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" and answer the questions below.

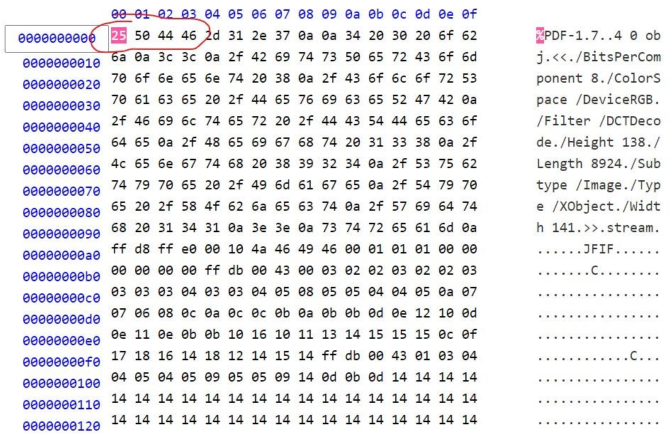
1. Convert this into hexadecimal notation: 1010 1011 1100 1101 (5 pts) ABCD
2. Convert this into binary notation: 8DE0 3FF9 (5 pts) 1000 1101 1110 0000 0011 1111 1111 1001
3. Using Gary Kessler's file signature database - https://filesignatures.net/, what is the file signature for a Microsoft Office document? (5 pts) D0 CF 11 E0 A1 B1 1A E1
4. What are the four uses of hex editing for cybercriminologists? (10 pts) Analyzing file signatures, recovering deleted files from a hard drive, identifying time stamps, and identifying malware that's embedded 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. (10 pts) The International Society of Forensic Computer Examiners (ISFCE) is an organization that tests for eligibility for a computer forensics certification at a reasonable cost. They conduct research and development into new and upcoming tech and methods for computer forensics. The organization gives a CCE cert (Certified Computer Examiner) that is available by submitting an CCE application and a notarized CCE statement via their application board to test for eligibility. The CCE cert is for those who wish to delve further into the field of computer forensics as well as test their knowledge and practicality on examination skills and abilities within digital forensics. It also sets high standards for the examiners at a fair and neutral process for the user's competency.

Part 2 – Practicing Hex Editing and Identifying File Signatures

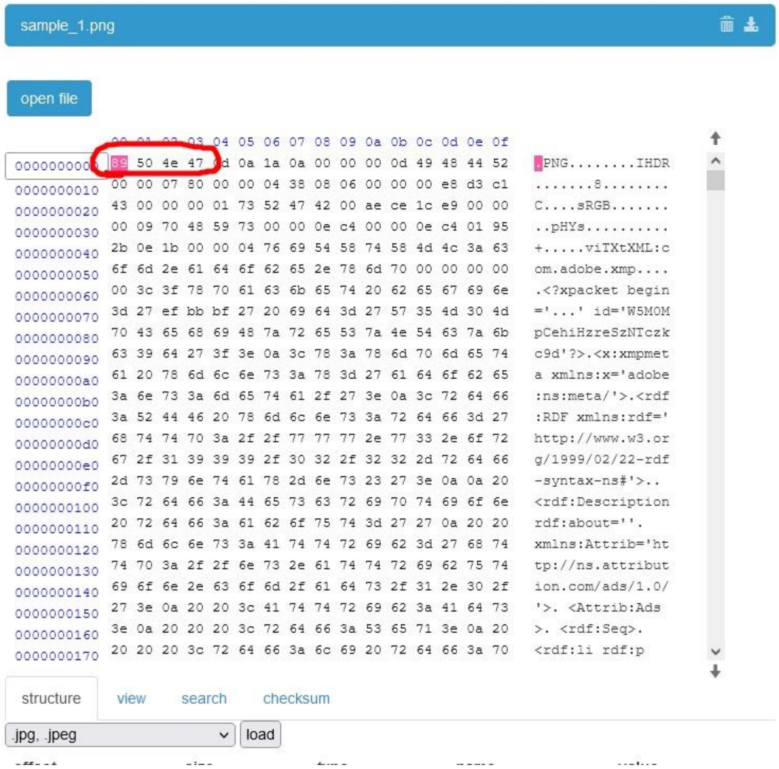
In this part of the activity, you will gain some experience working with a hex editor. We will be working with an online hex editor: Free Online Hex Editor & Viewer.

