DIGITAL FORENSICS LAB

Exercise 7	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulagara
Date	28th September, 2021

AIM

Comparing file structures with Hex editors.

PART A

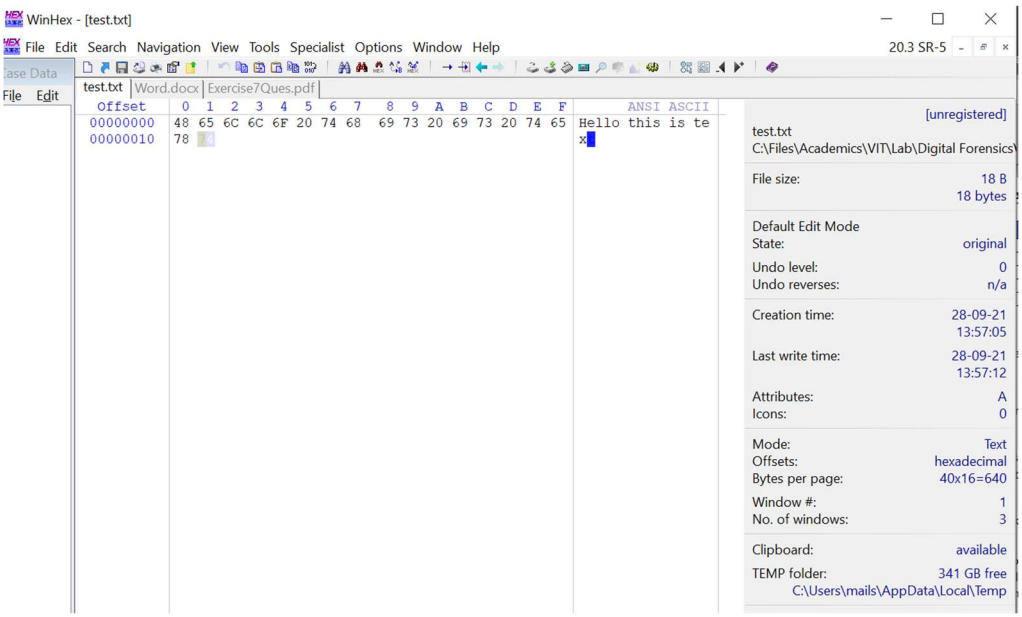
A few commands are executed and their outputs are shown below.

Q1

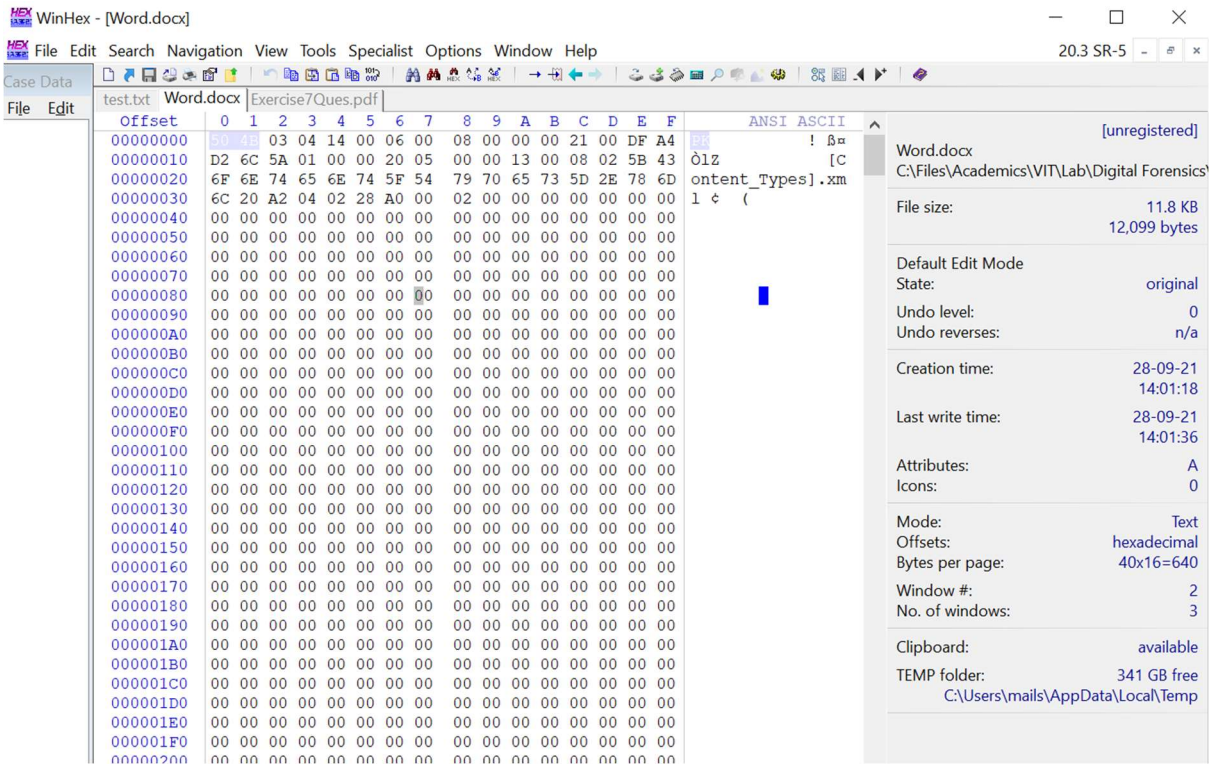
Create text files using these tools. Then use a Hex editor such as vim or WinHex to view these files. What similarities and differences do you notice?

