CSE 568 Forensic Report

Examiner: Luke Leveque

Case Name: 07042022_Missing_Mutts

Case Number: 07042022

Case Summary:

The client, Mr. Niceguy, has recently moved into his new house with his two dogs. However, his backdoor does not always latch completely which results in the dogs chasing his neighbor, Ms. Gunagetcha's, cat. Ms. Gunagetcha has called the police repeatedly on noise complaints. Mr. Niceguy and his family returned home to find their dogs gone from the backyard, door ajar. While searching for the dogs, Mr. Niceguy found a thumb drive just outside the door. He has checked the device into us to see if there are any clues as to the whereabouts of the dogs and if he should get the police involved. Our goal for this case is to determine if Mr. Niceguy should get the police involved.

Case Findings:

During the investigation of the image taken of the USB flash drive that was submitted, we were able to recover multiple files within the scope of work that have relevance to the case. It should be noted, all files found and referenced during the investigation were found in the unallocated data. Investigations suggest that the thumb drive was quick formatted as the files were not referenced in the root directory. Using AccessDisk FTK Toolkit, using an index of the image, we were able to find two plaintext references to "dogs" and three references to "niceguy," though two of them were within the same document, as shown in Exhibit A. There were four files that we believe to be of immediate relevance to the case. These were all found in the unallocated space, as shown in Exhibit B.

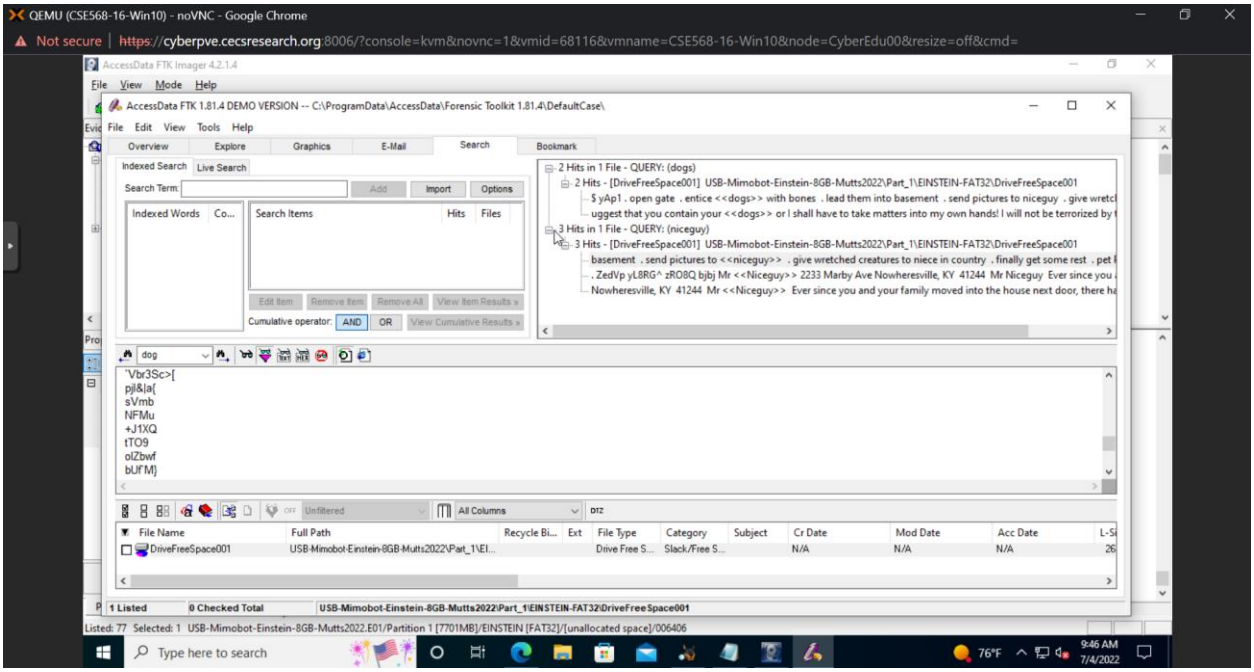
- A .txt file that consisted of a plan to lure dogs to a basement, "send pictures to niceguy," give "wretched creatures" to a niece, then get peace and pet a "Princess Kitty." (See Exhibit C-1)
- Two Images:
    - A JPEG of a golden retriever with text added to the bottom that read "the yellow dog barks too much – pay up or we will silence him." (See Exhibit C-2)
    - A JPEG of a pug that also had text added to the bottom which read, "Do you care about your pug???? Then PAY UP!!!!!!" (See Exhibit C-3)
    - The metadata on both of these images suggests that these JPEG images were taken with a Kodak Funsaver, a disposable camera.
- A Microsoft Word document. This document appears to be a letter to Mr. Niceguy, expressing displeasure about his dogs. (See Exhibit C-4)
    - The metadata on this document shows that the account that created the document was named Ima Gunagetcha on 2018-07-25.
    - The file was then last modified and saved by an account named ImaG on 2022-06-25.