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

6. What is the file signature for the file named "**Sample 1**"? Take a screenshot and circle the hex values like below: (10 pts)

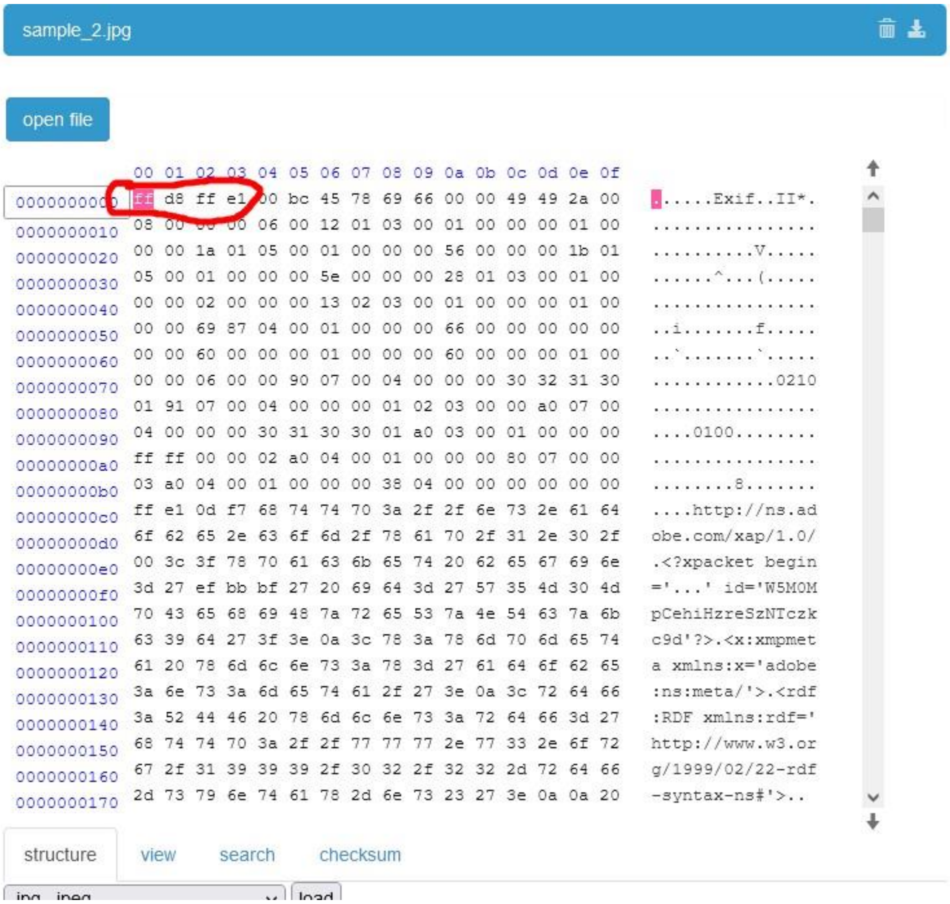


```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  25 50 44 46 2d 31 2e 37 0a 0a 34 20 30 20 6f 62    %PDF-1.7..4 0 ob
0000000010  6a 0a 3c 3c 0a 2f 42 69 74 73 50 65 72 43 6f 6d    j.<<./BitsPerCom
0000000020  70 6f 6e 65 6e 74 20 38 0a 2f 43 6f 6c 6f 72 53    ponent 8./ColorS
0000000030  70 61 63 65 20 2f 44 65 76 69 63 65 52 47 42 0a    pace /DeviceRGB.
0000000040  2f 46 69 6c 74 65 72 20 2f 44 43 54 44 65 63 6f    /Filter /DCTDeco
0000000050  64 65 0a 2f 48 65 69 67 68 74 20 31 33 38 0a 2f    de./Height 138./
0000000060  4c 65 6e 67 74 68 20 38 39 32 34 0a 2f 53 75 62    Length 8924./Sub
0000000070  74 79 70 65 20 2f 49 6d 61 67 65 0a 2f 54 79 70    type /Image./Typ
0000000080  65 20 2f 58 4f 62 6a 65 63 74 0a 2f 57 69 64 74    e /XObject./Widt
0000000090  68 20 31 34 31 0a 3e 3e 0a 73 74 72 65 61 6d 0a    h 141.>>.stream.
00000000a0  ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00    ......JFIF......
00000000b0  00 00 00 00 ff db 00 43 00 03 02 02 03 02 02 03    .......C........
00000000c0  03 03 03 04 03 03 04 05 08 05 05 04 04 05 0a 07    ................
00000000d0  07 06 08 0c 0a 0c 0c 0b 0a 0b 0b 0d 0e 12 10 0d    ................
00000000e0  0e 11 0e 0b 0b 10 16 10 11 13 14 15 15 15 0c 0f    ................
00000000f0  17 18 16 14 18 12 14 15 14 ff db 00 43 01 03 04    ...........C...
0000000100  04 05 04 05 09 05 05 09 14 0d 0b 0d 14 14 14 14    ................
0000000110  14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14    ................
0000000120  14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14    ................
```



```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52    .PNG........IHDR
