Using FTK Imager

Please note that this is an *imaging tool*, however for the purpose of learning and this lab we will use it for some basic analysis.

After completing this lab, I would suggest creating a forensic duplicate/image of your own laptop or storage device.

In this forensic analysis, we will delve into the examination of a thumb drive that has been obtained under peculiar circumstances by a group of UFO enthusiasts. They claim that this thumb drive contains vital evidence pertaining to a undercover government program. According to their claims, this program involves regular interactions with extraterrestrial civilizations and utilizes advanced alien technology for space exploration. The situation took a more ominous turn when their undercover agent within the government agency became apprehensive about potential compromise and made an attempt to destroy some of the sensitive information.

Following this event, the agent left the thumb drive at a pre-arranged location, known as a "dead drop," and subsequently disappeared without any further contact with the group. Faced with this puzzling scenario, the UFO enthusiasts have taken the careful step of creating an image of the thumb drive and have enlisted the services of our investigative firm to scrutinize the digital contents. Our primary objective is to determine what insights and conclusions can be derived from the information contained within this thumb drive image.

To facilitate this investigation, we will employ FTK Imager, a robust imaging utility developed by AccessData. Beyond its fundamental functionality of creating disk images, FTK Imager offers us the capability to thoroughly explore and analyse the contents of a disk image, revealing hidden insights that may shed light on the mysterious circumstances surrounding this case.

As we progress through this forensic analysis, it is essential to keep in mind that a set of questions has been provided at the conclusion of this lab. These questions serve as a crucial component of our assessment and must be answered thoroughly to ensure that we have comprehensively addressed all issues of this investigation. It is advisable to reference these questions as we navigate through the various steps of this lab.

FTK Imager will serve as our invaluable tool in unlocking the secrets concealed within the thumb drive image, ultimately enabling us to unravel the mysteries surrounding this intriguing case.

FTK Imager can be downloaded from the "FTK Imager" section of https://www.exterro.com/ftk-imager there is also a download version on moodle/brightspace

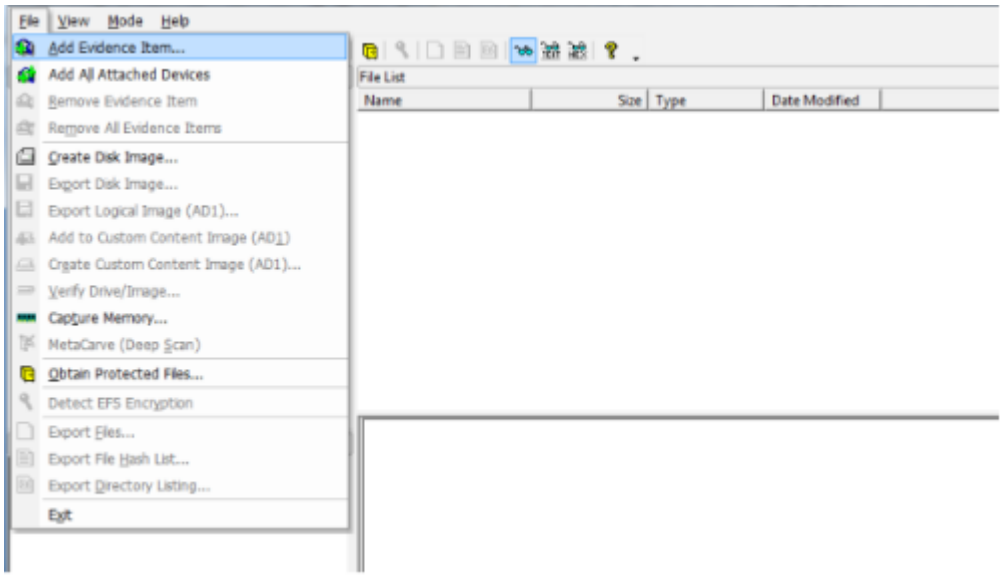
"As you prepare to start on this forensic investigation, it's worth noting that a comprehensive reference manual for the FTK Imager is at your disposal. This manual can be a valuable supplementary resource throughout the course of this lab, offering detailed insights and guidance on utilizing the software effectively".

To initiate this investigation, your first step is to download the provided folder, labelled 'AlienImage.zip,' which compresses the image of the secretive thumb drive, 'alienimage.dd,' along with its corresponding hash file, 'alienimage.md5.' You can access this folder from the course page on moodle/brightspace, and it should be saved to a designated directory on your computer/laptop.

