Lab 3

File System Forensics

Mina Salehi

University of Maryland Baltimore County

CYBR 642 Introduction to Digital Forensics

Presented to: Gina Scaldaferri

02/19/2025

Introduction

File system forensics is a critical aspect of digital investigations, enabling forensic analysts to examine and interpret data stored on digital devices. This lab focuses on analyzing file systems to extract forensic evidence, understand data structures, and identify hidden or deleted files. By utilizing forensic tools, investigators can examine file system metadata, timestamps, and directory structures to reconstruct events and validate the authenticity of digital evidence. Mastering file system forensics is essential for ensuring accurate data recovery, maintaining evidence integrity, and supporting legal proceedings (Nelson et al., 2020).

Pre-Analysis

In digital forensics a clear understanding of technical concepts is essential for accurately analyzing and presenting digital evidence. A forensic investigator must differentiate between partitions, file systems, physical and logical images, unallocated space, and slack space to interpret forensic data effectively. Additionally, explaining these concepts in court is crucial to establishing credibility and providing a clear and accurate testimony (Casey, 2011).

1. What is a Partition and Partition Type?

A partition is a logically defined storage space on a physical disk that an operating system treats as a separate entity. Partitions allow users to divide a single physical disk into multiple sections, each acting as an independent storage unit. This enables better file management, system performance optimization, and multiple operating system installations (Nelson et al., 2020).

Partition Types:

- Primary Partition: Contains the operating system and is required for booting. A disk can have up to four primary partitions.
- Extended Partition: Used when more than four partitions are needed; it acts as a container for logical partitions.
- Logical Partition: Exists within an extended partition and functions like a primary partition but cannot be used for booting.
- GPT (GUID Partition Table): A modern partitioning scheme that supports larger disk sizes and an unlimited number of partitions, replacing the older MBR (Master Boot Record) partitioning system (Bunting & Wei, 2021).

2. What is a File System?

A file system is a method used by an operating system to organize, store, and manage data on a storage device. It dictates how files are named, accessed, modified, and stored (Casey, 2011). Each partition must have a file system for the operating system to read and write data.

Common File Systems:

- NTFS (New Technology File System): Used in modern Windows systems, supports large files, encryption, and permissions.
- FAT32 (File Allocation Table 32): Compatible across multiple operating systems but has a file size limit of 4GB.
- exFAT (Extended FAT): Designed for flash drives, supports large file sizes without the limitations of FAT32.

- EXT4 (Fourth Extended File System): Used in Linux-based systems, offering journaling and efficient storage allocation.

Each file system has different features, security mechanisms, and performance characteristics, making the choice of file system critical in forensic investigations (Nelson et al., 2020).

3. What is a Physical Image?

A physical image is an exact bit-for-bit copy of an entire storage device, including all partitions, file systems, unallocated space, and hidden sectors. This method is used in forensics to ensure the most complete evidence collection possible. A physical image is useful when investigators need access to deleted files, slack space, and encrypted or hidden data (Baryamureeba & Tushabe, 2004).

Example: If a forensic investigator creates a physical image of a 500GB hard drive, the resulting forensic image file will be exactly 500GB, preserving every bit of data for analysis.

4. What is a Logical Image?

A logical image captures only the active files and folders that are accessible within a partition or file system. Unlike a physical image, it does not include deleted files, unallocated space, or system artifacts (Casey, 2011).

Example: A logical image of a 500GB hard drive may result in a significantly smaller file if only 100GB of files are actively stored, as it does not capture unused sectors or deleted data. Logical images are typically used when forensic investigators are only interested in live data and user-generated content.

5. What is Unallocated Space?

Unallocated space refers to areas of a storage device that are not currently assigned to any file but may contain residual data from previously deleted files. When a file is deleted, it is not immediately erased; instead, the system marks the space as "available," allowing new data to overwrite it over time (Nelson et al., 2020).

Importance in Forensics:

- Investigators can use forensic tools to recover deleted files from unallocated space.
- Unallocated space may contain fragments of old files, system logs, or metadata useful in investigations.

6. What is Slack Space?

Slack space is the unused space within a file cluster that remains after a file is written to disk. This occurs because file systems allocate space in fixed-size clusters, meaning a file may not fully utilize the allocated space, leaving remnants of previous data in the slack space (Casey, 2011).

Example:

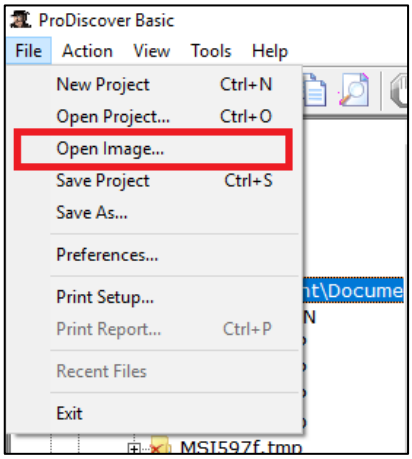
- A file system uses 4KB clusters, and a 2KB file is saved to disk. The remaining 2KB of unused space in the cluster is slack space.
- Slack space may contain fragments of previous files, making it a valuable source of forensic evidence for investigators.

Analysis

Digital forensic investigations require the ability to acquire and analyze forensic images to preserve evidence integrity and extract meaningful data. This lab simulates a real-world forensic scenario where investigators analyze previously acquired images USB storage devices. Building on the foundations of Lab 2, this exercise focuses on using forensic tools.

