Digital Forensic Examiner: Christian Anthony C. Stewart

First Responder: Godwin S. Monserate

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\Murder\murdercase.001**
5. Target Filename **murdercase.001**
6. Estimated time to finish developing the image **4 minutes 25 seconds**
7. Hash Value MD5 **10e2b252e1e947c7aedc3c79eedd7073**
8. Hash Value SHA1 **fd2b4a5991658e60524647537a9cc39ae22ee929**

Disk Analysis

1. Number of Files in the Source Drive **88**
2. Number of Files in the Target Image **178**
3. Number of Folders in the Source Drive **3**
4. Number of Folders in the Target Image **30**
5. Number of Deleted Files **91**
6. Number of Deleted Folders **27**

Data Recovery

1. Extract the Deleted Files in the Root
   Number of Files Extracted? **6**
2. Extract the Deleted Folders
   Number of Folders Extracted? **27**
   Number of Files Extracted in the Folder (Specify folder and number of files)
   Cyndi SAD – 8 files
   Topic 1 – 3 files
   Topic 2 – 2 files
   Topic 3 – 3 files
   sf QUIZ – 68 files

Data Analysis

1. Examine the contents of the file if it is an image file or a document file
   Number of JPEG Files: **19 files**
   Number of Document (.doc) Files: **1 file**
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? **Yes**
What is the signature format of a word document file? **ÐÏ.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: **19 files**
   Number of Document (.doc) Files: **1 file**

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

Source
MD5 value **10e2b252e1e947c7aedc3c79eedd7073**
SHA1 value **fd2b4a5991658e60524647537a9cc39ae22ee929**

Image
MD5 value **10e2b252e1e947c7aedc3c79eedd7073**
SHA1 value **fd2b4a5991658e60524647537a9cc39ae22ee929**

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 flash drive. Upon recovery of deleted files, 6 significant images have been found. 4 of them, shown below, are images which are deemed substantial evidence of murder done by the perpetrator **Robert John Rhodest**.

EVIDENCE TABLE		
Figure	**Date Deleted**	**Date Recovered**
Figure 1 Bob-Berdella-Robert-Sheldon-1.jpg	03/20/2021	10/10/2022
	03/20/2021	10/10/2022

Figure 2 Bob-Berdella-Robert-Sheldon-2.jpg		
 Figure 3 Bob-Berdella-Todd-Stoops.jpg	03/20/2021	10/10/2022
 Figure 4 Bob-Berdella-Robert-Sheldon-3.jpg	03/20/2021	10/10/2022

2 additional files have also been discovered from the flash drive that are letters made by the said perpetrator. Figure 5 is a **gif** file while figure 6 is a **jfif**. Both show detail of the perpetrator admitting to the killings of 2 separate people.

EVIDENCE TABLE		
Figure	**Date Deleted**	**Date Recovered**
Figure 5 Letter at Ocean.gif	03/20/2021	10/10/2022
Figure 6 R8fd9ee6c7bec84e34b4fd4823202ca46.jfif	03/20/2021	10/10/2022

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 perpetrator, Robert John Rhodest for

multiple murders. A trial is due for the convicted murderer and we strongly conform to the severe punishment of the accused based upon presented evidence of several crimes.