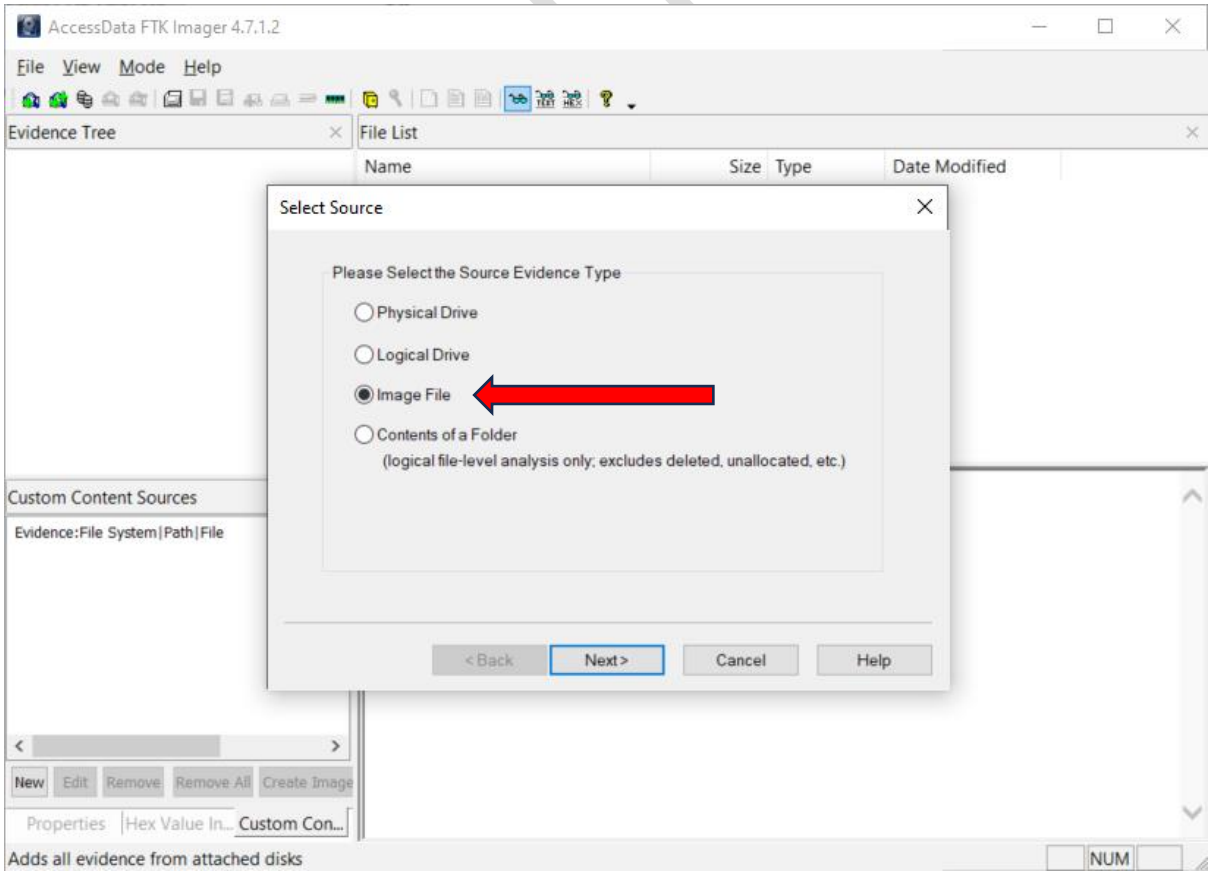
Note: We are using the latest version of FTK Imager, some steps maybe be different, so we need to troubleshoot and refer to the user manual.

Start FTK Imager by clicking on its icon If you receive a security warning, click OK to allow the program to run.

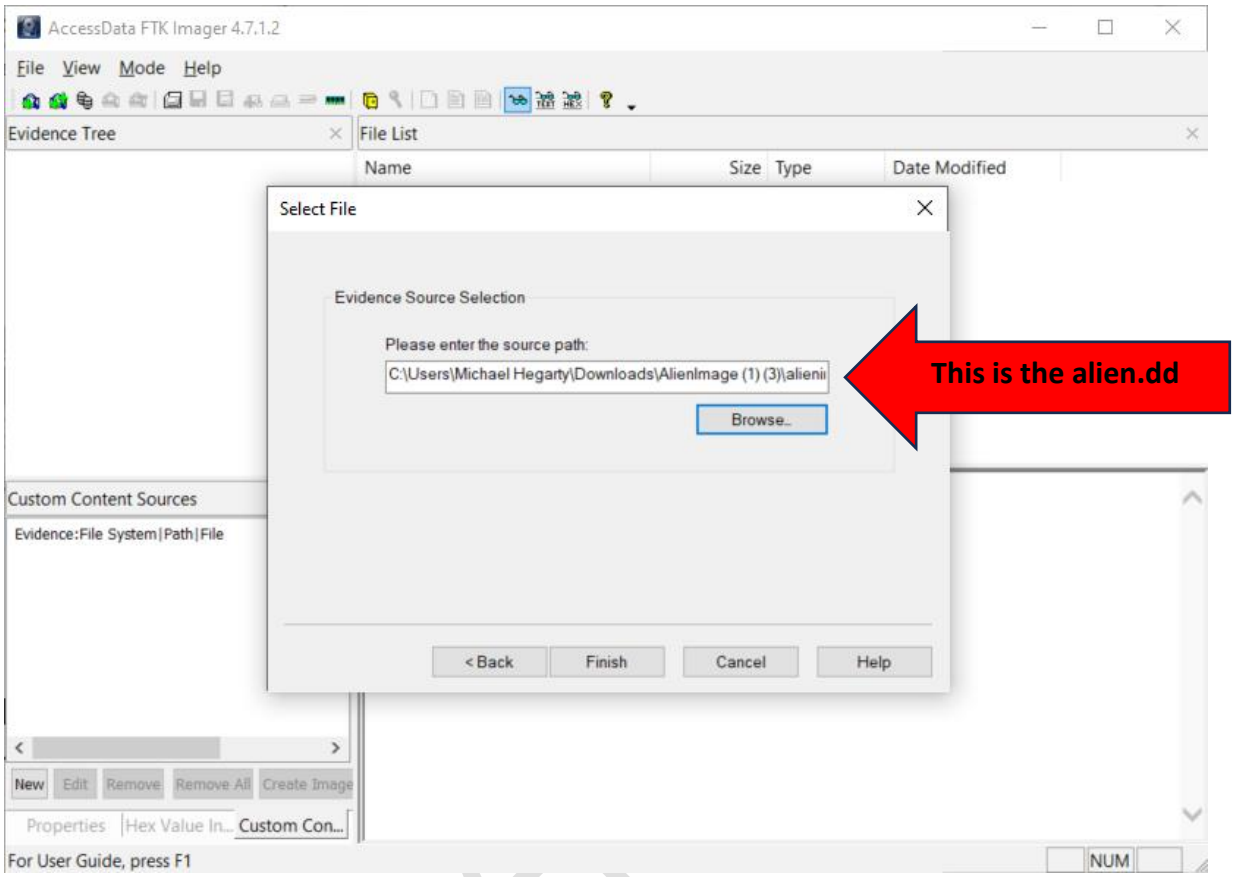
Click on “File” and then “Add Evidence Item”



