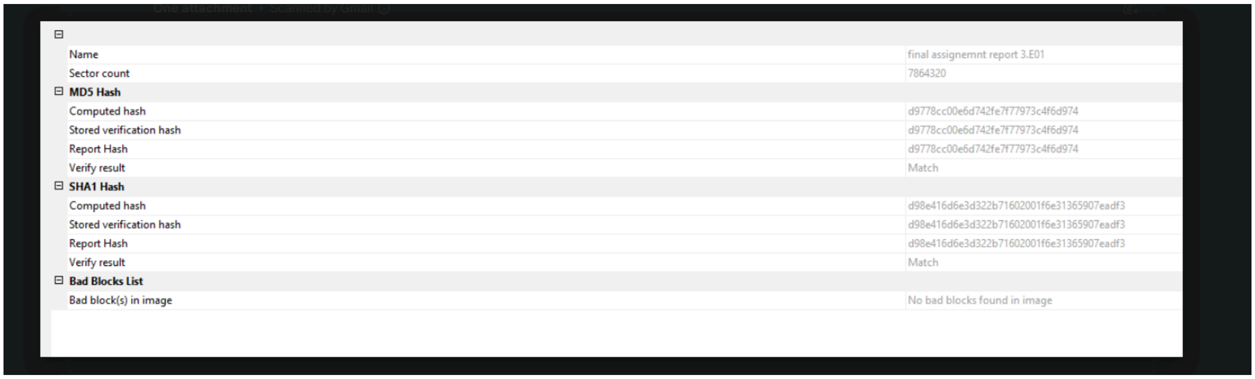
Matthew Montefusco 12/16/2024

Final Report
FCM 760

Examiner: Matthew Montefusco
Title: Digital Forensic Examiner
Agency: John Jay Forensics Team
Date: 12/16/24
Case Number: MT-2009-12-015

1. Introduction

This report presents the findings of the forensic examination conducted on digital evidence provided for two related incidents. The examination was requested by Monterey PD, California, to determine the presence of unusual content on the hard drive of a desktop computer and to trace the computer back to its original owner. The report also includes analysis of additional evidence seized under a search warrant. The analysis that was done was mostly done by using the software Autopsy. We also needed to do an acquisition for evidence 2 to have it as an image so we can use it for analysis. We did this using FTK Imager. Here is the verification, showing that the hash values match.



```
⊟
   Name                        final assignemnt report 3.E01
   Sector count                7864320
⊟  MD5 Hash
   Computed hash               d9778cc00e6d742fe7f77973c4f6d974
   Stored verification hash    d9778cc00e6d742fe7f77973c4f6d974
   Report Hash                 d9778cc00e6d742fe7f77973c4f6d974
   Verify result               Match
⊟  SHA1 Hash
   Computed hash               d98e416d6e3d322b71602001f6e31365907eadf3
   Stored verification hash    d98e416d6e3d322b71602001f6e31365907eadf3
   Report Hash                 d98e416d6e3d322b71602001f6e31365907eadf3
   Verify result               Match
⊟  Bad Blocks List
   Bad block(s) in image       No bad blocks found in image
```

2. Evidence

Incident 1 - Evidence 1

- Item: Desktop Hard Drive
- Source: Turned in by the buyer of the laptop from Craigslist
- It was a bit-by-bit forensic image created by the Monterey Police Department
- It has 3 reports along with the image file

Incident 2 - Evidence 2

- Item: Digital evidence recovered from a search warranted that was done at an office location
- The search warrant details are attached in the case folder
- The things found were subscriber information for all computers assigned to Jo Smith, a RAM image for any and all computers to Jo Smith, a hard drive disk image for all computers to Jo Smith, and all USB thumb drives in Jo Smith's possession.

3. Objectives

- Find out how many kitty images are on the desktop computer
- Trace the computer back to its original owner
- Analyze any additional evidence found in the investigation

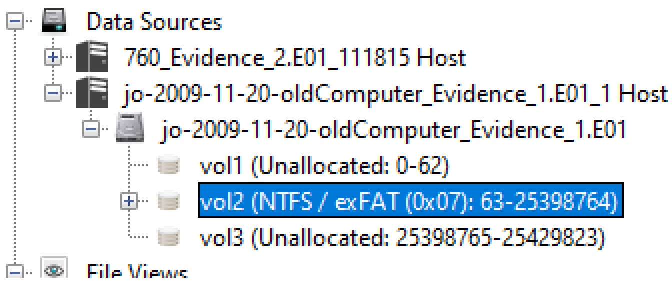
4. Examination

- Acquisition Tool - FTK Imager
- Analysis Tool - Autopsy
    1. Verified the image provided by the Monterey Police Department, and validated using the hash values, using FTK Imager
    2. Did a full analysis of all evidence and images using Autopsy
    3. Looked for kitty images on the computer, using keywords, metadata, and file signatures.

