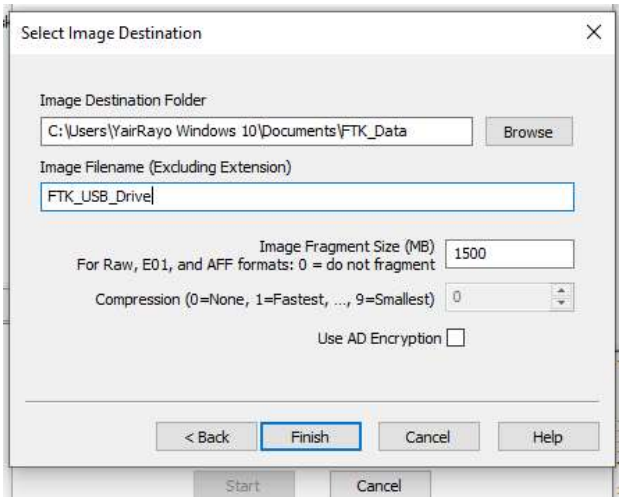


- In the next *Create Image window*, click on *Add…* > Select *Raw (dd)* as the image format and click *Next* from the *Select Image Type* window. In the *Evidence Item Information* enter pertinent information > Click *Next* which takes you to the *Select Image Destination* window

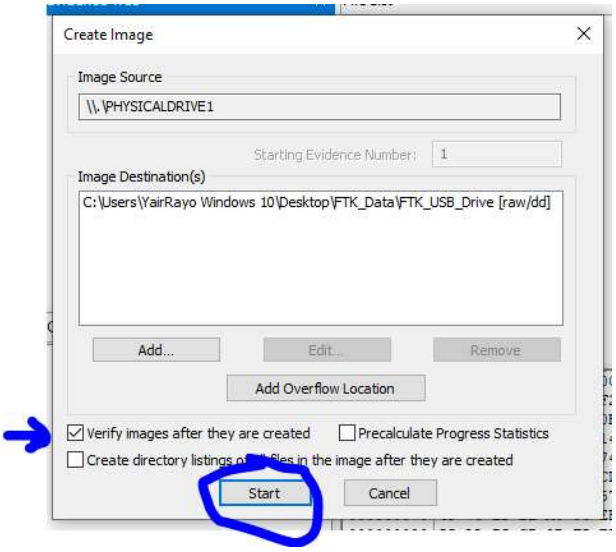




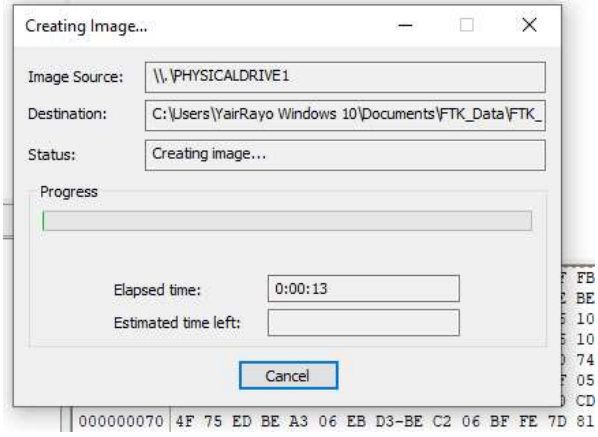
- From the *Select Image Destination* window, browse your image destination, name you image, set fragmentation to default, and click *Finish*



- You will now be returned to the *Create Image window*. Here, manually check and enable the option *Verify images after they are created*, and click on *Start*



- Start the imaging process and document the time taken

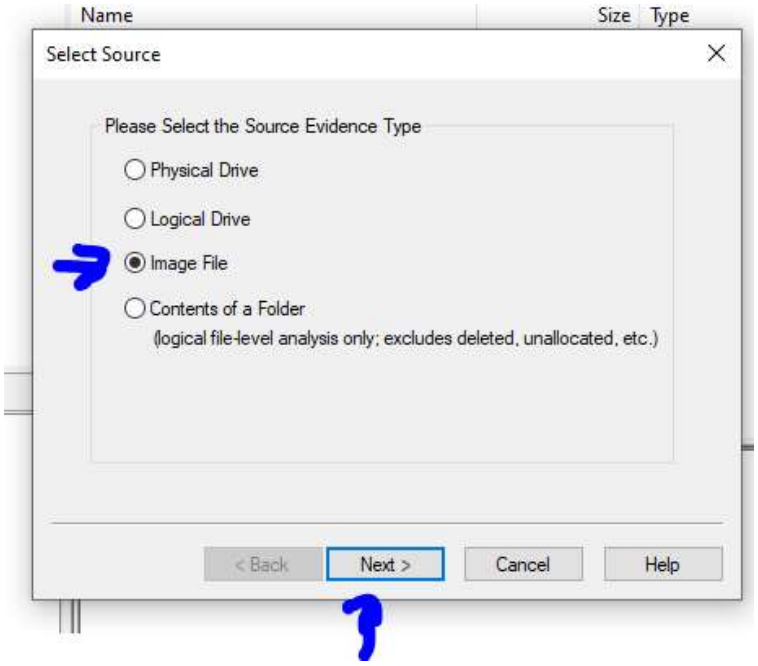


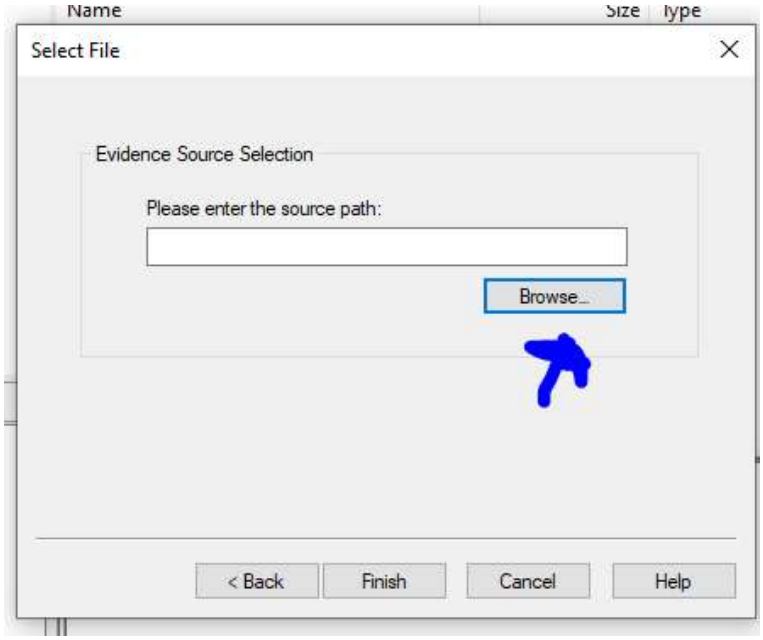
- Once the imaging process is completed in FTK Imager, a message will appear will a confirmation