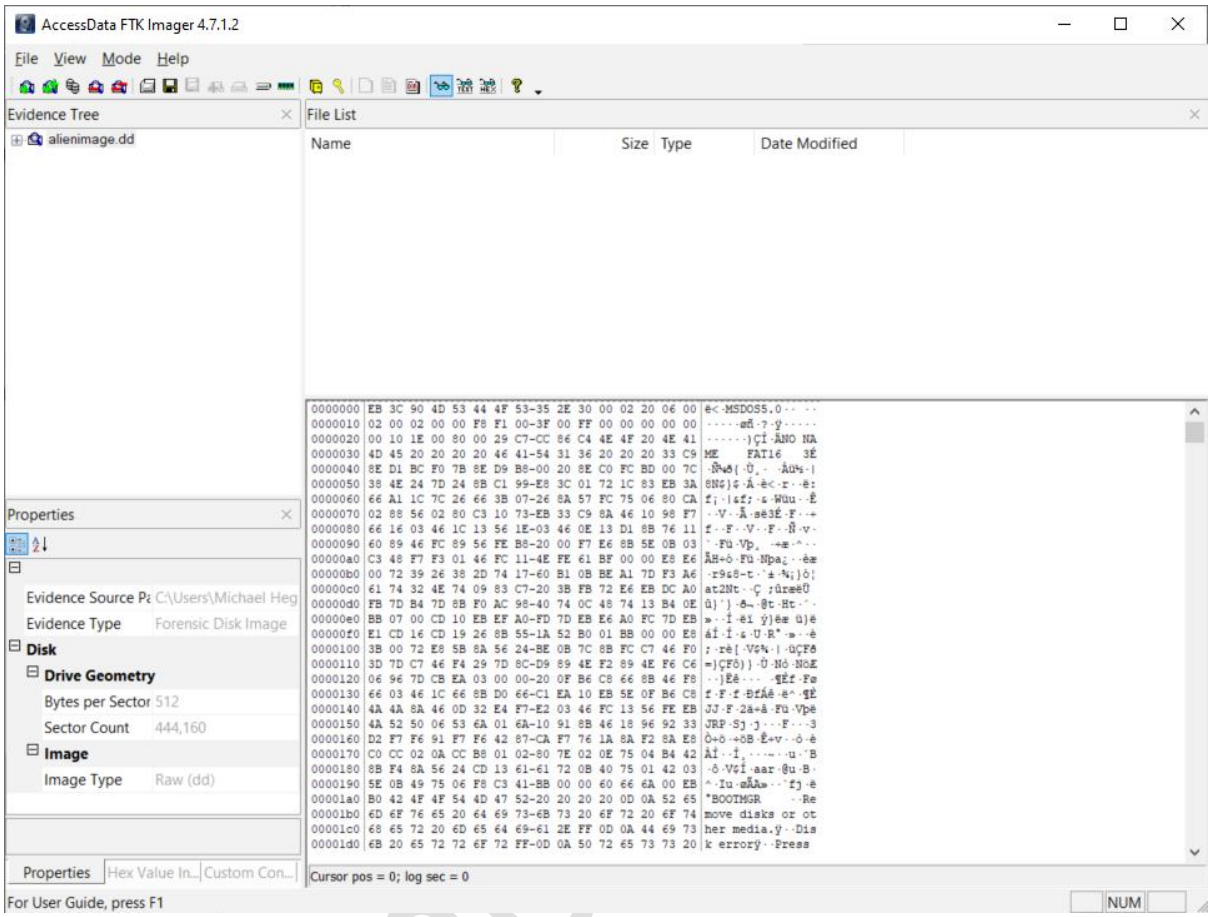
Select “Image File” in the “Select Source” dialog and click on “Next”.



