

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\Sextortion Pedo\SextortionCase.001**
5. Target Filename **SextortionCase.001**
6. Estimated time to finish developing the image **3 minutes 59 seconds**
7. Hash Value MD5 **e7ada1dda5b9017cdc516ab94028508f**
8. Hash Value SHA1 **7ef7e6a6c02394f947636bb92f0659e9e3955460**

Disk Analysis

1. Number of Files in the Source Drive **87 files**
2. Number of Files in the Target Image **164 files**
3. Number of Folders in the Source Drive **10 folders**
4. Number of Folders in the Target Image **12 folders**
5. Number of Deleted Files **72 files**
6. Number of Deleted Folders **2 folders**

Data Recovery

1. Extract the Deleted Files in the Root
Number of Files Extracted? **2**
2. Extract the Deleted Folders
Number of Folders Extracted? **2**
Number of Files Extracted in the Folder (Specify folder and number of files)
!emp - 21 files
Collection – 39 files

Data Analysis

1. Examine the contents of the file if it is an image file or a document file
Number of JPEG Files: **16**
Number of Document (.doc) Files: **1**
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? **0**
have you recovered the file back to its original format? **No**
What is the signature format of a word document file? **ÐÌ.à;±.á and PK**
how many doc files have been altered? **0**
have you recovered the file back to its original format? **No**
3. After recovering the file into its original form.
Number of JPEG Files: **16**
Number of Document (.doc) Files: **1**

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

Source

MD5 value **e7ada1dda5b9017cdc516ab94028508f**

SHA1 value **7ef7e6a6c02394f947636bb92f0659e9e3955460**

Image

MD5 value **e7ada1dda5b9017cdc516ab94028508f**



SHA1 value **7ef7e6a6c02394f947636bb92f0659e9e3955460**

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.

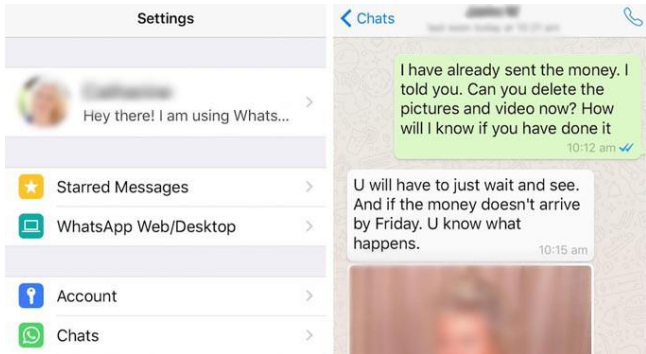
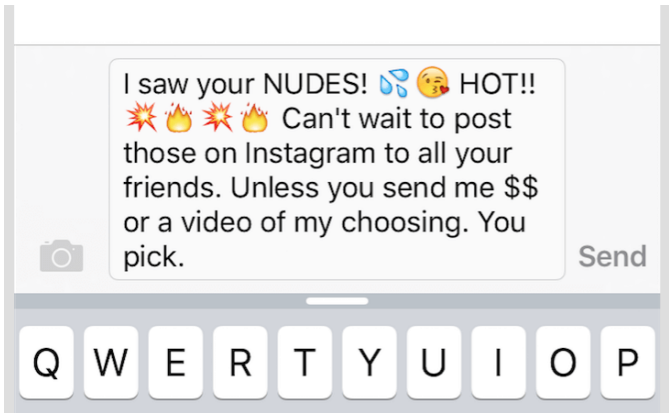
Conclusion

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, 6 significant images have been found and 4 of them shown below, are the deleted images which are deemed substantial evidence of sextortion done by the perpetrators **Willy Bruce, Linda Sturdy, and Mike Myer Jones**.

EVIDENCE TABLE		
Figure	Date Deleted	Date Recovered
<p>Anastasia @ August 28, 2018 at 1:49 AM</p> <p>Hi</p> <p>To: [REDACTED]</p> <p>Reply-To: Anastasia</p> <p>hi</p> <p>Im from in Russian federation. Now i am 19 yrs . old, and soon i really like to go to university or college. So, i certainly need to have some cash for this. Considering that i reside countryside, we still have a hard time with work here and also the young people have totally no place to work to gain cash for university. But i'm quite attractive and youthful, and so i can provide you my private shots and even video.</p> <ul style="list-style-type: none"> - For twenty bucks through BTC you will enjoy a collection of my erotic pics - For 40 bucks via bitcoin i will deliver private video clip with me - one hundred us dollars i'll record a video clip along with me and do every little thing you wish in this video. <p>my bitly link: https://bitly.com/1nwall/LjLj address: 1HUBQG3NsDQqnmF1cU2c1Cg18T66TYRy</p> <p>I really hope my business proposal will continue to be private and so you aren't going to notify any individual about it.</p> <p>If you will be interested, please let me know and i am going to mail you my wallet address, make sure you answer back to this email.</p> <p>anastasia.nikolina.84@bk.ru</p> <p>Thanks, Anastasia</p>  <p>Figure 1 !image13.png</p>	03/21/2021	10/12/2022
 <p>Figure 2 13474821_BG1.jpg</p>	03/20/2021	10/12/2022

