

ACME MEDICAL CENTER fORENSIC EXAM & FINDINGS

Forensic Case Number: ACME Medical Center 01



November 11, 2024

EXAMINER: yAIR rAYO

Table of Contents

[Section 1: Executive Summary 1](#_Toc182532586)

[1.1 Background 1](#_Toc182532587)

[1.2 Objective 2](#_Toc182532588)

[1.3 Findings 2](#_Toc182532589)

[Section 2: Hardware and Software 2](#_Toc182532590)

[2.1 Hardware Used 2](#_Toc182532591)

[2.2 Software Used 3](#_Toc182532592)

[Section 3: Methods 3](#_Toc182532593)

[3.1 Hardware Inspection 3](#_Toc182532594)

[3.2 Copies and Imaging 3](#_Toc182532595)

[3.3 Autopsy 4](#_Toc182532596)

[3.4 Final Hash Value 7](#_Toc182532597)

[Section 4: Findings 7](#_Toc182532598)

[Section 5: Appendix 8](#_Toc182532599)

[Appendix A: Hash Values 8](#_Toc182532600)

[Appendix B: Autopsy Software Ingest Settings 9](#_Toc182532601)

[Appendix C: Chain of Custody Report 9](#_Toc182532602)

# Section 1: Executive Summary

### 1.1 Background

On November 04, 2024, ACME Medical Center’s Director contacted our digital forensic unit to request an examination of a USB (Universal Serial Bus) drive brought in from an employee suspected of misconduct. The employee in question, Joe Bob, has been accused of potentially viewing illegal material on a company computer, specifically unauthorized images of *cats*. Given the degree of the allegations, ACME Medical Center’s leadership has emphasized the need for a forensic investigation of the USB device before expanding the inquiry to any other devices in their network. The Director has provided written authorization and has confirmed that ACME Medical Center’s policies allow a search of company-owned storage devices and computers if they are suspected of being involved in criminal activity. This permission is vital to ensure compliance with legal protocols, particularly if the findings may lead to further actions or be presented as evidence in court. The chain of custody documentation was thoroughly completed and preserved to ensure the evidence's integrity. See ‘Appendix C’ for chain of custody details.

### 1.2 Objective

My goal in this examination is to find and document all files present on the USB device, including deleted, hidden, or encrypted files. Given the potential for this investigation to support criminal proceedings, I will adhere strictly to chain-of-custody protocols, evidence handling, and forensic imaging procedures to ensure the integrity and admissibility of these findings.

### 1.3 Findings

Upon completing the forensic analysis of the USB device provided by ACME Medical Center, I discovered many files that show illegal activity (images and videos of cats). The device had both active and deleted files, which were recovered and analyzed for contraband content, specifically images of *cats*. See ‘Section 4: Findings’ for specific details on how I came to this conclusion.

Based on these findings, it is recommended that further investigative steps be taken, potentially including examination of Joe Bob’s assigned work on the computer and more devices he may have accessed within the ACME Medical Center network. All recovered materials and forensic logs are preserved and ready for court submission, if needed.

# Section 2: Hardware and Software

### 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 is either owned or licensed to (me, my company, etc.) and has been fully evaluated and confirmed.

* AccessData Forensic Toolkit Imager (FTK Imager) v4.7.1.2
* Autopsy v4.21.0
* Securite Multi-Secteurs - Version 1.3 (Write Blocker)

# Section 3: Methods

### 3.1 Hardware Inspection

Before beginning the investigation, I inspected and documented the USB (universal serial bus) drives manufacturer, model, and part number. USB drive is an *onn. Brand,* 16 GB, model 100140020, manufacture part number being the same as the model of 100140020. Assembled product dimensions (L x W x H) are 2.36 x 0.87 x 0.44 inches. USB weight is 0.02 pounds. The evidence drive does not appear to be damaged and is in good condition on the exterior.

Prior to creating an exact image of the provided drive, I enabled the write blocking software Securite Multi-Secteurs - Version 1.3 on my Windows 10 host machine to avoid damaging or altering data on the original evidence drive when inserted into the host machine USB port.