5. Analysis

1. What file system is present on this device and on what partition?

    - The file system that is present on this device is (NTFS / exFAT (0x07): 63-25398764) and it is on the second partition (vol2)

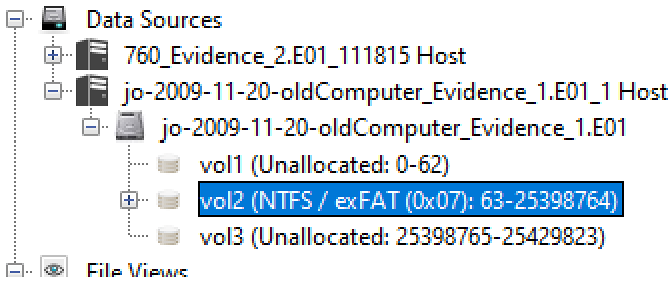


```
Data Sources
  760_Evidence_2.E01_111815 Host
  jo-2009-11-20-oldComputer_Evidence_1.E01_1 Host
    jo-2009-11-20-oldComputer_Evidence_1.E01
      vol1 (Unallocated: 0-62)
      vol2 (NTFS / exFAT (0x07): 63-25398764)
      vol3 (Unallocated: 25398765-25429823)
File Views
```

-

2. How many Logical Drives do you have?

- There are 3 logical drives

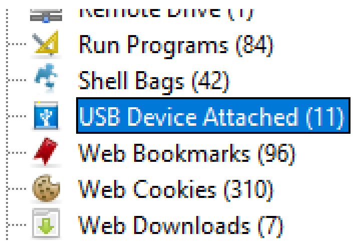


```
Data Sources
  760_Evidence_2.E01_111815 Host
  jo-2009-11-20-oldComputer_Evidence_1.E01_1 Host
    jo-2009-11-20-oldComputer_Evidence_1.E01
      vol1 (Unallocated: 0-62)
      vol2 (NTFS / exFAT (0x07): 63-25398764)
      vol3 (Unallocated: 25398765-25429823)
File Views
```

-

3. How many USB devices have been connected to this computer?

- There are 11 USB devices connected to this computer

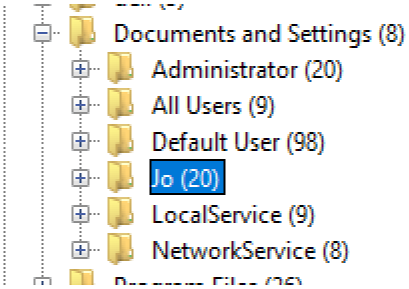


```
Remote Drive (1)
Run Programs (84)
Shell Bags (42)
USB Device Attached (11)
Web Bookmarks (96)
Web Cookies (310)
Web Downloads (7)
```

