**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**

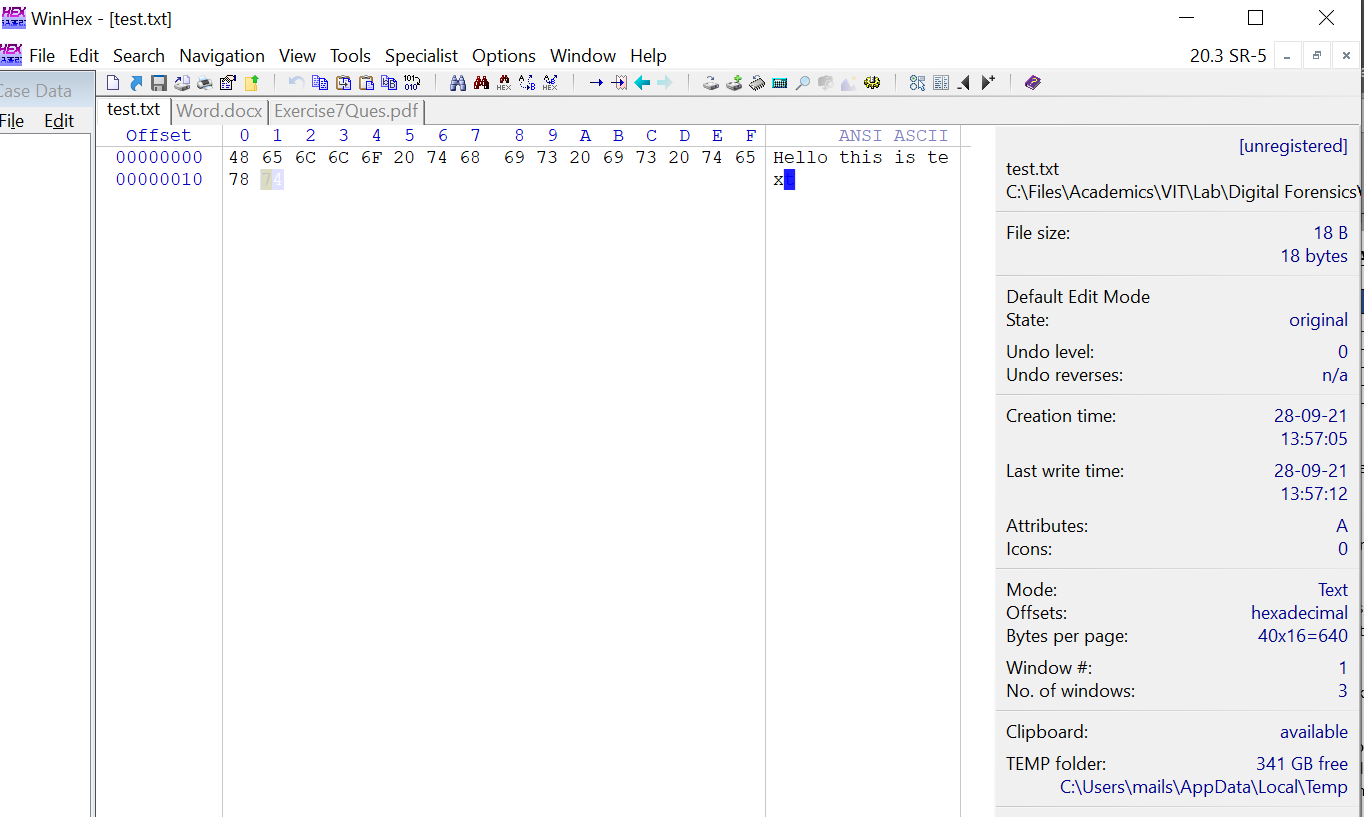
A few commands are executed and their outputs are shown below.