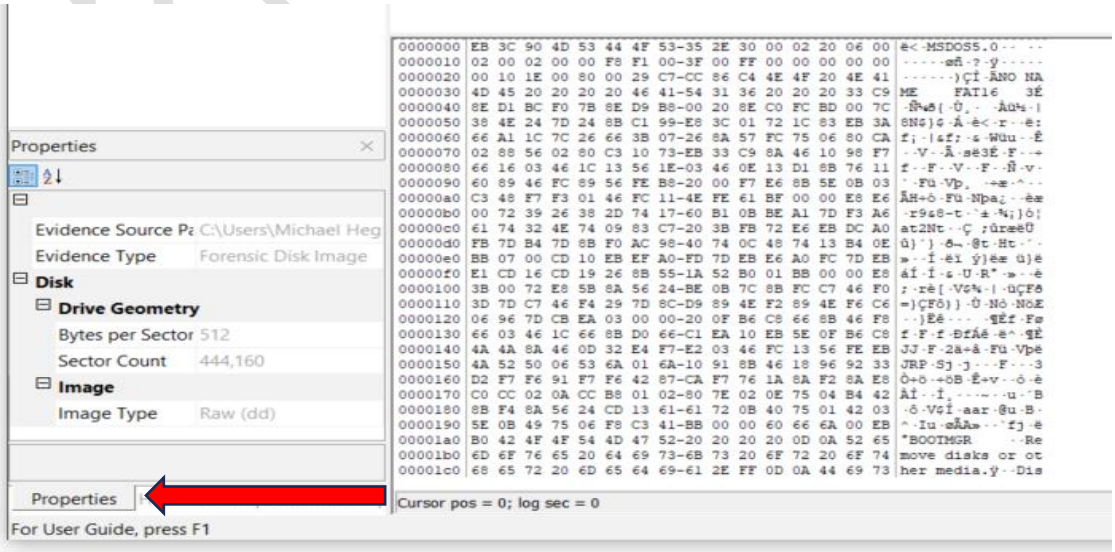
In the “Select File” dialog, browse to the location where you extracted the alienimage.dd file, select it and click on “Finish”.



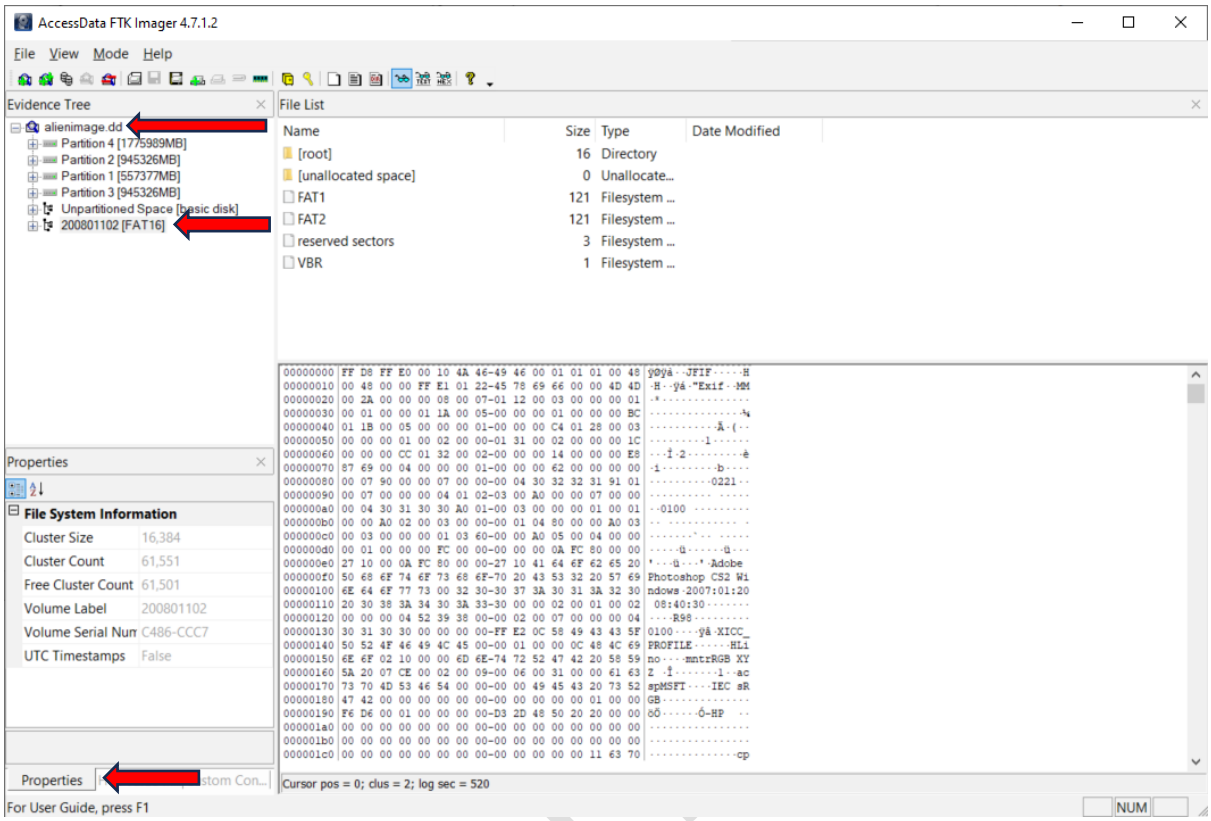
FTK Imager's default display will appear with the contents of the thumb drive visible in the "View" pane at the lower right.