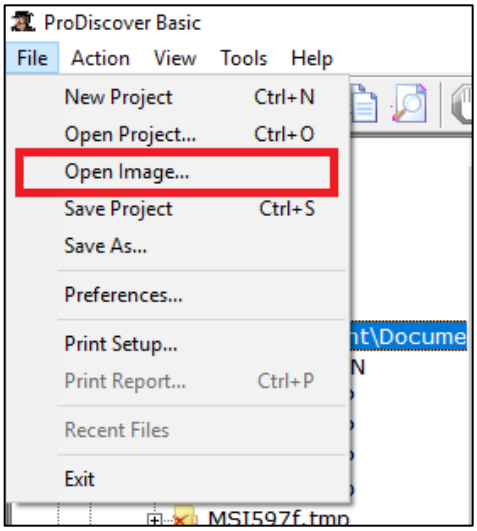
1. Viewing images in ProDiscover for USB F

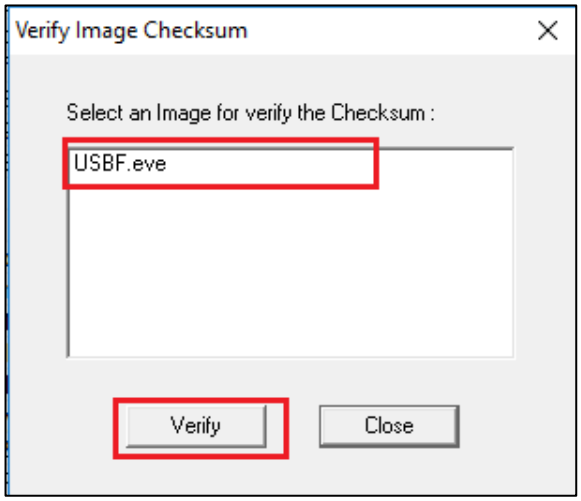
To access the USB image, navigate to File, select Open Image, and choose the USB image that was created during Lab 2.

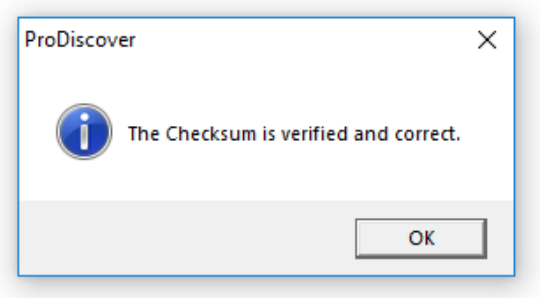


- What is the hash of the image (USB F)?
    - MD5 Checksum: e9cd3adcec8238201d9eca1994f077db

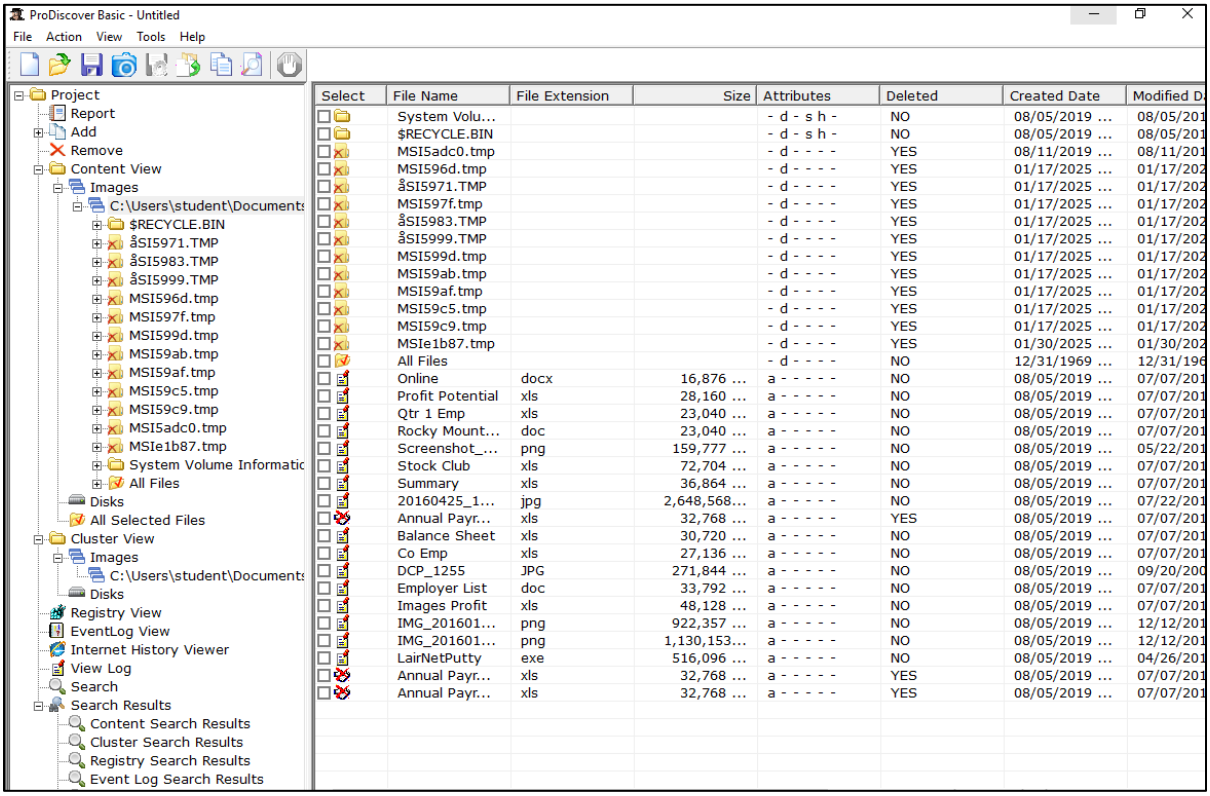
- Is it the same as last week's hash?
    - Yes, hash values are the same. This confirms data integrity, meaning the forensic image has not been modified.
    - To compare the hash values, navigate to Action and select Verify Image Checksum.







- What files are present in the image?