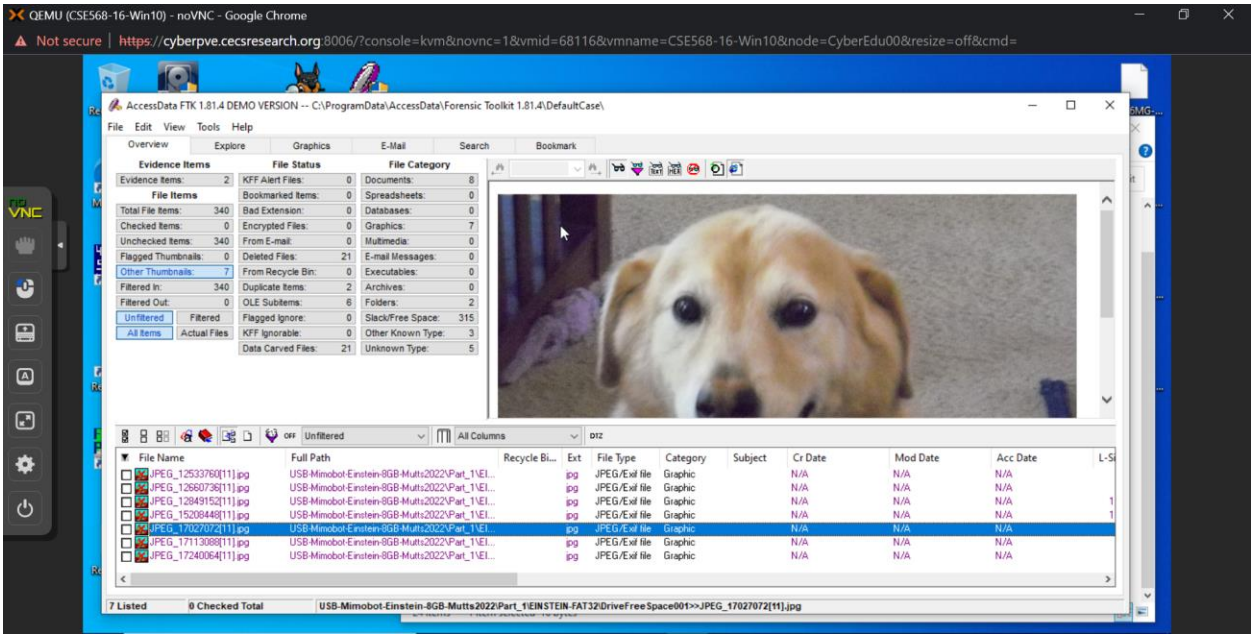
Case Conclusion:

Our company has decided that the best course of action would be to take the findings found within the thumb drive to the police as it contains information that may permit a warrant for further investigation. We have found information on a thumb drive that contains information specific to Ms. Gunagetcha and her complaints about the dogs.

Exhibits:

Exhibit A:



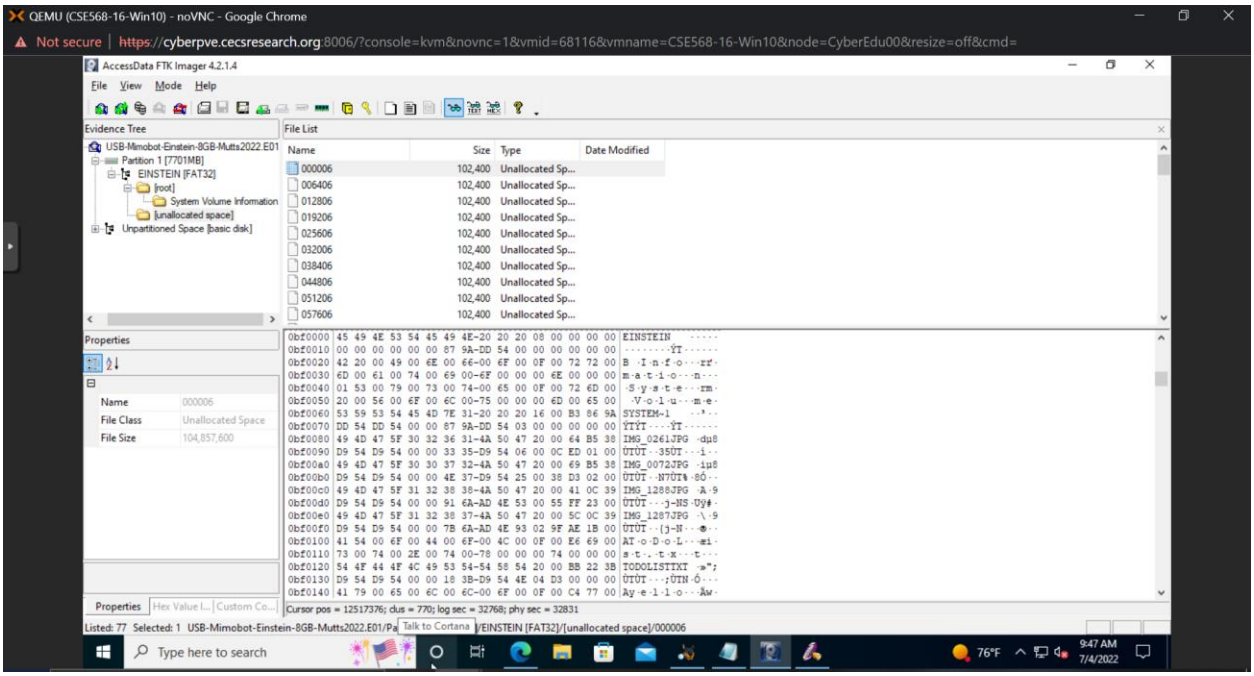


FTK Toolkit Search Results and file list of images that were carved..

This information was gathered using FTK Toolkit. Toolkit was able to carve the same information that was carved in Autopsy (See Exhibit 3), and, using the full index on the image, we were able to locate several hits on the keywords “dogs” and “niceguy”, the name of the client. The two results from the

keyword, “dog”, reference the plaintext text document detailing the plan to remove the dogs and the letter addressed to Mr. Niceguy. The results from the keyword, “niceguy”, resulted in the same two sources.

Exhibit B:



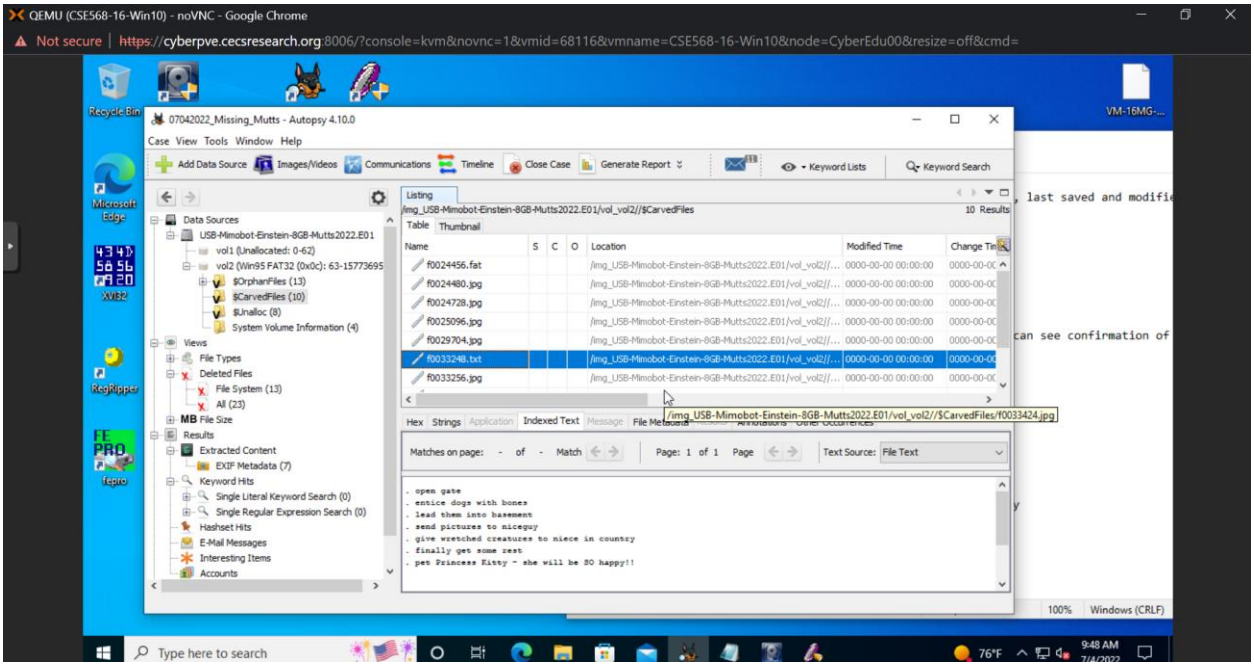
FTK Imager showing location of select images within the unallocated space.

This information was found by adding the forensic image to FTK Imager. There was no data shown in the root directory and as seen in the provided screenshot, the UAC contains remnants of the root directory and files that were on the thumb drive prior to it being quick formatted. Using the naming scheme in Autopsy when carving the relevant files (See Exhibit C), we can confirm the existence of multiple relevant files in the UAC remnant titled 000006, at cursor position 12517376.

Exhibit C:

The following files were carved from the image of the thumb drive that was provided to the examiner.