<div><div><div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div></div></div><div><div>Apr 10, 2020</div><div>sextortion</div><div>Baird zucker zahnonan@outlook.com</div><div>I know, ***** is your password. You don't know me and you're thinking why you received this e mail, right? Well, I actually placed a malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as a RDP (Remote Desktop) and a keylogger which provided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account. What exactly did I do? I made a split-screen video. First part recorded the video you were viewing (you've got a fine taste haha), and next part recorded your webcam (Yep! It's you doing nasty things!). What should you do? Well, I believe, \$1900 is a fair price for Google). BTC Address: bc1q067cu54upl69xkqmczytqctahm2p4r64xe Baird</div></div></div> <div><div><div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div></div></div><div><div>03/21/2021</div><div>10/12/2022</div></div></div>
<div><div><div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div></div></div><div><div>Figure 3</div><div>Screenshot-2020-04-20-at-15.59.04.png</div></div></div>
<div><div><div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div></div></div><div><div>03/21/2021</div><div>10/12/2022</div></div></div> <div><div><div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div></div></div><div><div>Attention! To your Email - [redacted]@gmail.com - 09/08/2018 - was accessed by me!</div><div><div><div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div></div></div><div><div>CR</div><div>[redacted]@gmail.com</div><div>Wednesday, December 5, 2018 at 1:00 PM</div><div>Show Details</div></div><div>Hello!</div><div>I have very bad news for you.</div><div>09/08/2018 - On this day, I got access to your OS and gained complete control over your system. [redacted]@gmail.com</div><div>On this day your account [redacted]@gmail.com has password: [redacted]</div><div>How I made it:</div><div>In the software of the router, through which you went online, was a vulnerability.</div><div>I just got into the router and got root rights and put my malicious code on it.</div><div>When you went online, my trojan was installed on the OS of your device.</div><div>After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).</div><div>A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock.</div><div>But I looked at the sites that you regularly visit, and I was shocked by what I saw!!!</div><div>I'm talk you about sites for adults.</div><div>I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course!</div><div>And I got an idea...</div><div>I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).</div><div>After that, I made a screenshot of your joys (using the camera of your device) and glued them together.</div><div>Turned out amazing! You are so spectacular!</div><div>As proof of my words, I made a video presentation in Power Point.</div><div>And laid out in a private cloud, look You can copy the link below and paste it into the browser:</div><div>https://google.com/url?q=https://www.dropbox.com/s/1JUVWqVw_orfjyfhJNKS0uXNalw</div><div>I'm know that you would not like to show these screenshots to your friends, relatives or colleagues.</div><div>I think \$381 is a very, very small amount for my silence.</div><div>Besides, I have been spying on you for so long, having spent a lot of time!</div></div></div><div><div><div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div></div></div><div><div>Figure 4</div><div>sei_43779174-e47e.jpg</div></div></div></div>

The following 2 files have not been deleted but merely discovered inside the obtained laptop from the convicted perpetrators. These files were hidden inside the folder “HideMedoc”. These images contain disturbing proof of the perpetrators methods to blackmail victims if they do not conform with their demands.

EVIDENCE TABLE		
Figure	Date Modified	Date Recovered
 <p>The screenshot shows a WhatsApp chat interface. On the left is the 'Settings' menu with options: 'Hey there! I am using Whats...', 'Starred Messages', 'WhatsApp Web/Desktop', 'Account', and 'Chats'. The main chat area shows a conversation with a contact. A green message bubble says: 'I have already sent the money. I told you. Can you delete the pictures and video now? How will I know if you have done it' with a timestamp of 10:12 am and a blue checkmark. A grey response bubble says: 'U will have to just wait and see. And if the money doesn't arrive by Friday. U know what happens.' with a timestamp of 10:15 am. Below the text is a blurred image of a person's face.</p> <p>Figure 5 1_NGRmZGHcxoGqKLSzJWwKrw.jpeg</p>	03/21/2021	10/12/2022
 <p>The screenshot shows a WhatsApp chat interface with a message being typed. The text in the input field reads: 'I saw your NUDES! 💦😱 HOT!! 🔥🔥🔥 Can't wait to post those on Instagram to all your friends. Unless you send me \$\$ or a video of my choosing. You pick.' There is a camera icon on the left and a 'Send' button on the right. Below the input field is a virtual keyboard with keys Q, W, E, R, T, Y, U, I, O, P.</p> <p>Figure 6 Screen-Shot-2016-09-03-at-8.23.21-PM.png</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 to convict the perpetrators, **Willy Bruce, Linda Sturdy,** and **Mike Myer Jones** 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.