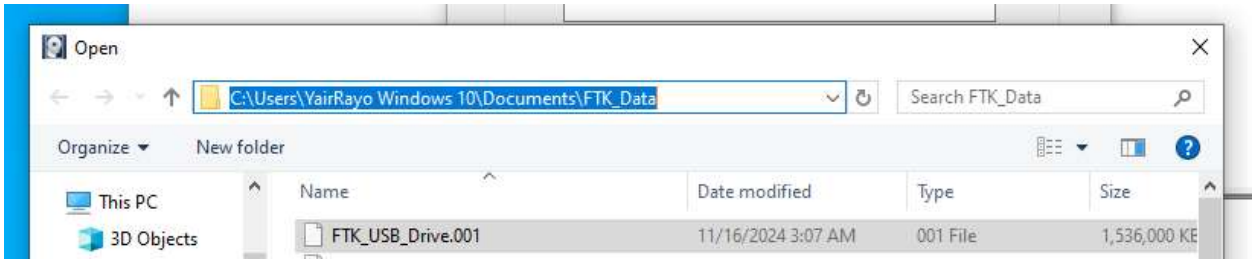
3.3 Recover Deleted Files in FTK Imager

Load the created disk image back into FTK Imager. Locate the saved disk image from the previously saved location above:

- In FTK Imager, click on *File* > select Add Evidence Item... > from the *Select Source* window, select *Image File* and click *Next* > from the *Select File* window, click *Browse*... > locate and select the image file FTK image generated. In my case, it is located in path "C:\Users\YairRayo Windows 10\Documents\FTK_Data\FTK_USB_Drive.001"

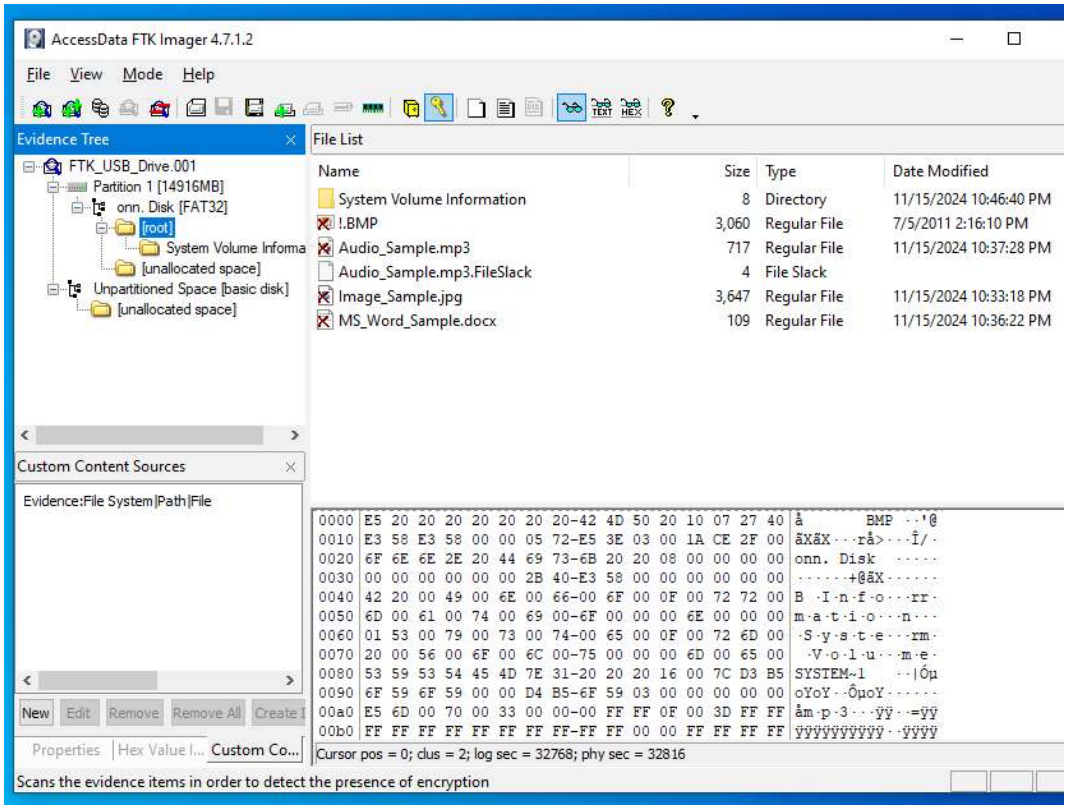






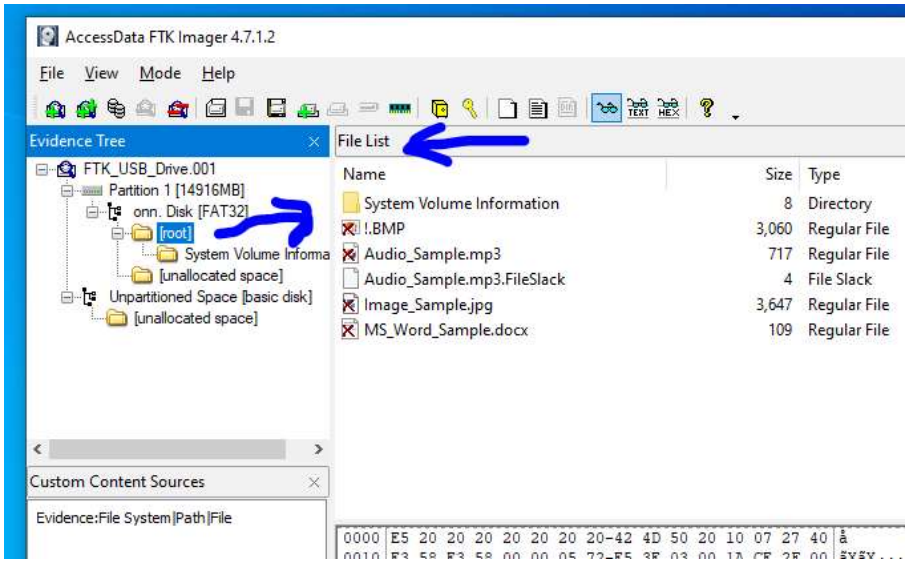
- Once you select your directory you will be redirected back to *Select File* window. Click *Finish*. In FTK Imager, you will now be able to see your *Evidence Tree* filled

with data from the image drive you just uploaded. Do not close FTK Imager. Now it's time to search for the 3 deleted files.

