Emma Crook 620 Lab Quiz

Discussion

This assignment builds on your skills by (1) emphasizing how forensics is a multi-tool environment and (2) provides you some hands-on work.

Case Scenario

Today is September 15, 2004. The time is 3:15 PM. Mr. Jim Boss, the owner of the Really Big Company (RBC) called and you responded to his office. Mr. Boss advised that he suspected that his assistant, Emma Crook, was providing company sensitive material to some of his competitors. At 2:00 PM today he confronted Ms. Crook with his suspicions. He told her that he would be back at 3:00 PM for an explanation. When Mr. Boss went to Ms. Crook's office at 3:00 PM, she was gone.

Her office was completely cleaned out of all of her belongings. Mr. Boss tried to turn on Ms. Crook's computer, but it would not boot. Mr. Boss found a floppy diskette in the trash can. Mr. Boss wants you to examine the computer and the floppy diskette and to tell him exactly what Ms. Crook was up to. He is willing to pay big bucks for a 100% thorough examination. "Leave no stone unturned" as he said. Mr. Boss tells you to check with Scooter Ben Nice who has taken a forensic image of the diskette.

Below are three ways to get the evidence. It's your decision which one to choose. If you select the self-extracting option, copy this file to your hard drive and unzip it. To extract this file, format a 3 1/2 inch 1.44 MB diskette and execute the CCE-SAMP.EXE file. This will create an exact image of our original floppy diskette. Treat the extracted floppy diskette as the original in this case. Conduct your examination, document your findings and compare your findings and answer the questions below.

http://www.isfce.com/CCE_Sample_PE_RAW.zip	**Raw format (.001) evidence media**
http://www.isfce.com/CCE_Sample_PE_VirtualPC.zip	**Virtual Machine Download**
http://www.isfce.com/cce-samp.zip	**Floppy disk self-extracting**

Copy and paste the link of your choice into your URL and click enter. This should start to download the zip file. If it doesn't download, work through it. This is part of the job of a forensic investigator.

Walking You Through the Lab

- Scooter Ben Nice has provided you a raw image file (.001) or also known as a DD image file. This is provided on Sakai

For 1 point: What is an DD Image file and why are there different forensic image files and what are the considerations you should take when selecting an particular type of image file (.E01, .AD1, .001, .AFF, etc) you want?

Answer:

A **DD (Disk Dump) image file** is a raw, bit-for-bit copy of a storage device, such as a hard drive, USB drive, or floppy disk. It is commonly created using the dd command in Unix/Linux environments. This format preserves the exact data structure of the source, including files, directories, and unallocated space, making it ideal for digital forensics. The unallocated space often contains remnants of deleted files, which can be recovered and analyzed as part of an investigation. The DD image format typically has a .dd or .001 extension and is uncompressed, providing a direct representation of the original data.

Why Are There Different Forensic Image Formats?

Various forensic image formats exist because each has unique features that cater to different investigative needs. Factors such as the need for compression, metadata storage, error checking, and tool compatibility all influence the choice of format. Forensic tools often have their own preferred formats, and some formats offer enhanced capabilities, such as compression, encryption, and the inclusion of additional case-related metadata.

Common Forensic Image Formats:

1. **.DD / .001 (Raw Image Format)**:
   - **Description**: A raw, uncompressed bit-by-bit copy of a storage device.
   - **Advantages**: Widely compatible across various forensic tools and includes all disk data, including unallocated space.
   - **Disadvantages**: Large file size due to lack of compression, and it doesn't include metadata or built-in integrity checks.
2. **. E01 (EnCase Image Format)**:
   - **Description**: Proprietary format used by the EnCase forensic tool, which supports compression and includes metadata.
   - **Advantages**: Reduces storage size with compression, includes case-related metadata and checksums for verifying file integrity.
   - **Disadvantages**: Proprietary nature limits compatibility to specific tools, primarily EnCase.
3. **. AFF (Advanced Forensic Format)**:
   - **Description**: An open-source image format that supports optional compression, encryption, and metadata.
   - **Advantages**: Flexible, supports compression and encryption, and allows the inclusion of detailed metadata. It's also widely supported.
   - **Disadvantages**: May have slower performance when dealing with compressed or encrypted data.
4. **.AD1 (AccessData Custom Content Image)**:
   - **Description**: A proprietary format used by FTK (Forensic Toolkit), specifically designed for capturing and storing selected files or directories.
   - **Advantages**: Allows selective imaging, reducing storage needs for large datasets. It also supports compression.
   - **Disadvantages**: Limited to tools that support AD1 format, such as FTK.

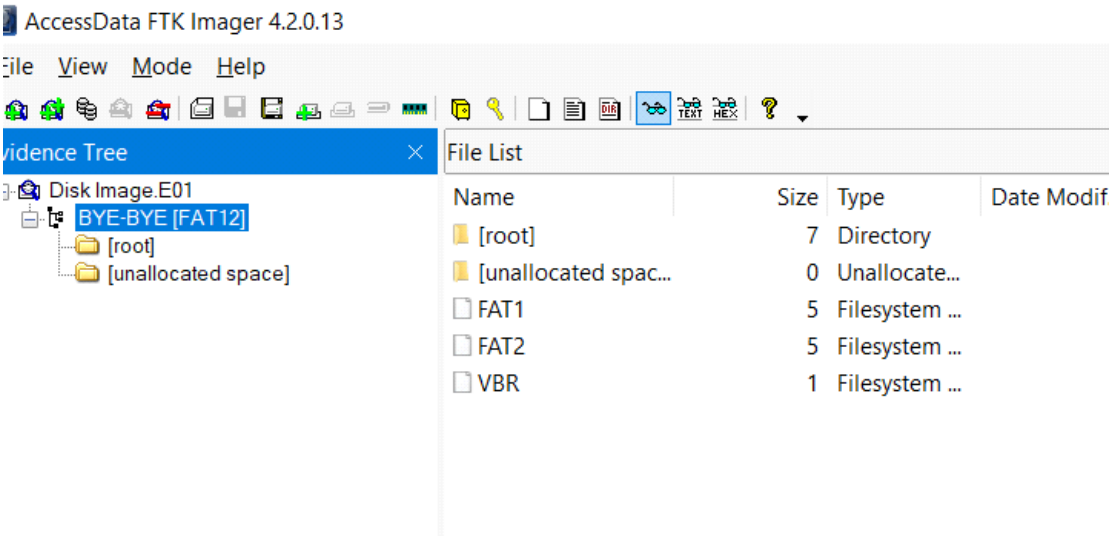
Key Considerations When Selecting a Forensic Image Format