-

4. Who is the User to this PC?

- The user to this PC is Jo Smith

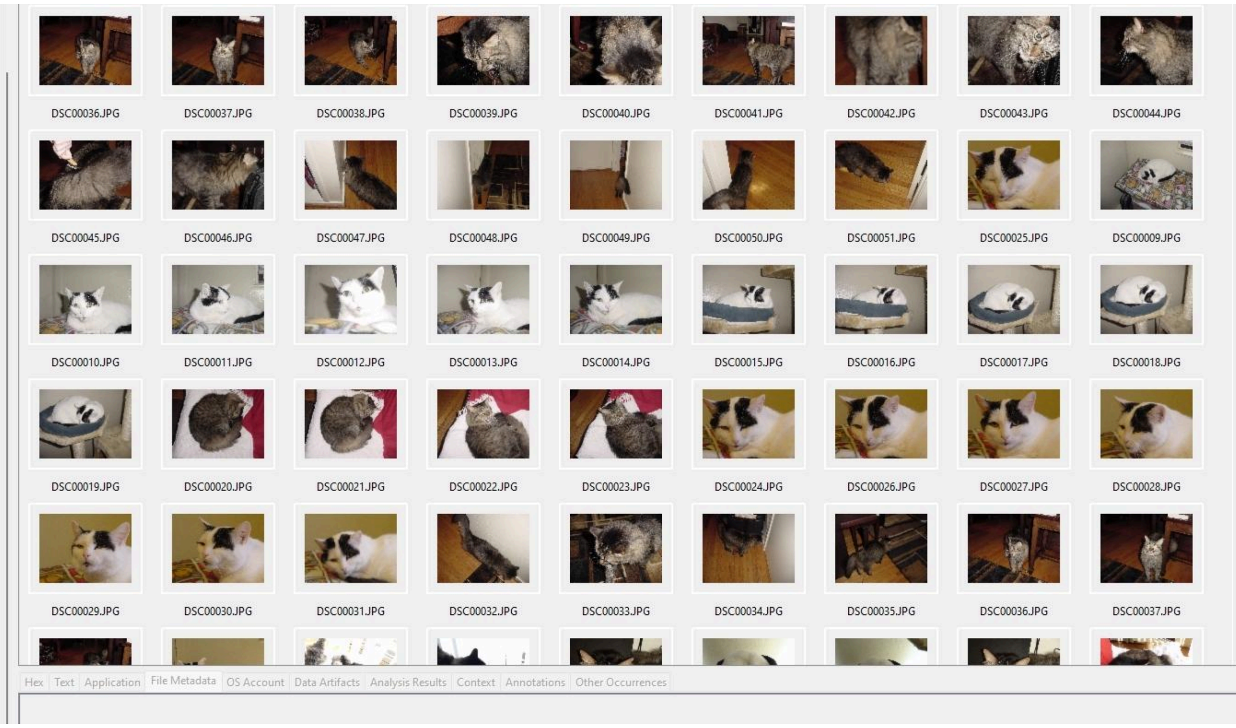


```
Documents and Settings (8)
  Administrator (20)
  All Users (9)
  Default User (98)
  Jo (20)
  LocalService (9)
  NetworkService (8)
Program Files (26)
```

-

5. How many images of Kitty do you find on this computer?

- There are 266 images of kitties on this computer

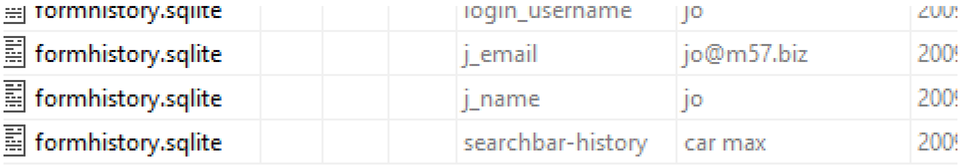


6. Bookmark all images of Kitties and generate an electronic report of your findings

    - They are all bookmarked, as I found them in the EXIF Metadata folder on autopsy.

7. Are there any personal identifiers on this image file that can help find its owner?

    - Yes there is. One personal identifier is that under the web autofill section it shows an email of Jo Smith's that she has on the computer (jo@m57.biz). Also there are photos from both evidence 1 and evidence 2 that are the exact same, along with some objects in the pictures that are the same (such as the garfield pillow that the cat is laying on).



formhistory.sqlite				login_username	jo	200
formhistory.sqlite				j_email	jo@m57.biz	200
formhistory.sqlite				j_name	jo	200
formhistory.sqlite				searchbar-history	car max	200

6. Image Evidence 2

1. Find Evidence of Kitty files on Evidence 2

    - There are 55 images on Evidence 2 of kitties, as shown below.

