Experiment No:3

**Aim:** Performance to Recover Digital Evidence with WinHex.

**Theory:**

You are a senior computer forensics investigator. Your junior technician seized a floppy disk into evidence and cloned it. The bit stream image file (clone) is on the forensics server (Blackboard). The image file is called CatPlus.e01. You will check out the image file and analyze it. You will also try to recover a deleted file.

#### **Create a Case Folder and Activity Log**

1. Create a folder on your **F** drive for this case. The case number is 7777. Call the folder something like **Case7777**.
2. Using **Microsoft Word** or **Notepad**, start an activity log that documents the major steps that you take.
3. Note: Each student should write an activity log, even if you work together on the WinHex hands-on activities.
4. In your activity log, include the date, case number, and timestamps as you work.
5. As you work with disks and files, use the MD-5 algorithm to create a hash code, and copy and paste the resulting hash code in your activity log to document that you have not tainted the evidence.
6. Save your activity log in the case folder you created on your F drive. You will be submitting it via Blackboard.

**Check out the Image File**

1. Copy the image file [**CatPlusFile**](http://www.priscilla.com/Courses/ComputerForensics/Labs/CatPlusFile)from Blackboard to your case folder.
2. To copy the image file, **right click** on the **CatPlusFile** filename and select **Save Target As ...** Save it as **CatPlus.e01**.
3. Navigate to the case folder that you created on your F drive and save the image file in that folder.

**Start the WinHex Software**

1. Click on the Windows **Start** button and navigate to **All Programs->SOU Student Lab Menu->Departmental Programs->Computer Science**.
2. You should see a list of software that we use in the Computer Science department. It may take a while for the list to come up. Be patient.
3. Start the **WinHex** software.

**Open and Authenticate the Image File**

1. From the **File** menu in WinHex, select **Open**.
2. Find the **CatPlus.e01** file that you put in your case folder on your F drive.
3. Click on the **Open** button.
4. From the **Tools** menu, select **Calculate Hash**.
5. Select the **MD5 (128-bit)** hash algorithm and let the computer make the calculation. It could take a while. Be patient.
6. Copy and paste the results (the hash) into your activity log (with a note about what it is, e.g. the MD-5 hash of the image file at the start of your work session).

**Analyze the Physical View**

1. You’re looking at the data exactly as it was on the floppy disk. We call this the *physical view*.
   1. The middle section of the display shows the contents of the disk. Each row displays 16 bytes of data, expressed in hexadecimal. (Hexadecimal means the base-16 number system. It's often just called *hex*.) The first byte, byte 0, is EBh and the 11th byte is 43h. (The *h* means *hex*).
   2. The left section shows the offset (distance from the beginning expressed in hex) of the first byte in the row shown in the middle section. For example, the first byte in the 4th row is offset 30h. (Note that offset 30h means [3 x 16] + [0 x 1] or 48 in decimal. You're looking 48 bytes into the data.)
   3. The right section interprets each row of 16 bytes using the ASCII character set. For example, the 11th byte in the first row (43h) represents the character C. Many hex values cannot be represented by ASCII symbols; these are shown with a dot.
2. In your activity log, jot down any suspicious or other relevant information that you notice in the Physical View. You may have to scroll down to see anything legible.

**Analyze the Logical View**

1. To see a logical view of the data that was on the original floppy disk, go to the **Specialist** menu in WinHex and select **Interpret Image File As Disk**. (If the menu item is grayed out, then you are already interpreting the image file as disk.)
2. Interpreting as disk lets you see files and directories (folders), even files and directories that the user deleted. (WinHex shows deleted files and directories in a paler color.) The bottom portion of the window should still show the physical view (offset, hex values, and ASCII values) with an added "Access" menu.
3. Whenever you look at a file in a new way, it's a good idea to authenticate the file again (recalculate the hash), to ensure you haven't tainted the evidence. So calculate the hash again and jot it down in your activity log.
4. In the top section of WinHex, which shows the logical view, you may notice duplicated file and directory names. If you do, jot this down in your activity log with a possible explanation. (Perhaps the suspect kept multiple versions of the files and directories as he worked?)
5. What files were deleted but then never created again (there is no new version?) Jot this down in your activity log.

**Analyze and Recover a Deleted File**

1. Scroll down in the logical view to the **Copy of bad\_bad\_jpg** file. The user deleted this file, but notice that its size is not zero! How big is it? (Number of kilobytes (KB)? Jot this down in your activity log.
2. **Right click** on **Copy of bad\_bad\_cat.jpg** and select **Go to beginning of file**.
3. What is the offset of the beginning of this file (in hex)? Include the question and answer in your activity log.
4. What are the first four bytes of the file (in hex)? Include the question and answer in your activity log. The first four bytes of a file often hold a "file signature," which identifies the type of file. We'll learn more about file signatures next week.
5. **Right click** on **Copy of bad\_bad\_cat.jpg** in the logical view again.
6. Select **Recover/Copy** and save the recovered file in your case folder on your F drive.
7. Read any warnings that WinHex gives you, but unless they sound really scary, you can probably just click **Yes** or **OK**.

**Authenticate the Recovered File**

1. The recovered file is now a new piece of evidence. Authenticate it immediately using the following procedures.
2. From the WinHex **File** menu, select **Open**. Find the recovered file in your case folder and click the **Open** button.
3. From the **Tools** menu, select **Calculate Hash**.
4. Select the **MD5 (128-bit)** hash algorithm and let the computer make the calculation.
5. Copy and paste the results (the hash) into your activity log (with a note about what it is, e.g. the MD-5 hash of the recovered file).
6. Close the file. (Click on the **X** icon for the file window. Don't close WinHex, though!) Examine the Recovered File
7. Open the file from Windows.
8. From the **Start Menu**, go to **MyComputer** and navigate to your case folder on your **F** drive.
9. **Double click** on the icon for your recovered file.
10. Document your conclusions about the contents of the file and its usefulness in the criminal case.

**End Your Session**

1. Back in WinHex, open the recovered file again and verify that you didn't change it (Calculate the hash).
2. Also calculate the hash for the original image file to prove that you didn't taint it.
3. Copy and paste the results in your activity log.
4. Quit WinHex.

**Conclusion:**

The tests that were conducted on WinHex attempted to prove that this tool is important to a forensic investigator. The test tried to prove the many different capabilities this one tool holds.