Computer & Network Forensics

Lab 2

Using FTK Imager

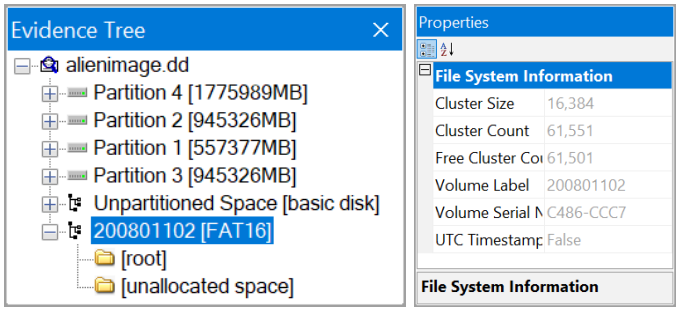
Questions

1. Drive Image File System Identification:

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

   FAT16

   – The hex content of the drive image indicates that the file system in use is FAT16. This is confirmed by the FTK Imager “Properties” tab under the image tree, where “200801102 [FAT16]” is shown. FAT16 was commonly used on small storage devices, which aligns with the fact that this is a thumb drive.

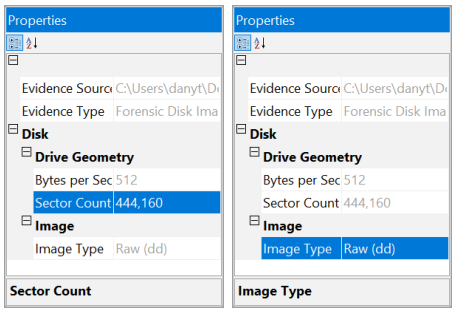


2. Drive Image Properties Analysis:

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

   Sector Count: 444,160

   Image Type: Raw (dd)



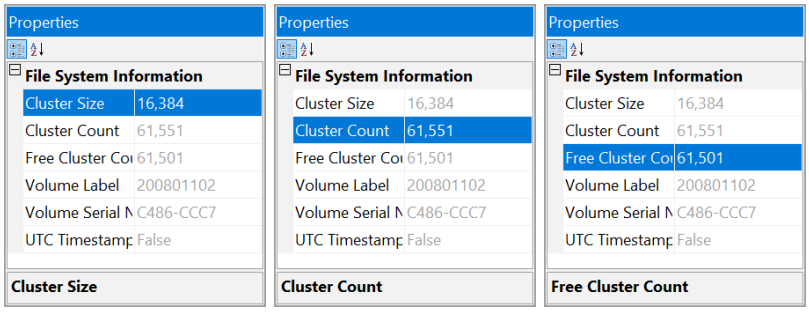
3. File System Examination:

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?

Cluster Size: 16,384

Clusters in Use: 61,551 - 61,501 = 50 (*'Cluster Count' - 'Free Cluster Count'*)

Free Cluster Count: 61,501

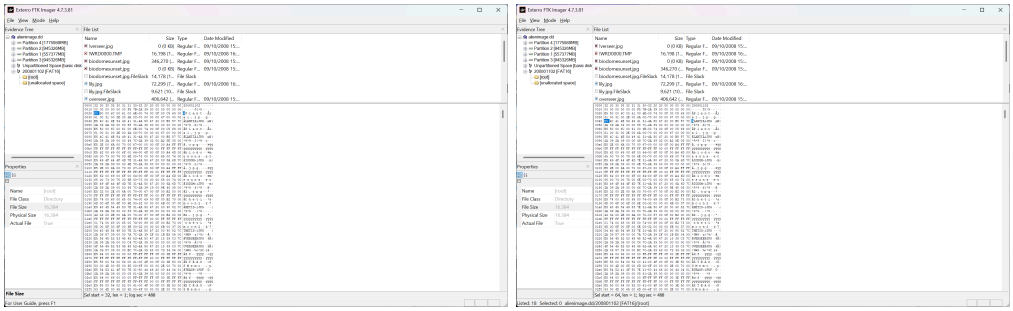


4. Interpreting Hexadecimal Patterns:

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?

If the entry is deleted the first byte is changed to E5

– The recurring “E5” in hex denotes a deleted file entry. In FAT file systems, when a file is deleted, the first byte of the filename is replaced with “E5” to mark it as deleted while leaving the rest of the entry intact until it is overwritten.