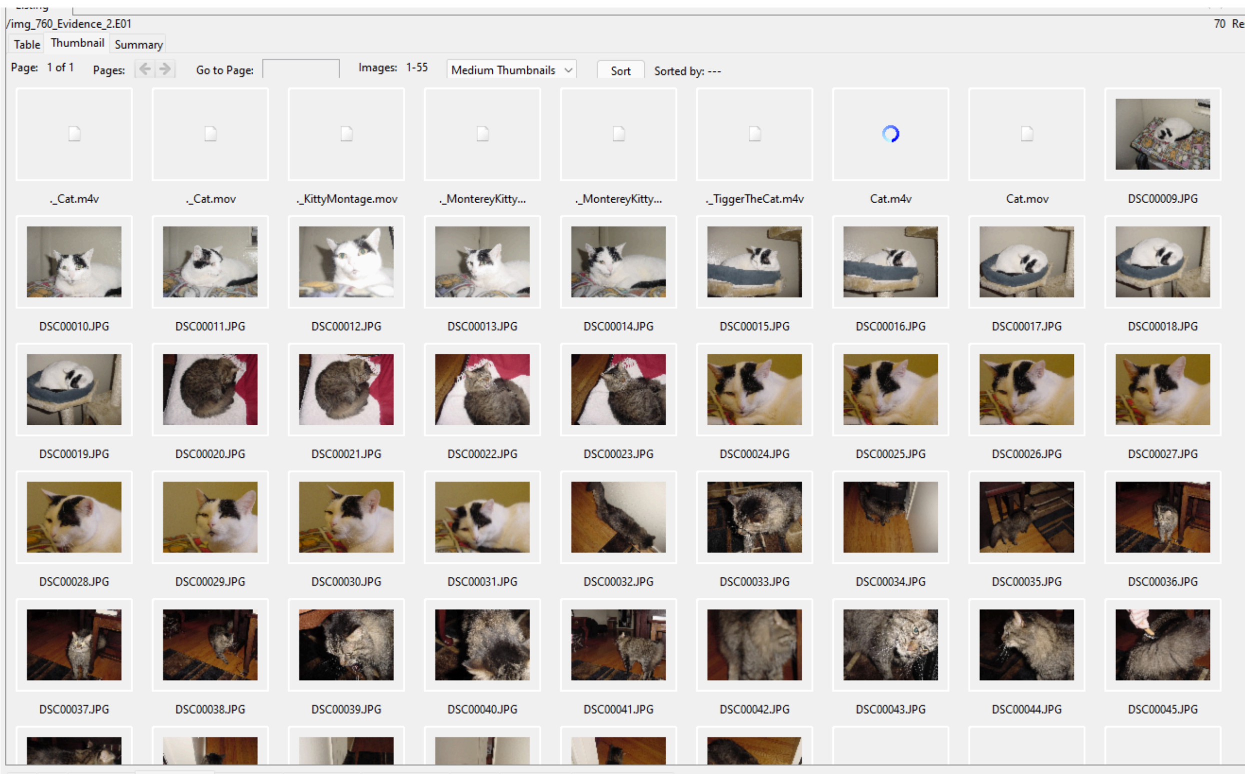

/img_760_Evidence_2.E01 70 Re

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page: Images: 1-55 Medium Thumbnails Sort Sorted by: ---

._Cat.m4v ._Cat.mov ._KittyMontage.mov ._MontereyKitty... ._MontereyKitty... ._TiggerTheCat.m4v Cat.m4v Cat.mov DSC00009.JPG

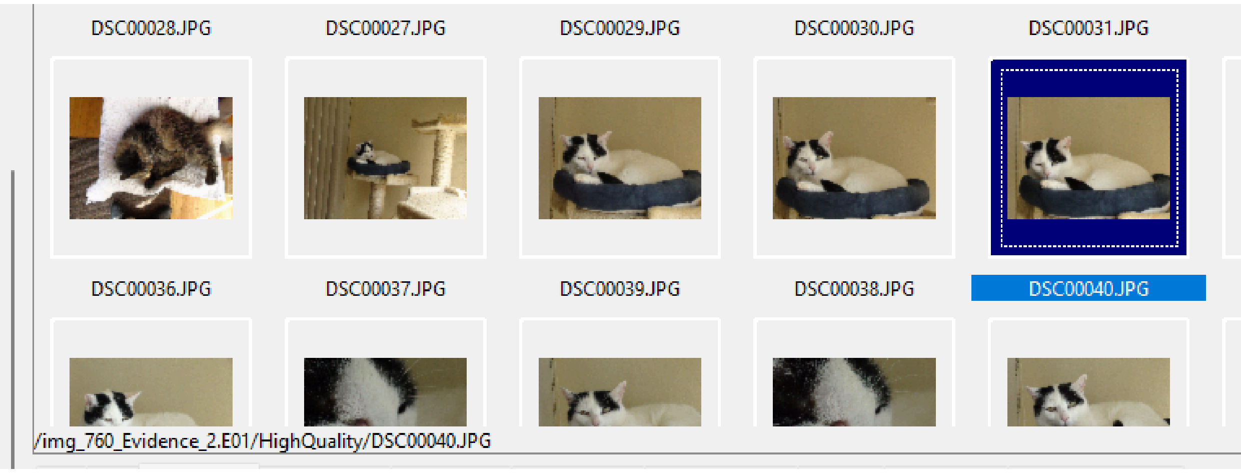
DSC00010.JPG DSC00011.JPG DSC00012.JPG DSC00013.JPG DSC00014.JPG DSC00015.JPG DSC00016.JPG DSC00017.JPG DSC00018.JPG

