Experiment No:4

**Aim:** Performance to Analyze 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 bitstream image file (clone) is on the forensics server. The image file is called Evidence.e01. You will check out the image file and analyze it, using a variety of WinHex features.

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 on your F drive. Last week 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. Copy the image file Evidence.e01 from the server to your F drive.
2. 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.)
3. 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.)

Analyze a Renamed File

1. Sometimes criminals change the three-letter extension of a filename to hide their evil deeds. An inexperienced investigator might overlook this evidence. The criminal can still look at the file in its original format, because the file hasn't really changed. Knowledgeable investigators can also look at the file.
2. Scroll down in the logical view to the CatHumor.jpg file.
3. Right click on CatHumor.jpg and select Go to beginning of file.
4. Does this file really seem to be a jpg (picture or photo)? Take a guess at what kind of file it really is by looking at the ASCII text in the right column. If you don't have a clue, ask one of the CS majors to help you. They will easily recognize it!? Jot down some hunches in your activity log.
5. Right click on CatHumor.jpg in the logical view again.
6. Select Recover/Copy and save the recovered file 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.

Make Sure Windows Shows Useful Information

1. From the Start Menu, go to MyComputer and navigate to your case folder on your F drive.
2. From the Tools menu, select Folder Options.
3. Click on the View tab.
4. Make sure a Hide extension for known file types is not checked.
5. Click Apply and then click OK.
6. Find the file that you recovered. What is its full name (including its three-letter extension)?
7. Double click on the file icon and document what happens.
8. Now try changing the three-letter extension, based on the hunch that you have regarding the type of file. Double click on the file again and document what happens and any more hunches that you have about the nature of the evidence.

Analyze another Renamed File

1. Scroll down in the logical view to the Cat\_bear.txt file.
2. Right click on Cat\_bear.txt and select Go to beginning of file.
3. Does this file really seem to be text?
4. What are the first three bytes of the file (in hex)? Include the question and answer in your activity log. The first few bytes of a file often hold a "file signature," which identifies the type of file.
5. On the server, download either FileTypeSignatures.txt or FileTypeSignatures.xls to help you with your analysis. The first file is in text format, but is sort of hard to read without tinkering with the tabs. The second file is the same data, but in Excel format. (Both files are included to accommodate anti-Microsoft people who don't use Excel.:-)
6. Right click on Cat\_bear.txt in the logical view again.
7. Select Recover/Copy and save the recovered file on your F drive.
8. Read any warnings that WinHex gives you, but unless they sound really scary, you can probably just click Yes or OK.
9. Using Windows, find the file that you just recovered. Double click on it and document what happens.
10. Now try changing the three-letter extension, based on the hunch that you have regarding the type of file. Double click on the file again and document what happens and any more hunches that you have about the nature of the evidence.

Search for Text

1. The Specialist version of WinHex has a nice feature that lets you search for multiple examples of text.
2. From the WinHex Specialist menu, select Simultaneous Search.
3. Type in a list of words related to your investigation. Try words related to drugs, especially drugs of interest to cats, such as tuna or catnip. Try words related to terrorism, such as guns, violence, attack. Try words related to other suspicious activity. (These are some Bad Cats! :-)
4. Click on Archive occurrence positions and select Tab-delimited text file.
5. Tell WinHex to save the report on your F drive.
6. Once WinHex has saved the report, find it on your F drive and double click its icon to open the report.
7. Document the results of your search for text in your activity log.

End Your Session

1. In WinHex, calculate an MD5-128 hash for the image file to prove that you didn't taint it.
2. Copy and paste the results in your activity log.
3. 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.