- **Tool Compatibility**:
  - It's essential to choose a format that is compatible with the forensic software you're using. For example, **.E01** is preferred for EnCase, while **.001** (raw format) is compatible with a wide range of tools like FTK, Autopsy, and others.
- **File Size and Storage Efficiency**:
  - Some formats, such as **.E01** or **.AFF**, offer compression options that reduce the amount of storage space required for large datasets, which is beneficial when working with sizable storage devices.
  - In contrast, raw formats like **.DD** or **.001** don't provide compression, which means they require more storage space but allow for more universal compatibility.
- **Metadata and Integrity Checks**:
  - Formats such as **.E01** and **.AFF** can include important metadata, such as case details, investigator information, and timestamps, which may be crucial for maintaining the chain of custody and validating the evidence.
  - **Checksums** and **hash values** are embedded in formats like **.E01** to ensure data integrity, allowing for easy verification that the image has not been altered.
- **Error Recovery and Handling**:
  - Some forensic image formats, particularly **.E01**, provide robust error-checking mechanisms. This is particularly important when imaging devices with physical damage or read errors, as the format can log and handle these errors more effectively.

❖ **Encryption and Security**:
- If sensitive or classified data needs to be secured, formats like **.AFF** offer encryption options, which provide an extra layer of protection for the stored data.

❖ **Data Type and Investigative Scope**:
- For cases where only certain files or directories need to be captured, selective imaging formats like **.AD1** might be more efficient than capturing an entire disk, as they focus on specific data of interest.

- You decide that you want to use and FTK Imager which is available here at https://accessdata.com/product-download/ftk-imager-version-4.2.0 so you download it and then install it on your computer. ***please install this on your computer if you haven't done so already**
- Now you ingest the .001 image into FTK Imager. This is what you should be seeing. Please browse and answer these questions



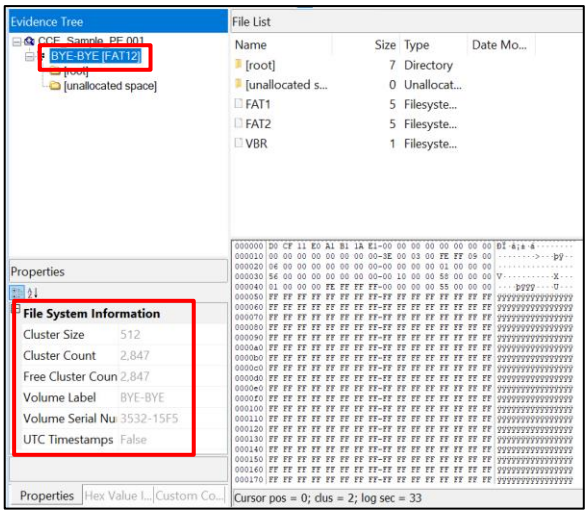
For 4 points:

- What is the file system of this image e.g. FAT 12, FAT 32, NTFS?

Answer: FAT12

Verification:

This is evident from the label "**BYE-BYE [FAT12]**" in the Evidence Tree section of FTK Imager. FAT12 is typically used for smaller storage devices such as floppy disks, which aligns with the nature of this image file.



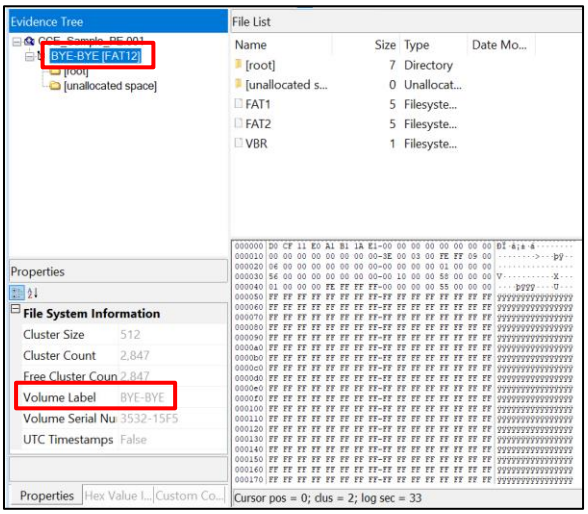
Here's why:

1. **Cluster Size**:
   - The **Cluster Size** is 512 bytes, which is typical for the FAT12 file system, particularly when used on smaller storage devices like floppy disks.

2. **Cluster Count**:
    - The **Cluster Count** is **2,847**, which is well within the limits of the FAT12 file system. FAT12 can support up to approximately 4,084 clusters (12 bits per cluster entry), so this cluster count fits within the FAT12 range.
3. **Volume Label and Serial Number**:
    - The **Volume Label** is listed as "BYE-BYE," matching what is displayed in the evidence tree. The **Volume Serial Number** is also provided, which is a standard part of the metadata stored in the boot sector of a FAT file system.

- What is the volume label of this image?

Answer: The volume label of this image, as displayed in the **File System Information** in the screenshot, is **"BYE-BYE"**.



- This image looks to be empty – where do you think data could be recovered e.g. FAT 1, FAT 2, VBR, unallocated space and why?
    - Hint you may want to do some research on the Internet on “unallocated space”.
    - Another hint – sometimes looking at the file size of the artifacts can be useful too.

Answer:

Upon initial examination, this forensic image may appear to be empty; however, several key areas within the file system can still provide opportunities for data recovery. These areas include **unallocated space**, **File Allocation Tables (FAT1 and FAT2)**, and the **Volume Boot Record (VBR)**. Additionally, examining the file sizes of key artifacts can provide insights into potential data hiding or system tampering. Here’s a detailed analysis:

1. **Unallocated Space**:
    - **Why**: Unallocated space refers to sections of the disk that are no longer assigned to active files or directories. However, data from deleted files may still reside here until it is overwritten. The system does not erase the data immediately; it merely marks the space as available for new data.
    - **Recovery Method**: Searching for file remnants, signatures, or patterns in unallocated space can reveal deleted files or fragments. Even if the directory structure no longer shows a file, its content may still be recoverable from this area. This is a prime target for carving techniques to recover lost data.
    - **File Size Consideration**: In this case, the unallocated space shows a size of 0 bytes, indicating that the space has been marked as empty. However, unallocated space can still contain data remnants, which may be uncovered through more detailed analysis.