A

To open a file using WinHex, click 'File'->'open'. Then browse for the file and open it. For this question, two forms of text files (one using Notepad and the other using MS Word) were created and a PDF file was also used. When opened in WinHex, the following was displayed on the window.



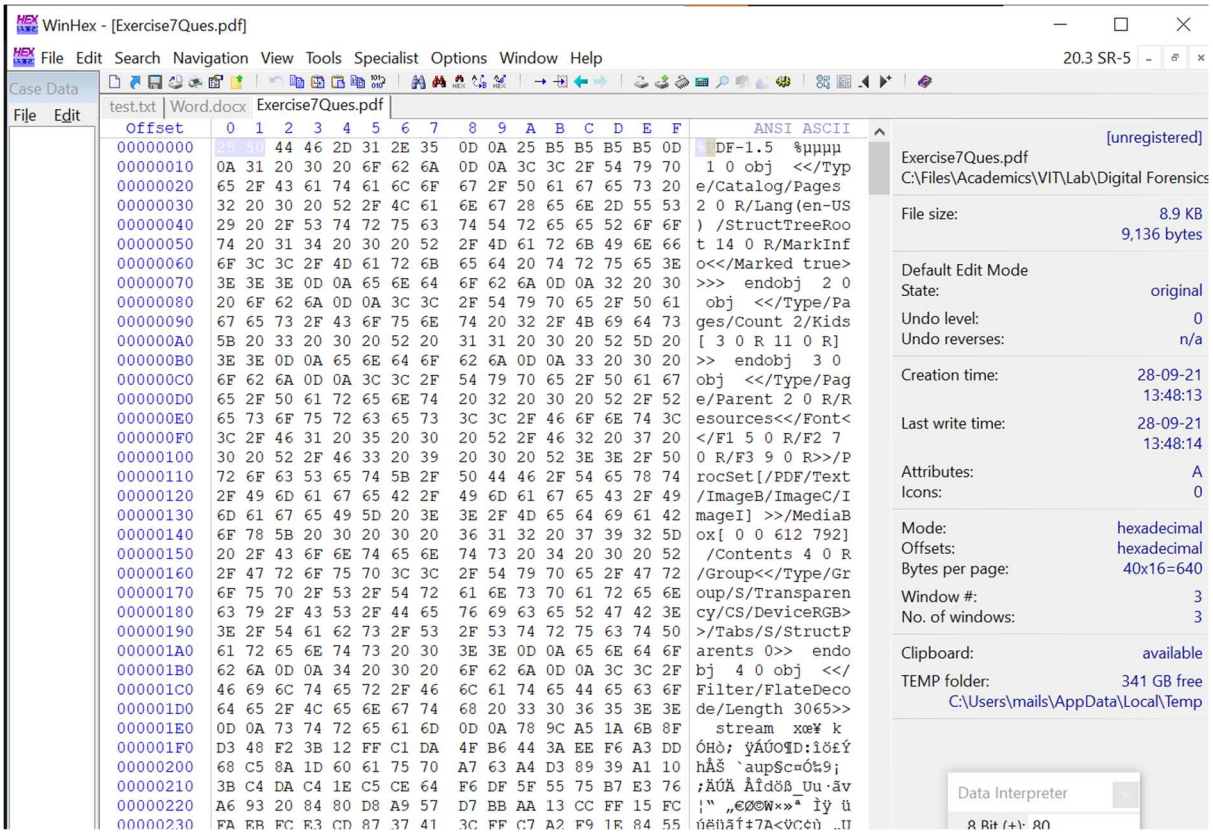
Made using notepad: test.txt



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
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           [C
00000020  6F 6E 74 65 6E 74 5F 54  79 70 65 73 5D 2E 78 6D  ontent_Types].xm
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
000001C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