### 3.2 Copies and Imaging

To ensure data integrity before imaging, I launched Forensic Toolkit Imager (AccessData FTK Imager version 4.7.1.2) on the forensic workstation and added the USB drive as a physical evidence item. These first hash values serve as a baseline for confirming that no data alterations occur during the imaging and analysis process. The USB drive was noted to be called ‘Furry.’ The following steps were conducted:

* **Hash Calculation**: Right-clicked on the USB drive entry and selected "Verify Drive/Image," opting for both MD5 and SHA-1 hash types.
* **Documentation of Hash Values**: Recorded the first MD5 and SHA-1 hash values for later verification:
  + **MD5**: bc8531b7ac4fd0d37bfd356490a5c543
  + **SHA-1**: 89c461928ea150a4d85c2e6e52fa62a8777ed680

Using FTK imager, I created 2 exact copies of the provided USB drive. The first image was a forensic copy (*Analysis\_Forensic\_Copy\_1.001*) which will be stored on the ‘Desktop’ of my host Windows 10 forensic workstation. The second copy is a forensic working copy (*Analysis\_Working\_Copy\_2.001*). I used the forensic working copy (*Analysis\_Working\_Copy\_2.001*) to conduct the analysis of the data. Raw (dd) bit-by-bit copies of the original evidence generated using FTK Imager for both copies:

* **Image Copy 2 (*Analysis\_Working\_Copy\_2.001*)**: After imaging, the calculated MD5 and SHA-1 hashes matched the original “Furry” USB hash values, ensuring a verified, intact duplicate.
  + **MD5**: bc8531b7ac4fd0d37bfd356490a5c543
  + **SHA-1**: 89c461928ea150a4d85c2e6e52fa62a8777ed680
* **Image Copy 1 (*Analysis\_Forensic\_Copy\_1.001*)**: This copy also matched the original “Furry” USB hash values, ensuring a verified, intact duplicate.
  + **MD5**: bc8531b7ac4fd0d37bfd356490a5c543
  + **SHA-1**: 89c461928ea150a4d85c2e6e52fa62a8777ed680

Once imaging was complete, I stored *Analysis\_Forensic\_Copy\_1.001* within my Windows 10 host machine’s hard drive folder ("C:\Users\YairRayo Windows 10\Desktop\Forensic Images of USB Furry Stored Copy"), and I removed the original USB drive from the workstation and stored it in a safe, controlled environment. All analysis was performed on the "*Analysis\_Working\_Copy\_2.001*" to preserve the integrity of the original evidence. See Appendix A for a complete list of all MD5 and SHA-1 hash values.

### 3.3 Autopsy

I used Autopsy v4.21.0 to examine the forensic image copy called *Analysis\_Working\_Copy\_2.001*. When I added the image to Autopsy, the only default setting changes made were during step 4, ‘Configure Ingest’, during data source addition. I removed the ‘Plaso,’ ‘DJI Drone Analyzer,’ and ‘Cyber Triage Malware Scanner’ ingest modules. All other modules were left as default. See Appendix B for a visual to ensure reproducibility. During the forensic examination of the USB drive "FURRY" using Autopsy version 4.21.0, a detailed analysis of the storage structure was conducted. The data source information provided an overview of the drive’s partitioning scheme, showing both allocated (used) and unallocated (unused) space. The sectors were organized as follows:

* vol1 (Unallocated: 0-62)
  + This part of the forensic report describes a section of the drive labeled vol1 (Unallocated: 0-62) that holds 32,256 bytes of empty data (all zeros) in unused space. All date fields are set to "0000-00-00 00:00:00," showing no record of when it was last changed or used. Because this area is empty and has no recognizable file information, it likely represents space that was cleared or simply hasn’t been used. No evidence was found in this section.
* vol2 (Win95 FAT32 (0x0b): 63-2047940
  + Various files across various categories were noted within this sector, some of which hold evidence. The scan found orphaned files, FAT tables, and an MBR, alongside system folders such as ".fseventsd," ".Spotlight-V100," and ".Trashes." Additionally, there were several unallocated image files, notably JPEGs, and Apple-specific files in MOV and M4V formats. Other notable folders included "Pictures," "Harmless Folder," and a "Secret Folder," suggesting potential hidden or sensitive content. This volume has several instances of images and videos of ‘cats’ and were bookmark for the software generated report to show.
* vol3 (Unallocated: 2047941-30548095)
  + The forensic analysis of unallocated data from volume 3 revealed a directory named "1" within the $CarvedFiles directory, having 32 files with a ".mft" extension. Data was found to be removed or overwritten, and the records held low-level details that could not be recovered or associated with any meaningful data. As a result, it was not possible to find any useful information from this volume due to fragmentation.

After analyzing the Analysis\_Working\_Copy\_2.001 file with Autopsy, *vol2 (Win95 FAT32 (0x0b): 63-2047940* has been identified as the volume having all the data that will be referenced from this point onward as holding images and videos of cats.

#### 3.3.1 $CarvedFiles Directory

During the forensic analysis of the directory */img\_Analysis\_Working\_Copy\_2.001/vol\_vol2/$CarvedFiles/1/*, a total of 81 .jpg images of cats were found. These images have been bookmarked for inclusion in the forensic report and can be found in */img\_Analysis\_Working\_Copy\_2.001/vol\_vol2/$CarvedFiles/1/*. For reference, the bookmarked images can be found under this specified directory, all .jpg images. Since these images were carved data, there is no timeline, changed, accessed, created, or created time details for these images. What is certain is that ‘cat’ images exist within this file system path.