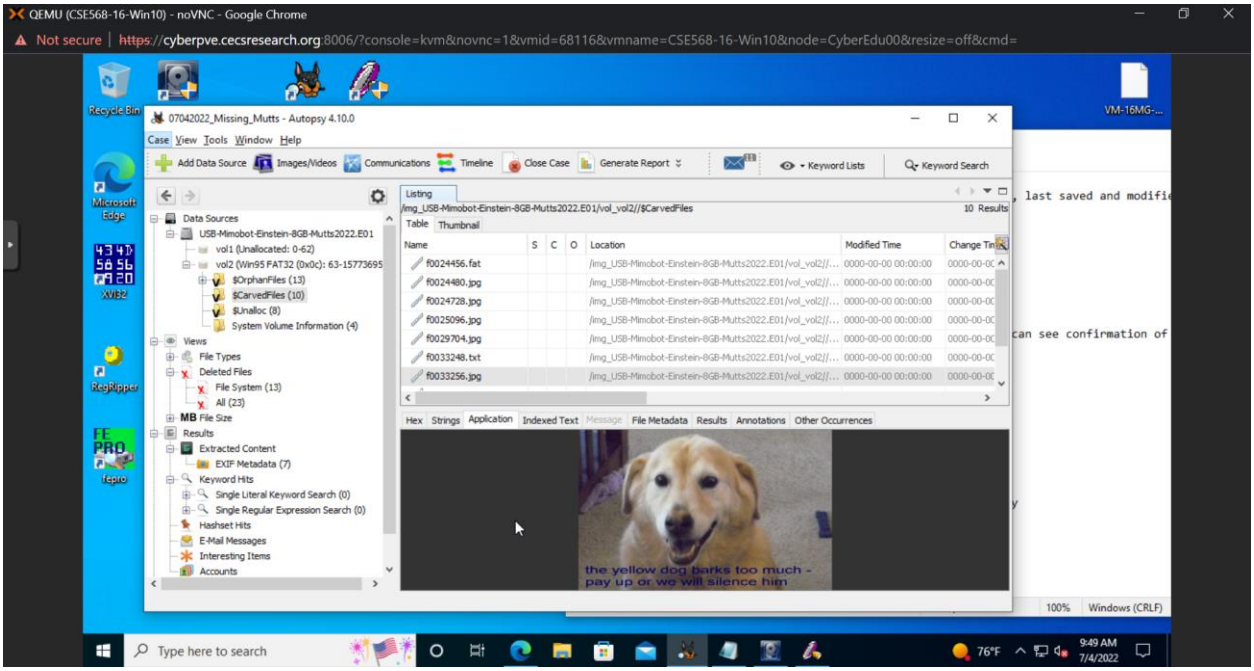
Exhibit C-1:



Autopsy result showing text document with plan for dogs.

This file was found within the unallocated space of the image. This text document contains a roughly written plan for releasing dogs and enticing them with a bone to the basement. The plan then lists “sending pictures to niceguy”. The document then has information that implies the previously mentioned dogs being given away to a niece in country to get some rest. The final step in the plan then talks about petting Princess Kitty as it will make her, “SO happy!!”

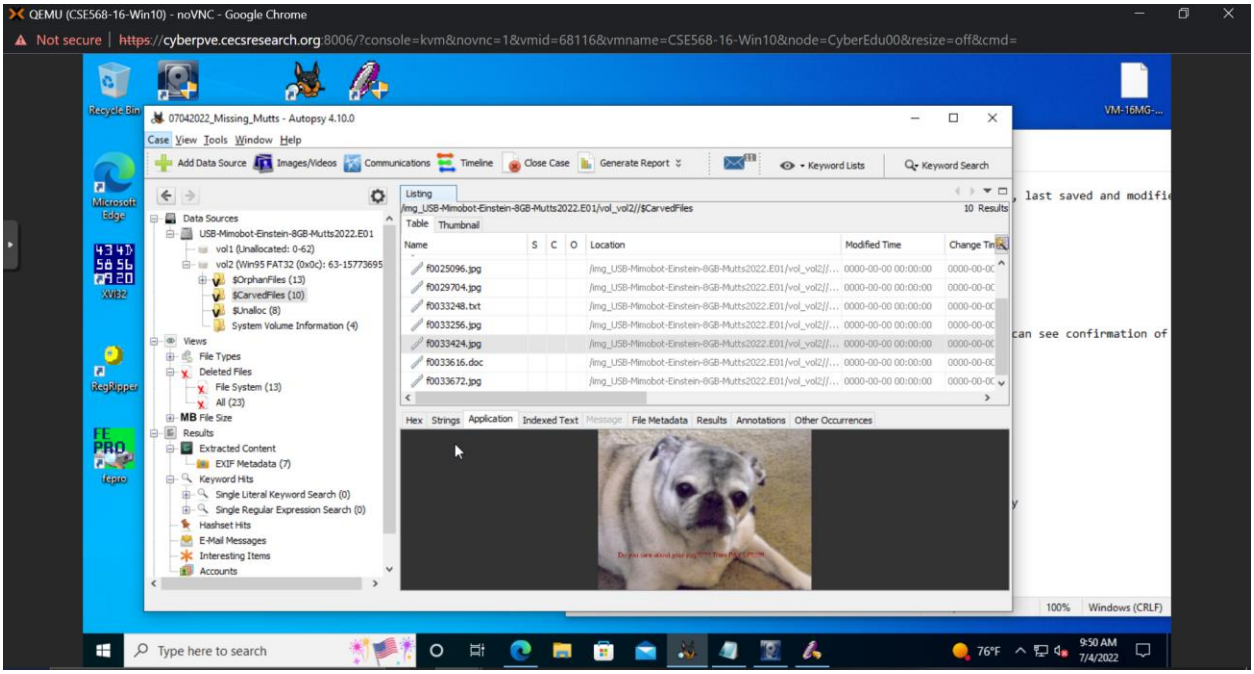
Exhibit C-2:



Autopsy result showing first dog image.

This file was found and is an obvious picture of what looks to be a golden retriever. Blue text has been edited in on the bottom that read “the yellow dog barks too much – pay up or we will silence him”. The metadata in this image, as retrieved by Autopsy, informs us that the device model is a Kodak Funsaver, a disposable camera.

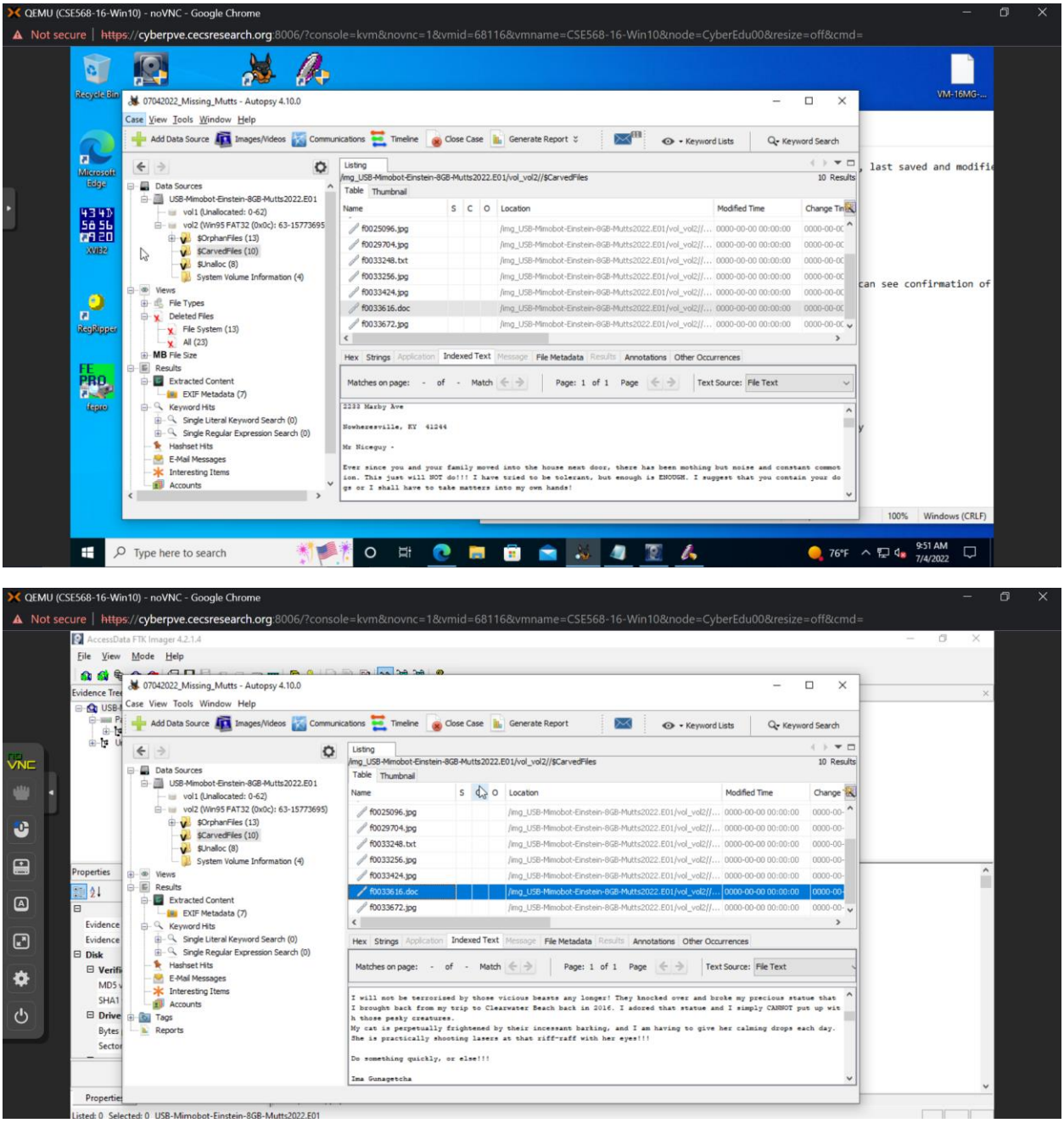
Exhibit C-3:



Autopsy result showing second dog image.