2. **FAT1 and FAT2 (File Allocation Tables)**:
   - **Why**: FAT1 and FAT2 record the allocation of disk clusters to files. If files were deleted, their cluster allocation information might still be present in these tables. The second FAT (FAT2) serves as a backup, providing redundancy in case FAT1 is damaged. These tables can provide clues about the past state of the file system and its contents.
   - **Recovery Method**: By analyzing the contents of FAT1 and FAT2, it is possible to trace which clusters were previously allocated to files and attempt to reconstruct the files. Discrepancies between FAT1 and FAT2 could indicate file system corruption or tampering.
   - **File Size Consideration**: The FAT1 and FAT2 tables are listed as 5 bytes each, which is much smaller than expected for a standard file allocation table. This unusually small size could suggest that the disk has been wiped or formatted, reinforcing the need for a deeper investigation into potential deleted data or system alterations.
3. **Volume Boot Record (VBR)**:
   - **Why**: The VBR contains metadata about the file system, such as the cluster size and disk geometry, and is essential for booting and managing the file system. Though the VBR does not store user data, any irregularities in this record could signal attempts to manipulate or obscure the file system.
   - **Recovery Method**: Examining the VBR can reveal if there have been any modifications or tampering. For example, the VBR may contain clues about file system settings or formatting attempts that could hide data. Additionally, the volume label and other metadata stored here can provide insights into the disk's original setup.
   - **File Size Consideration**: The VBR is listed as 1 byte in size, which is unexpectedly small. This may suggest that the boot record was altered or cleared, which could imply attempts to cover up past data or system usage. Further investigation into how the VBR compares with expected FAT12 structures is needed.
4. **Slack Space**:
   - **Why**: Slack space refers to the unused portion of a disk cluster when a file does not completely fill its assigned space. This residual area can contain fragments of data from previously deleted or overwritten files. As the FAT12 file system operates with fixed cluster sizes, slack space could hold critical remnants of old data.
   - **Recovery Method**: Slack space can be examined to recover partial files or file fragments. Though these fragments may not appear in the directory structure, they can be pieced together to reconstruct meaningful data.
5. **File Size of Artifacts**:
   - **Why**: Analyzing the size of key file system artifacts like FAT1, FAT2, and the VBR can reveal potential anomalies. If these artifacts are smaller than expected, it may indicate tampering, disk wiping, or formatting. These discrepancies can offer insights into whether the file system has been modified to hide data or if any structural changes were made.
   - **File Size Consideration**: The unusually small sizes of the FAT1 (5 bytes), FAT2 (5 bytes), and VBR (1 byte) point to potential disk wiping or formatting. These sizes are much smaller than typical file system artifacts, suggesting that the image has undergone some alteration, and further investigation is necessary.

Conclusion:

Despite the image initially appearing empty, several areas—such as **unallocated space**, **FAT1 and FAT2**, and **slack space**—offer significant potential for data recovery. The small file sizes of key system artifacts such as FAT1, FAT2, and the VBR indicate possible disk wiping or tampering. A thorough analysis of these areas can reveal deleted or hidden data, and further investigation using forensic tools will help uncover the full scope of recoverable evidence.

- You decide that file carving is necessary. What is file carving and how might that be helpful to you?

File carving is a forensic data recovery technique used to extract files or fragments of files from a storage medium based on file signatures, without relying on the file system's metadata (like file names or directory structures). It involves scanning raw disk data, including unallocated space, for recognizable file headers and footers, which are unique byte sequences that identify specific file types (such as PDFs, images, or text documents).
Unlike traditional recovery methods that rely on file system structures like File Allocation Tables (FAT) or Master File Tables (MFT), file carving focuses on the content of the data itself. This technique is particularly useful when file system metadata is missing, corrupt, or deliberately deleted.

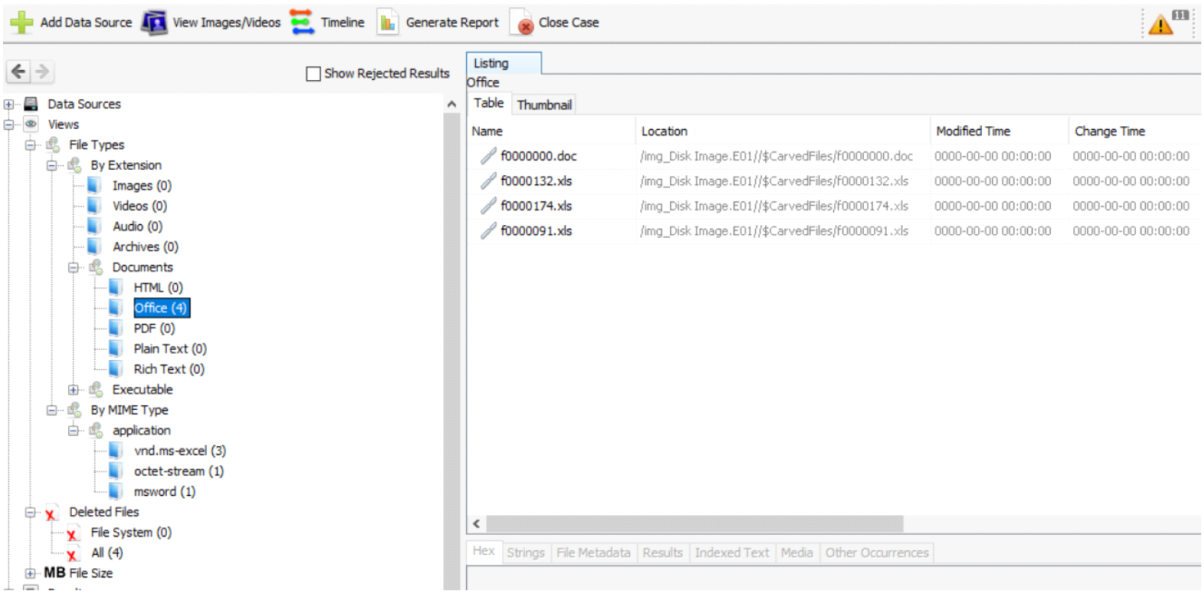
How File Carving is Helpful in This Investigation:

1. **Recovering Deleted or Fragmented Files**:
   - If files were deleted or the file system was intentionally wiped, file carving enables the recovery of these files by identifying and reconstructing the raw data blocks that remain on the disk. Given that the image appears empty and certain system artifacts (like FAT1 and FAT2) have small sizes, it's likely that some files have been deleted or the disk was formatted. Carving can bypass the file system to recover this lost data directly from unallocated space or slack space.
2. **Extracting Data from Unallocated Space**:
   - In this forensic image, unallocated space may contain remnants of deleted files. File carving allows you to scan through this unallocated space to identify files by their unique signatures. Since the file system doesn't track these files anymore, carving is a critical technique to find hidden or lost data in areas that would otherwise be overlooked.
3. **Rebuilding Files Without File System Metadata**:
   - When file system metadata (like file names or directory structures) is unavailable or corrupted, traditional recovery methods may fail. File carving, however, operates by identifying the actual content of the file, making it possible to rebuild the file based solely on its structure and signature. This is particularly relevant in cases where the VBR, FAT1, and FAT2 tables appear altered or wiped, as it allows the recovery of files even without the original directory listing.
4. **Handling Fragmented Files**:
   - Sometimes, files may be fragmented across multiple clusters on the disk. File carving tools can attempt to reassemble these fragmented pieces based on the file signatures and logical sequence, allowing partial or full recovery of the files. This could be especially important if this image involves partial overwrites or disk wiping efforts.
5. **Recovering Specific File Types**:
   - Carving is useful when you are looking for specific types of files, such as documents, images, or emails. For example, if you know that sensitive documents or communication logs are critical in this case, file carving can help focus on those file types by targeting their known headers and footers.

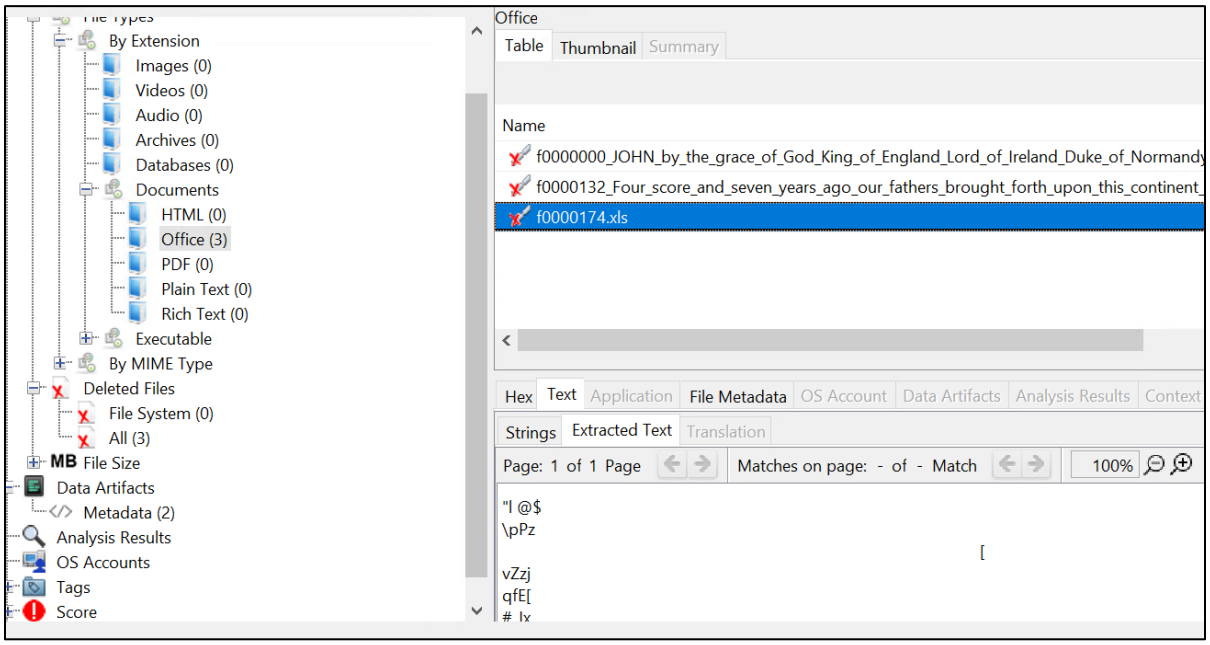
How File Carving Can Be Performed:

1. **Signature-Based Carving**: Forensic tools can be configured to search for specific file types based on their known byte sequences (e.g., JPEG starts with **FF D8** and ends with **FF D9**).
2. **Fragment Reassembly**: In cases where files are broken into fragments across different parts of the disk, the carving tool attempts to reassemble these fragments to create a usable file.
3. **Validation of Recovered Files**: After carving, each recovered file can be validated against its expected structure to ensure the file is complete and usable.

- Now FTK Imager is limited in analysis unless you have the full license. No problem. You decide that you want to use Autopsy to perform file carving. You download and install Autopsy on your PC from https://www.sleuthkit.org/autopsy/download.php where you should look for version 4.8.0 which works best for this exercise. If not, you can download the latest version-- 4.17.0 ***please install this on your computer**
- Then you load the .dd image and Autopsy does the work.
- You see the following contents. **be advised the version of Autopsy, your operating system and/or your computer will make the image look slightly different. Do not worry about this. Work through it.



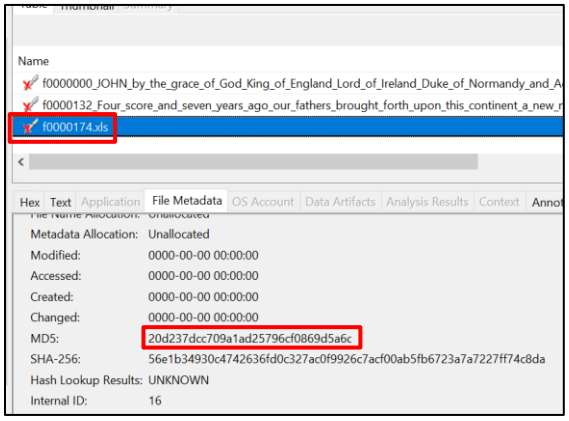
- You start the analysis.