[unregistered]
Word.docx
C:\Files\Academics\VIT\Lab\Digital Forensics\
File size: 11.8 KB 12,099 bytes
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 28-09-21 14:01:18
Last write time: 28-09-21 14:01:36
Attributes: A
Icons: 0
Mode: Text
Offsets: hexadecimal
Bytes per page: 40x16=640
Window #: 2
No. of windows: 3
Clipboard: available
TEMP folder: 341 GB free C:\Users\mails\AppData\Local\Temp

Made using MS Word: Word.docx



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  25 50 44 46 2D 31 2E 35  0D 0A 25 B5 B5 B5 B5 0D  %PDF-1.5  %µµµµ
00000010  0A 31 20 30 20 6F 62 6A  0D 0A 3C 3C 2F 54 79 70   1 0 obj  <</Typ
00000020  65 2F 43 61 74 61 6C 6F  67 2F 50 61 67 65 73 20  e/Catalog/Pages
00000030  32 20 30 20 52 2F 4C 61  6E 67 28 65 6E 2D 55 53  2 0 R/Lang(en-US
00000040  29 20 2F 53 74 72 75 63  74 54 72 65 65 52 6F 6F  ) /StructTreeRoo
00000050  74 20 31 34 20 30 20 52  2F 4D 61 72 6B 49 6E 66  t 14 0 R/MarkInf
00000060  6F 3C 3C 2F 4D 61 72 6B  65 64 20 74 72 75 65 3E  o<</Marked true>
00000070  3E 3E 3E 0D 0A 65 6E 64  6F 62 6A 0D 0A 32 20 30  >>>  endobj  2 0
00000080  20 6F 62 6A 0D 0A 3C 3C  2F 54 79 70 65 2F 50 61   obj  <</Type/Pa
00000090  67 65 73 2F 43 6F 75 6E  74 20 32 2F 4B 69 64 73  ges/Count 2/Kids
000000A0  5B 20 33 20 30 20 52 20  31 31 20 30 20 52 5D 20  [ 3 0 R 11 0 R]
000000B0  3E 3E 0D 0A 65 6E 64 6F  62 6A 0D 0A 33 20 30 20  >>  endobj  3 0
000000C0  6F 62 6A 0D 0A 3C 3C 2F  54 79 70 65 2F 50 61 67  obj  <</Type/Pag
000000D0  65 2F 50 61 72 65 6E 74  20 32 20 30 20 52 2F 52  e/Parent 2 0 R/R
000000E0  65 73 6F 75 72 63 65 73  3C 3C 2F 46 6F 6E 74 3C  esources<</Font<
000000F0  3C 2F 46 31 20 35 20 30  20 52 2F 46 32 20 37 20  </F1 5 0 R/F2 7
00000100  30 20 52 2F 46 33 20 39  20 30 20 52 3E 3E 2F 50  0 R/F3 9 0 R>>/P
00000110  72 6F 63 53 65 74 5B 2F  50 44 46 2F 54 65 78 74  rocSet[/PDF/Text
00000120  2F 49 6D 61 67 65 42 2F  49 6D 61 67 65 43 2F 49  /ImageB/ImageC/I
00000130  6D 61 67 65 49 5D 20 3E  3E 2F 4D 65 64 69 61 42  mageI] >>/MediaB
00000140  6F 78 5B 20 30 20 30 20  36 31 32 20 37 39 32 5D  ox[ 0 0 612 792]
00000150  20 2F 43 6F 6E 74 65 6E  74 73 20 34 20 30 20 52   /Contents 4 0 R
00000160  2F 47 72 6F 75 70 3C 3C  2F 54 79 70 65 2F 47 72  /Group<</Type/Gr
00000170  6F 75 70 2F 53 2F 54 72  61 6E 73 70 61 72 65 6E  oup/S/Transparen
00000180  63 79 2F 43 53 2F 44 65  76 69 63 65 52 47 42 3E  cy/CS/DeviceRGB>
00000190  3E 2F 54 61 62 73 2F 53  2F 53 74 72 75 63 74 50  >/Tabs/S/StructP
000001A0  61 72 65 6E 74 73 20 30  3E 3E 0D 0A 65 6E 64 6F  arents 0>>  endo
000001B0  62 6A 0D 0A 34 20 30 20  6F 62 6A 0D 0A 3C 3C 2F  bj  4 0 obj  <</
000001C0  46 69 6C 74 65 72 2F 46  6C 61 74 65 44 65 63 6F  Filter/FlateDeco
000001D0  64 65 2F 4C 65 6E 67 74  68 20 33 30 36 35 3E 3E  de/Length 3065>>
000001E0  0D 0A 73 74 72 65 61 6D  0D 0A 78 9C A5 1A 6B 8F    stream  xœ¥ k
000001F0  D3 48 F2 3B 12 FF C1 DA  4F B6 44 3A EE F6 A3 DD  ÓHò; ÿÁÚO¶D:îö£Ý
00000200  68 C5 8A 1D 60 61 75 70  A7 63 A4 D3 89 39 A1 10  hÅŠ `aup§c¤Ó‰9¡
00000210  3B C4 DA C4 1E C5 CE 64  F6 DF 5F 55 75 B7 E3 76  ;ÄÚÄ ÅÎdöß_Uu·ãv
00000220  A6 93 20 84 80 D8 A9 57  D7 BB AA 13 CC FF 15 FC  ¦" „€Ø©W×»ª Ìÿ ü
00000230  FA EB FC E3 CD 87 37 41  3C FF C7 A2 F9 1E 84 55  úëüãÍ‡7A<ÿÇ¢ù „U
```

[unregistered]
Exercise7Ques.pdf
C:\Files\Academics\VIT\Lab\Digital Forensics
File size: 8.9 KB 9,136 bytes
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 28-09-21 13:48:13
Last write time: 28-09-21 13:48:14
Attributes: A
Icons: 0
Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 40x16=640
Window #: 3
No. of windows: 3
Clipboard: available
TEMP folder: 341 GB free C:\Users\mails\AppData\Local\Temp
8 Bit (+): 80

A PDF file: Exercise7Ques.pdf

The following observations are made which tell us the differences observed among the files when viewed using WinHex:

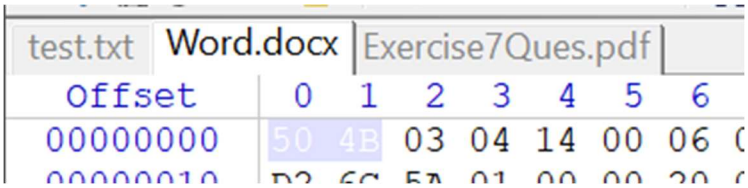
- The windows of each file show us the offset, the content, hexadecimal equivalent of the content and the ANSI ASCII form.
- For text file, the window is simple. We see the contents of test.txt directly on the window and its Hexadecimal equivalent.
- For word files, it is a bit more complicated. We do not see the text content of the docx file, rather, we see the XML files associated with the docx file.
- The same is the case for PDF. Unlike the txt file, we see the formatting used for the content within the PDF.

Q2

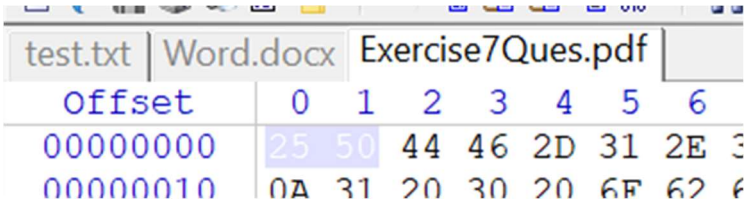
How can you tell what type of file you are looking at by what vim or WinHex shows in the Hex window?

A

We can verify the file type by looking at the first few hexadecimal characters as highlighted below.



DOCX File



PDF File

These few characters tell us what file we are working with.

’50 4B’ represents zip file format and formats based on it, such as DOCX, EPUB, JAR, ODF, OOXML etc.

’25 50 44 46 2D’ is the signature for PDF files.

PART B

Working with NTFS hidden streams.

Q1

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

A

NTFS file streams or Alternate Data Streams (ADS) can provide attackers with a method of hiding hacker tools on a system and allowthem to execute withour being detected.

A new folder called 'secret' is created and is kept empty as shown.