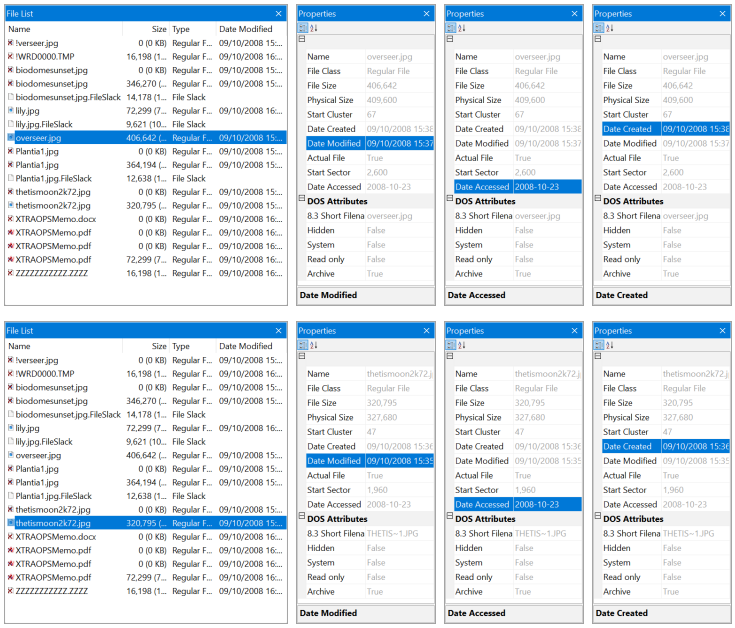


5. Timeline Construction:

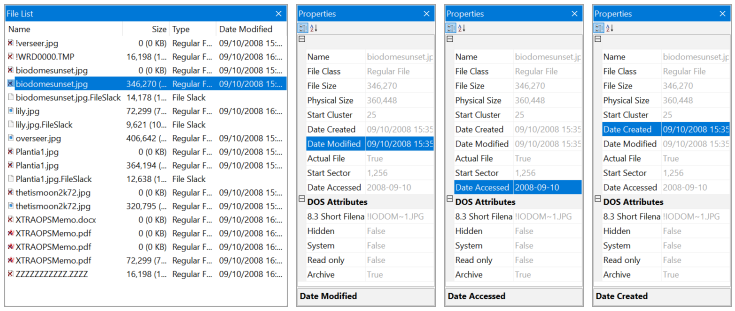
When examining the MAC-times (Modified, Accessed, Created) for all files in the root directory, do these timestamps align with the narrative presented by the UFO group?

overseer.jpg and thetismoon2k72.jpg

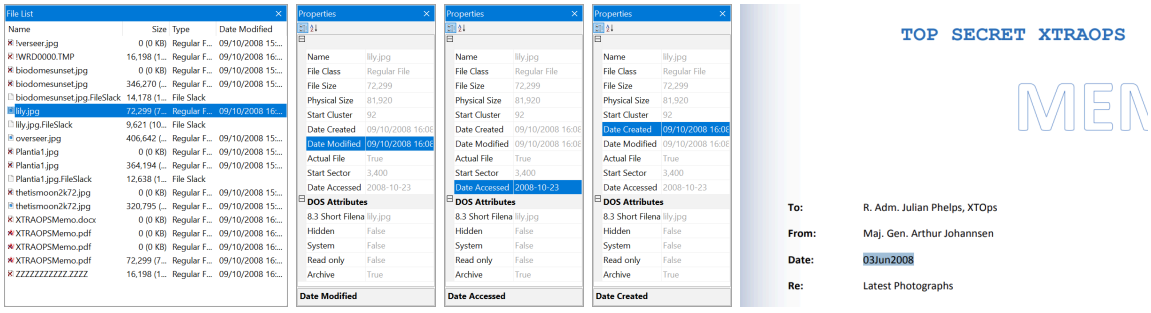
– When analyzing the MAC times of files such as overseer.jpg and thetismoon2k72.jpg, I observed inconsistencies. For example, overseer.jpg shows a Modified time of 09/10/2008 15:37:56 but a Created time of 09/10/2008 15:38:06 (10 seconds later). Similarly, thetismoon2k72.jpg was Modified at 15:35:52 but Created at 15:36:05.