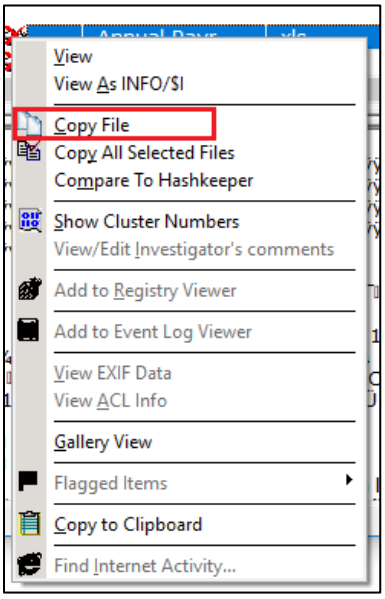


  - USB F contains several deleted files, some .xls and .doc files related to payroll and employee information, few images (jpg, png)
    - Annual Payroll 1 Excel File (deleted), Annual Payroll 2 – Copy Excel File (deleted), Qtr 1 Emp Excel File, Summary Excel File, Balance Sheet Excel File, Annual Payroll 2 Excel File (deleted), Images Profit Excel File, Profit Potential Excel File, Stock Club Excel File, Co Emp Excel File
    - IMG_20160113_151435, IMG_20160111_160355, Screenshot_2016-06-19-11-15-06, DCP_1255
  - Deleted files
    - MSI5adc0.tmp (Casey, 2011), MSI192bc.tmp, MSI192b8.tmp, MSI1928c.tmp, aSI19290.TMP, MSI192a6.tmp, MSI192aa.tmp

- LairNetPutty Executable: In lab 1 we determine this file was malicious and this was a virus ran on port 4444.

- Were any related to the crime of fraud.
  - Considering the nature of the case, the forensic investigator should conduct a thorough review of all recovered files to identify any evidence related to fraudulent activities. This includes examining financial documents, transaction records, email communications, or any altered files that could indicate fraudulent intent. Additionally, analyzing metadata and timestamps may reveal unauthorized modifications or attempts to conceal evidence. A comprehensive forensic analysis will help determine whether any files are directly linked to the suspected fraud.

- Were any deleted could you recover them?
  - To recover a deleted file, right-click on it, select Copy File, and save it to the designated location



	A	B	C	D	E
1	Annual Payroll Totals				
2	Employee	Hours Worked	Gross Pay		
3	QR2603	1,641.00	18,461.25		
4	RH1287	2,364.50	21,162.28		
5	ST4234	2,174.75	38,601.81		
6	ZX2137	2,116.75	40,218.25		
7	Total	8,297.00	118,443.59		
8					
9					

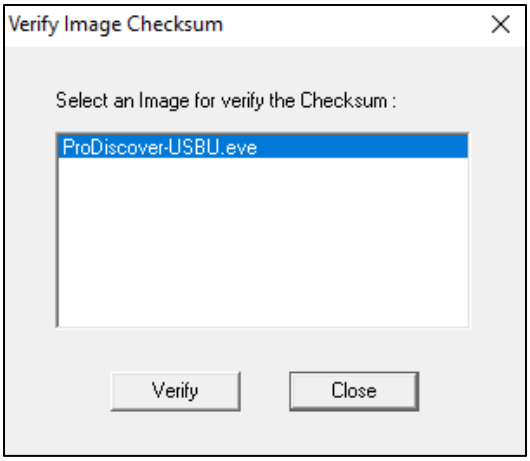
2. Viewing images in ProDiscover for USB U

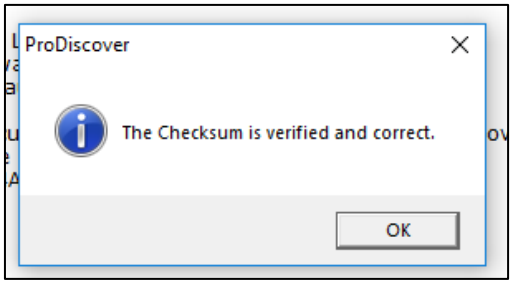
Repeated the same steps as USB F

- What is the hash of the image (USB U)?

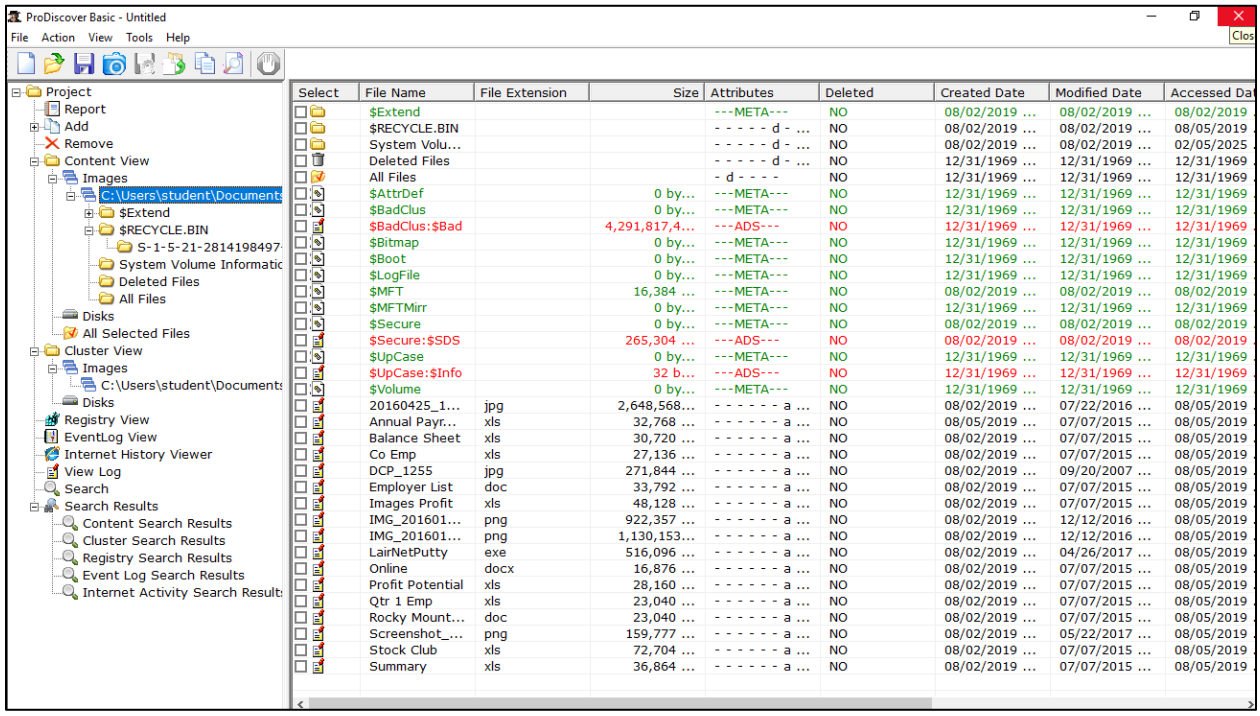
- MD5 Checksum: 6ab43cbcea475d2ccdbf2011a9eee562