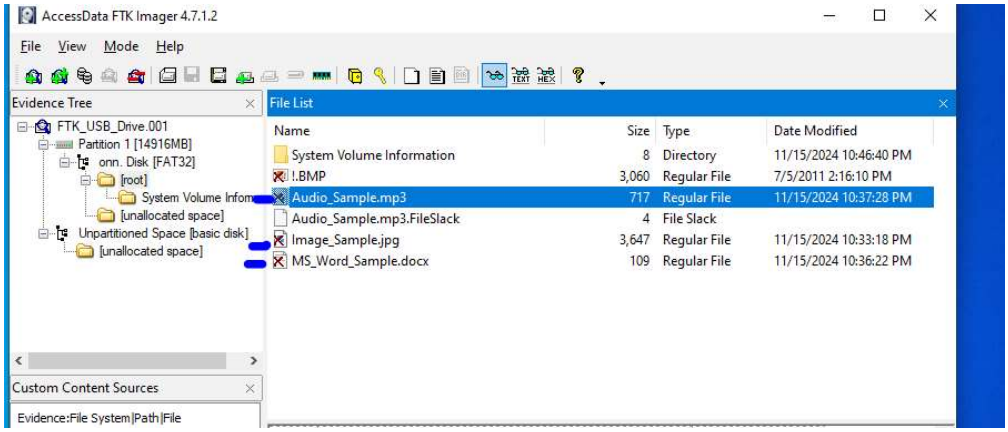


Now that our image drive is loaded into FTK Imager, we can proceed to search, recover, export, and save the 3 deleted files we are interested in. To accomplish this, follow these steps:

- In FTK Imager, go to *Evidence Tree*, drop down all child directories within the main directory. My main directory is *FTK_USB_DRIVE.001*. Find a *[root]* directory and select to see *File List* content to the right. Yours may have data but will look something like this.

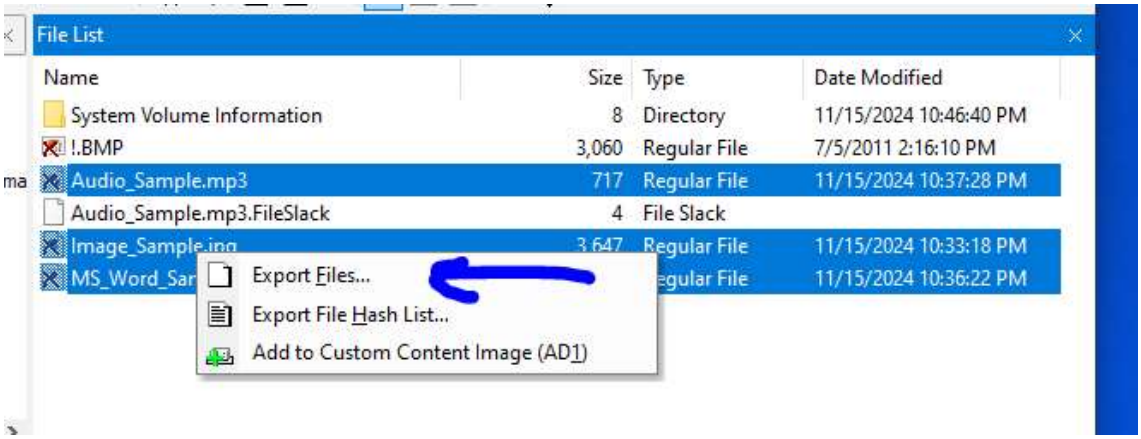


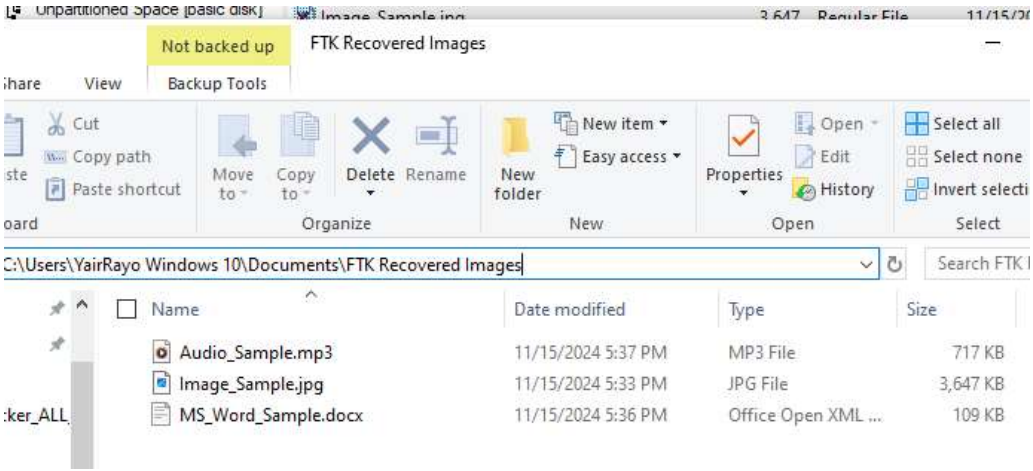
- From the *File List* window, you will see a list of directories and files the system found. Notice that there are four files that have a red '*x*' on it. This means FTK Imager has found 4 files that were deleted but recoverable. Of those 4 files, 3 files are the ones we are looking for, which are *Audio_Sample.mp3*, *Image_Sample.jpg*, and *MS_Word_Sample.docx*. In your case, look for your deleted files and identify them throughout this or other directories.



- Select all 3 files (in your case the files that apply to you) in FTK Imager by holding the 'ctrl' button while clicking on all 3 images to have all 3 files selected.

- Hover over one of the 3 highlighted images and right click with mouse. *Select Export Files…* and save to a location on your local host machine. In my case I saved the images to path "C:\Users\YairRayo Windows 10\Documents\FTK Recovered Images"





With the recovery of 3 previously deleted files complete, we will now verify their integrity using QuickHash-GUI. By comparing the current MD5 hashes of the recovered files with the original hashes generated earlier, we can confirm whether the recovered files are identical to the original images that existed before deletion.