All images were created on the same day - 09/10/2008
– The MAC-times (Modified, Accessed, Created) mostly cluster around similar dates, which appear manually manipulated rather than natural use. While they could align with the UFO group's narrative of a "rushed attempt to destroy data," the suspicious uniformity and lack of normal variation suggest the timestamps may not be reliable.



TOP SECRET file – Date in "lily.pdf" file is 03Jun2008, but the file was created at 09/10/2008 16:08:45 (10Sep2008)

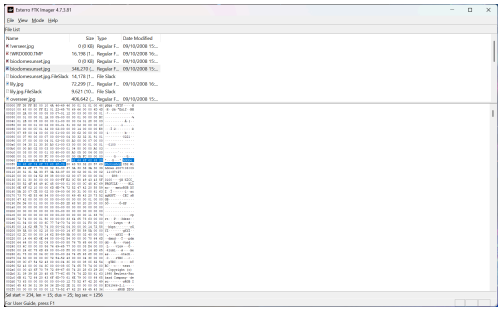


6. EXIF Data Insights:

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

   biodomesunset.jpg

   – The image file contained EXIF metadata showing they were edited in Adobe Photoshop. This undermines claims that the images are “raw alien evidence”, since they have been manipulated.

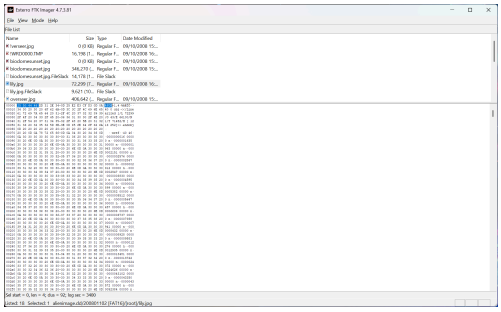


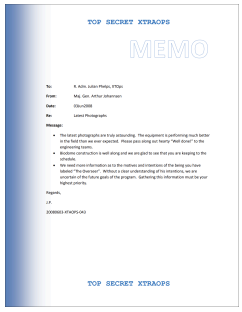
7. File Signature Mismatch:

   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?

   lily.jpg → lily.pdf

   – Yes, “lily.jpg” shows a file signature mismatch. Its extension is “.jpg”, but its hex header begins with “%PDF”, which identifies a PDF file.
   When renamed and opened as “lily.pdf”, it displays a PDF document. This shows intentional obfuscation, suggesting sensitive information was hidden under misleading extensions.





8. 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?

   No

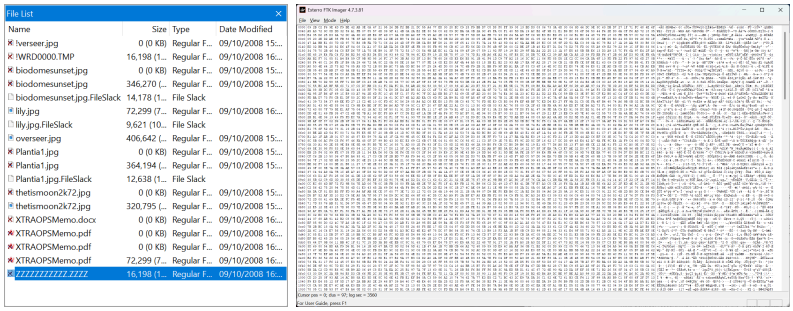
   – The images and documents recovered do not provide credible proof of extraterrestrial contact. Instead, they show signs of editing, hidden PDFs, and mismatched metadata. This suggests that while the files may be part of a hoax or cover operation, there is no verifiable evidence of alien technology.

9. Detecting Secure Deletion:

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

   ZZZZZZZZZZZ.ZZZZ

   – During analysis, a suspicious file named ZZZZZZZZZZZ.ZZZZ was discovered on the drive image. This naming pattern is consistent with the behavior of the Sysinternals “SDelete” utility, which not only overwrites file contents but also renames deleted files with repetitive or placeholder names (such as ZZZZ...) to obscure the original filename in the file system metadata. Therefore, it can be reasonably concluded that a secure deletion tool, likely SDelete, was used on this thumb drive.