- Is it the same as last week's hash?





- What files are present in the image?



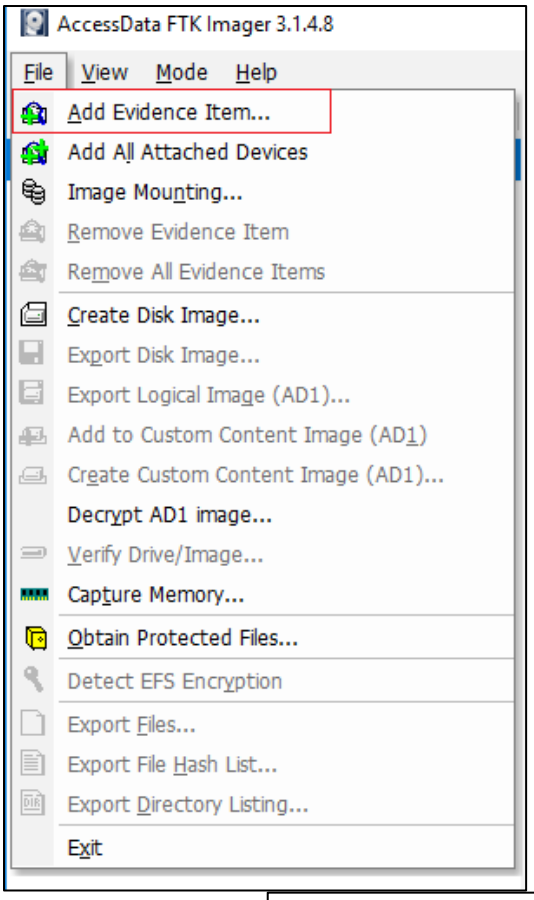
- Employee, Payroll, and HR files

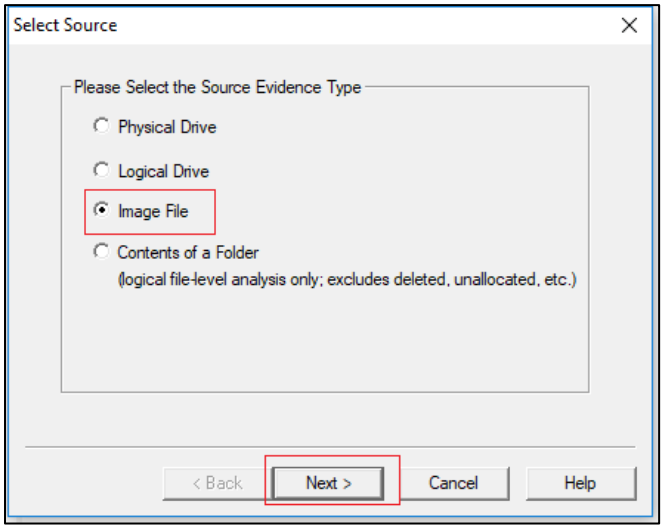
    - Annual Payroll 2 Excel File, Qtr 1 Emp Excel File, Profit Potential Excel File, Balance Sheet Excel File, Stock Club Excel File, Summary Excel File, Co Emp Excel File, Employer List Document

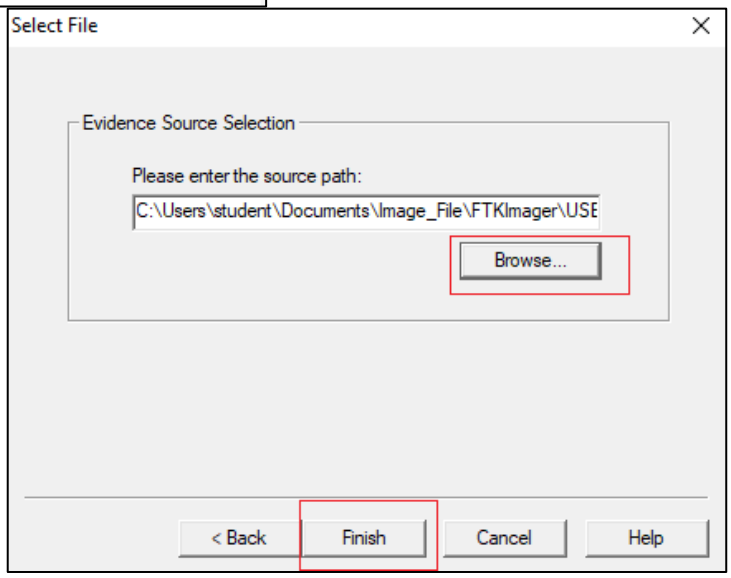
- Images in PNG and JPG formats: oIMG_20160113_151435 PNG, IMG_20160111_160355 PNG, Screenshot_2016-06-19-11-15-06 PNG 20160425_142807(0) JPG, DCP_1255 JPG
- LairNetPutty Executable: This file exhibits characteristics of a potential virus. It should be handled with caution and only executed within a virtual machine environment to prevent system compromise.
- Were any deleted could you recover them?
    - Found one delete file but was not able to recover it. ($IAH3DU9.xls)