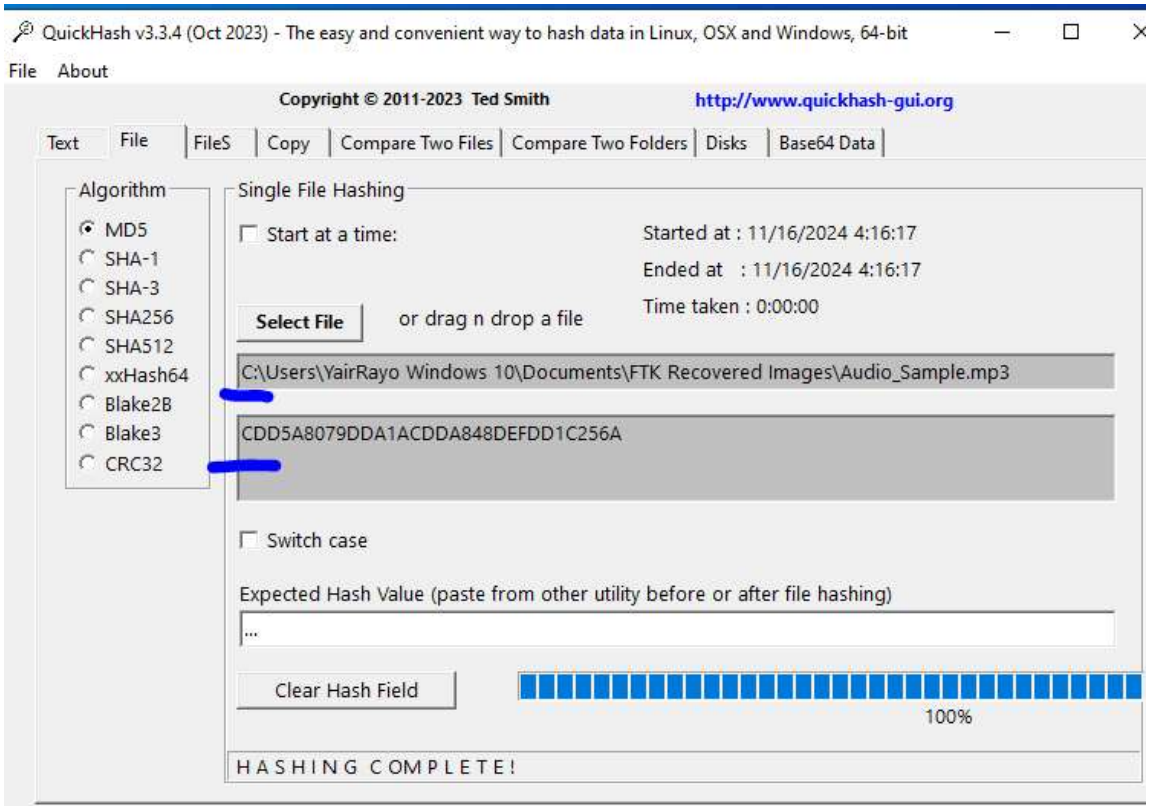
3.4 Verify Results with QuickHash-GUI

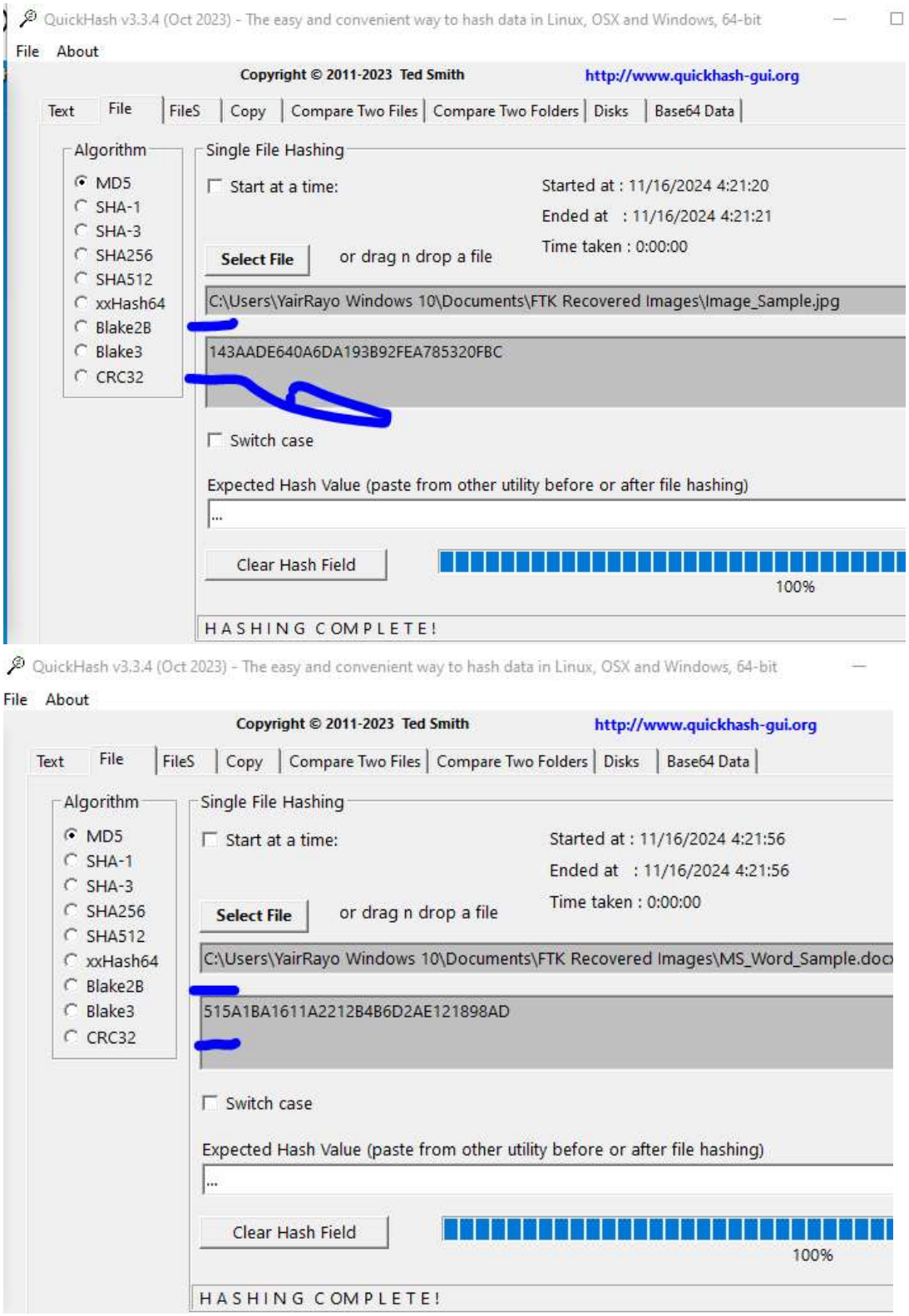
We will launch *Quickhash-GUI* and generate hashes of the 3 recovered files to later compare these hashes in our concluding report and opinion. Follow these steps:

- Open *Quickhash-GUI* and select the *Files* tab. Select 'MD5' from the 'Algorithm' option and drag/drop the desired file one-by-one within the 'Select File' button. At this point, *Quickhash-GUI* will automatically generate the hash value within

the window visible above the ‘Switch Case’ button. Do this process for all 3 files we recovered.

