Disk ImageForensic using FTK imager

KELOMPOK:

- Jonathan : 2501986611
- Maximilian Ryan Japri : 2502011360
- Christina Kartika : 2502004235
- I Made Prama Sedana : 2502005723
- Hugo Cuandri : 2501997016

1. Open / Install Access Data’s FTK Imager 3

2. Select File > Add Evidence Item > Select Image File > Browse to Vader_Home_Computer.001 image and add it.

3. Navigate to the C:\Documents and Settings\Owner\My Documents\Secret pics folder.

4. Export the “Secret Pics” folder to your local hard drive.

Disk ImageForensic using FTK imager

5. On your computer, examine the three pictures inside the Secret pics folder. Using Windows, right click on the three provided pictures and record the size of each file.
me & the guys1.jpg size: 252 KB
me & the guys2.jpg size: 252 KB
me & the guys3.jpg size: 252 KB

6. Open each image and describe the contents.
me & the guys1.jpg Description: Darth Vader and the gangs
me & the guys2.jpg Description: Darth Vader and the gangs
me & the guys3.jpg Description: Darth Vader and the gangs

7. Are the pictures all identical? Yes they are

8. Install Hashcalc.exe.

Disk ImageForensic using FTK imager

9.Use Hashcalc to calculate the hashes of all 3 files. Record the Md5 Hash value for each file.
me & the guys1.jpg Md5 Hash: 2c88e88976c4379d117854d216e36681
me & the guys2.jpg Md5 Hash: f22d2acdbb1884af86b40d72f447eca2
me & the guys3.jpg Md5 Hash: 2c88e88976c4379d117854d216e36681

10. Install the HxD Hex Editor on your computer and open it.

11. In HxD, select “open” under the file menu. Open one of 2 duplicate files. You know they are duplicate because they have an identical hash.

12. Go to the bottom of the file and change the last byte by selecting it and typing any character

Disk ImageForensic using FTK imager

13. Select “Save as” under “File” and save this picture under a different name. Use Windows to record the file size and hash calc for the md5 hash of the new file new file.

New File: “me & the guys1 (MODIFIED).jpg”
Description: Darth Vader and the gangs
Size: 252 KB
Md5 Hash: 0a98a53ab49b7caabea5b06bca56bd6f

14. Based on the results of this test, what are your thoughts on the reliability of Md5 as a “digital fingerprint”?

Answer:From the test, we know that if you change 1 byte of the file, it will change the MD5 hash of the file, therefore is one of a best and reliable digital fingerprint form computer forensic

Disk ImageForensic using FTK imager

15. Use HxD to examine the last few bytes of each of the files provided and record anything that might be of suspicion.

Answer: From file “me & the guys2.jpg” we can find hidden text that says “DEATH_STAR_PASSWORD IS: CutePuppies123:)”

Thankyou