EX NO : 8 **Comparing file structures using a Hex editor**

a) Text editing tools such as Notepad, Wordpad, MS Word provide additional formatting information to text files. Create text files using these tools. Then use a Hex editor such as WinHex to view these files. What similarities and differences do you notice? How can you tell what type of file you are looking at by what WinHex shows in the Hex window?

Note: WinHex is a universal hexadecimal editor, particularly helpful in the realm of computer forensics. Download an evaluation copy of WinHex from https://www.x-ways.net/winhex/
WinHex is used to inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards.

b) NTFS hidden streams

NTFS streams allow us to store more than a single file under the same name. Create a folder dirtysecret. (If one already exists, remove all its contents.) In the dirtysecret folder we first create a file and then a stream.
c:\dirtysecret echo "This is a file" > file.txt
c:\dirtysecret echo "This is another file" > file.txt:hiddenstream.txt
Try now to find the second file using the DIR command. You cannot find it, but you can use it by employing tools such as Notepad:
c:\dirtysecret notepad file.txt:hiddenstream.txt
To discover an alternative data stream (ADS), we need to use tools such as Streams.exe from SysInternals
See https://docs.microsoft.com/en-us/sysinternals/downloads/streams
Getting rid of an ADS without destroying the original file is difficult. One can copy to a FAT file system, which would get rid of it or one can run the file through ftp. However, all of this becomes more tedious, if we associate an ADS to a directory. We can also connect the ADS to a file protected by Windows File Protection, which would make it nearly impossible to delete.
Include screenshots in your submission.

Aim :

To understand file structure using a Hex editor and to understand the working of NTFS hidden streams.

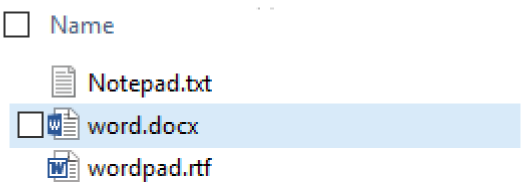
Algorithm / Procedure:

Use Hex editor such as WinHex to understand file structure. Follow the steps given above to see the functioning of NTFS hidden streams.

Sample Coding : Not applicable

Sample Output :

a) Created Files:



☐ Name

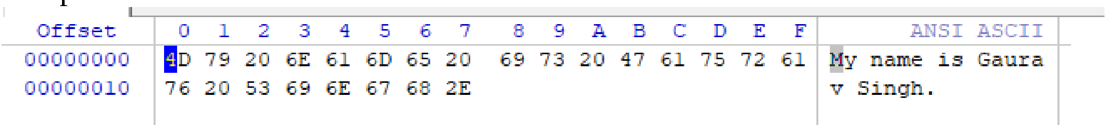
Notepad.txt

☐ word.docx

wordpad.rtf

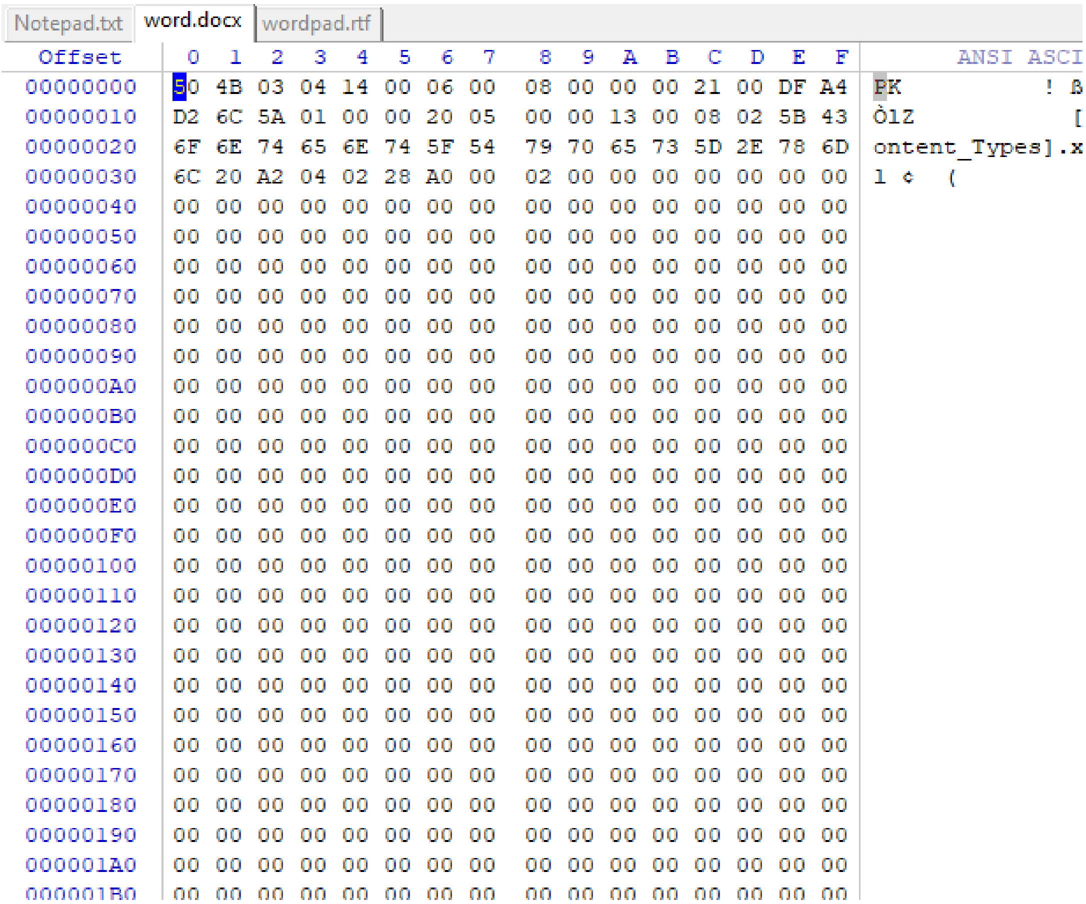
WinHex Screenshots:

Notepad:



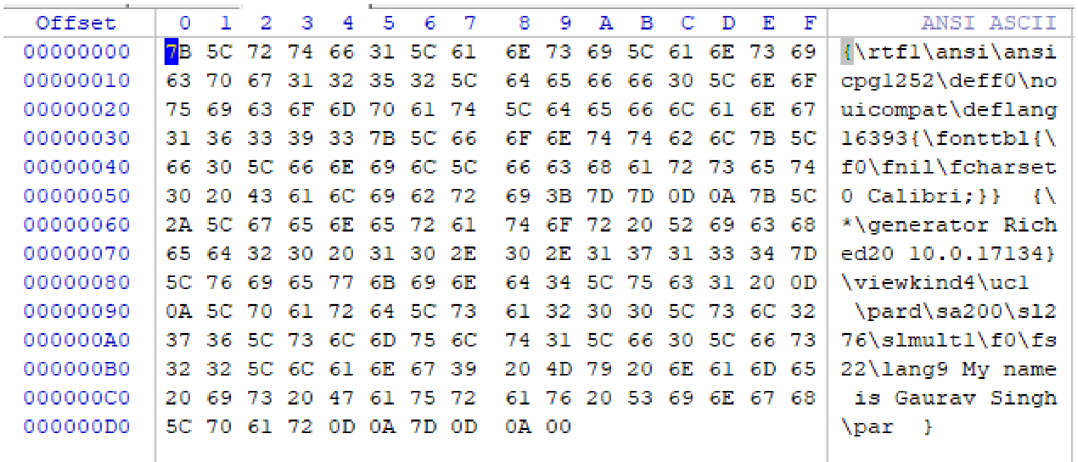
```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F      ANSI ASCII
00000000  4D 79 20 6E 61 6D 65 20  69 73 20 47 61 75 72 61   My name is Gaura
00000010  76 20 53 69 6E 67 68 2E                            v Singh.
```

Word:



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F      ANSI ASCI
00000000  50 4B 03 04 14 00 06 00  08 00 00 00 21 00 DF A4   PK          ! ß
00000010  D2 6C 5A 01 00 00 20 05  00 00 13 00 08 02 5B 43   ÒlZ           [
00000020  6F 6E 74 65 6E 74 5F 54  79 70 65 73 5D 2E 78 6D   ontent_Types].x
00000030  6C 20 A2 04 02 28 A0 00  02 00 00 00 00 00 00 00   l ¢  (
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Wordpad:



```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000   7B 5C 72 74 66 31 5C 61  6E 73 69 5C 61 6E 73 69  {\rtf1\ansi\ansi
00000010   63 70 67 31 32 35 32 5C  64 65 66 66 30 5C 6E 6F  cpg1252\deff0\no
00000020   75 69 63 6F 6D 70 61 74  5C 64 65 66 6C 61 6E 67  uicompat\deflang
00000030   31 36 33 39 33 7B 5C 66  6F 6E 74 74 62 6C 7B 5C  16393{\fonttbl{\
00000040   66 30 5C 66 6E 69 6C 5C  66 63 68 61 72 73 65 74  f0\fnil\fcharset
00000050   30 20 43 61 6C 69 62 72  69 3B 7D 7D 0D 0A 7B 5C  0 Calibri;}}  {\
00000060   2A 5C 67 65 6E 65 72 61  74 6F 72 20 52 69 63 68  *\generator Rich
00000070   65 64 32 30 20 31 30 2E  30 2E 31 37 31 33 34 7D  ed20 10.0.17134}
00000080   5C 76 69 65 77 6B 69 6E  64 34 5C 75 63 31 20 0D  \viewkind4\uc1 
00000090   0A 5C 70 61 72 64 5C 73  61 32 30 30 5C 73 6C 32   \pard\sa200\sl2
000000A0   37 36 5C 73 6C 6D 75 6C  74 31 5C 66 30 5C 66 73  76\slmult1\f0\fs
000000B0   32 32 5C 6C 61 6E 67 39  20 4D 79 20 6E 61 6D 65  22\lang9 My name
000000C0   20 69 73 20 47 61 75 72  61 76 20 53 69 6E 67 68   is Gaurav Singh
000000D0   5C 70 61 72 0D 0A 7D 0D  0A 00                    \par  }
```