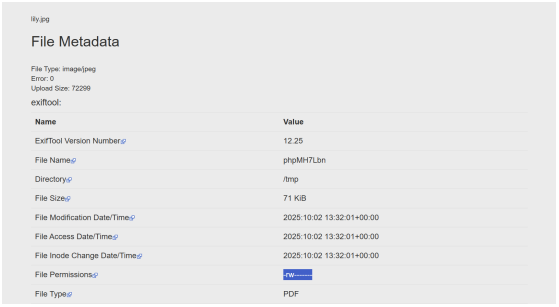


   Hint: Consider researching the operation of the "sdelete" utility, available from the Sysinternals website.

10. Metadata Analysis:

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

    File Permissions: All files exhibit permissions of -rw-------, meaning they are only accessible for read/write by the owner.



lily.jpg

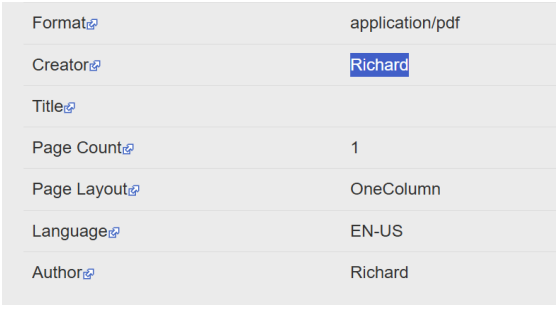
File Metadata

File Type: image/jpeg
Error: 0
Upload Size: 72299

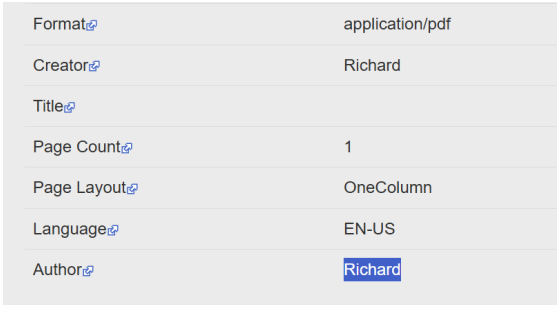
exiftool:

Name	Value
ExifTool Version Number	12.25
File Name	phpMH7Lbn
Directory	/tmp
File Size	71 KiB
File Modification Date/Time	2025:10:02 13:32:01+00:00
File Access Date/Time	2025:10:02 13:32:01+00:00
File Inode Change Date/Time	2025:10:02 13:32:01+00:00
File Permissions	-rw-------
File Type	PDF

Author/Creator Information: The file lily.jpg (actually identified as a PDF) lists its author/creator as Richard, providing a personal attribution link to the file's origin. This may indicate the system user who created the document.

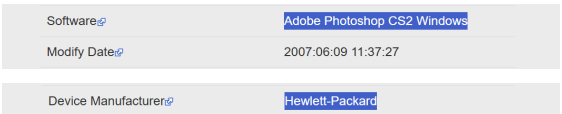


Format	application/pdf
Creator	Richard
Title	
Page Count	1
Page Layout	OneColumn
Language	EN-US
Author	Richard

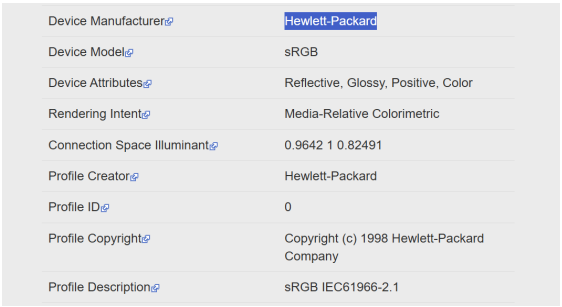


Format	application/pdf
Creator	Richard
Title	
Page Count	1
Page Layout	OneColumn
Language	EN-US
Author	Richard

EXIF/Software Metadata: Examination of biodomesunset.jpg shows it was modified using Adobe Photoshop CS2 on Windows, with a Hewlett-Packard color profile embedded. This reinforces earlier findings that the images were edited and are unlikely to be untouched "evidence."