3. Viewing images in FTK Imager – USB F

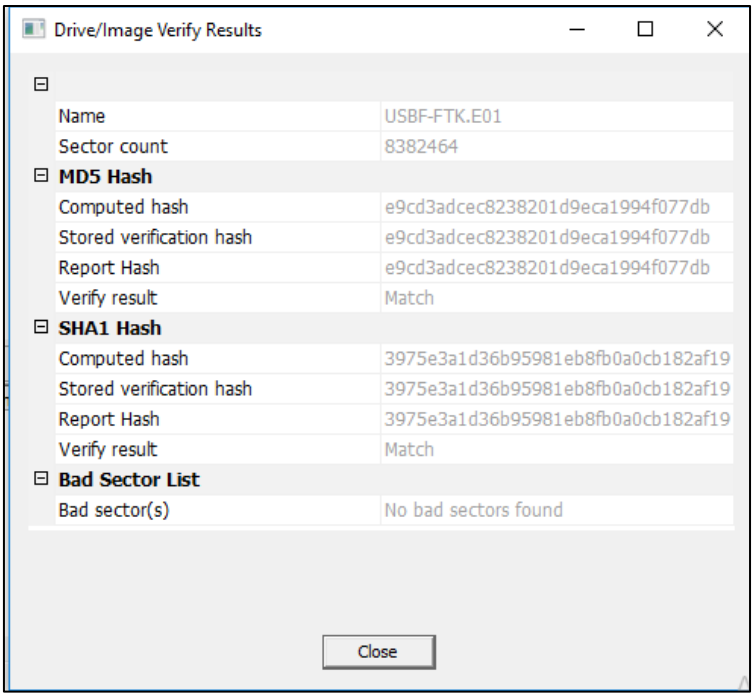
To access the USB image, navigate to File, Add Evidence Item, then select image file, browse the file and finish







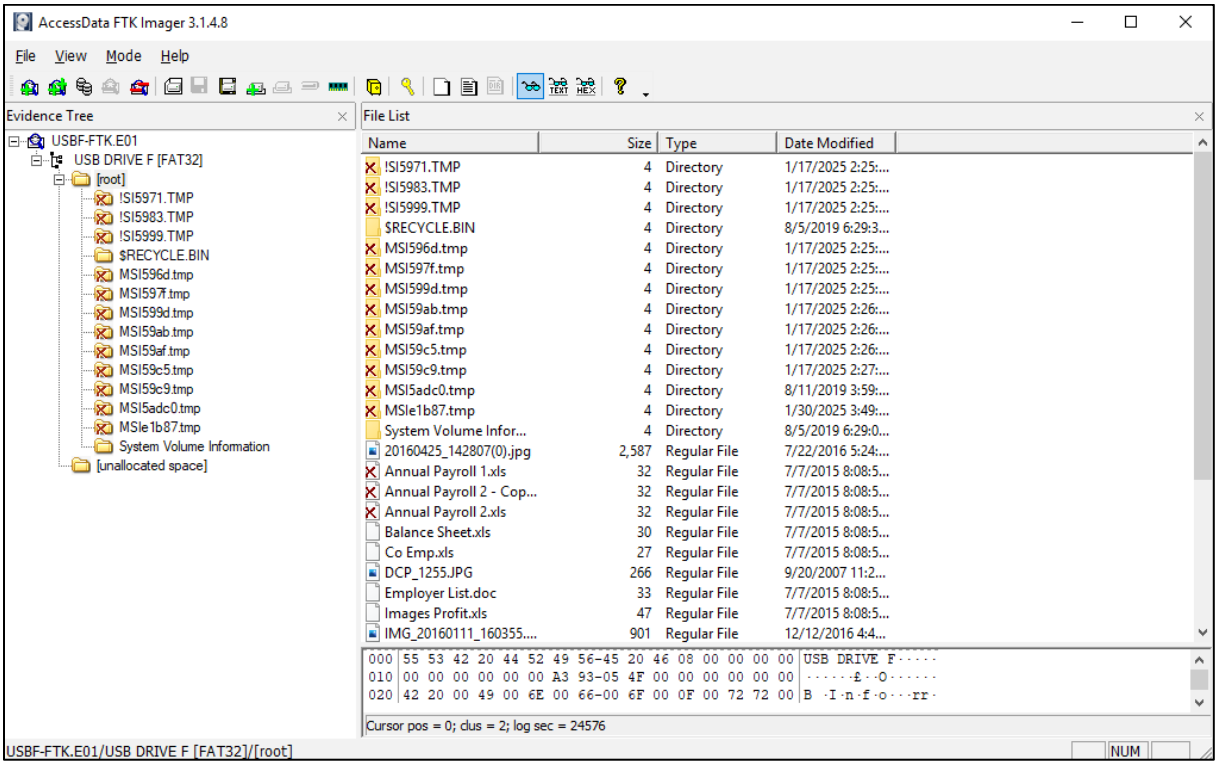
- What is the hash of the image?
  - MD5 checksum: e9cd3adcec8238201d9eca1994f077db
  - SHA1 checksum: 3975e3a1d36b95981eb8fb0a0cb182af194ff014



