Answer the following in this section Creating an Image

1. Source Drive

Imation Nano USB Device

2. The capacity of the source disk in # of bytes

955 MB

3. Type of Forensic Tool Used

FTK Imager

4. Destination Location

C:\Users\Godwin Monserate\Desktop\USC Files 2022-23\Classes 1st Sem 2022-2023\Information Assurance and Security\Lab Activity 5005\Evidence Case 1001.001

5. Target Filename

Evidence Case 1001.001

6. Estimated time to finish developing the image

1 minute

7. Hash Value MD5

f438c0143a0b0bc8c90e188e0fcbe226

8. Hash Value SHA1

8ba5edb401f0950fa8cc8882631f72da5d6bcb09

Disk Analysis

1. Number of Files in the Source Drive **146**
2. Number of Files in the Target Image **219**
3. Number of Folders in the Source Drive **3**
4. Number of Folders in the Target Image **4**
5. Number of Deleted Files **73**
6. Number of Deleted Folders **1**

Data Recovery

1. Extract the Deleted Files in the Root
   Number of Files Extracted? **73**

   Number of Files that have size > 0 bytes – **29**
   Number of Files that have size = 0 bytes – **44**

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

Data Analysis

1. Examine the contents of the file if it is an image file or a document file
   Number of JPEG Files: **31**
   Number of Document (.doc) Files: **8**
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? **1**
   have you recovered the file back to its original format? **Yes**
   What is the signature format of a word document file? **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: **9**

4. Use HASH calculator for the image file and the source file, and compare both hash values.
   MD5 value **f438c0143a0b0bc8c90e188e0fcbe226**
   SHA1 value **8ba5edb401f0950fa8cc8882631f72da5d6bcb09**
   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.

Reflection:

1. What did you learn about this activity? 5pts

Digital forensics is a tedious process that requires thorough analysis and being an examiner requires you to truly think of every nook and cranny. Think out of the box if you must. This activity showed to me how important it is to take into account every single tiny detail which can change the course of a certain case.

2. What is the significance of Digital forensics in your course? 5pts

Digital forensics provide good information security and assurance to me as a computer science student since it allows me to protect myself against any intrusions or attackers. Helps me identify and trace any information that was copied or distributed in a lawful way. I can also apply some computer science techniques like algorithm efficiency on certain hashing functions. Digital Forensics also teach me certain methods that I can apply to my computer science career like how information travels through the Internet and how I may be able to protect this or even intercept such.

3. Cite at least 3 examples of the useful application of digital forensics. 10pts

1. Can help in crime prevention.
2. Can be used in digital crime recognition. Digital forensics can be used to reconstruct how previous events have unfolded.
3. Extraction of data from an electronic device to prove that an attacker is using a bitcoin sextortion scam on a victim.