£4NinetyEight

Computer Forensics 2 – Lab 3

By Dr Diane Gan

1. Comparing Hashes

Run **HashText.exe**

- Enter some text into the MD5 hash generator - include the number 5 in the text.

- Record the hash or copy it into notepad ………………………………………………

- Keeping the text the same, change the 5 to a 4 look at the hash value.

- Record the new hash or copy it into notepad ………………………………………………

- Compare the before and after values above

  What happened to the hashes? ....

  Why has the hash changed? …………………………………………………………

  How many bits have been changed in your text? ..………………………………………
  (Hint – compare the binary for 4 and 5)

2. Investigating the Thumbs.db

The suspect denies being guilty of possession of child pornography. There are currently no files on his computer. However, we have found a thumbs.db file that appears to have incriminating graphics in it. In this exercise we will view thumbs.db files. We will also create a hash set for comparative purposes.

Creating the files

- Create a folder called **Suspect Graphics** in your folder on the C drive (C:\Users\Student\yourname)
- Copy the graphics files and the thumbs.db file from Dianes Utils Exercises\Ex5.2 into your folder.
- If you do not see the thumbs.db then you may have to change your settings to **Show hidden files and folders** – also check **Show protected operating systems files.**

The suspect moves the graphics

The suspect moved the files from their computer onto removable media, in an attempt to hide their activities. While copying the images, the suspect also copied over the thumbs.db file as well. He was not aware that he left the original thumbs.db behind in the folder.

- Create a second folder called **Moved Graphics**
- Copy your images and the thumbs.db. files across to this new folder
- Delete the graphics files from the original folder (Suspect Graphics), but leave the Thumbs.db file behind. If the suspect did not have his Explorer set to view hidden files then he would not have seen this file because the Thumbs.db is a protected system hidden file.

  DO NOT LOOK AT THE MOVED IMAGES – this writes out to the Thumbs.db and makes changes. Remember, in the crime that was committed that we are recreating, the suspect copied the files onto a DVD which is a read only device and does not write back.

Adding Evidence into FTK (using either 1.8 or 6)

1. **Using FTK vs 1.8**

- Open **FTK** and select **“Go directly to working in program”**
- Select **File > Add Evidence –** select Next
- Deselect all check boxes except MD5 Hash > click Next
- Select **Add Evidence > Contents of a Folder >** click continue
- Navigate to the **Suspect Graphics folder > select OK >** Next and Finish

Hashing the Thumbnails (using FTK 1.8)

- Make sure that you are looking at the **Overview Tab**
- Click the **Total File Items** button
- In the File List Pane (at the bottom) highlight all the images and the thumbs.db file. Right click and select **Copy Special**.
- In the **Copy Special** dialog box click the “**Unselect All**” button (on the right)
- Select **File Name** and **MD5 Hash** from the list (scroll down to see this near the bottom)
- In the **Copy destination** section, select **File** and browse to the Desktop (or to a folder) and name it **Suspect Graphics Hashes.**
- Select the **Copy** button to send the hash list to the file you have just specified.

You should now have a hash list of the thumbnails that existed in the thumbs.db file, as well as the thumbs.db itself. Now we will compare these to the contents of the **Moved Graphics** folder.

2. Using FTK vs 6

- Login to FTK (icon on the Desktop) – login ID = ftk and password = accessdata
- Start a new case – give this a name (Hashes)
- Manage Evidence box opens
- Click Add and select Contents of a Directory and click OK
- Navigate to each of your two folders and add them
- Say “yes” to the warning box
- Make sure the Time Stamp is set to Europe/London and click OK

You should now be able to see the two folders.
Investigate the files

- Compare the hashes from the **Suspect Graphics** folder with those in the **Moved Graphics** folder.

Try sorting the MD5 column by double clicking on the header box

Are the two hashes the same? ....

What does this prove? ....