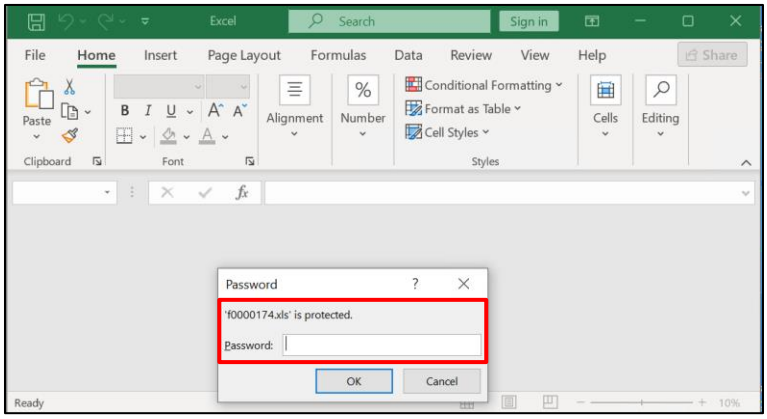


For five points, please answer these questions:

- You see some Word and Excel documents. One of those Excel files is password-protected. What is the MD5 Hash value of that password protected file?
    - Hint: In the viewing screen of Autopsy, each artifact will have an MD5 hash value.
    - Hint – you may have to exact the files from Autopsy to your computer to open it so you can see what files are password protected.

Answer: 20d237dcc709a1ad25796cf0869d5a6c

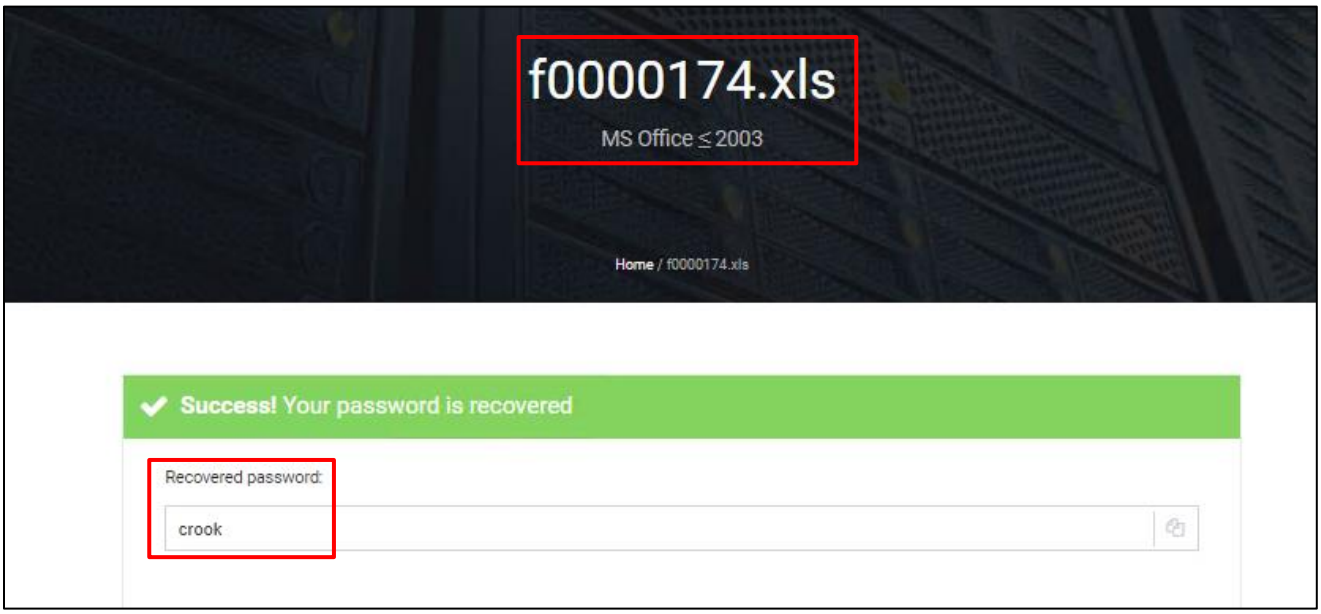




- You find the password protected file. It is asking you for a password. What is the password?
    - Hint – don't overthink this. Sometimes people might use their first or last names as passwords… try this. You can also use an online password cracker. Try both

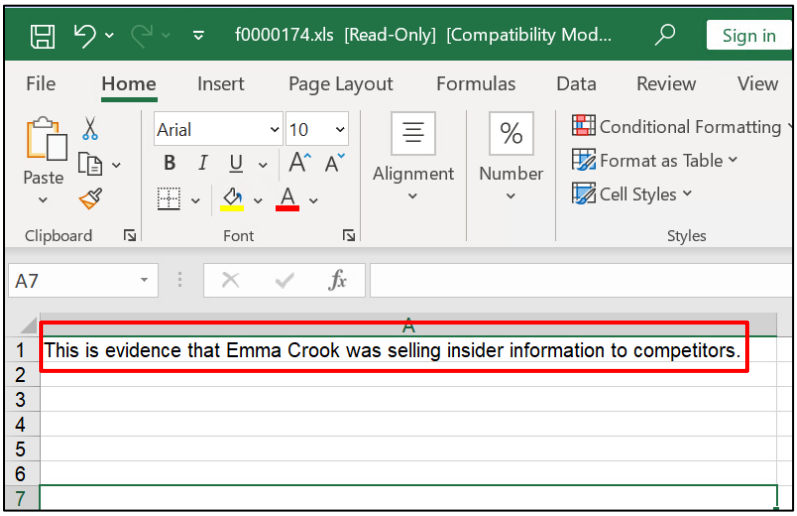
Answer: Randon Guess: crook

Online Cracker Tool: crook

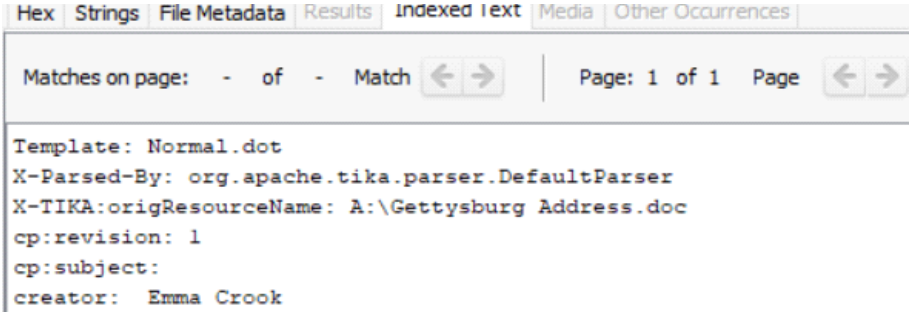


- You figure out the password – what is the information in the file?
    - Hint: The information starts with "*This is evidence that.. "*

Answer: This is evidence that Emma Crook was selling insider information to competitors.