- Hash *Audio_Sample.mp3* file: CDD5A8079DDA1ACDDA848DEFDD1C256A
- Hash *Image_Sample.jpg* file: 143AADE640A6DA193B92FEA785320FBC
- Hash *MS_Word_Sample.docx* file: 515A1BA1611A2212B4B6D2AE121898AD





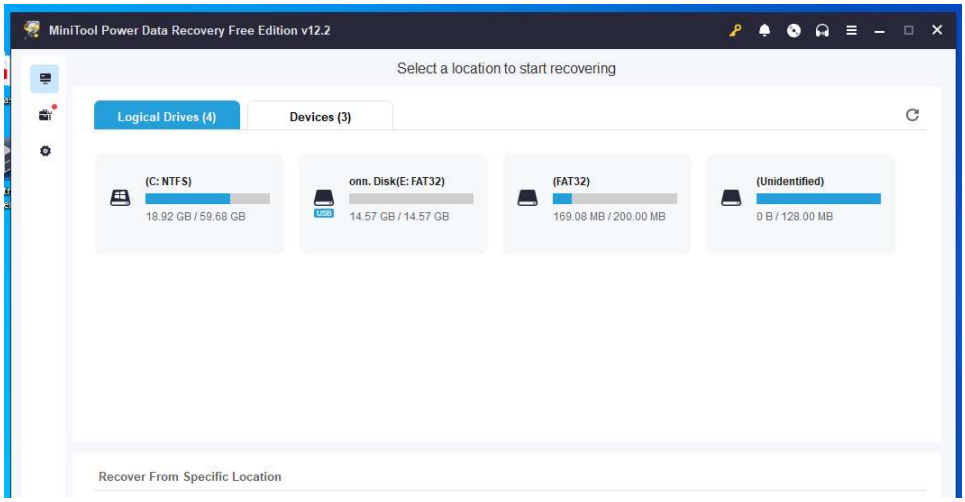
Now let's move on to recovering, finding, exporting, and savings these 3 deleted files from our MiniTool Power Data Recovery (New Tool). The process

Section 4: Perform Recovery with MiniTool Power Data Recovery (New Tool)

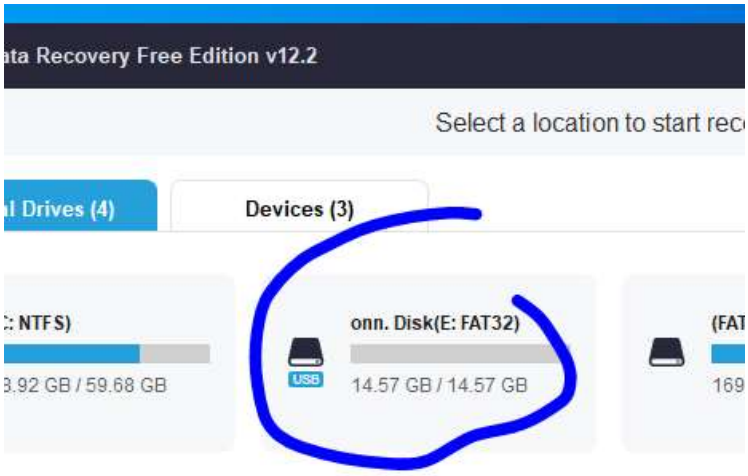
4.1 Add, Recover, and Export Deleted Files

For this portion, we will redo the same process we did with FTK Imager, but now with our 'New Tool'. Follow these instructions:

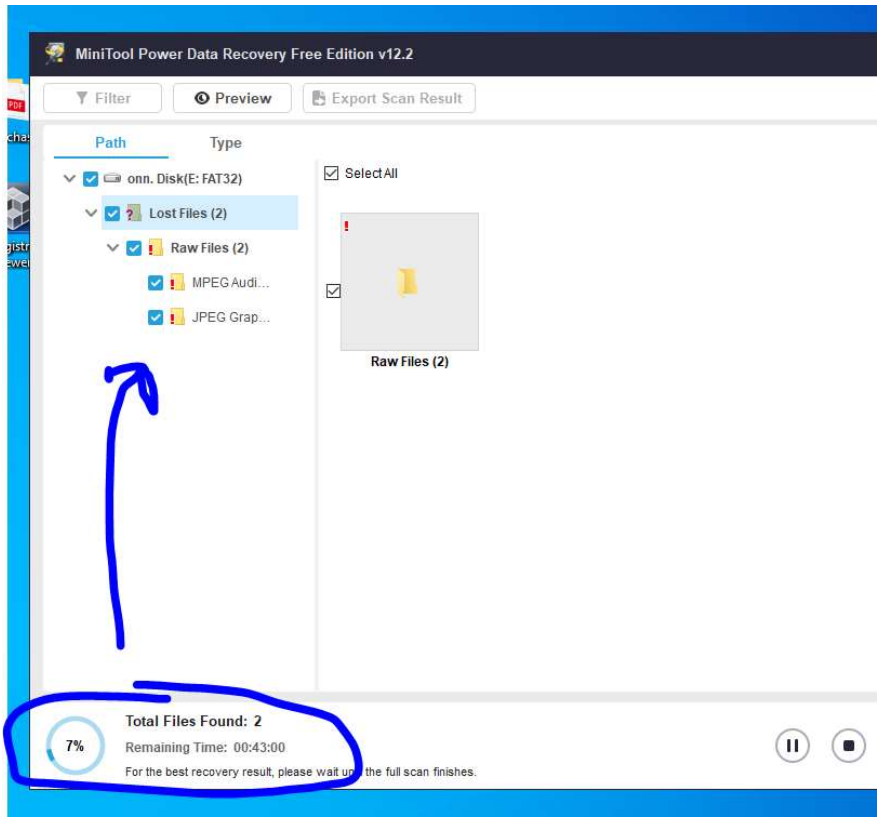
- Launch MiniTool Power Data Recovery



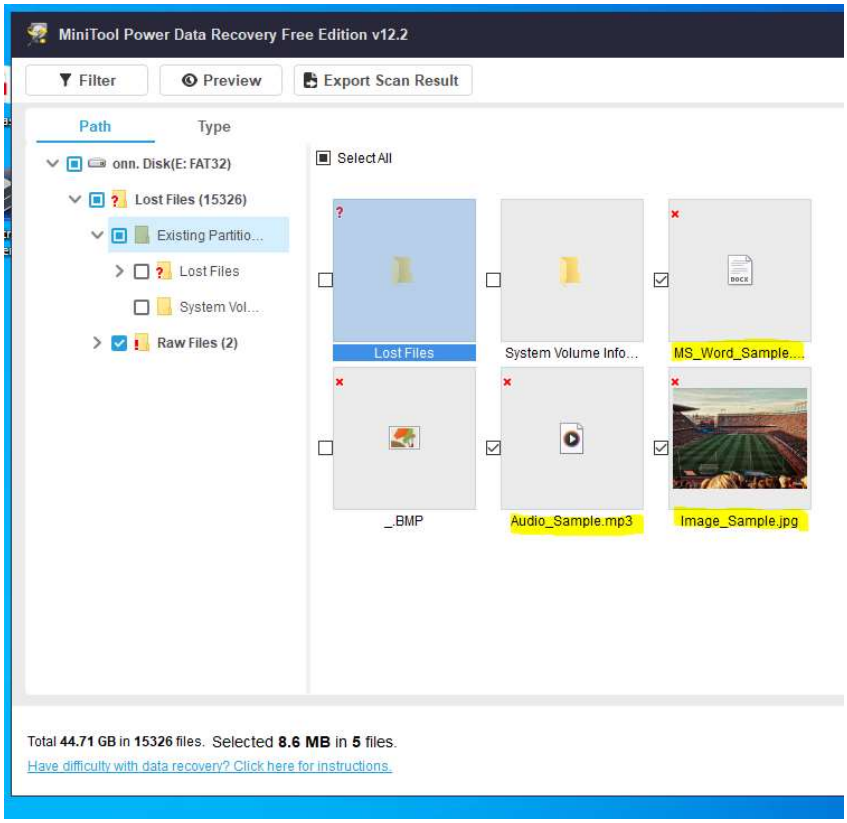
- Open the tool and select the appropriate Disk Drive from the main interface. In my case, it's called *onn. Disk(E: FAT32)*. Hover over the drive and click on *Scan* button



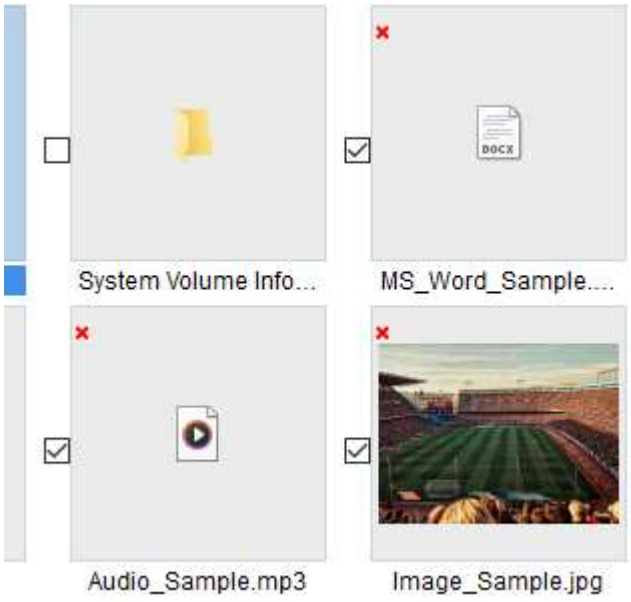
- At this point, allow for MiniTool Power Data Recovery to finish the scanning of the USB drive



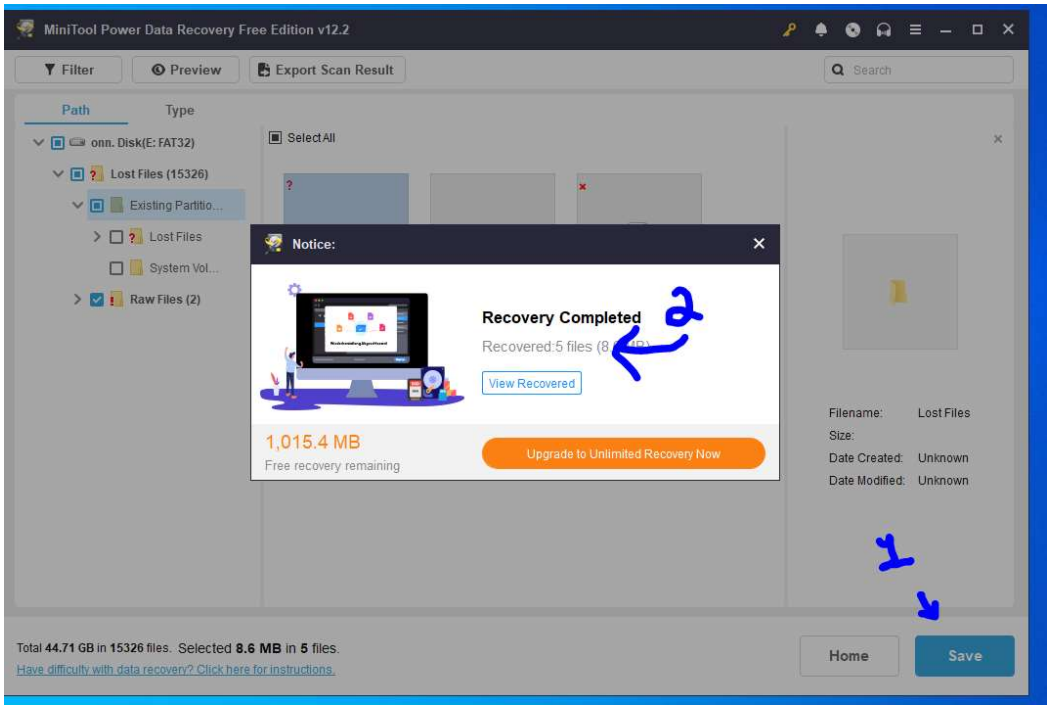
- Once scanning is complete, go through and investigate all files found within the *Path* section. In my case, all 3 deleted files were found and located within the *Existing Partition* folder of the recovered drive.