**Q1**

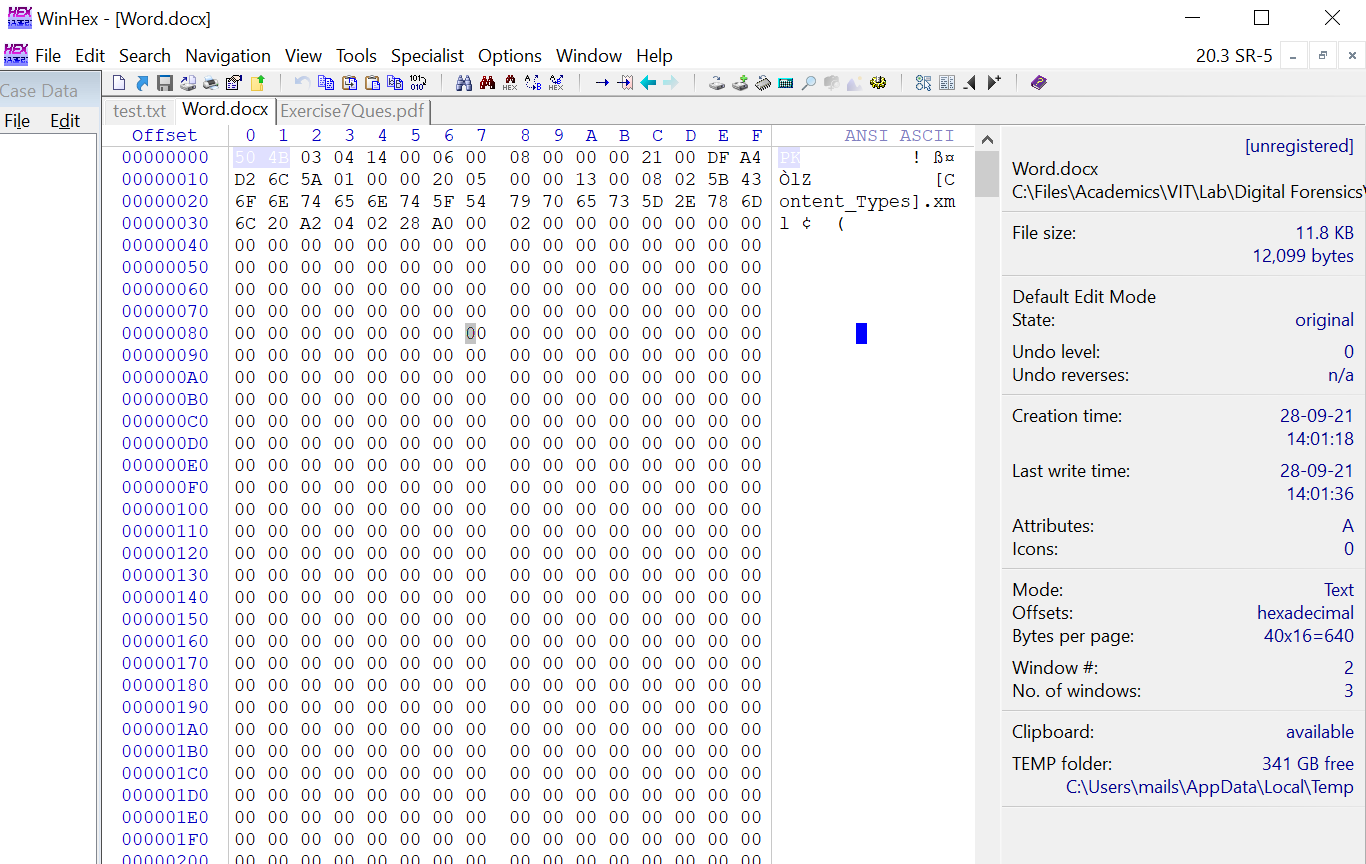
Create text files using these tools. Then use a Hex editor such as vim or WinHex to view these files. What similarities and differences do you notice?