0000000010  00 00 07 80 00 00 04 38 08 06 00 00 00 e8 d3 c1    .......8........
0000000020  43 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00    C....sRGB.......
0000000030  00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95    ..pHYs..........
0000000040  2b 0e 1b 00 00 04 76 69 54 58 74 58 4d 4c 3a 63    +.....viTXtXML:c
0000000050  6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00    om.adobe.xmp....
0000000060  00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e    .<?xpacket begin
0000000070  3d 27 ef bb bf 27 20 69 64 3d 27 57 35 4d 30 4d    ='...' id='W5M0M
0000000080  70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b    pCehiHzreSzNTczk
0000000090  63 39 64 27 3f 3e 0a 3c 78 3a 78 6d 70 6d 65 74    c9d'?>.<x:xmpmet
00000000a0  61 20 78 6d 6c 6e 73 3a 78 3d 27 61 64 6f 62 65    a xmlns:x='adobe
00000000b0  3a 6e 73 3a 6d 65 74 61 2f 27 3e 0a 3c 72 64 66    :ns:meta/'>.<rdf
00000000c0  3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 27    :RDF xmlns:rdf='
00000000d0  68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72    http://www.w3.or
00000000e0  67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66    g/1999/02/22-rdf
00000000f0  2d 73 79 6e 74 61 78 2d 6e 73 23 27 3e 0a 0a 20    -syntax-ns#'>..
0000000100  3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e    <rdf:Description
0000000110  20 72 64 66 3a 61 62 6f 75 74 3d 27 27 0a 20 20    rdf:about=''.
0000000120  78 6d 6c 6e 73 3a 41 74 74 72 69 62 3d 27 68 74    xmlns:Attrib='ht
0000000130  74 70 3a 2f 2f 6e 73 2e 61 74 74 72 69 62 75 74    tp://ns.attribut
0000000140  69 6f 6e 2e 63 6f 6d 2f 61 64 73 2f 31 2e 30 2f    ion.com/ads/1.0/
0000000150  27 3e 0a 20 20 3c 41 74 74 72 69 62 3a 41 64 73    '>. <Attrib:Ads
0000000160  3e 0a 20 20 20 3c 72 64 66 3a 53 65 71 3e 0a 20    >. <rdf:Seq>.
0000000170  20 20 20 3c 72 64 66 3a 6c 69 20 72 64 66 3a 70    <rdf:li rdf:p
```