This file is similar to the file mentioned in Exhibit C-2. The image contains a picture of a pug with text that reads, “Do you care about your pug???? Then PAY UP!!!!!!” in red text. Metadata from Autopsy suggests this picture was also taken with a Kodak Funsaver disposable camera, however, there is also a time stamp of 2022-06-25T17:47:17.

Exhibit C-4:

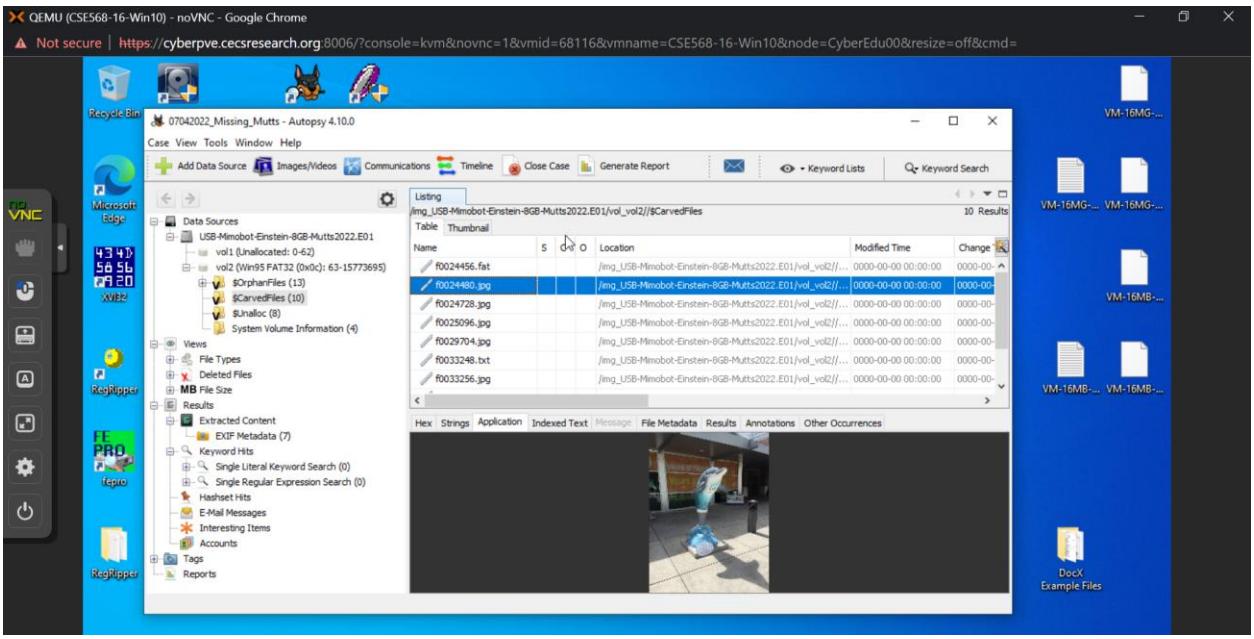


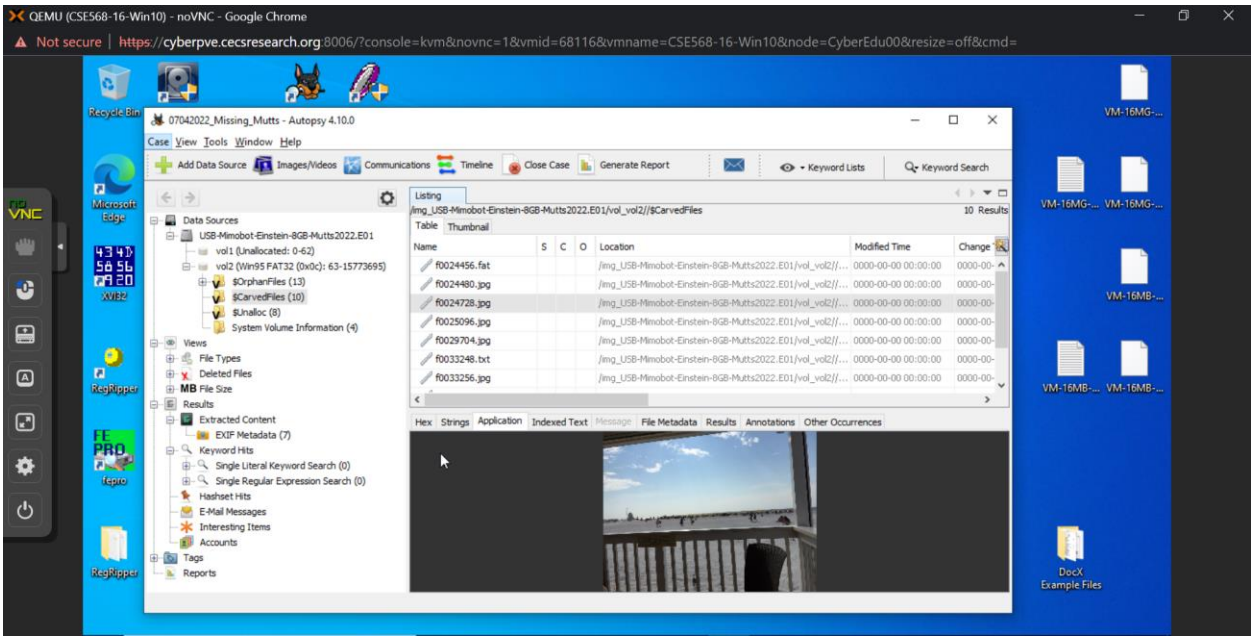
Autopsy result showing letter to Mr. Niceguy.