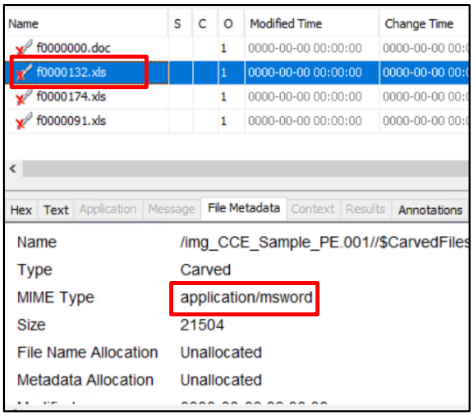


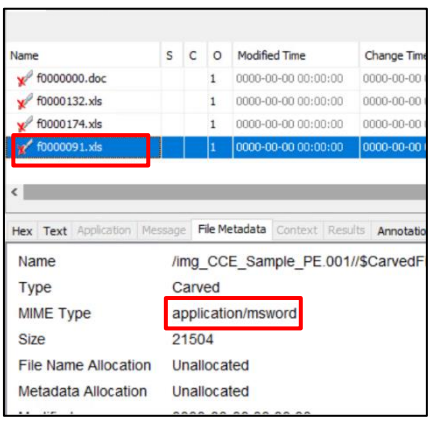
- You look at the other Excel spreadsheet file(s). You can view the metadata and its content in Autopsy but when you extract them and try to open them in Excel you get an "invalid file format". You puzzle over it then you figure it out – it's because this is not an Excel file. It is something else. What kind of file (document type) is this? and how can you fix this?
    - Hint: Look at the metadata – here is a snippet

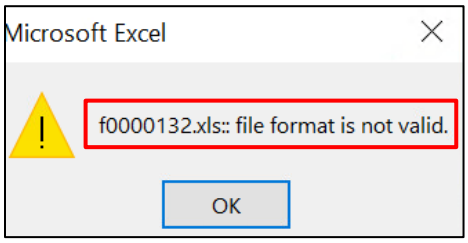


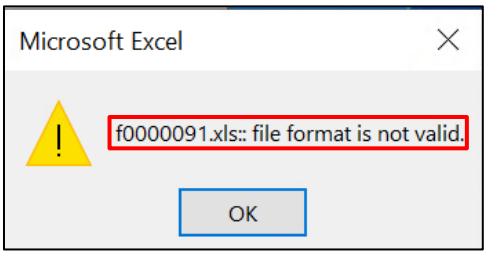
    - Hint: When you fix this – this is done by changing the file extension

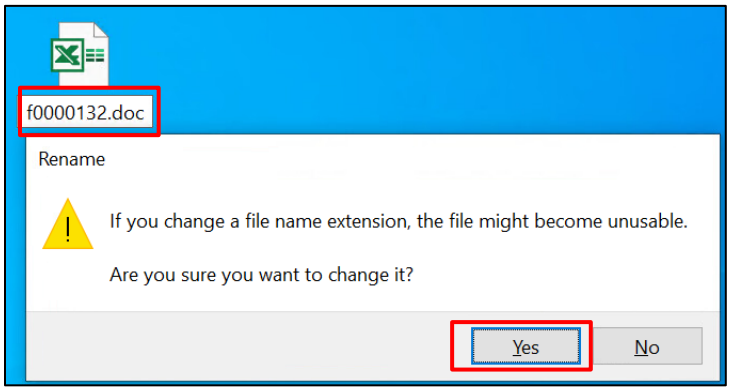
Answer: Microsoft Word documents (.doc)
We can change the extension to **.doc** and view them as **Microsoft Word Document**.