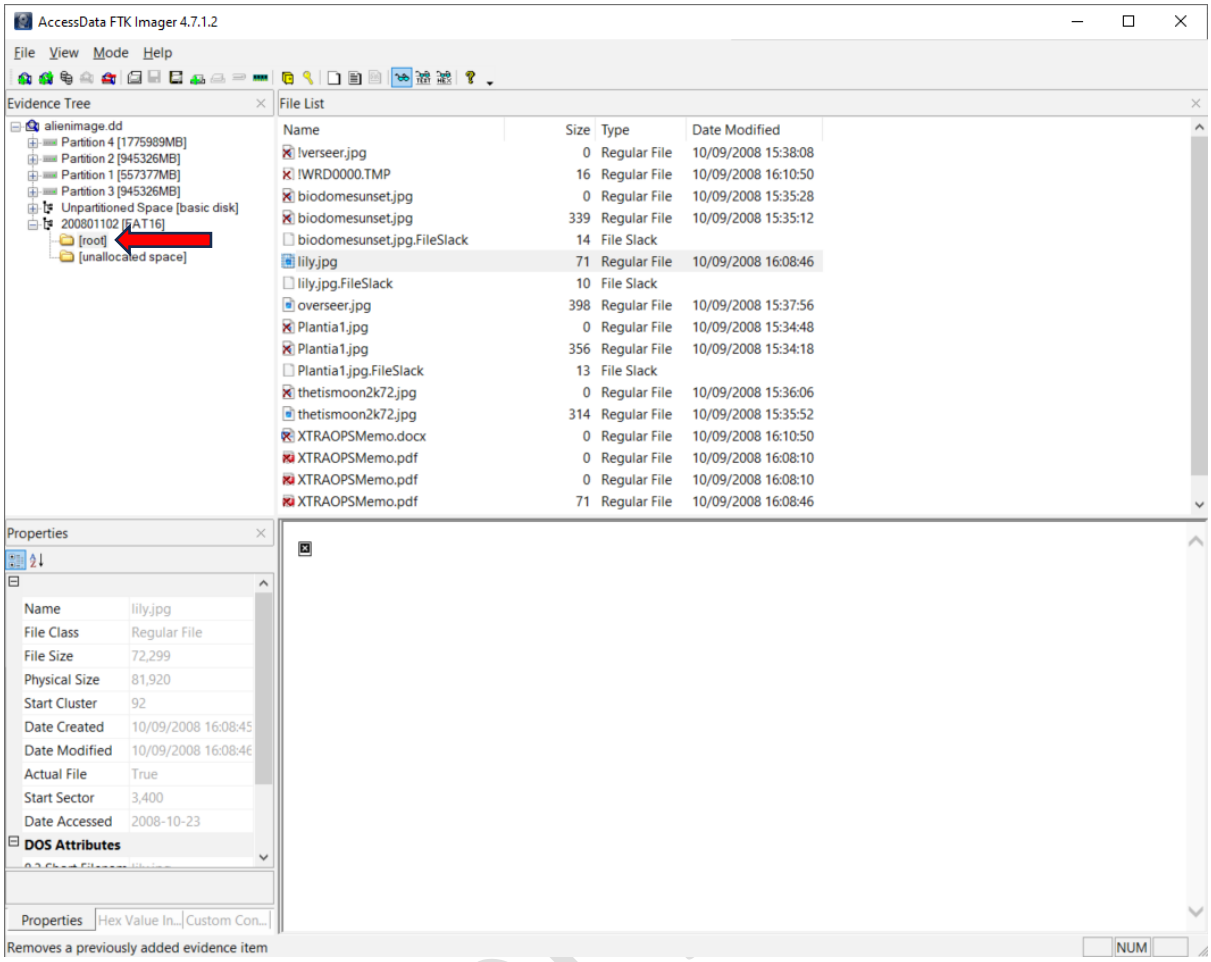


Click on the "Properties" tab below the lower left pane to view the properties for the disk image.



Click on the “+” sign next to “alenimage.dd” in the “Evidence Tree” and then on “200801102 [FAT16}” to cause the file system properties to appear in the “Properties” tab.