```
C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>dir
 Volume in drive C is OS
 Volume Serial Number is 8239-227E

 Directory of C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret

03-Oct-21  01:45 PM    <DIR>          .
03-Oct-21  01:45 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  363,980,099,584 bytes free

C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>
```

The, we create a text file with some content.

```
C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>echo "Hello your compooter has virus">file.txt

C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>dir
 Volume in drive C is OS
 Volume Serial Number is 8239-227E

 Directory of C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret

03-Oct-21  01:48 PM    <DIR>          .
03-Oct-21  01:48 PM    <DIR>          ..
03-Oct-21  01:48 PM                34 file.txt
               1 File(s)             34 bytes
               2 Dir(s)  363,952,926,720 bytes free

C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>
```

Then, we create a stream with another file.

```
C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>echo "This IS the VIRUS" > file.txt:hiddenstream.txt

C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>dir
 Volume in drive C is OS
 Volume Serial Number is 8239-227E

 Directory of C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret

03-Oct-21  01:48 PM    <DIR>          .
03-Oct-21  01:48 PM    <DIR>          ..
03-Oct-21  01:49 PM                34 file.txt
               1 File(s)             34 bytes
               2 Dir(s)  363,951,337,472 bytes free

C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>
```

But we see that the second file is not listed by the 'dir' command. We can open it with the notepad however.