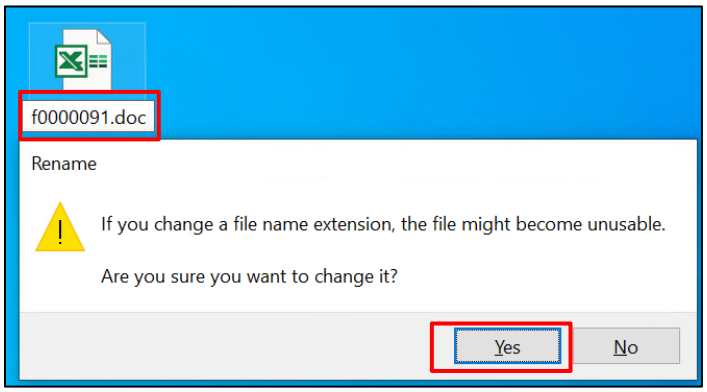


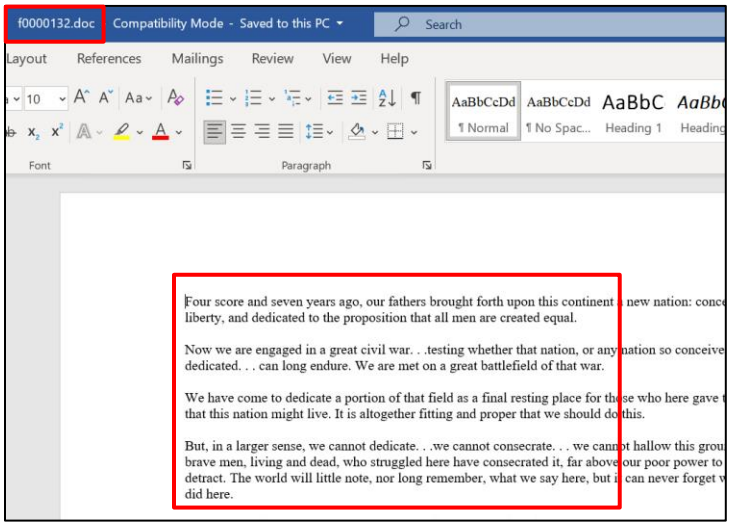


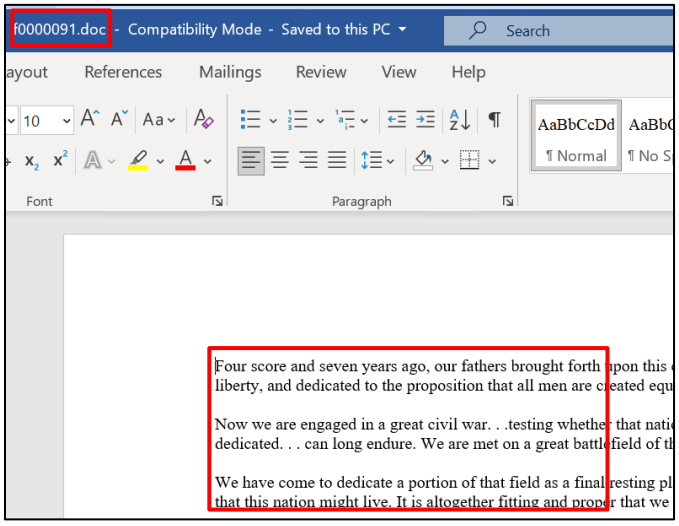












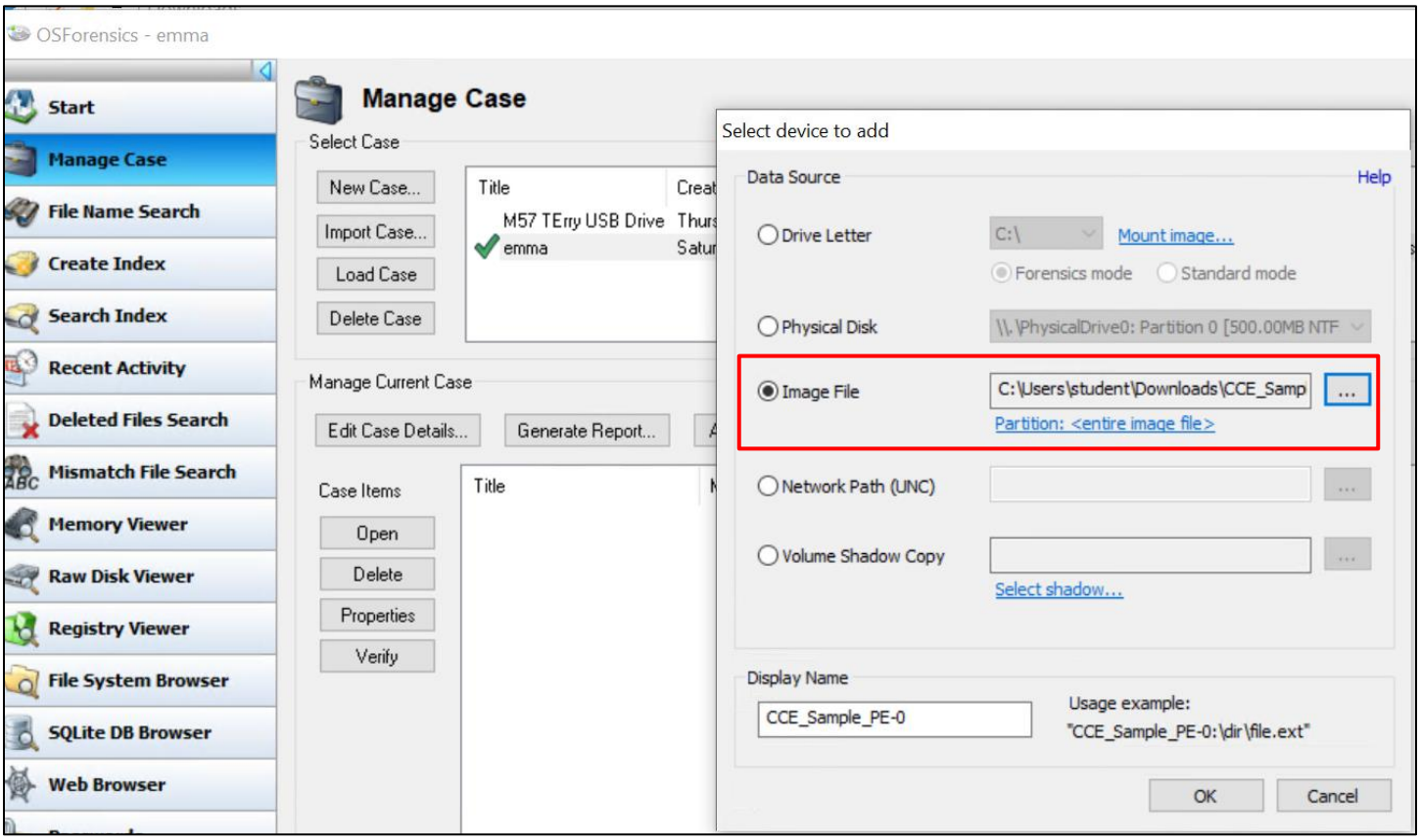
Bonus Question – 5 points

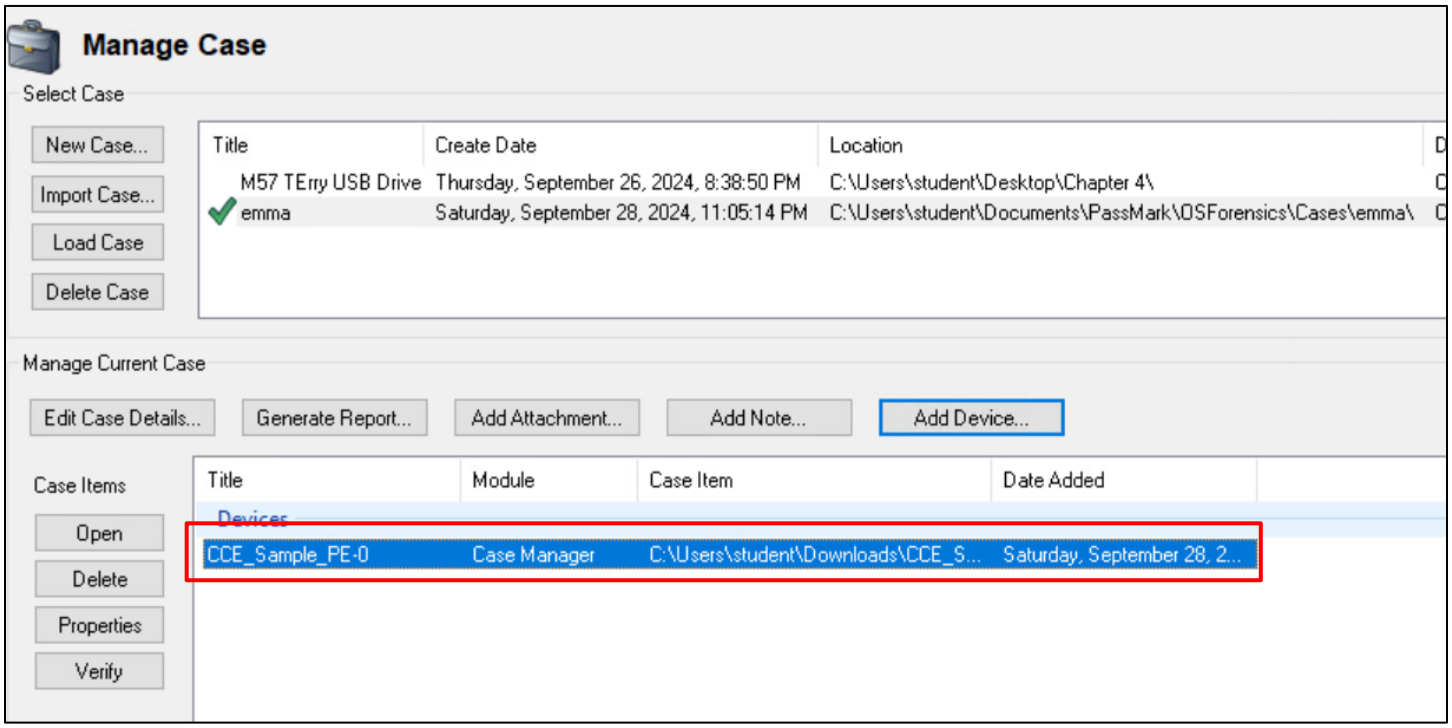
You may have a tool that will not work with .001 images (DD) images but the tool can handle E01 files. How can you convert the DD image into an E01 image? Figure this out and if you send me the E01 image then I will give you 5 extra points which will make this quiz 10/10 + 5