- Is it the same as last week's hash?
    - Yes, it is the same value
- What files are present in the image?
    - USB DRIVE F [FAT32]
    - Following files relevant to corporation HR/finance
        - Annual Payroll 1 Excel File (deleted), Annual Payroll 2 – Copy Excel File (deleted), Qtr 1 Emp Excel File, Summary Excel File, Annual Payroll 2 Excel File (deleted), Images Profit Excel File, Profit Potential Excel File, Stock Club Excel File, Co Emp Excel File, Balance Sheet Excel File
    - Some files seem to be random with potential malware
        - LairNetPutty Executable, Online Documentx, Employer List Document, Rocky Mountain Online document
    - Deleted Files:

- MSI5adc0.tmp, MSI927a.tmp, MSI1928c.tmp, MSI928c.tmp oaSI19290.TMP, MSI192a6.tmp, MSI192aa.tmp, MSI192b8.tmp, MSI192bc.tmp**,** Annual Payroll 1.xls, Annual Payroll 2.xls, Annual Payroll 2 copy.xls

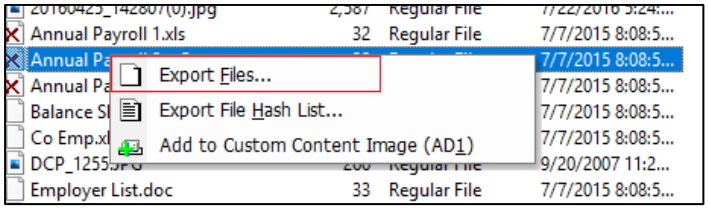
- Do you see any files that show a red X? What does this mean?
    - Yes, the red X indicates deleted files

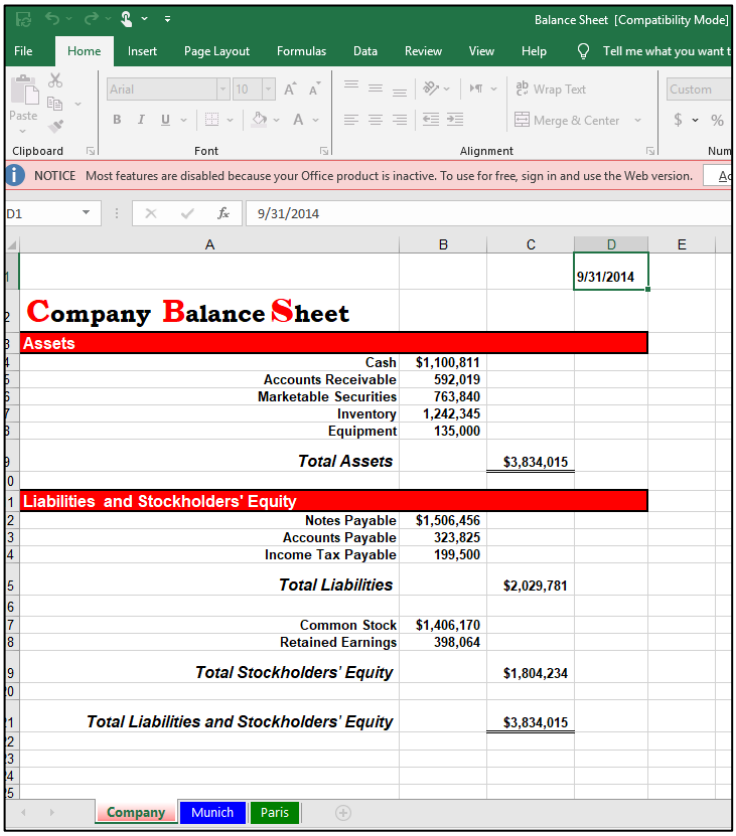


- Were any related to the crime of fraud.
    - Considering the nature of the case, the forensic investigator should conduct a thorough review of all recovered files to identify any evidence related to fraudulent activities. This includes examining financial documents, transaction records, email communications, or any altered files that could indicate

fraudulent intent. Additionally, analyzing metadata and timestamps may reveal unauthorized modifications or attempts to conceal evidence. A comprehensive forensic analysis will help determine whether any files are directly linked to the suspected fraud.

- If there were files with a red X try to recover them.
    - Yes, there are several files with red X.
    - To restore the files, right-click on the file and choose the Export File option.