7. What is the file signature for the file named "**Sample 2**"? Take a screenshot and circle the hex values.



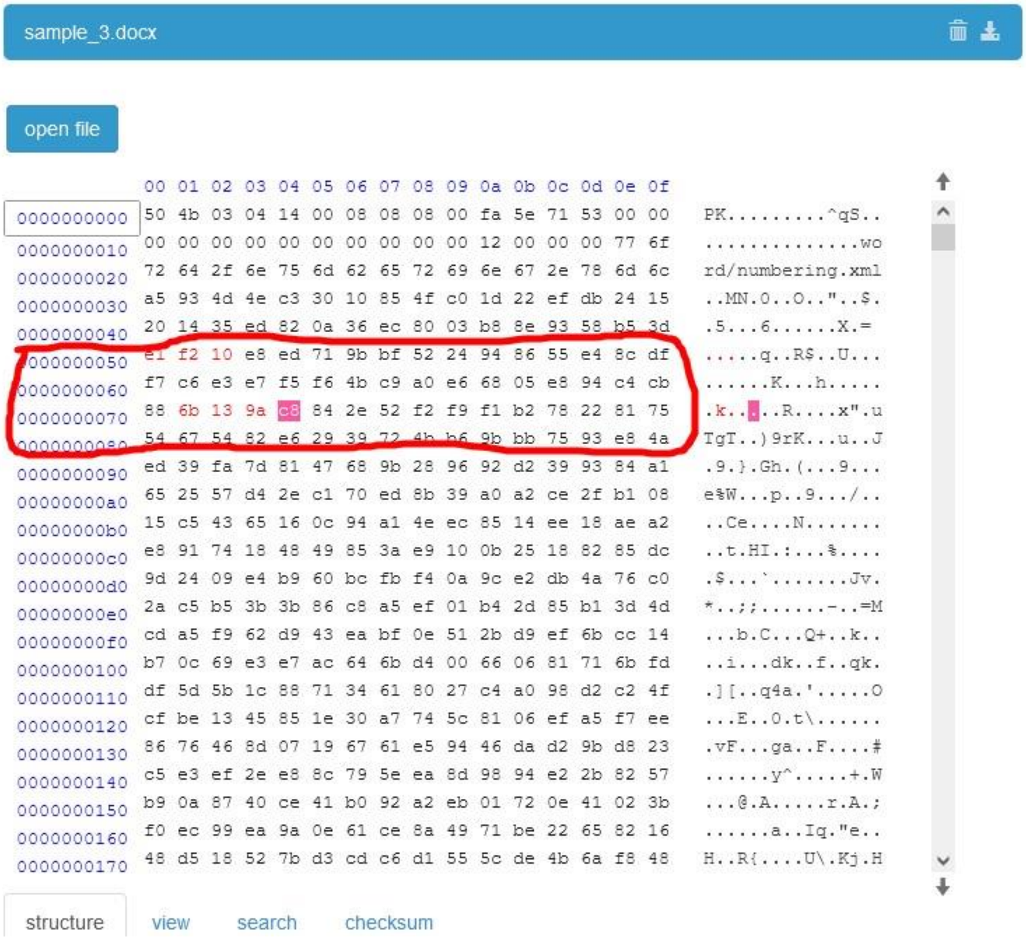
```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  ff d8 ff e1 00 bc 45 78 69 66 00 00 49 49 2a 00   ......Exif..II*.
0000000010  08 00 00 00 06 00 12 01 03 00 01 00 00 00 01 00   ................
0000000020  00 00 1a 01 05 00 01 00 00 00 56 00 00 00 1b 01   ..........V.....
0000000030  05 00 01 00 00 00 5e 00 00 00 28 01 03 00 01 00   ......^...(.....
0000000040  00 00 02 00 00 00 13 02 03 00 01 00 00 00 01 00   ................
0000000050  00 00 69 87 04 00 01 00 00 00 66 00 00 00 00 00   ..i.......f.....
0000000060  00 00 60 00 00 00 01 00 00 00 60 00 00 00 01 00   ..`.......`.....
0000000070  00 00 06 00 00 90 07 00 04 00 00 00 30 32 31 30   ............0210
0000000080  01 91 07 00 04 00 00 00 01 02 03 00 00 a0 07 00   ................
0000000090  04 00 00 00 30 31 30 30 01 a0 03 00 01 00 00 00   ....0100........
00000000a0  ff ff 00 00 02 a0 04 00 01 00 00 00 80 07 00 00   ................
00000000b0  03 a0 04 00 01 00 00 00 38 04 00 00 00 00 00 00   ........8.......
00000000c0  ff e1 0d f7 68 74 74 70 3a 2f 2f 6e 73 2e 61 64   ....http://ns.ad
00000000d0  6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f   obe.com/xap/1.0/
00000000e0  00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e   .<?xpacket begin
00000000f0  3d 27 ef bb bf 27 20 69 64 3d 27 57 35 4d 30 4d   ='...' id='W5M0M
0000000100  70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b   pCehiHzreSzNTczk
0000000110  63 39 64 27 3f 3e 0a 3c 78 3a 78 6d 70 6d 65 74   c9d'?>.<x:xmpmet
0000000120  61 20 78 6d 6c 6e 73 3a 78 3d 27 61 64 6f 62 65   a xmlns:x='adobe
0000000130  3a 6e 73 3a 6d 65 74 61 2f 27 3e 0a 3c 72 64 66   :ns:meta/'>.<rdf
0000000140  3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 27   :RDF xmlns:rdf='
0000000150  68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72   http://www.w3.or
0000000160  67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66   g/1999/02/22-rdf
0000000170  2d 73 79 6e 74 61 78 2d 6e 73 23 27 3e 0a 0a 20   -syntax-ns#'>..
```

