Lab 2 Comparing File Structures with a Hex Editor

Theory

Files re created using different text editors. It is therefore imperative that Computer forensics scientists are able to view these files without the native text editor and using debug in order to determine their actual file structures. This aids in investigations when determining a forensics scenario.

Objective

To demonstrate how various text editing tools such as Word, Notepad, WordPad etc., provide additional formatting information to text files and the various information leakage resulting from formatting.

Tools/Equipment

Hex Editor (Hex Workshop v5, or WinHex)
You can download WinHex from the website http://ww.x-ways.net/wnhex/ or you can simply use the copy in the CFR folder in isNotes.

Virtual Software (Virtual PC or Vmware) running Windows
You may need to work on a virtual machine in case you have no administrator rights (all labs except Lab 5) to install WinHex or Hex Workshop.

Activities

1. Set up Windows Server 2003/XP in a Virtual Environment

2. Install WinHex or Hex Workshop if not installed.

3. Open Notepad with a file name **File1.txt**

   Insert the following text into File1.txt:

   ABCDEFGHIJKLMNOPQRSTUVWXYZ
   0123456789
   This is the end of the file!

4. Close File1.txt

5. Open WordPad with a file name **File2**. Use the default filename extension.

   Insert the following text into File2:

   ABCDEFGHIJKLMNOPQRSTUVWXYZ
   0123456789
   This is the end of the file!

6. Close File2.

7. Open Microsoft Word with a file name File3. Use the default file name extension.

   Insert the following text into File3:

   ABCDEFGHIJKLMNOPQRSTUVWXYZ
   0123456789
   This is the end of the file!

8. Close File3.

9. Open Microsoft Word with a file name File4. Use the default filename extension. Select Tools, Options, Security. Enter a two character password such as *zz, ww, dd, etc.*

   Insert the following text into File4:

   ABCDEFGHIJKLMNOPQRSTUVWXYZ
   0123456789
   This is the end of the file!

10. Close File4.

11. Initialise the WinHex program. Open each file and view the information contained within.

    a. What similarities do you notice?

    ____
    ____
    ____

    b. What differences do you notice?

    ____
    ____
    ____
    ____

    c. How can you tell what type of file you are looking at by what WinHex shows in the Hex Window?

    ____
    ____
    ____
    ____
    ____

12. Perform Step 11 using the DOS editor. Compare the output of viewing the file in WinHex editor with that of Step 11. What do you notice?

    ____
    ____
    ____

Self Documentation is encouraged to outline difficulties and uncertainties.

>>>>> End of Lab Exercise <<<<<