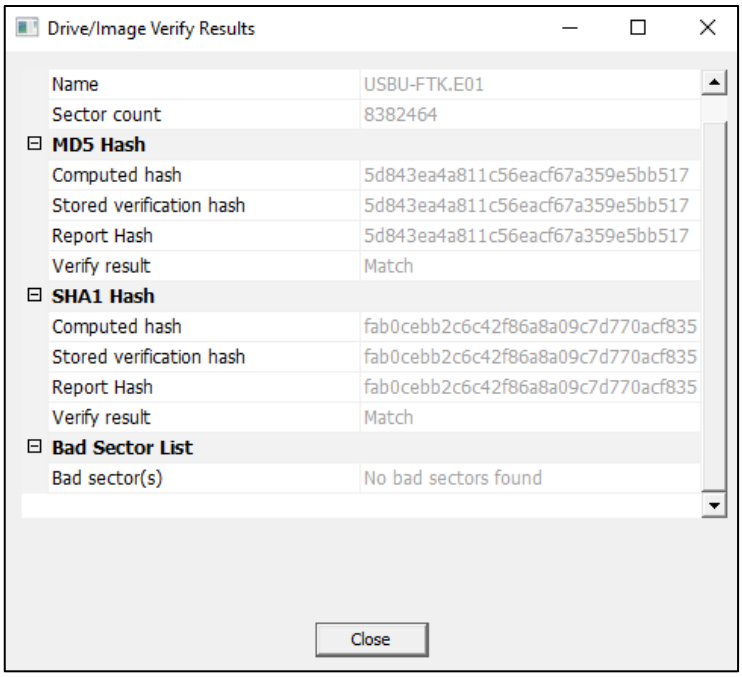




4. Viewing images in FTK Imager – USB U

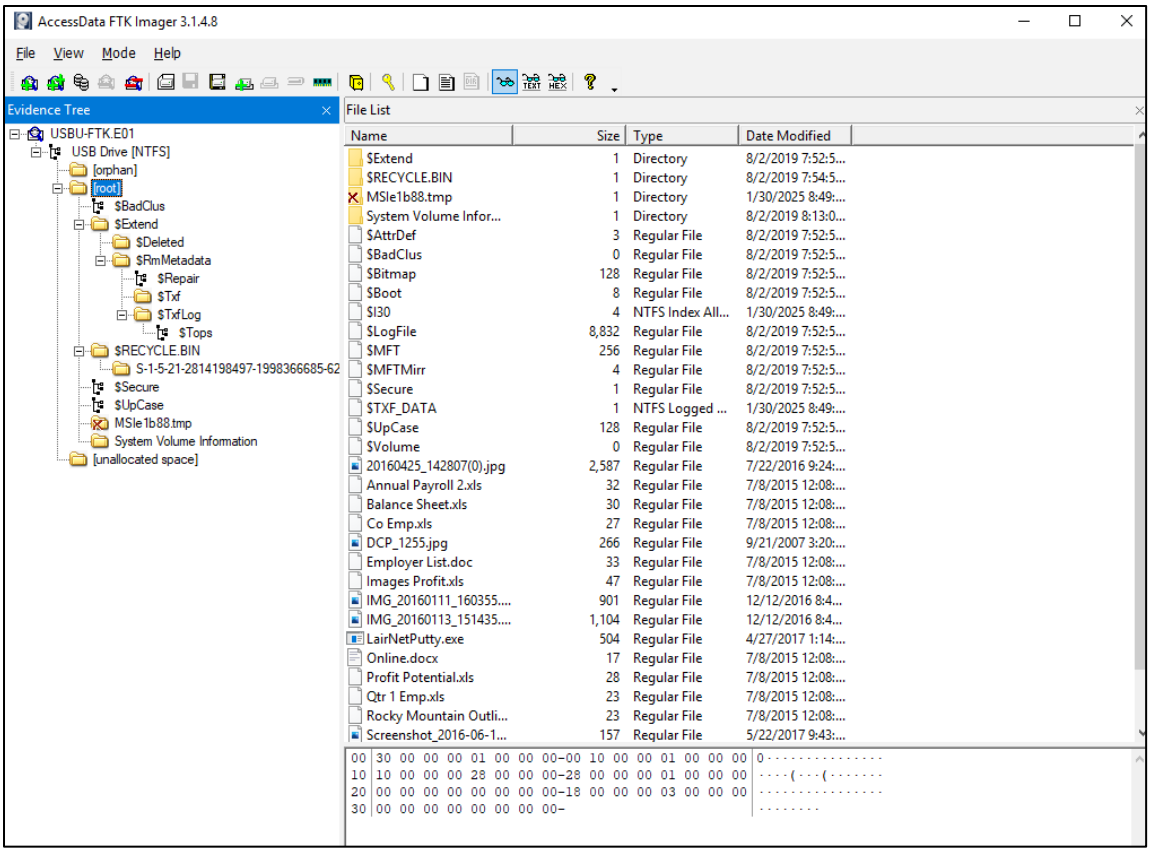
Repeated the same steps to access USB U.

- What is the hash of the image?
  - MD5 checksum: 5d843ea4a811c56eacf67a359e5bb517
  - SHA1 checksum: fab0cebb2c6c42f86a8a09c7d770acf83505e328



- Is it the same as last week's hash?
  - Yes, it is the same value
- Relevant Files to Discuss on the U:
  - The following files are a corporation HR / finance trend such as being payrolls and employee information.

        - Annual Payroll 2 Excel File, Balance Sheet Excel File, Co Emp Excel File, Employer List Document oImages Profit Excel File, Profit Potential Excel File, Qtr 1 Emp Excel File, Stock Club Excel File, Summary Excel File
    - These files are random and need to be vetted for potentially having malware
        - LairNetPutty Executable, Rocky Mountain Online Document, Employer List Document
    - Image files
        - IMG_20160113_151435 PNG, IMG_20160111_160355 PNG, Screenshot_2016-06-19-11-15-06 PNG, 20160425_142807(0) JPG, DCP_1255 JPG
    - Files that are marked as deleted. This is denoted by a red x on them
        - MSI192d7.tmp, $IAH3DU9 Excel File (located in $RECYCLE.BIN)
        - Unallocated Space
            - 44 files located in Unallocated Space, None of these files can be recovered
    - Steps attempted at recovery:
        - Right click on a file, In the dropdown that displays click on “Export Files”
    - Files that pose as evidence of virus are: LairNetPutty Executable



5. Analysis of Images

Forensic imaging tools are essential for acquiring and analyzing digital evidence, but differences in how they process and capture data can lead to variations in forensic images. This comparison evaluates the images acquired using ProDiscover and FTK Imager, identifying discrepancies in file system contents, missing files, and unallocated space between the two tools. Understanding these differences is crucial for forensic investigators to select the most appropriate tool for a given case and ensure that no critical evidence is overlooked (Nelson et al., 2020).

Are the file system contents of each image the same? There are differences between the two images

Are There Any Files Missing from an Image? Yes, some files were missing depending on the forensic tool used:

- ProDiscover USB U: Missing files MSIe1b88.tmp, $IAH3DU9 (located in $Recycle.BIN), MSIe1b88.BIN, and unallocated space
- ProDiscover USB F: Missing unallocated space

These differences suggest that ProDiscover may not have fully captured unallocated space, whereas FTK Imager struggled to retain file system records properly in some instances. This reinforces the importance of using multiple forensic tools for validation and comprehensive analysis (Bunting & Wei, 2021).