```
C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>notepad file.txt:hiddenstream.txt
```

file.txt:hiddenstream.txt - Notepad

File Edit Format View Help

"This IS the VIRUS"

What is happening here is that we have stored data behind a filename (file.txt) with the help of a stream name (hiddenstream.txt). The name after the colon (:) is the hidden stream name. We can discover it only through the terminal.

We can detect hidden streams using the command *'dir /R'*.

```
C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>dir /R
 Volume in drive C is OS
 Volume Serial Number is 8239-227E

 Directory of C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret

03-Oct-21  01:48 PM    <DIR>          .
03-Oct-21  01:48 PM    <DIR>          ..
03-Oct-21  02:06 PM                34 file.txt
                                    6 file.txt:hola.txt:$DATA
               1 File(s)             34 bytes
               2 Dir(s)  366,605,524,992 bytes free

C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>
```

But there are command line applications too like 'streams' which we can use to detect files that have streams and their names.

```
C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>streams file.txt

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret\file.txt:
   :hiddenstream.txt:$DATA      22

C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>
```

In the screenshot above, we see that '*streams <filename>*' shows the names of streams associated with the filename given (here, file.txt). The hidden stream *'hiddenstream.txt'* is listed.

We can also delete all streams using the *'d'* parameter as follows. We can't, however, delete a single specific stream.

```
C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>streams -d file.txt

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret\file.txt:
   Deleted :hiddenstream.txt:$DATA