- Select the same 3 deleted files as recovered by *FTK Imager*



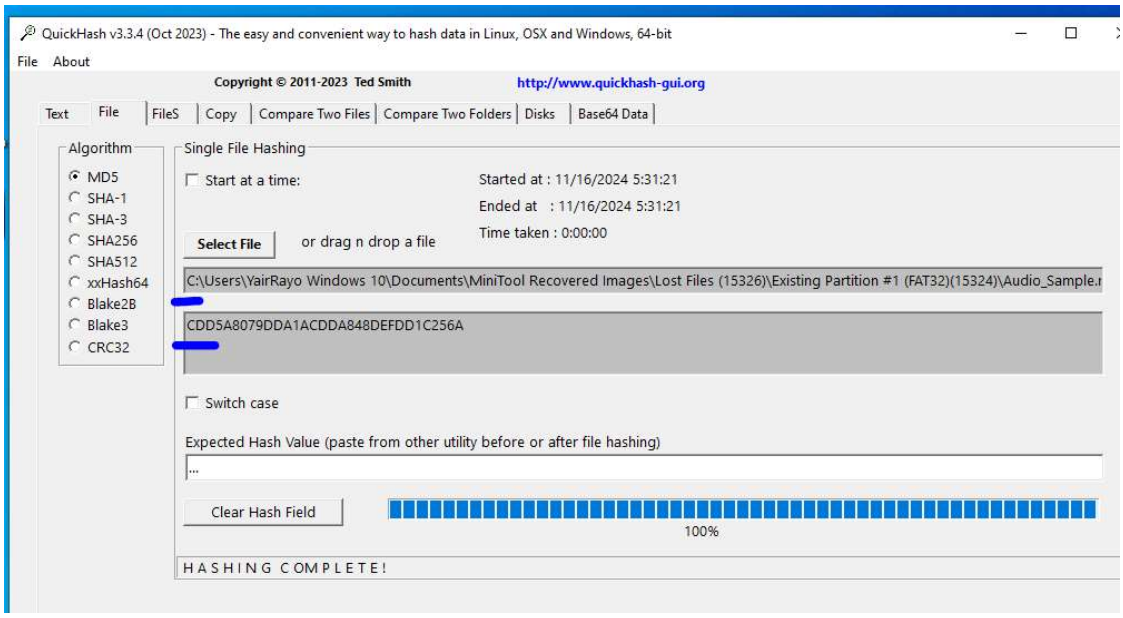
- Export the recovered files to a separate folder by clicking on the blue *Save* button, then choose the path you will save the 3 images. If done correctly, you will see a *Notice:* window that states your recovery was completed. In my case I saved the 3 files *MiniTool Power Data Recovery* found to path "C:\Users\YairRayo Windows 10\Documents\MiniTool Recovered Images"