(10 pts)

8. "**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)

   E69EBE3167BC95B0D4393DBB8B38F8E736698F7453702B914DB4D4DB0C2E1C2A

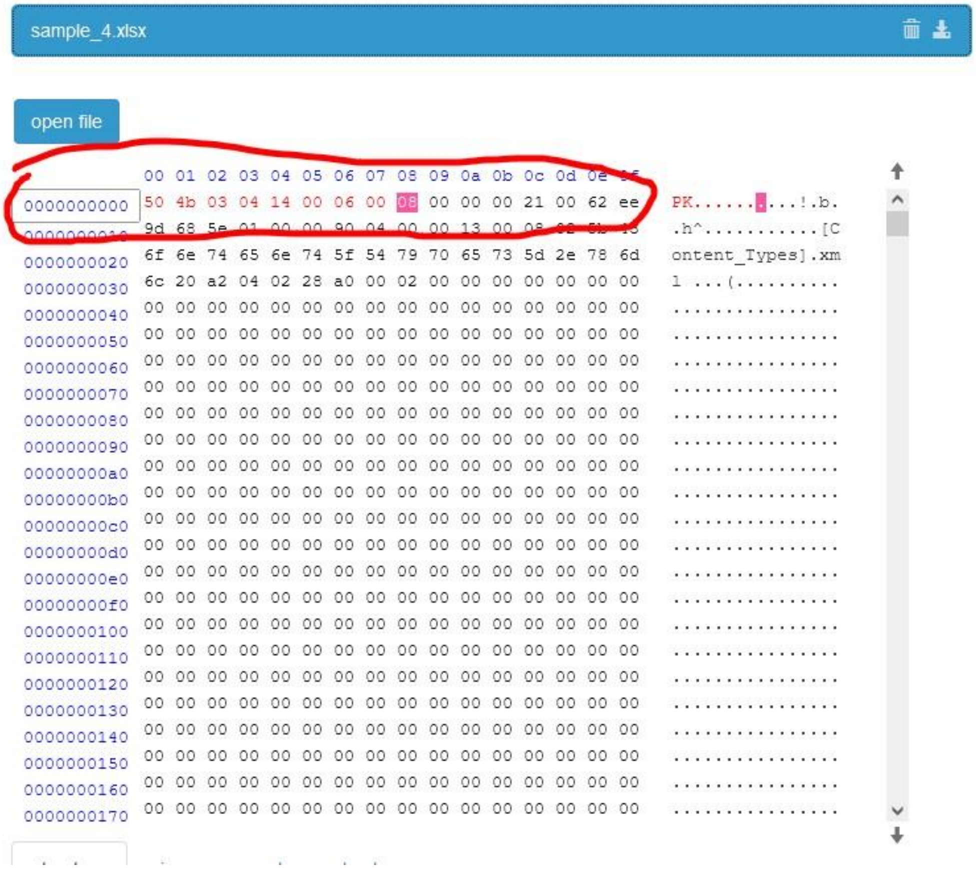
9. Now open "**Sample 3**" in the hex editor, and change 6 bytes between offsets 50 and 80. Take a screenshot and circle it. (10 pts)



```
           00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000 50 4b 03 04 14 00 08 08 08 00 fa 5e 71 53 00 00   PK.........^qS..
0000000010 00 00 00 00 00 00 00 00 00 00 12 00 00 00 77 6f   ..............wo
0000000020 72 64 2f 6e 75 6d 62 65 72 69 6e 67 2e 78 6d 6c   rd/numbering.xml
0000000030 a5 93 4d 4e c3 30 10 85 4f c0 1d 22 ef db 24 15   ..MN.0..O.."..$.
0000000040 20 14 35 ed 82 0a 36 ec 80 03 b8 8e 93 58 b5 3d   .5...6......X.=
0000000050 e1 f2 10 e8 ed 71 9b bf 52 24 94 86 55 e4 8c df   .....q..R$..U...
0000000060 f7 c6 e3 e7 f5 f6 4b c9 a0 e6 68 05 e8 94 c4 cb   ......K...h.....
0000000070 88 6b 13 9a c8 84 2e 52 f2 f9 f1 b2 78 22 81 75   .k.....R....x".u
0000000080 54 67 54 82 e6 29 39 72 4b b6 9b bb 75 93 e8 4a   TgT..)9rK...u..J
0000000090 ed 39 fa 7d 81 47 68 9b 28 96 92 d2 39 93 84 a1   .9.}.Gh.(...9...
00000000a0 65 25 57 d4 2e c1 70 ed 8b 39 a0 a2 ce 2f b1 08   e%W...p..9.../..
00000000b0 15 c5 43 65 16 0c 94 a1 4e ec 85 14 ee 18 ae a2   ..Ce....N.......
00000000c0 e8 91 74 18 48 49 85 3a e9 10 0b 25 18 82 85 dc   ..t.HI.:...%....
00000000d0 9d 24 09 e4 b9 60 bc fb f4 0a 9c e2 db 4a 76 c0   .$...`.......Jv.
00000000e0 2a c5 b5 3b 3b 86 c8 a5 ef 01 b4 2d 85 b1 3d 4d   *..;;......-..=M
00000000f0 cd a5 f9 62 d9 43 ea bf 0e 51 2b d9 ef 6b cc 14   ...b.C...Q+..k..
0000000100 b7 0c 69 e3 e7 ac 64 6b d4 00 66 06 81 71 6b fd   ..i...dk..f..qk.
0000000110 df 5d 5b 1c 88 71 34 61 80 27 c4 a0 98 d2 c2 4f   .][..q4a.'.....O
0000000120 cf be 13 45 85 1e 30 a7 74 5c 81 06 ef a5 f7 ee   ...E..0.t\......
0000000130 86 76 46 8d 07 19 67 61 e5 94 46 da d2 9b d8 23   .vF...ga..F....#
0000000140 c5 e3 ef 2e e8 8c 79 5e ea 8d 98 94 e2 2b 82 57   ......y^.....+.W