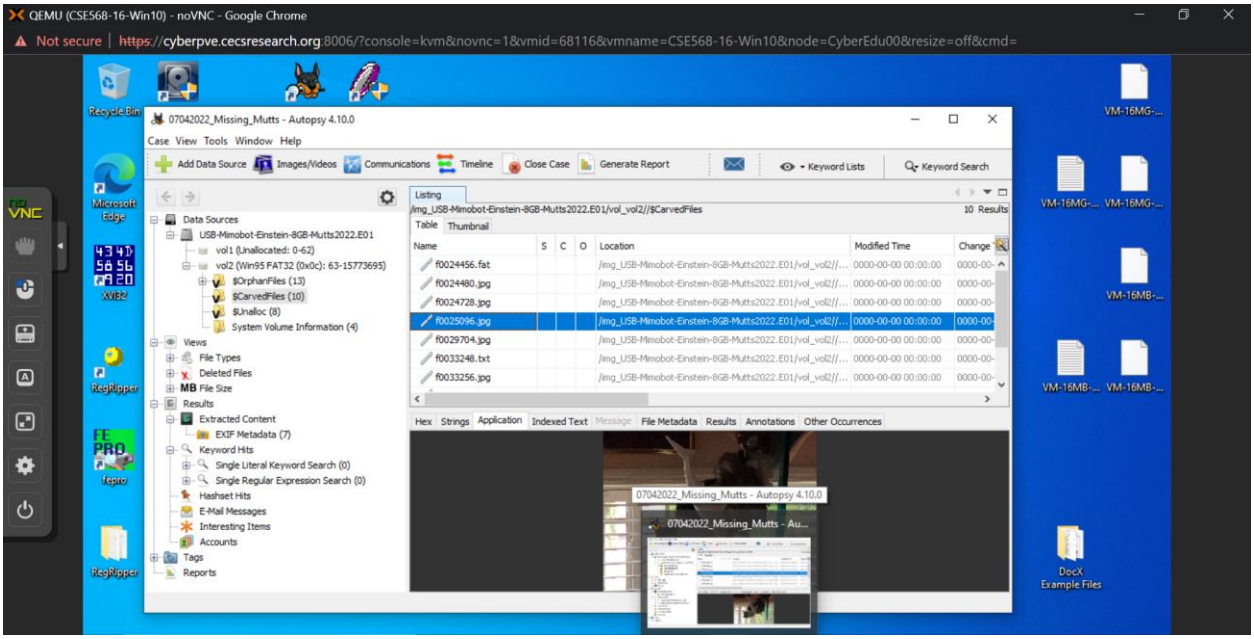
This file is a Microsoft Word document. This document is in the format of a letter which has been addressed to Mr. Niceguy from Ima Gunagetcha. The letter expresses displeasure with Mr. Niceguy's dogs and says that they will "take matters into her own hands." The metadata on this document shows that the account that created the document was named Ima Gunagetcha on 2018-07-25. The file was then last modified and saved by an account named ImaG on 2022-06-25. It should be noted that the document was created in 2018, then modified four years later, on the same day that the image on Exhibit C-3 was reportedly taken.

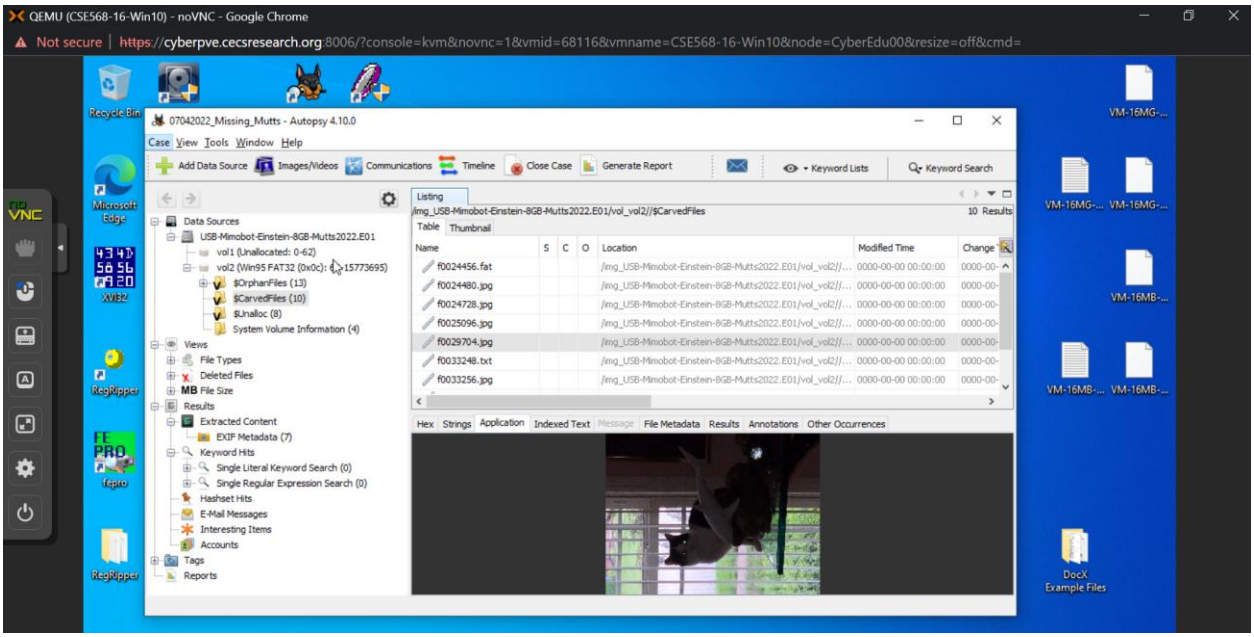
Exhibit C-5:

Exhibit C-5 is the other images on the thumb drive that were carved. These are significant as they show a pet, travel locations, and property that may belong to Ima Gunagetcha.






QEMU (CSE568-16-Win10) - noVNC - Google Chrome
Not secure | https://cyberpve.cecsresearch.org:8006/?console=kvm&novnc=1&vmid=68116&vmname=CSE568-16-Win10&node=CyberEdu00&resize=off&cmd=
07042022_Missing_Mutts - Autopsy 4.10.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
Close Case
Generate Report
Keyword Lists
Keyword Search
Data Sources
USB-Mimobot-Einstein-8GB-Mutts2022.E01
vol1 (Unallocated: 0-62)
vol2 (Win95 FAT32 (0x0c): 63-15773695)
$OrphanFiles (13)
$CarvedFiles (10)
$Unalloc (8)
System Volume Information (4)
Views
File Types
Deleted Files
File Size
Results
Extracted Content
EXIF Metadata (7)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
/img_USB-Mimobot-Einstein-8GB-Mutts2022.E01/vol_vol2//$CarvedFiles
10 Results
Table
Thumbnail
Name
S
C
O
Location
Modified Time
Change
f0024456.fat
f0024480.jpg
f0024728.jpg
f0025096.jpg
f0029704.jpg
f0033248.txt
f0033256.jpg
Hex
Strings
Application
Indexed Text
Message
File Metadata
Results
Annotations
Other Occurrences
07042022_Missing_Mutts - Autopsy 4.10.0
07042022_Missing_Mutts - Au...
Recycle Bin
Microsoft Edge
XVB2
RegRipper
fepro
RegRipper
VM-16MG-...
VM-16MG-...
VM-16MG-...
VM-16MB-...
VM-16MB-...
VM-16MB-...
DocX Example Files


QEMU (CSE568-16-Win10) - noVNC - Google Chrome
Not secure | https://cyberpve.cecsresearch.org:8006/?console=kvm&novnc=1&vmid=68116&vmname=CSE568-16-Win10&node=CyberEdu00&resize=off&cmd=
07042022_Missing_Mutts - Autopsy 4.10.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
Close Case
Generate Report
Keyword Lists
Keyword Search
Data Sources
USB-Mimobot-Einstein-8GB-Mutts2022.E01
vol1 (Unallocated: 0-62)
vol2 (Win95 FAT32 (0x0c): 15773695)
$OrphanFiles (13)
$CarvedFiles (10)
$Unalloc (8)
System Volume Information (4)
Views
File Types
Deleted Files
File Size
Results
Extracted Content
EXIF Metadata (7)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
/img_USB-Mimobot-Einstein-8GB-Mutts2022.E01/vol_vol2//$CarvedFiles
10 Results
Table
Thumbnail
Name
S
C
O
Location
Modified Time
Change
f0024456.fat
f0024480.jpg
f0024728.jpg
f0025096.jpg
f0029704.jpg
f0033248.txt
f0033256.jpg
Hex
Strings
Application
Indexed Text
Message
File Metadata
Results
Annotations
Other Occurrences
Recycle Bin
Microsoft Edge
XVB2
RegRipper
fepro
RegRipper
VM-16MG-...
VM-16MG-...
VM-16MG-...
VM-16MB-...
VM-16MB-...
VM-16MB-...
DocX Example Files