Which Tool Would You Prefer to Use as Your Main Tool, and Why?

The choice between ProDiscover and FTK Imager depends on the forensic requirements of a case.

- FTK Imager is generally preferred for:
    - Capturing raw forensic images with industry-standard E01 format, which includes compression and metadata storage.
    - Handling unallocated space better, ensuring the ability to recover deleted files.
    - Being widely compatible with forensic tools such as Autopsy, EnCase, and X-Ways Forensics (Nelson et al., 2020).

- ProDiscover is useful for:
    - Live forensics and disk analysis, providing an interactive way to explore forensic images.
    - Easier navigation of file structures in some cases.
- Did You Notice Any Differences Between the Images of the Two USB Drives (F: and U:)?
    - Yes, there were significant differences between the images of USB F and USB U. These findings highlight the limitations of relying on a single forensic imaging tool. To maximize data acquisition and ensure integrity, investigators should cross-validate forensic images using multiple tools (Baryamureeba & Tushabe, 2004).

Conclusion

The comparison of forensic images obtained using ProDiscover and FTK Imager underscores the importance of tool selection in digital forensic investigations. While both tools have strengths and weaknesses, forensic investigators must understand their capabilities and limitations to avoid data loss or incomplete evidence collection. In cases where active files need to be examined, ProDiscover may be preferable, whereas FTK Imager is better suited for complete forensic imaging, including unallocated space and deleted file recovery. Using multiple tools for verification ensures that forensic evidence is comprehensive, verifiable, and admissible in court (Nelson et al., 2020).

Glossary

Digital Forensics

Digital forensics is the process of collecting, analyzing, and preserving electronic data to be used as evidence in criminal investigations, cybersecurity incidents, or legal proceedings. It involves recovering deleted files, examining file systems, and verifying data integrity (Casey, 2011).

Forensic Image

A forensic image is a bit-for-bit copy of a storage device, preserving its file system, metadata, and unallocated space. It ensures that no data is altered during the acquisition process, allowing investigators to analyze digital evidence without modifying the original data (Nelson et al., 2020).

ProDiscover

ProDiscover is a forensic software tool used for disk imaging, file system analysis, and live forensics. It allows forensic analysts to examine active files, deleted files, and system metadata while preserving evidence integrity (Bunting & Wei, 2021).

FTK Imager

FTK Imager is a forensic imaging tool that captures exact copies of storage devices in various formats, such as E01 (EnCase Image Format) and RAW images. It is widely used for evidence acquisition, hash verification, and file system analysis (Nelson et al., 2020).

File System

A file system is a structured method that an operating system uses to store, organize, and manage files on a storage device. Common file systems include NTFS, FAT32, exFAT, and EXT4, each with different storage structures and metadata handling techniques (Casey, 2011).

Partition

A partition is a logically defined section of a physical storage device, allowing multiple operating systems or file systems to exist on the same drive. Partitions are categorized as primary, extended, or logical, depending on their function and structure (Bunting & Wei, 2021).

Physical Image

A physical image is a bit-for-bit forensic copy of an entire storage device, including active files, deleted files, unallocated space, and system metadata. It is the most comprehensive form of forensic imaging, ensuring that all potential evidence is preserved (Nelson et al., 2020).

Logical Image

A logical image captures only active files and directories from a storage device without including unallocated space or deleted files. This imaging method is useful when only user-generated content needs to be examined (Casey, 2011).

Unallocated Space

Unallocated space refers to disk areas that are not assigned to any active file but may contain residual data from deleted files. Forensic tools can recover lost or hidden evidence from unallocated space by reconstructing file fragments (Nelson et al., 2020).

Slack Space

Slack space is the unused portion of a file cluster that remains after a file is stored. Because file systems allocate data in fixed cluster sizes, the leftover space may contain remnants of previous files, making it valuable for forensic investigations (Casey, 2011).

E01 File Format

The E01 format (EnCase Image Format) is a forensic image file format that preserves metadata, supports compression, and includes hash verification. It is widely used in forensic investigations for maintaining data integrity and ensuring evidence authenticity (Bunting & Wei, 2021).

Hash Value

A hash value is a unique digital fingerprint generated using cryptographic algorithms like MD5 or SHA-256. It ensures that a file or forensic image has not been altered, playing a crucial role in maintaining data integrity and admissibility in court (Schneier, 1996).

Fraud Investigation in Digital Forensics

A fraud investigation in digital forensics involves analyzing electronic records, financial documents, metadata, and transaction logs to uncover evidence of fraudulent activities. Investigators examine file modifications, deleted files, and system artifacts to determine fraudulent intent (Casey, 2011).

Metadata

Metadata is data about data, providing details such as file creation date, modification timestamps, and access history. Forensic analysts use metadata to track digital activity, reconstruct events, and detect unauthorized modifications (Nelson et al., 2020).

.TMP File

A .TMP file is a temporary file created by applications or operating systems to store intermediate data, backup files, or session information. These files are typically used during software installation, file editing, or system processes and are often deleted automatically when no longer needed (Nelson et al., 2020).

Reference

Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. Digital Investigation, 1(1), 29-36. https://doi.org/10.1016/j.diin.2003.12.003

Bunting, S., & Wei, W. (2021). EnCase computer forensics–The official EnCE: EnCase Certified Examiner study guide (3rd ed.). Wiley.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press.

Nelson, B., Phillips, A., & Steuart, C. (2020). Guide to computer forensics and investigations (6th ed.). Cengage Learning.