C:\Files\Academics\VIT\Lab\Digital Forensics\Lab8\secret>
```

CONCLUSION

We have worked with WinHex, a hex editor, to view contents of files byte by byte and analyse them. We also explored how hidden streams can be made and store files in them.

DIGITAL FORENSICS LAB

Exercise 8	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulagara
Date	5th September, 2021

AIM

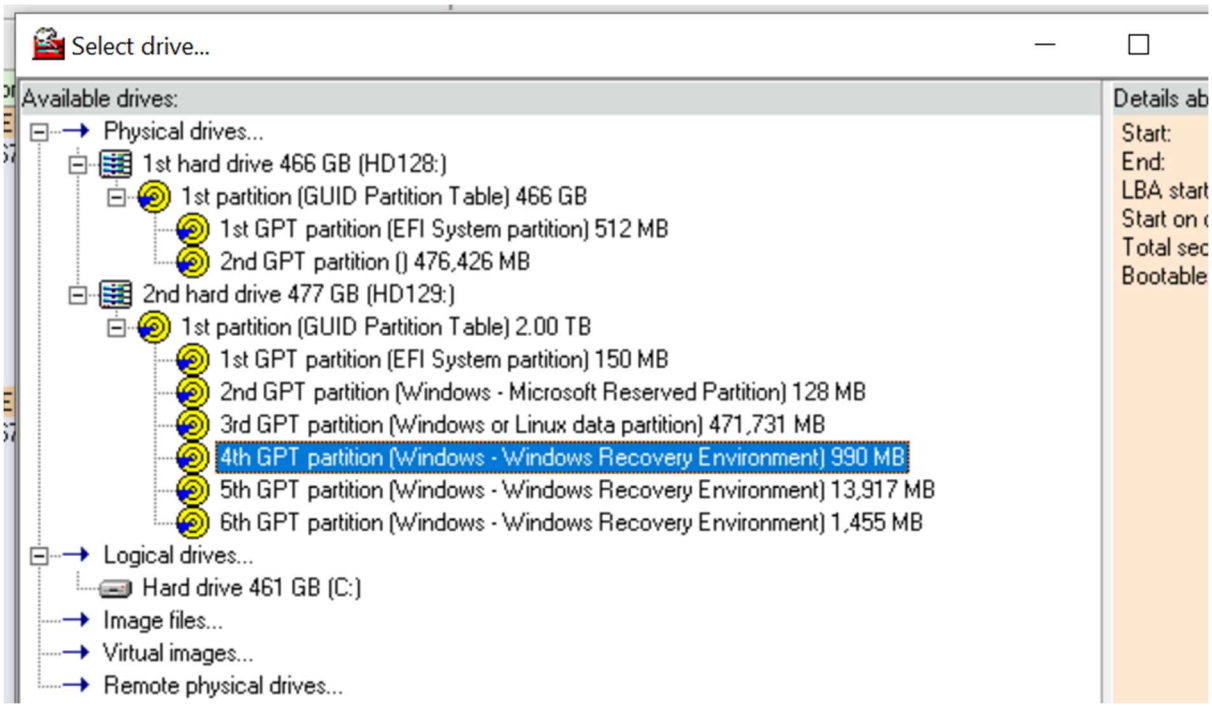
Working with DiskExplorer exploring disks and their file entries, partition table etc.

Q1

Navigate your NTFS drive by jumping to the partition table, boot record, Master file table or the root directory.

A

We select a drive first.



Partition table:

Runtime's DiskExplorer for NTFS

File Goto Link Edit View Tools Help

Sector	Partition table										
x399E5000	Valid Partition Table										
966,676,480	Entry			Starting			Ending			Relative	Total
	No	System	Boot	Cylinder	Head	Sector	Cylinder	Head	Sector	Start Sector	Sectors
	1	Unknown	No	x050	x0D	x0A	x173	x65	x33	x72744320	x6C412B6C
				80	13	10	371	101	51	1920221984	1816210284
	2	Unknown	???	x165	x2B	x04	x16F	x20	x34	x73657220	x74726174
				357	43	4	367	32	52	1936028192	1953653108
	3	Free	???	x000	x0A	x00	x000	x00	x00	x00000000	x00000000
				0	10	0	0	0	0	0	0
	4	Free	No	x000	x00	x00	x000	x00	x00	x01A7018A	x000001BF
				0	0	0	0	0	0	27722122	447

Boot Record:

Runtime's DiskExplorer for NTFS

File Goto Link Edit View Tools Help

Sector	Boot sector (NTFS)					
x399E5000	Valid Boot Sector					
966,676,480	NTFS Signature:	NTFS		Physical drive #:	x80	128
	Bytes per sector:	x0200	512	Sectors in volume:	x0000001EEFFF	2027519
	Sectors per cluster:	x08	8	1st MFT cluster:	x00014A00	84480
	Media descriptor:	xF8	248	1st MFT mirror cluster:	x00000002	2
	Sectors per FAT:	x0000	0	Clusters/file record:	x000000F6	246
	Sectors per track:	x003F	63	Clusters/index block:	x00000001	1
	Heads:	x00FF	255	Volume serial number:	x6C6C1285	1819021957
	Hidden sectors:	x0000399E5000	966676480			
