Experiment No: 5

**Aim:** To study Documentation of 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. The image file is called Evidence.e01. You will check out the image file, analyze it, and document your findings.

Start an Activity Log

1. Using Microsoft Word or Notepad, start an activity log that documents the major steps that you take.
2. Note: Each student should write an activity log, even if you work together on the WinHex hands-on activities.
3. In your activity log, include the date, case number, and timestamps as you work. The case number is still 7777.
4. Save your activity log. Two weeks ago you created a folder on your F drive for evidence related to Case 7777. That would be a good place to save your work for this week also.

Check Out the Image File

1. Note: This is the same image file that we used last week. If you still have it on your F drive, you can skip to the next section.
2. Otherwise, copy the image file Evidence.e01 from the server to your F drive.
3. To copy the image file, right click on the Evidence.e01 filename on the server and select Save Target As ... (If you're using Mozilla instead of Internet Explorer, left click and save the file when Mozilla prompts you to do so.)
4. Navigate to your F drive and save the image file there.

Start the WinHex Software

1. Click on the Windows Start button and navigate to WinHex.
2. Start the WinHex software.

Open and Authenticate the Image File

1. From the File menu in WinHex, select Open.
2. Find the Evidence.e01 file that you put 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).
7. 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.)

Create a Drive Contents Table

1. The Specialist version of WinHex has a nice feature that lets you create an Excel spreadsheet (or tab-delimited text file) of the contents of a disk. The spreadsheet includes information about the size of the file, when it was last accessed, a hash value for the file, etc.
2. From the Specialist menu, select Create Drive Contents Table.
3. Click all the checkboxes, except Directory browser.
4. Click on the button beside Calculate hash and select CRC16. (This is shorter and more appropriate for a spreadsheet than the MD5-128 hash.)
5. In the next window, select all the file types. (Shift click allows you to select more than one type.)
6. Save the Drive Contents Table file to your F drive.
7. Excel should open with the contents of the disk displayed.
8. Use your Excel skills to make this large amount of information comprehensible. For example, make columns wider by dragging the right column boundary. Hide columns that aren't interesting by right clicking on the top of the column and choosing Hide.
9. Based on information in the Excel spreadsheet, when was this evidence last used by the suspect? Jot this down in your activity log.

Recover a Deleted File

1. According to the Drive Contents Table, how many files were deleted? To help you answer this, try sorting on the Deleted column in Excel. (Select the column. From the Data menu, select Sort.)
2. Of those files, which ones might be recoverable? (Think about what it means to be recoverable.)
3. Choose a file that you could recover.
4. Document its CRC16 hash. (Check the CRC16 column in the Excel spreadsheet (the Drive Contents Table).
5. Back in WinHex, try recovering the file. (Find its name in the list in the logical view, right click on it and select Recover/Copy. Make sure you get the right version of the file. Remember, the suspect kept many versions of the files.)
6. Save the recovered file on your F drive.

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 CRC16 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).
6. Close the file. (Click on the X icon for the file window. Don't close WinHex, though!)

Examine the Recovered File

1. Open the file from Windows.
2. From the Start Menu, go to My Computer and navigate to your case folder on your F drive.
3. Double click on the icon for your recovered file.
4. Document your conclusions about the contents of the file and its usefulness in the criminal case.
5. Include in your activity log information about the file that the Drive Contents Table tells you.
6. End your Session
7. Back in WinHex, open the recovered file again and verify that you didn't change it (calculate the hash).
8. Also calculate the hash for the original image file to prove that you didn't taint it.
9. Copy and paste the results in your activity log.
10. 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.