0000000150 b9 0a 87 40 ce 41 b0 92 a2 eb 01 72 0e 41 02 3b   ...@.A.....r.A.;
0000000160 f0 ec 99 ea 9a 0e 61 ce 8a 49 71 be 22 65 82 16   ......a..Iq."e..
0000000170 48 d5 18 52 7b d3 cd c6 d1 55 5c de 4b 6a f8 48   H..R{....U\.Kj.H
```

10. Save your edited "**Sample 3**", and then open the file. Does it look the same as the original or different and in what ways? How can this situation be exploited by hackers? (10 pts) It looks the same as the original. It can be exploited by adding bits of hex code to make the file malicious.

11. You have been given a copy of what looks like an excel file - "**Sample 4**" from your supervisor who has been working on a drug case. Your supervisor says he cannot open the file. This file is not in the Google lab folder but linked here via my Dropbox, and if that does not work, it is also in the Blackboard folder. You will have to download it from there before analyzing Can you fix this file so that your supervisor can open it? Describe how you did it, and show a screenshot of what you did. (15 pts) I used the file signature website given and searched up the signatures for an excel file. I tried the first one given and it wanted to repair it, so I tried the second one given and it opened without repair.



```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
0000000000  50 4b 03 04 14 00 06 00 08 00 00 00 21 00 62 ee   PK..........!.b.
0000000010  9d 68 5e 01 00 00 90 04 00 00 13 00 08 02 5b 43   .h^...........[C
0000000020  6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d   ontent_Types].xm
0000000030  6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00   l ...(..........
0000000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000000b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000000c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000000d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000000e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000000f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```