#### 3.3.2 .Spotlight-V100 Directory

Based on the analysis of the metadata, there is no evidence of images related to 'cats' within this dataset. However, the metadata strongly suggests that the files are from a Mac OS device, as shown by specific mentions of the Spotlight index system, a feature that is found within Mac OS.

* The files are in the directory path */img\_Analysis\_Working\_Copy\_2.001/vol\_vol2/.Spotlight-V100/Store-V1/Stores/BC650BA8-C5B5-4A64-8BDB-18A9533BF1D7/*, which is part of the Spotlight indexing system used by Mac OS to organize and search files. For reference, the bookmarked images can be found under this specified directory. The modified, access, and creation timestamps for the files range from November 17, 2009, to November 20, 2009. The data includes files with names like *.store.db*, *0.indexArrays*, and *1.indexHead,* which are part of the Mac OS Spotlight indexing database. While no cat images were found in this search, it is possible that more data relevant to a personal or work Mac OS device may be present elsewhere within the system. If this investigation requires further investigation of devices, a Mac OS device may have more data.

#### 3.3.3 .Trashes Directory

Directory found at */img\_Analysis\_Working\_Copy\_2.001/vol\_vol2/.Trashes/*, similar to *.Spotlight-V100*, stores metadata rather than actual images of cats.

* Metadata here includes references to video files such as "KittyMontage," "MontereyKitty.m4v," "TiggerTheCat.m4v," and "Cat.mov," suggesting prior media files related to "cats" or "kitty" themes. This file, classified as "application/octet-stream" and unallocated, was created and last changed on November 17, 2009, at 16:45:28 EST. This content mentioned in *.Trashes* was added as a bookmark for the software-generated report for reference for path */img\_Analysis\_Working\_Copy\_2.001/vol\_vol2**/.Trashes/\_502~1*.

#### 3.3.4 Harmless Folder Directory

This directory path is */img\_Analysis\_Working\_Copy\_2.001/Harmless Folder*. Directory was accessed and viewed on 2024-03-27. This directory holds one unallocated deleted subdirectory called *HighQuaility* with the path of */img\_Analysis\_Working\_Copy\_2.001/vol\_vol2/Harmless Folder/HighQuality*. Clicking on the folder *HighQuality* I found 81 images of cats that had been deleted by the user. The metadata of just one image (\_SC00023.JPG) found within the *HighQuality* gives the similar story to the other 80 cat images of when they were all viewed by the ‘Accessed Time’ metadata:

* The forensic analysis of the image file \_SC00028.JPG reveals key details about its creation and access. The image was created on November 8, 2009, at 11:22 AM using a SONY HDR-SR10 camera. Although the file appears to have been deleted or hidden ("unallocated" status), the file's metadata shows it was last accessed on March 27, 2024. This suggests the image has been recovered or accessed recently. Other images in the same directory, ranging from \_SC00003.JPG to \_SC00026.JPG, share similar timestamps from 2009 but were also accessed on March 27, 2024, pointing to manipulation or relocation of the files. All these references JPG files can be found within the software generated report, under */img\_Analysis\_Working\_Copy\_2.001/vol\_vol2/Harmless Folder/HighQuality*

This same *Harmless Folder* directory has one allocated subdirectory called *Videos* with the path of */img\_Analysis\_Working\_Copy\_2.001/vol\_vol2/Harmless Folder/Videos* that is not deleted and in plain view. Clicking on the subdirectory *Videos* I found 6 videos of cats (combination of .MOV and .M4V extensions), and 43 images of cats. The metadata and analysis of this directory gives the similar story to the remaining content of this subdirectory:

* All images were created by a Sony Cybershot camera on November 12, 2009, at 09:11:33 EST. The metadata reveals that the image was created on November 18, 2009, at 04:36:37 EST, and accessed by the user on November 24, 2009. The files are allocated in the file system, meaning it is available for access. Most images have not been accessed since the year 2009; however, there is one exception to the ‘Access Time’ metadata for one image. Of the 43 images, 1 image (DSC00009.JPG) metadata shows it was last accessed on March 27, 2024. This suggests the image has been recovered or accessed recently. All these references video and image files can be found within the software generated report, under */img\_Analysis\_Working\_Copy\_2.001/vol\_vol2/Harmless Folder/Videos.*

#### 3.3.5 Pictures Directory

The files within this directory are allocated and in plain view. The forensic analysis of the directory */img\_Analysis\_Working\_Copy\_2.001/vol\_vol2/Pictures/* reveals several image files, with a total of 10 images of dogs found, all of which are in JPEG format.