x399E5001	Invalid Boot Sector					
966,676,481	NTFS Signature:	O O T M		Physical drive #:	x00	0
	Bytes per sector:	x4700	18176	Sectors in volume:	x000000000000	0
	Sectors per cluster:	x00	0	1st MFT cluster:	x00000000	0
	Media descriptor:	x00	0	1st MFT mirror cluster:	x00000000	0
	Sectors per FAT:	x0033	51	Clusters/file record:	x00000000	0
	Sectors per track:	x0030	48	Clusters/index block:	x00000000	0
	Heads:	xD400	54272	Volume serial number:	x00000000	0
	Hidden sectors:	x1000240000000	603979776			

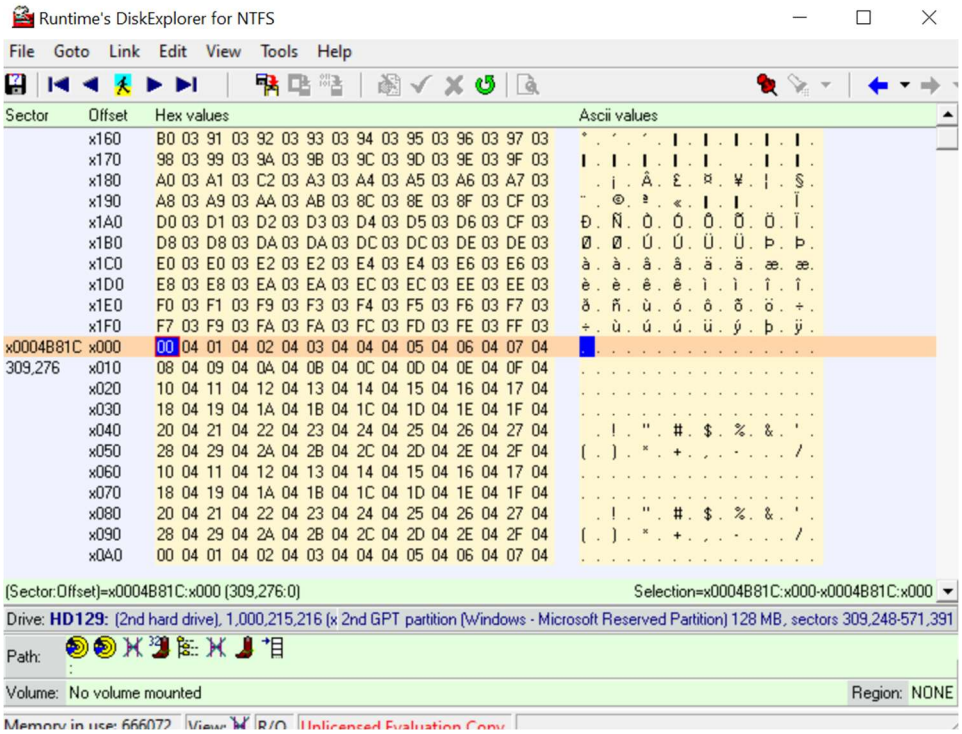
INVALID

Q2

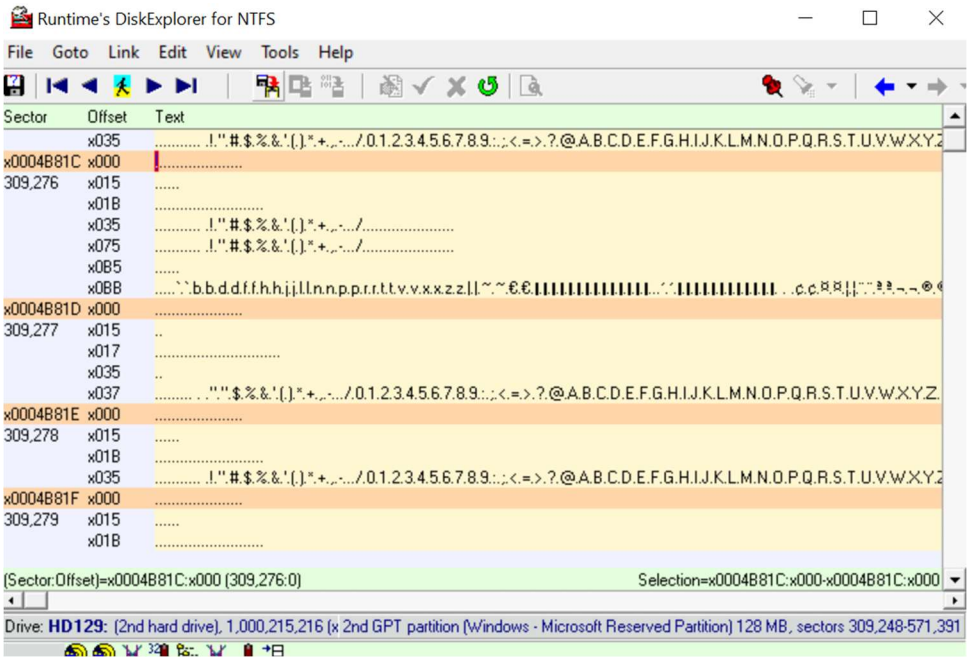
Choose between views such as hex, text, index allocation, MFT, boot record, partition table.

A

Hex View:



Text View:



MFT:

Runtime's DiskExplorer for NTFS

File Goto Link Edit View Tools Help

Sector	Name	Type	Attributes	Size	Date	1st cluster	NT Attributes
x0004B80E	Invalid MFT entry						
309,262							
x0004B810	**$MFT**	FILE	__sh__	262144	25-Jul-20 7:13:35 AM	x040000	10 30 80 B0
309,264	No: ???[x1] (x0), Parent directory: x5[x5], Run: 31:40 00 00 04						
x0004B812	**$MFTMirr**	FILE	__sh__	4096	25-Jul-20 7:13:35 AM	x000002	10 30 80
309,266	No: ???[x1] (x1), Parent directory: x5[x5], Run: 11:01 02						
x0004B814	**$LogFile**	FILE	__sh__	6356992	25-Jul-20 7:13:35 AM	x03F9DF	10 30 80
309,268	No: ???[x2] (x2), Parent directory: x5[x5], Run: 32:10 06 DF F9 03						
x0004B816	**$Volume**	FILE	__sh__	0	25-Jul-20 7:13:35 AM	Resident	10 30 60 70 80
309,270	No: ???[x3] (x3), Parent directory: x5[x5], Run: Resident						
x0004B818	Invalid MFT entry						

Boot record:

Runtime's DiskExplorer for NTFS

File Goto Link Edit View Tools Help

Sector	Boot sector (NTFS)					
x0004B810	Invalid Boot Sector					
309,264	NTFS Signature:	E0 Q		Physical drive #:	x00	0
	Bytes per sector:	x0000	0	Sectors in volume:	x000000000007	7
	Sectors per cluster:	x00	0	1st MFT cluster:	x00000002	2
	Media descriptor:	x00	0	1st MFT mirror cluster:	x00000010	16