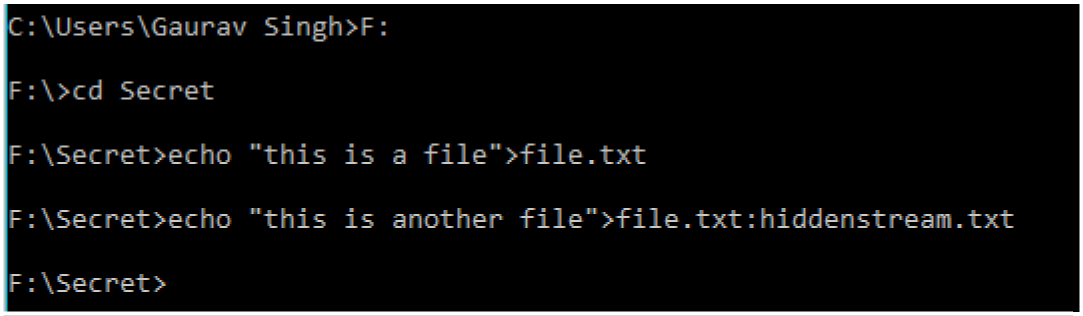
Difference:

Here we can see that in case of notepad the data is only restricted to the text present in the document. In case of notepad the data contained in the document is only the text.

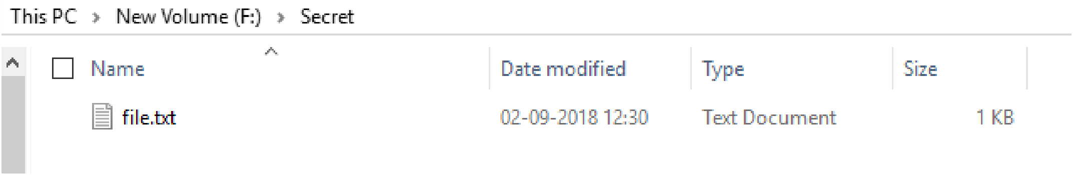
In case of Microsoft Word the data is not restricted to the text, even if text is not there the data displays 00 for the empty space and we can see that the text displayed is in the coded form.

In case of word pad the text is displayed in the form of a code which has all the data about the font type, font size and all the other properties of the text.

b) **Created file:**



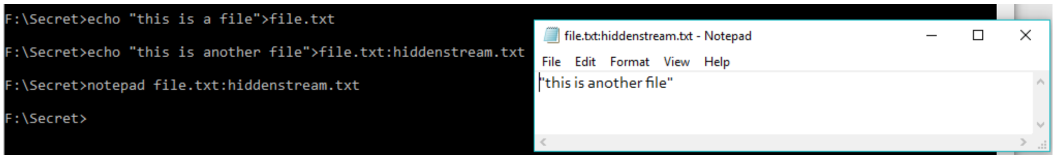
```
C:\Users\Gaurav Singh>F:

F:\>cd Secret

F:\Secret>echo "this is a file">file.txt

F:\Secret>echo "this is another file">file.txt:hiddenstream.txt

F:\Secret>
```



This PC › New Volume (F:) › Secret

Name	Date modified	Type	Size
file.txt	02-09-2018 12:30	Text Document	1 KB

We can clearly see that the hidden file is not visible.



```
F:\Secret>echo "this is a file">file.txt

F:\Secret>echo "this is another file">file.txt:hiddenstream.txt

F:\Secret>notepad file.txt:hiddenstream.txt

F:\Secret>
```

file.txt:hiddenstream.txt - Notepad
File Edit Format View Help

"this is another file"

We can see that on executing through the command prompt we can open the hidden file.