* These files include both fully allocated files (such as 5.jpg, 667.jpg, and 7667.jpg) and partially downloaded files with the .crdownload extension (showing an interrupted download). The files were primarily changed and created on March 27, 2024, with access times also logged on this same date. Notably, there are no images related to cats in this folder, and the content does not appear to be relevant to the ongoing case. These findings point to standard image files, with no unique or suspicious metadata.

#### 3.3.6 System Volume Information Directory

This directory has a file named *WPSettings.dat* and another called *IndexerVolumeGuid*. They are not related to user Joe Bob or any relevant content in an investigation. These files show normal system operation but do not provide any direct evidence relevant to the case.

### 3.4 Final Hash Value

After completing the analysis, I verified the MD5, and SHA-1 hash values of the forensic working copy to ensure no data was changed during the investigation. I opened FTK Imager, added the forensic working copy image as evidence, clicked file, and selected “Verify Image.” The MD5, and SHA-1 hash values produced by FTK Imager matched the pre-analysis hash values.

# Section 4: Findings

After completing the analysis of the forensic image copy titled *Analysis\_Working\_Copy\_2.00*1 using Autopsy v4.21.0, evidence of contraband in the form of illegal images and videos (cats) was discovered. The analysis of vol2 *(Win95 FAT32 (0x0b): 63-2047940)* revealed directories and files having 81 cat-related images in unallocated space and 6 videos and 43 additional images in an allocated directory titled "Harmless Folder." Metadata analysis confirmed that the media originated from two distinct device models, the SONY HDR-SR10 and SONY Cybershot cameras. Creation timestamps for most files ranged from November 8, 2009, to November 18, 2009, with recent access to some of these cat images on March 27, 2024, suggesting recent file manipulation. Further metadata analysis found 32 deleted files in volume 3’s unallocated space, though these were irrecoverable. Directories such as *.Spotlight-V100* and .*Trashes* provided indirect evidence of Mac OS usage but no direct connection to the contraband. The integrity of the forensic image was verified using matching MD5 and SHA-1 hash values. Based on the illegal nature of the discovered images and videos, I recommend handing over this report and its findings to law enforcement and to further investigate all devices Joe Bob has used or accessed, particularly focusing on internal machines within ACME Medica Center.

# Section 5: Appendix

### Appendix A: Hash Values

|  |  |  |
| --- | --- | --- |
| **File Name** | **MD5 Hash Value** | **SHA-1 Hash Value** |
| "FURRY” USB (Original Evidence) | bc8531b7ac4fd0d37bfd356490a5c543 | 89c461928ea150a4d85c2e6e52fa62a8777ed680 |
| Analysis\_Forensic\_Copy\_1.001 (Forensic Stored Copy) | bc8531b7ac4fd0d37bfd356490a5c543 | 89c461928ea150a4d85c2e6e52fa62a8777ed680 |
| Analysis\_Working\_Copy\_2.001 (Forensic Working Copy) | bc8531b7ac4fd0d37bfd356490a5c543 | 89c461928ea150a4d85c2e6e52fa62a8777ed680 |
| Analysis\_Working\_Copy\_2.001 (Post Analysis Forensic Working Copy) | bc8531b7ac4fd0d37bfd356490a5c543 | 89c461928ea150a4d85c2e6e52fa62a8777ed680 |

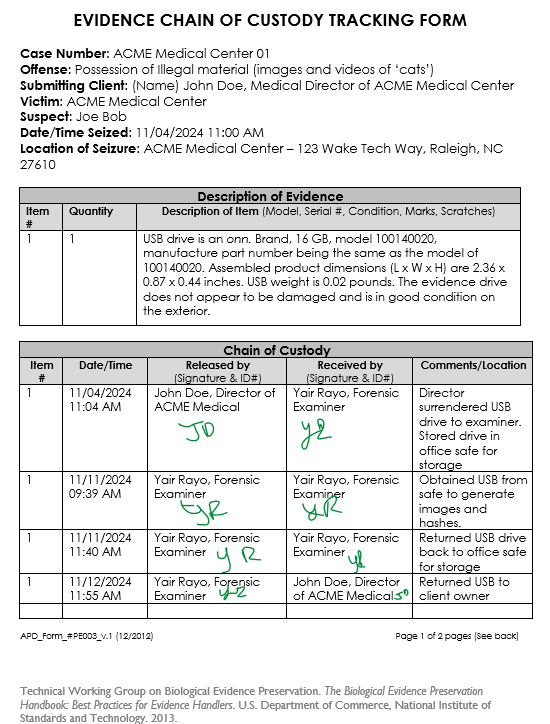
### Appendix B: Autopsy Software Ingest Settings

A screenshot of a computer

Description automatically generated

### Appendix C: Chain of Custody Report

Page 1:



Page 2:

