

Answer the following in this section Creating an Image

1. Source Drive **Generic Flash Disk USB Device**
2. The capacity of the source disk in # of bytes **246 MB**
3. Type of Forensic Tool Used **AccessData® FTK® Imager 3.1.5.0**
4. Destination Location **C:\Users\Godwin Monserate\Desktop\2ND Sem 2020-2021\Information Assurance and Security\Digital Forensics\Photo Crime\Pedophile\Pedophile-Case.001**
5. Target Filename **Pedophile-Case.001**
6. Estimated time to finish developing the image **3 minutes 58 seconds**
7. Hash Value MD5 **514cad8d821a1404ece56c78ebc62b9d**
8. Hash Value SHA1 **a8f7f7387396ef06a9eb0c73ee5b3ac96067cebb**

Disk Analysis

1. Number of Files in the Source Drive **184 files**
2. Number of Files in the Target Image **203 files**
3. Number of Folders in the Source Drive **12 folders**
4. Number of Folders in the Target Image **12 folders**
5. Number of Deleted Files **8 files**
6. Number of Deleted Folders **0 folders**

Data Recovery

1. Extract the Deleted Files in the Root
Number of Files Extracted? **4 files**
2. Extract the Deleted Folders
Number of Folders Extracted? **0**
Number of Files Extracted in the Folder (Specify folder and number of files) **0**

Data Analysis

1. Examine the contents of the file if it is an image file or a document file
Number of JPEG Files: **17 files**
Number of Document (.doc) Files: **2 files**
2. After Examining the signature format of the files, Identify the following:
What is the signature Format of JPEG files? **ÿØÿà**
how many jpeg files have been altered? **None**
have you recovered the file back to its original format? **None**
What is the signature format of a word document file? **Ï.à;±.á and PK**
how many doc files have been altered? **None**
have you recovered the file back to its original format? **None**
3. After recovering the file into its original form.
Number of JPEG Files: **17 files**
Number of Document (.doc) Files: **2 files**

4. Use HASH calculator for the image file and the source file, and compare both hash values.

Source

MD5 value **514cad8d821a1404ece56c78ebc62b9d**

SHA1 value **a8f7f7387396ef06a9eb0c73ee5b3ac96067cebb**

Image

MD5 value **514cad8d821a1404ece56c78ebc62b9d**

SHA1 value **a8f7f7387396ef06a9eb0c73ee5b3ac96067cebb**

Does the output between the source and the target image render a similar value?

Yes, it has the same hash value because for the altering of files, I used an image of the image instead of using the first image for the recovery of files.

Conclusion

With all the provided evidence, an image copy of data was created to preserve the evidence using **FTK Imager** which was done by **Christian Stewart, Digital Forensic Examiner**. This information was obtained from **First Responder Insp. Godwin S. Monserate** and digital forensic process was used to undergo significant and thorough analysis on a laptop. Upon recovery of deleted files and thorough file searching, 14 significant images have been found and a significant number of them shown below, are the images of **James Carl Liboon**, his child, **Janine** and his wife, who went unnamed. Other images also appear to be children – who are not related to the arrested in any way.



EVIDENCE TABLE		
Figure	Date Modified	Date Recovered
 Figure 1 baby1.jfif	03/21/2021	10/12/2022
 Figure 2 baby2.jfif	03/20/2021	10/12/2022



Figure 3
baby3.jfif

03/21/2021

10/12/2022



Figure 4
baby-wearing.jpg

03/21/2021

10/12/2022



Figure 5
daughter janine at school.jfif

03/21/2021

10/12/2022



Figure 6
father daughter love.jfif

03/21/2021

10/12/2022



Figure 7
i love my little girl.jfif

03/21/2021

10/12/2022



Figure 8
janine's BFFs.jfif

03/21/2021

10/12/2022



Figure 9
me and janine.jfif

03/21/2021

10/12/2022



Figure 10
me and janine2.jfif

03/21/2021

10/12/2022

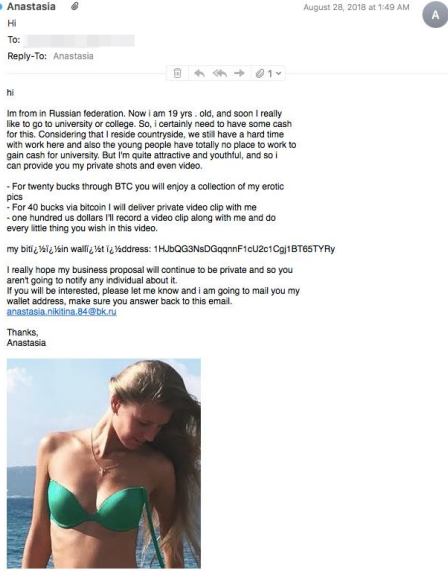
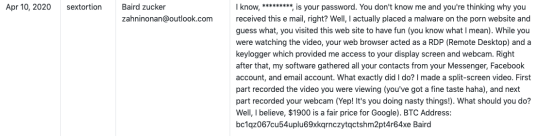


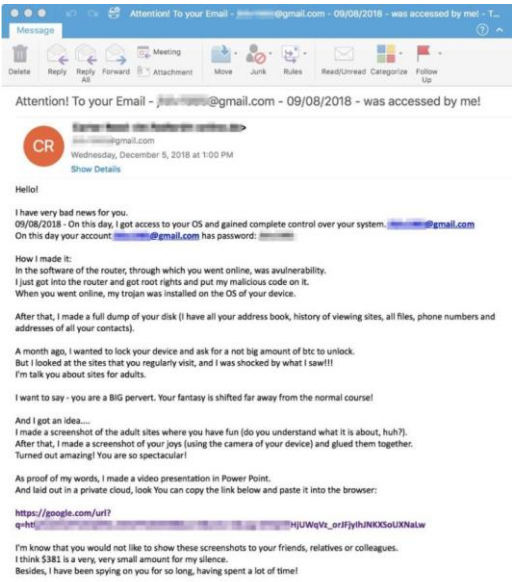
Figure 11
wifey.jfif

03/21/2021

10/12/2022

Although it seems very suspicious to be deleting images of yourself, your wife and your daughter and also other images of children whom which are not your own, it does not provide concrete evidence for one to be convicted of pedophilia. Despite such, other evidence was recovered from the deleted files of Mr. Liboon's laptop which indicate some form of sextortion.

EVIDENCE TABLE		
Figure	Date Modified	Date Recovered
 <p>Figure 12 !image13.png</p>	03/21/2021	10/12/2022
 <p>Figure 13 Screenshot-2020-04-20-at-15.59.04.png</p>	03/21/2021	10/12/2022

 <p style="text-align: center;">Figure 14 sei_43779174-e47e.jpg</p>	03/21/2021	10/12/2022
-----------------------------------------------------------------------------------------------------------------------------------------------------------------	------------	------------

Recommendation

The Digital Forensic team comprised of the First Responder Insp. Godwin S. Monserate and Digital Forensic Examiner, Christian Anthony C. Stewart, have analyzed the information obtained and have obtained substantial evidence. The evidence obtained is not enough to convict **James Carl Liboon** of the accused Pedophilia. The images do not present a conclusive enough argument that proves the arrested is an actual pedophile.

Despite such, another case may be raised against to convict the perpetrator, **James Carl Liboon** for multiple instances of sextortion. A trial is due for the convicted and we strongly conform to the severe punishment of the accused based upon presented evidence of several instances of crime.