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\Rape and Murder\rape-murder-case.001**
5. Target Filename **rape-murder-case.001**
6. Estimated time to finish developing the image **4 minutes**
7. Hash Value MD5 **594d897f7dd60f5bcc4ff5c8beac79b9**
8. Hash Value SHA1 **15b82048487f51892ad16cae5e45e922612aea4b**

Disk Analysis

1. Number of Files in the Source Drive **142 files**
2. Number of Files in the Target Image **228 files**
3. Number of Folders in the Source Drive **8 folders**
4. Number of Folders in the Target Image **20 folders**
5. Number of Deleted Files **86 files**
6. Number of Deleted Folders **12 folders**

Data Recovery

1. Extract the Deleted Files in the Root
   Number of Files Extracted? **54**
2. Extract the Deleted Folders
   Number of Folders Extracted? **8**
   Number of Files Extracted in the Folder (Specify folder and number of files)
   !ata – 16 files
   !emp - 7 files
   2019 Files – 3 files

Data Analysis

1. Examine the contents of the file if it is an image file or a document file
   Number of JPEG Files: **30**
   Number of Document (.doc) Files: **2**
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? **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: **30**
   Number of Document (.doc) Files: **2**

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

Source
MD5 value **594d897f7dd60f5bcc4ff5c8beac79b9**
SHA1 value **15b82048487f51892ad16cae5e45e922612aea4b**

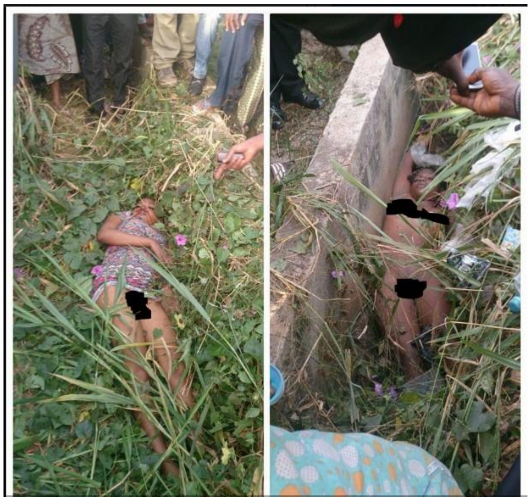
Image
MD5 value **594d897f7dd60f5bcc4ff5c8beac79b9**
SHA1 value **15b82048487f51892ad16cae5e45e922612aea4b**

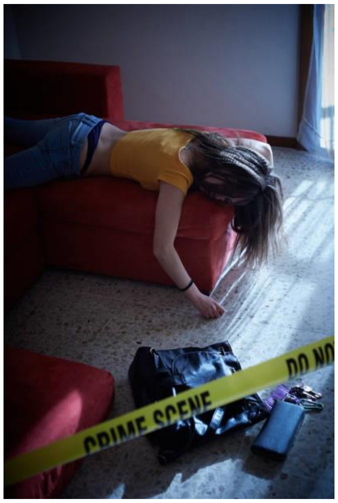
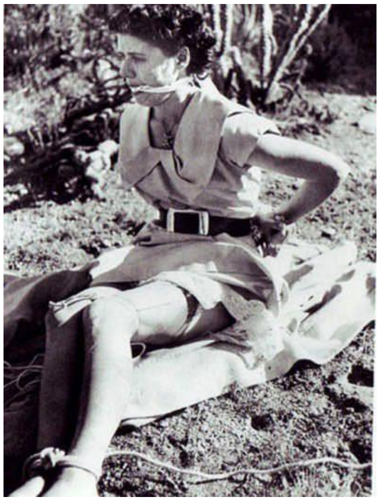
Does the output between the source and the target image render a similar value?

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, 3 significant images have been found and shown below, are the images which are deemed substantial evidence of rape and murder done by the perpetrator **Jim Rice Copenhagen**.

EVIDENCE TABLE		
Figure	**Date Modified**	**Date Recovered**
 **Figure 1** 3199485_3198117capturejpeg6d0ce43c2e6495dc5ba7597dd3872afd_jpegb76877d130a718e0f81b3688921c82b4.jfif	03/21/2021	10/10/2022

 **Figure 2** istockphoto-831068278-612x612.jpg	03/21/2021	10/10/2022
 **Figure 3** Shirley-Ann-Bridgeford-01.jpg	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, Jim Rice Copenhagen for multiple rape and murders. A trial is due for the convicted rapist murderer and we strongly conform to the severe punishment of the accused based upon presented evidence of several crimes.