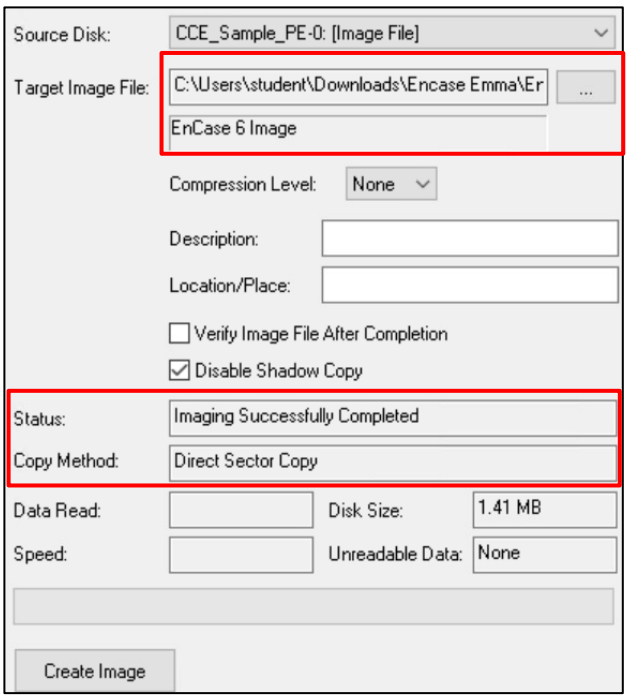
Hint: check out the EnCase Imager tool at https://www.guidancesoftware.com/encase-forensic-imager . Here, you could ingest the .001 image into EnCase and then "reacquire" it as an 001 image. Do you think you can figure this out? This is a very useful nugget to know. **You may not be able to download EnCase as you need a paid license. What will you do now?

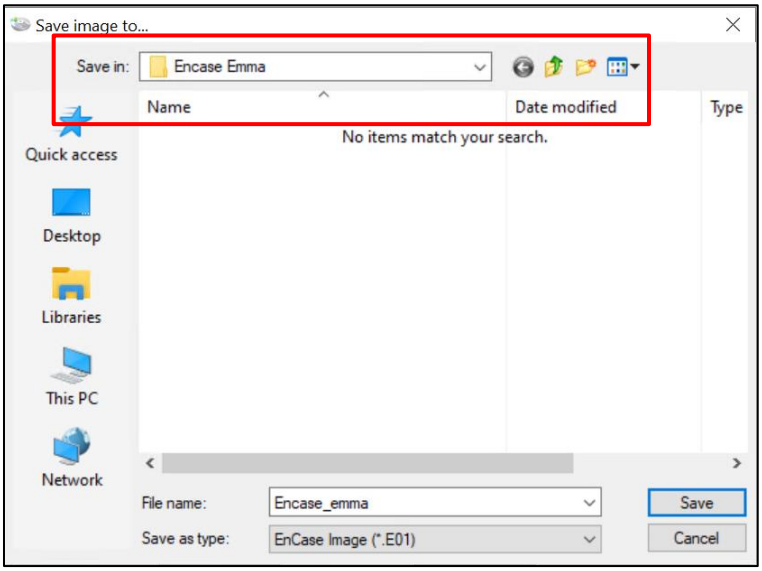
Tools you can use: (but certainly not the only tools) WinMD5, FTK, ProDiscover, Free Word-Excel password cracker. All of these tools are free online

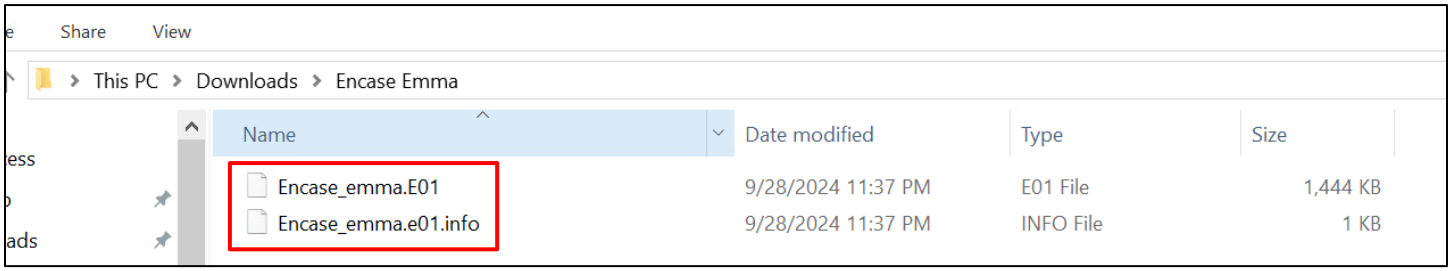
We are doing with OS forensics:











Link for File: [Encase_emma.E01]