	Sectors per FAT:	x0001	1	Clusters/file record:	x00180000	1572864
	Sectors per track:	x01A0	416	Clusters/index block:	x00000000	0
	Heads:	x0000	0	Volume serial number:	x00000048	72
	Hidden sectors:	x0000000000400	1024			
x0004B811	Invalid Boot Sector					
309,265	NTFS Signature:	ÿ		Physical drive #:	x00	0
	Bytes per sector:	x0000	0	Sectors in volume:	x000000000000	0
	Sectors per cluster:	x00	0	1st MFT cluster:	x00000000	0
	Media descriptor:	x00	0	1st MFT mirror cluster:	x00000000	0
	Sectors per FAT:	x0000	0	Clusters/file record:	x00000000	0
	Sectors per track:	x0000	0	Clusters/index block:	x00000000	0

Partition table:

Runtime's DiskExplorer for NTFS

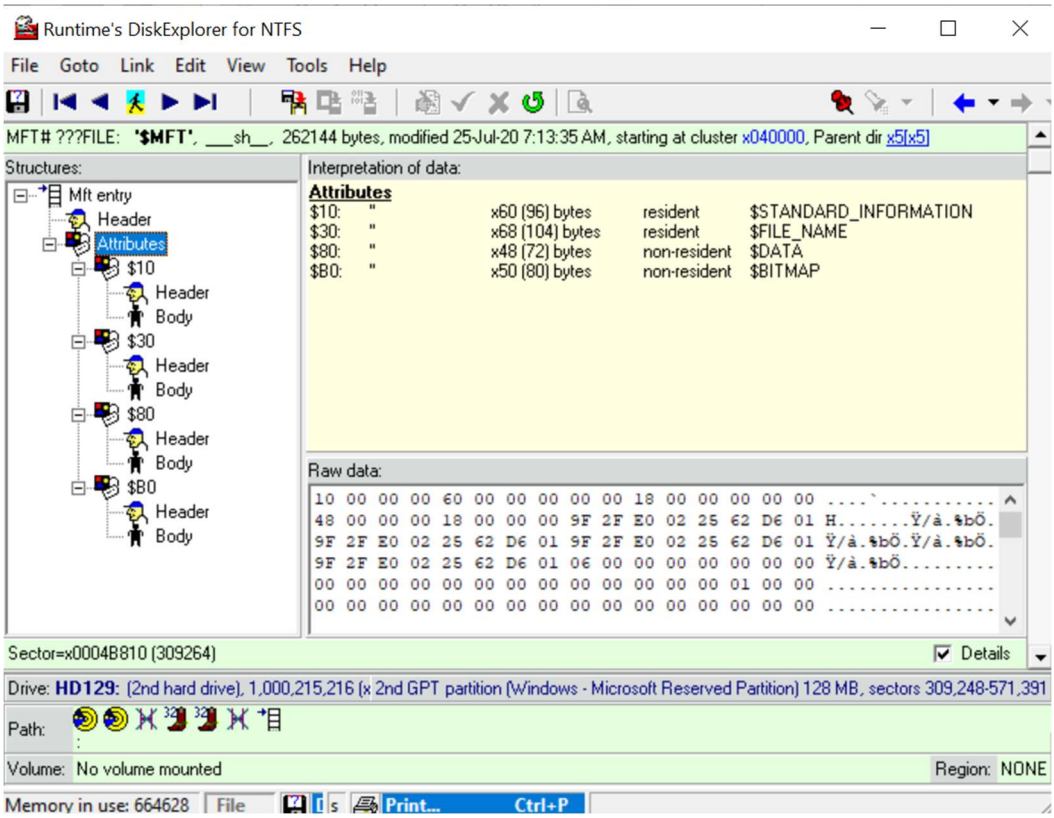
File Goto Link Edit View Tools Help

Sector	Partition table										
x0004B810	Invalid Partition Table										
309,264	Entry No	System	Boot	Starting Cylinder	Starting Head	Starting Sector	Ending Cylinder	Ending Head	Ending Sector	Relative Start Sector	Total Sectors
	1	Free	???	x000	x00	x00	x000	x00	x00	x00010000	x00000000
				0	0	0	0	0	0	65536	0
	2	Free	No	x100	x00	x00	x000	x00	x00	x20000000	x00000000
				256	0	0	0	0	0	536870912	0
	3	Free	No	x010	x00	x08	x000	x00	x00	x10080000	x00000000
				16	0	8	0	0	0	268959744	0
	4	Xenix Bad Block Table	No	x001	x00	x31	x031	xFF	x03	x00C80101	x00000000
				1	0	49	49	255	3	13107457	0

Q3

Inspect the file entry details, NT attributes etc.

A



OBSERVATIONS

DiskExplorer is a low-level disk editor which we use to view and manipulate information at a sector level. It is also used for data recovery from drives. As seen in screenshots above, se can see what each sector of a drive holds. This is used in Digital Forensics so as to get an idea of the suspect drive and its contents. We can see the partition table

CONCLUSION

We have worked with DiskExplorer and discovered its capability and functionalities. The tool is powerful enough to interact with the disk on a sector level and recover data.