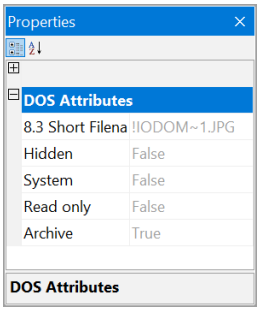


Software	Adobe Photoshop CS2 Windows
Modify Date	2007:06:09 11:37:27



Device Manufacturer	Hewlett-Packard
Device Model	sRGB
Device Attributes	Reflective, Glossy, Positive, Color
Rendering Intent	Media-Relative Colorimetric
Connection Space Illuminant	0.9642 1 0.82491
Profile Creator	Hewlett-Packard
Profile ID	0
Profile Copyright	Copyright (c) 1998 Hewlett-Packard Company
Profile Description	sRGB IEC61966-2.1

DOS/File Attributes: FAT-based attributes (such as archive, hidden, and read-only flags) are present but reveal nothing unusual. They simply indicate normal file handling.



Properties

DOS Attributes

8.3 Short Filena	!IODOM~1.JPG
Hidden	False
System	False
Read only	False
Archive	True

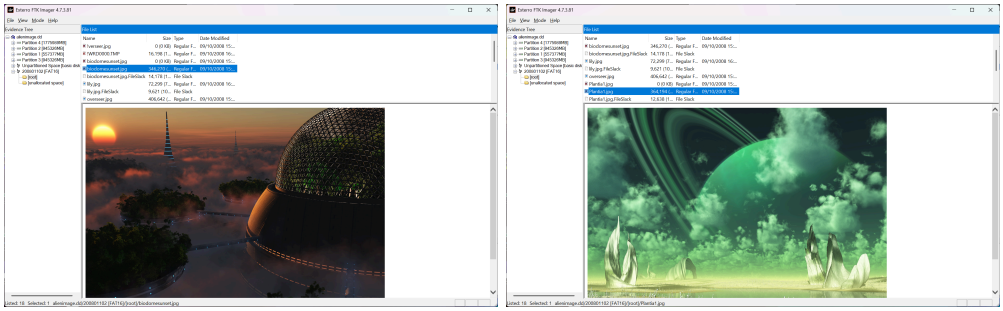
DOS Attributes

11. Recovery Potential:

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

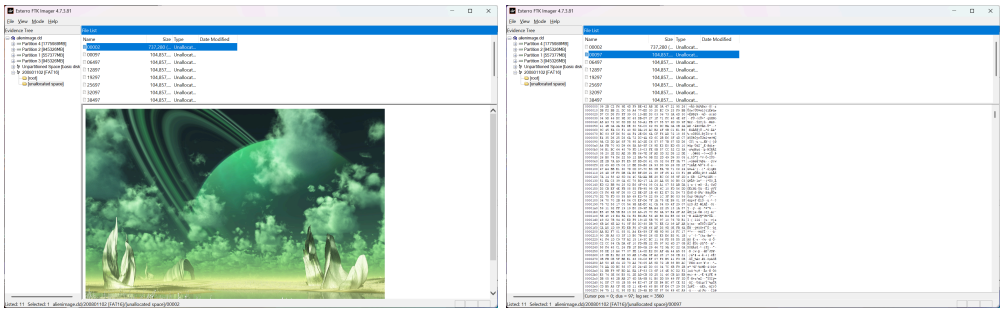
Yes, there is some deleted files in root

– In the drive image, several deleted files were identified with sizes greater than 0 KB. Since these files still point to valid cluster allocations, they may be partially or fully recoverable depending on whether their data blocks have been overwritten.



Unallocated Space

– There is also img file and unreadable file (looks like ZZZZZZZZZZZ.ZZZZ – secure deleted)



12. 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?

No

– Analysis of the thumb drive image revealed no direct location data (such as GPS coordinates) within EXIF metadata of the recovered images. For example, biodomesunset.jpg and other photographs lacked GPS fields, and instead showed signs of post-processing in Adobe Photoshop, which would normally strip or overwrite camera metadata.

The only identifiable attribution metadata was the author field (“Richard”) in the lily.jpg (PDF) file. While this links the file to a potential user, it provides no geographic correlation.

No filenames, metadata fields, or recovered content from unallocated space revealed references to geographic locations or the supposed dead drop. The presence of overwritten/deleted files suggests deliberate removal of sensitive content, which may have originally contained such data.

13. Imaging Tools

List four different forensic imaging tools that are available.

- FTK Imager by Accessdata
- Encase Forensic Imager by OpenText
- Belkasoft Acquisition Tool by Belkasoft
- Paladin by Sumuri
- Guymager by Guy Voncken
- OSFClone by PassMark