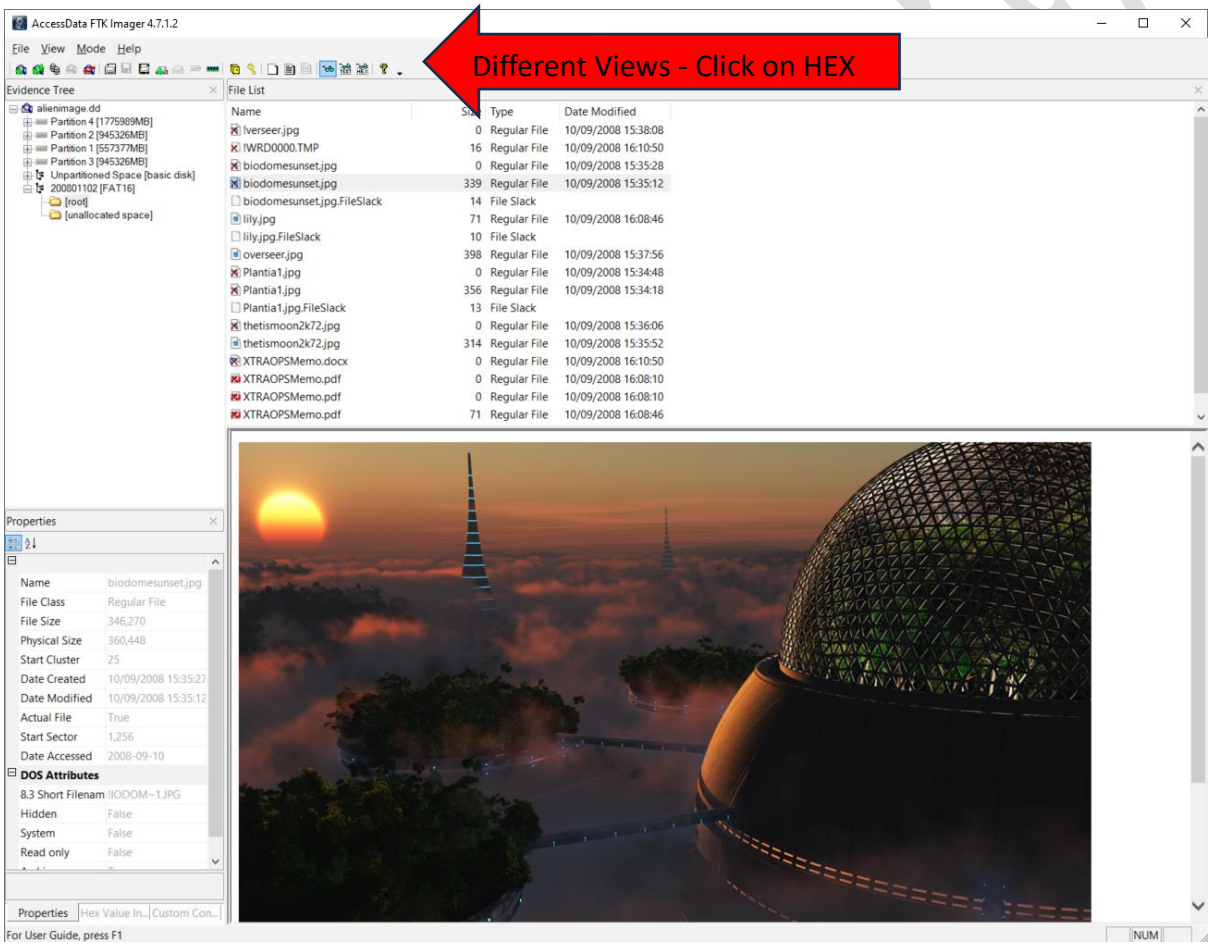


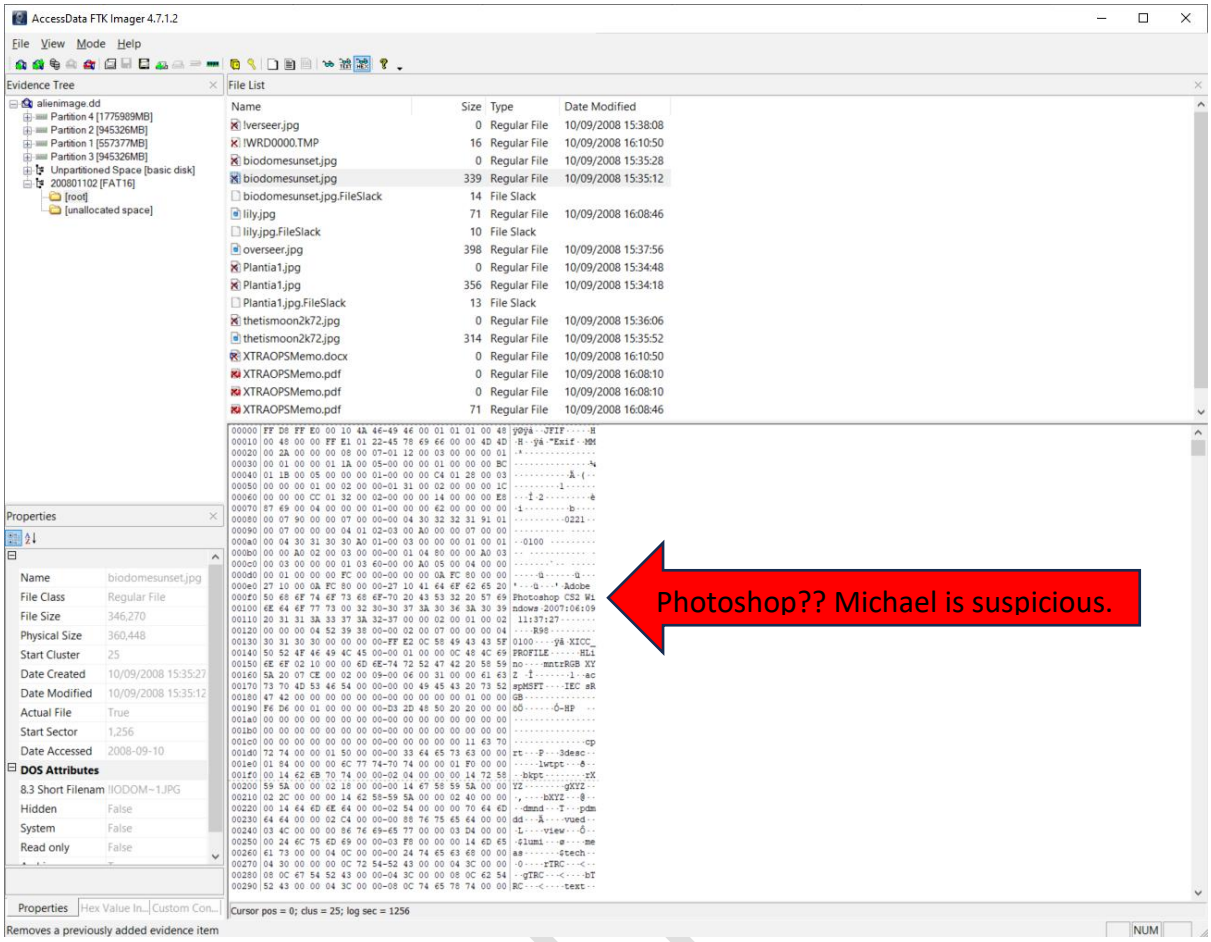


Accessing the Root Directory: Start by clicking on the “[root]” entry in the “Evidence Tree” pane. This action will display the root directory of the thumb drive within the "File List" pane. Keep in mind that within this list, deleted files are easily identifiable by a red "X" superimposed over the icon derived from their file extension. Notably, some deleted files may show a size of 0KB, indicating that their data has been overwritten and is no longer recoverable. Additionally, in the "View" tab, you will notice that the hex contents of the directory are displayed, providing a deeper insight into the file structure.

Selecting a File for Inspection: Proceed to select a file of interest from the “File List” by simply clicking on it. Observe that the "Properties" pane and the "View" pane will dynamically update to provide you with pertinent information about the selected file. Within the "Properties" pane, you'll find details such as the file's Modified, Accessed, and Created (MAC) times, its size, and other relevant information. This data can be invaluable for establishing a timeline and understanding the file's characteristics.

Examining an Image File: Take the file named “biodomesunset.jpg” (Click on the file that size is 339) as an example, with a file size of 339KB. As you select this file, you'll notice that an image preview appears in the "View" pane, allowing you to visually inspect the image content. To delve deeper into the file's hexadecimal content, navigate to the "Mode" option and select “Hex” from the dropdown menu. This action will transition the view pane from displaying the image to presenting the hexadecimal representation of the file. This shift to the hex view can be crucial for forensic analysis, as it exposes the raw data, which may contain hidden information or clues.

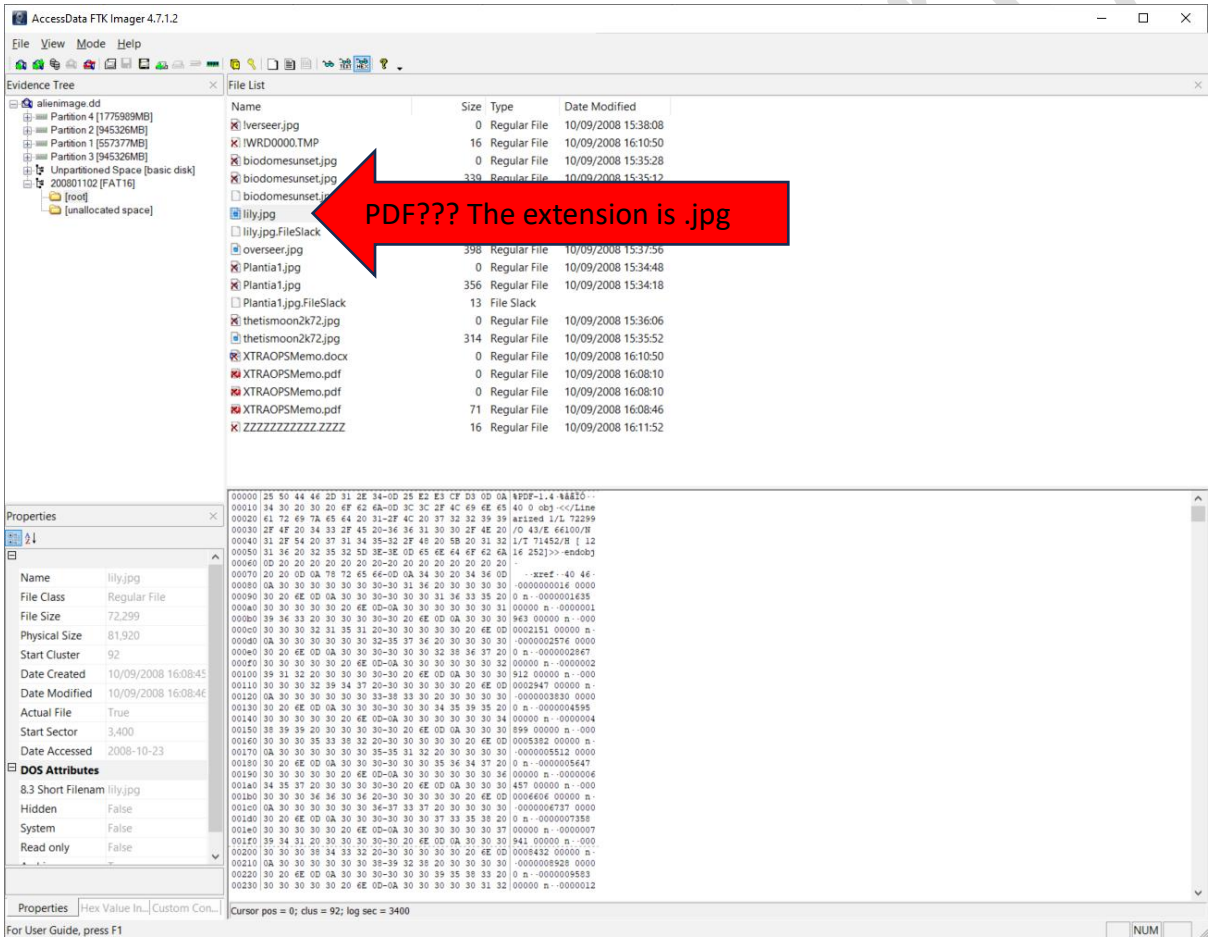




Identifying EXIF Information: While in the hex view, carefully examine the text within the hex content. Pay special attention to any arrowed text that mentions "Adobe Photoshop." This text is part of the "Exchangeable Image File Format" or "EXIF" information, which is commonly inserted into image files by various digital cameras and graphics programs. EXIF data contains valuable details about the image's creation and editing history. To make full use of this information, an EXIF viewer can be employed, and you can find many such tools available on the Internet.

Returning to Automatic View Mode: To revert to the automatic view mode, ensuring that the image is once again visible, follow these steps. Click on the "Mode" option located on the toolbar and select "Automatic" from the dropdown menu. This action will switch the view pane back to displaying the image content, making it easier to visually assess the file.

Analyzing the "Lily.jpg" File: Now, shift your focus to the file named "Lily.jpg" in the "File List" pane. You'll observe that a red "x" is displayed in the "View" pane, indicating that the file cannot be interpreted as an image in its current state. Several factors could contribute to this situation, including file corruption or other issues affecting its integrity. As before, you can switch the view to hex mode by employing the same method as earlier.



Identifying a Signature Mismatch: Take note of the presence of the string "PDF" in the first few bytes of the file. This observation suggests that there may be a mismatch between the file's actual contents and its file extension. To further investigate this, perform the following steps:

- Right-click on the file "lily.jpg" within the "File List" pane.
- From the pop-up menu that appears, select "Export Files."
- Follow the ensuing dialog prompts to export the file from the image into a file stored on your computer.
- After exporting, navigate to the location where you saved the file on your computer.
- Rename the exported file to "lily.pdf."
- Attempt to open this file as a PDF document, and if necessary, download and install Adobe Acrobat Reader if it's not already installed on your system. This step aims to assess whether the file indeed contains PDF content despite its misleading file extension.

Examining the "ZZZZ" Extension File: The file with the "ZZZZ" extension appears unconventional and warrants further investigation. Explore its contents meticulously to determine if you can draw any conclusions regarding its nature or purpose.

Assessing Remaining Files: Continue your examination by reviewing the contents of the remaining files present in the thumb drive image. Consider their potential relevance and significance to the overarching questions of the case. Carefully examine each file for any clues or information that might shed light on the mysterious government program and its connection to extraterrestrial activities.

These instructions guide your forensic analysis using FTK Imager and encourage a thorough exploration of the digital evidence contained within the thumb drive image to unravel the mysteries associated with the case.

PLEASE READ: Michael Hegarty in NOT a conspiracy theorist 😊

In conclusion, our exploration of FTK Imager has demonstrated the significant value that can be derived from this free forensic tool in the context of a digital investigation. While FTK

Imager may not provide the extensive capabilities of a comprehensive forensic suite (which we will cover in the coming weeks), it nonetheless underscores the wealth of information that can be uncovered when examining digital evidence.

Throughout this analysis, we have uncovered critical insights into the thumb drive's contents, including the discovery of potentially mismatched file signatures, the ability to export and manipulate files, and the examination of unusual file extensions. These findings underscore the importance of thorough and systematic forensic analysis, even when working with limited tools.

FTK Imager serves as a valuable introduction to forensic techniques and methodologies, offering a glimpse into the world of digital investigations. It highlights the significance of file metadata, hexadecimal analysis, and the interpretation of hidden data such as EXIF information within image files. These skills are fundamental for forensic practitioners, emphasizing the importance of both file content and file metadata in establishing timelines, identifying anomalies, and ultimately unravelling the truth behind digital mysteries.

FTK Imager may not be a fully comprehensive forensic solution, it serves as an essential steppingstone in the realm of digital investigations, showcasing the substantial insights that can be gleaned from even a free and readily accessible tool.

Although available for free download, FTK Image is a commercial validated tool that is widely used by industry professionals.

https://www.dhs.gov/sites/default/files/publications/test_results_for_ftk_imager_version_4.3.0.18_with_coverjd1gd2.pdf

Answer the following questions to the best of your ability (you may use screenshots to support your answers). Answer questions on a MS Word document and upload to moodle/brightspace when finished.

Drive Image File System Identification:

What can we deduce about the file system in use on the drive based on the hex content of the drive image?

Drive Image Properties Analysis:

Extracting information from the image file properties, what are the sector count and image type associated with the drive image?

File System Examination:

Investigating the file system properties within the image, what is the cluster size?

How many clusters are currently in use, and how many remain free?

Interpreting Hexadecimal Patterns:

In the hex view of the directory, what is the significance of the recurring "E5" pattern, often appearing as the first character of a filename?

Timeline Construction:

When examining the MAC-times (Modified, Accessed, Created) for all files in the root directory, do these timestamps align with the narrative presented by the UFO group?

EXIF Data Insights:

Analysing the EXIF information found within some of the photographs, what conclusions can be drawn regarding their origin and history?

File Signature Mismatch:

Does the file "lily.jpg" exhibit a signature mismatch?

If so, does the content of this file provide any substantial insights that influence our overall conclusions?

Assessing UFO Group Claims:

Based on the images that have been recovered, what conclusions can be drawn regarding the UFO group's suspicions regarding off-world activities by a secret government organization?

Detecting Secure Deletion:

While examining the files within the image, can any traces of a secure deletion utility be identified?

Hint: Consider researching the operation of the "sdelete" utility, available from the Sysinternals website.

Metadata Analysis: (Metadata refers to data that provides information about other data)

What additional information can be gleaned from metadata within the image, such as file owner details, permissions, and file attributes?

Recovery Potential:

Are there any signs of data fragments or remnants in unallocated space that may be recoverable or relevant to the investigation?

Correlation with Dead Drop Location:

Can any information within the image provide insights into the whereabouts or fate of the agent who left the thumb drive at the dead drop location?

Imaging Tools

List four different forensic imaging tools that are available.