**Hex Editing Assignment**

Although most examinations of digital evidence are done with the aid of forensic software, there are occasions when cybercrime investigators may need to look at the raw data on a computer. To "hex edit" means to make changes to the raw binary data -- 1's and 0's -- on a computer. "Hex" is short for hexadecimal. A hex editor is a software application that presents the raw data of a file and allows the user to edit that data.

In this assignment students will:

* Learn what hexadecimal notation is and why it is used when editing a document.
* Become familiar with a hex editing application and use this application to identify file signatures

**Part 1 – Reading**

Read the selection “[An Introduction to Hex Editing for Cybercrime Investigators](https://roderickshawngraham.medium.com/an-introduction-to-hex-editing-for-cybercrime-investigators-15041a1f3911)” and answer the questions below.

1. **Convert this into hexadecimal notation: 1010 1011 1100 1101** (10 pts) The hexadecimal notation for the binary notation 1010 1011 1100 1101 is ABCD.
2. **Convert this into binary notation: 8DE0 3FF9** (10 pts) The binary notation for the hexadecimal 8DE0 is 1000 1101 1110 0000 and the binary notation for the hexadecimal 3FF9 is 0011 1111 1111 1001; together it is 1000 1101 1110 0000 0011 1111 1111 1001.
3. **Using Gary Kessler’s file signature database -** [**https://filesignatures.net/**](https://filesignatures.net/)**, what is a file signature for a Microsoft Office word document?** (5 pts) The file signature for a Microsoft Office word document is D0 CF 11 E0 A1 B1 1A E.
4. **What are the four uses of hex editing for cybercriminologists (as described in the reading)?** (10 pts) The four uses of hex editing for cybercriminologists is analyzing file signatures since cybercriminals will modify the extension of a file to conceal it , recovering erased files from a hard drive, finding records or timestamps of when something has transpired, and discovering malware in a file since hackers will unknowingly embed malicious code in specific areas in a file.
5. **Look up one of the computer investigator organizations mentioned in the text and describe it in a few sentences. Talk about what certificates or licenses they offer and how one goes about acquiring one.** (15 pts) International Society of Computer Forensic Examiners (ISFCE) is a private organization that focuses on offering computer forensics certification that is internationally acknowledged. Anybody can try to take the certification test; law enforcement and non-law enforcement forensic computer examiners will be able to take it. In order to take the test, the examiner must first submit a CCE application first and a notarized CCE Statement. Then, it will be evaluated by the application board who will inform the examiner on their eligibility to sit for this testing process.

**Part 2 – Practicing Hex Editing and Identifying File Signatures**

In this part of the activity, you will gain some experience working with a hex editor. We will be working with an online hex editor: [Free Online Hex Editor & Viewer](https://www.onlinehexeditor.com/).

Note: Sometimes you may have to refresh the application when moving between documents.

1. **What is the file signature for the file named “Sample 1”? Take a screenshot and circle the hex values like below:** (10 pts) The file signature for the file “Sample 1” is 89 50 4E 47 0D 0A 1A 0A.

|  |
| --- |
| Text  Description automatically generated |

1. **What is the file signature for the file named “Sample 2”? Take a screenshot and circle the hex values.** (10 pts) The file signature for the file name “Sample 2” is FF D8 FF E1.

|  |
| --- |
| Text  Description automatically generated |

1. **“Sample 3” is a Microsoft Office Word document. What is the SHA-256 checksum for this document (do you remember how to do it?).** (10 pts) The SHA-256 checksum for “Sample 3”, the Microsoft Office Word document is 0x99e890778f2f8398888bbea6c7184b674bd4c0cb5c01325f3d72a6aa02073879.
2. **Now open “Sample 3” in the hex editor and change 6 bytes between offsets 50 and 80. Take a screenshot and circle it.** (15 pts)

|  |
| --- |
| A screenshot of a computer  Description automatically generated with medium confidence |

1. **Now create your own PowerPoint file (or whatever presentation software is on your computer). Upload the file, and circle its file signature. Then check the database to make sure it matches, and circle that one as well.** (15 pts)

|  |
| --- |
| A screenshot of a computer  Description automatically generated with medium confidence |

|  |
| --- |
|  |