DSC00019.JPG DSC00020.JPG DSC00021.JPG DSC00022.JPG DSC00023.JPG DSC00024.JPG DSC00025.JPG DSC00026.JPG DSC00027.JPG

DSC00028.JPG DSC00029.JPG DSC00030.JPG DSC00031.JPG DSC00032.JPG DSC00033.JPG DSC00034.JPG DSC00035.JPG DSC00036.JPG

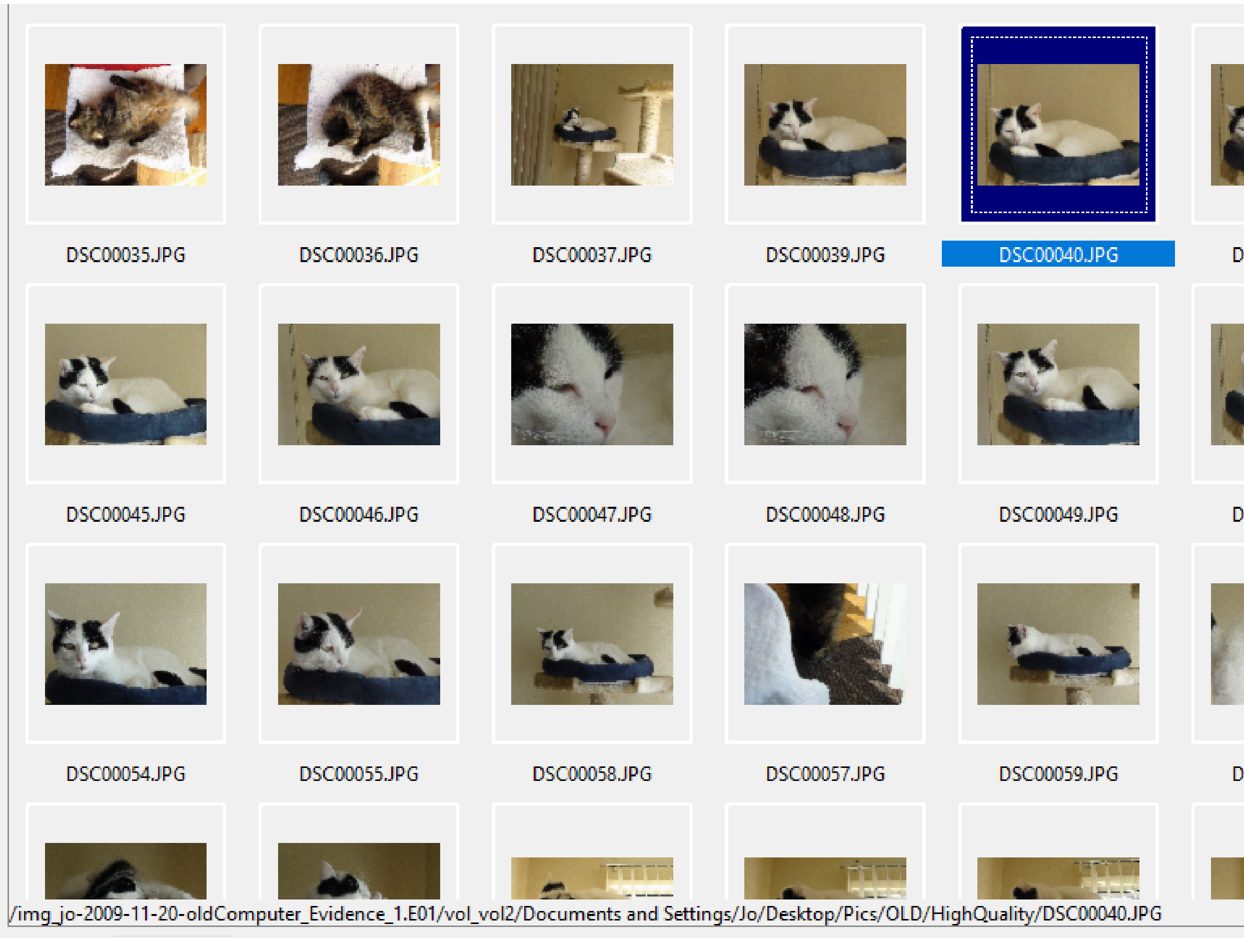
DSC00037.JPG DSC00038.JPG DSC00039.JPG DSC00040.JPG DSC00041.JPG DSC00042.JPG DSC00043.JPG DSC00044.JPG DSC00045.JPG

2. Find evidence that evidence 2 was used in Evidence 1.
   - There are a lot of the same exact images of kitties in both evidence 1, and in evidence 2 which shows that evidence 2 was used in evidence 1. Shown below is the same picture in both evidence 1, and in evidence 2.