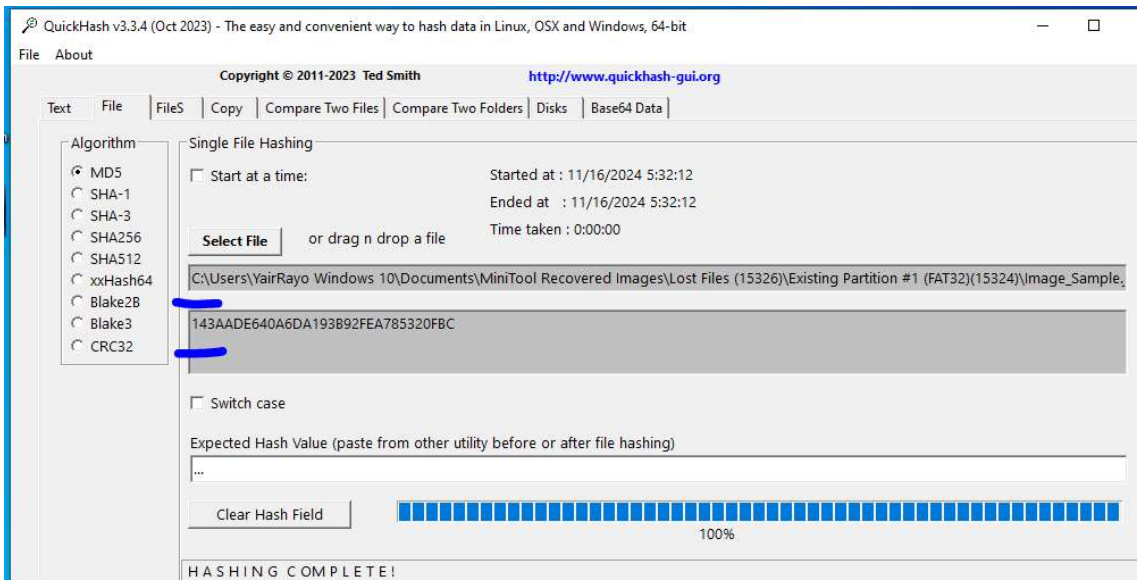


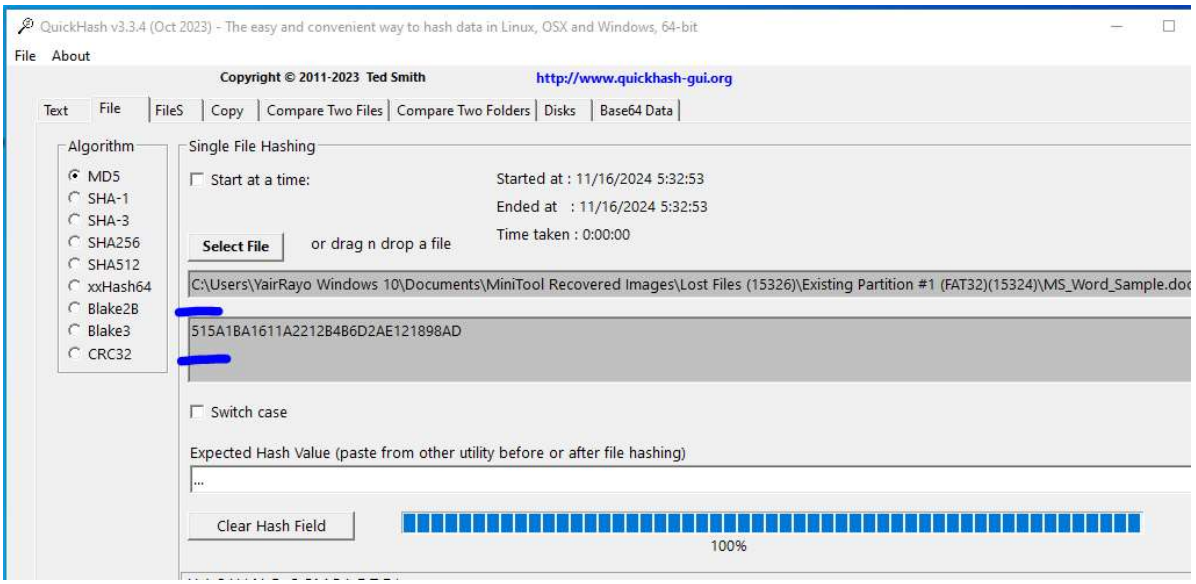
4.2 Verify Results with QuickHash-GUI

We will launch *Quickhash-GUI* and generate hashes of the 3 recovered files to later compare these hashes in our concluding report and opinion. Follow these steps:

- Open *Quickhash-GUI* and select the *Files* tab. Select 'MD5' from the 'Algorithm' option and drag/drop the desired file one-by-one within the 'Select File' button. At this point, *Quickhash-GUI* will automatically generate the hash value within the window visible above the 'Switch Case' button. Do this process for all 3 files we recovered.
    - Hash *Audio_Sample.mp3* file: CDD5A8079DDA1ACDDA848DEFDD1C256A
    - Hash *Image_Sample.jpg* file: 143AADE640A6DA193B92FEA785320FBC
    - Hash *MS_Word_Sample.docx* file: 515A1BA1611A2212B4B6D2AE121898AD


QuickHash v3.3.4 (Oct 2023) - The easy and convenient way to hash data in Linux, OSX and Windows, 64-bit
File About
Copyright © 2011-2023 Ted Smith
http://www.quickhash-gui.org
Text File FileS Copy Compare Two Files Compare Two Folders Disks Base64 Data
Algorithm
MD5
SHA-1
SHA-3
SHA256
SHA512
xxHash64
Blake2B
Blake3
CRC32
Single File Hashing
Start at a time:
Started at : 11/16/2024 5:31:21
Ended at : 11/16/2024 5:31:21
Time taken : 0:00:00
Select File
or drag n drop a file
C:\Users\YairRayo Windows 10\Documents\MiniTool Recovered Images\Lost Files (15326)\Existing Partition #1 (FAT32)(15324)\Audio_Sample.
CDD5A8079DDA1ACDDA848DEFDD1C256A
Switch case
Expected Hash Value (paste from other utility before or after file hashing)
...
Clear Hash Field
100%
HASHING COMPLETE!


QuickHash v3.3.4 (Oct 2023) - The easy and convenient way to hash data in Linux, OSX and Windows, 64-bit
File About
Copyright © 2011-2023 Ted Smith
http://www.quickhash-gui.org
Text File FileS Copy Compare Two Files Compare Two Folders Disks Base64 Data
Algorithm
MD5
SHA-1
SHA-3
SHA256
SHA512
xxHash64
Blake2B
Blake3
CRC32
Single File Hashing
Start at a time:
Started at : 11/16/2024 5:32:12
Ended at : 11/16/2024 5:32:12
Time taken : 0:00:00
Select File
or drag n drop a file
C:\Users\YairRayo Windows 10\Documents\MiniTool Recovered Images\Lost Files (15326)\Existing Partition #1 (FAT32)(15324)\Image_Sample.
143AADE640A6DA193B92FEA785320FBC
Switch case
Expected Hash Value (paste from other utility before or after file hashing)
...
Clear Hash Field
100%
HASHING COMPLETE!



At this point, we have successfully found, extracted, hashed, and snipped all information needed to decide on our software validation report. Let proceed with a comparison of all three sets of hashes for all 3 files.

Section 5: Comparing Hash Results

5.1 Hash Values

After recovering the 3 deleted files, we used QuickHash-GUI to verify the integrity of the recovered data by generating and comparing MD5 hash values. The MD5 algorithm is a accepted method for validating file integrity, as any changes or corruptions to the content of a file would produce a different hash value. The following results were obtained:

File Name	Original Hash	FTK Imager Recovered Hash	MiniTool Power Recovered Hash
Audio_Sample .mp3	CDD5A8079DDA1ACDDA8 48DEFDD1C256A	CDD5A8079DDA1ACDDA8 48DEFDD1C256A	CDD5A8079DDA1ACDDA8 48DEFDD1C256A
Image_Sample .jpg	143AADE640A6DA193B92F EA785320FBC	143AADE640A6DA193B92F EA785320FBC	143AADE640A6DA193B92F EA785320FBC
MS_Word_Sa mple.docx	515A1BA1611A2212B4B6D 2AE121898AD	515A1BA1611A2212B4B6D 2AE121898AD	515A1BA1611A2212B4B6D 2AE121898AD

The hash values of the original files, the files recovered using *FTK Imager*, and the files recovered using *MiniTool Power Data Recovery* are identical for all three test cases. This indicates that both forensic tools successfully recovered the files without any alterations to their content.

Section 6: Results

6.1 What Does This Data Tell Us?

MiniTool Power Data Recovery (New Tool) showed strengths in its user-friendly interface and quick scanning ability, making it accessible for users with varying levels of technical savviness. It identified and recovered the deleted files with no observed corruption, as confirmed by hash comparisons. However, a limitation was its lack of advanced options for forensic validation, such as detailed logging of recovery processes or integrated hashing during recovery.

Section 7: Conclusion

7.1 Concluding Thoughts

This test compared *FTK Imager*, a trusted forensic tool, with *MiniTool Power Data Recovery* to see how well they could recover deleted files. Both tools successfully retrieved the same files without any changes, as proven by matching MD5 hash values across all tests. Both tools performed well for this task of recovering deleted files from a device, showing that *MiniTool Power Data Recovery* can be a reliable option for basic data recovery, specific to recovery efforts of deleted files.

Section 8: Tester Information

I, Yair Rayo, completed the software validation. I conducted testing of FTK Imager and MiniTool Power Data Recovery, verified file integrity using Quickhash-GUI, and documented all steps. Here's my contact information:

- Name: Yair Rayo
- Role: Student, Digital Forensic Examiner
- Email: Yrayo@my.waketech.edu
- Testing Date: 11/13/2024
- Class: Computer Crime Invest. (2024FA.CCT.121.0001)
- Instructor: Mr. Wood