DSC00028.JPG DSC00027.JPG DSC00029.JPG DSC00030.JPG DSC00031.JPG

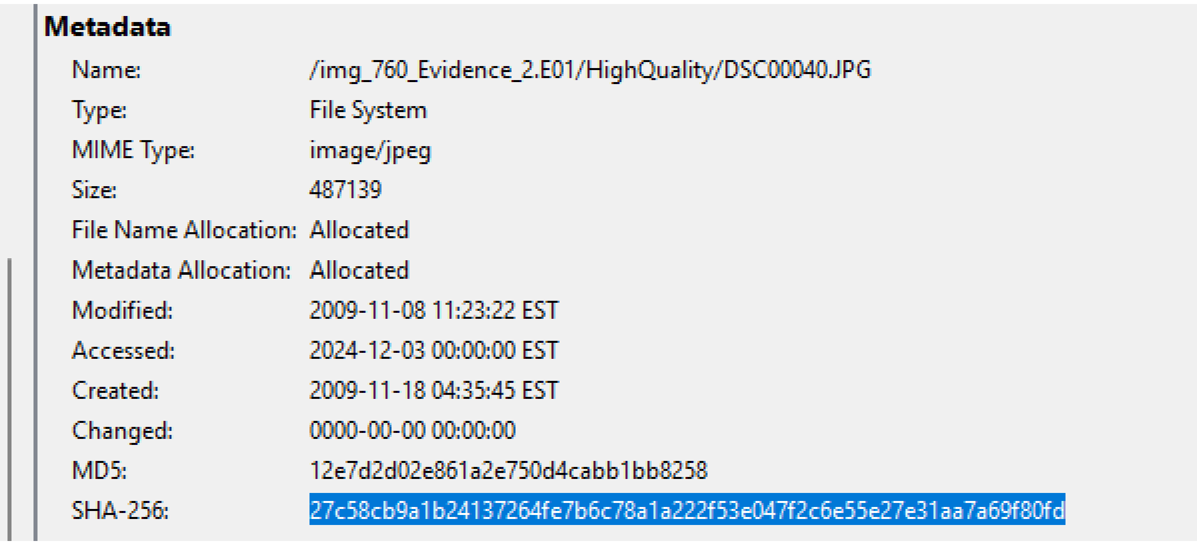
DSC00036.JPG DSC00037.JPG DSC00039.JPG DSC00038.JPG DSC00040.JPG

/img_760_Evidence_2.E01/HighQuality/DSC00040.JPG

- 

/img_jo-2009-11-20-oldComputer_Evidence_1.E01/vol_vol2/Documents and Settings/Jo/Desktop/Pics/OLD/HighQuality/DSC00040.JPG

3. Find correlation between users in both devices.
   - A correlation between the two users in both devices are the images that they use in both evidence 1 and 2. The two pictures that are the same in both, also have the same hash values. The SHA-256 in both of the images is 27c58cb9a1b24137264fe7b6c78a1a222f53e047f2c6e55e27e31aa7a69f80fd.



Metadata

Name:	/img_760_Evidence_2.E01/HighQuality/DSC00040.JPG
Type:	File System
MIME Type:	image/jpeg
Size:	487139
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2009-11-08 11:23:22 EST
Accessed:	2024-12-03 00:00:00 EST
Created:	2009-11-18 04:35:45 EST
Changed:	0000-00-00 00:00:00
MD5:	12e7d2d02e861a2e750d4cabb1bb8258
SHA-256:	27c58cb9a1b24137264fe7b6c78a1a222f53e047f2c6e55e27e31aa7a69f80fd

7. Conclusion

- In conclusion, we at the John Jay Forensic Lab, found that there were 266 images of kitties on this computer, and we were able to trace it back to its original owner, who we identified as Jo Smith. We did an acquisition on FTK imager to verify the image file, and then we did extensive analysis of everything we had using autopsy to come to these conclusions. There were kitty files on both evidence 1 and evidence 2, which shows that there was a correlation between both the devices, and even had the same exact pictures on both of the pieces of evidence.

8. Documents

The documents are attached with the report.