**A**

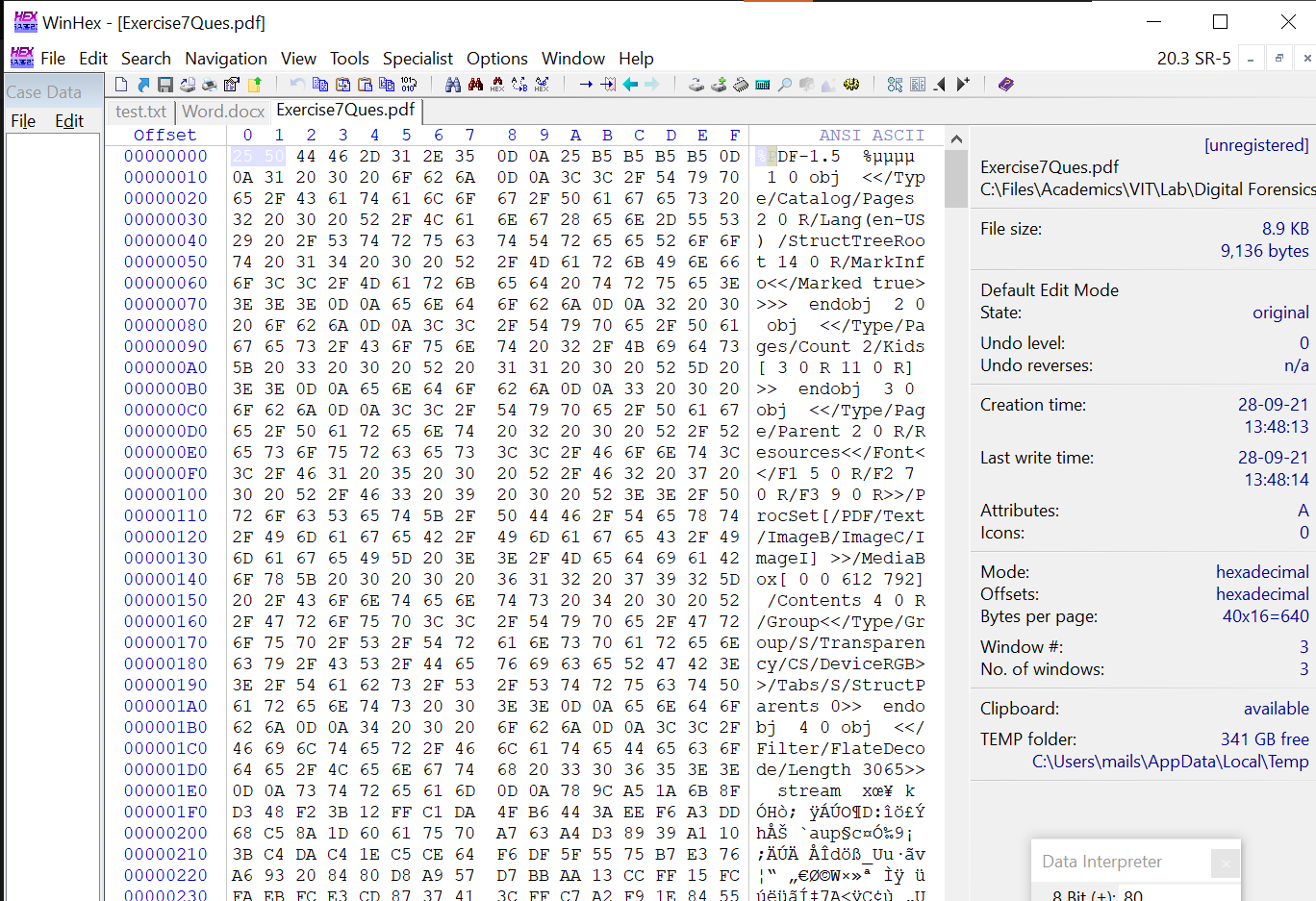
To open a file using WinHex, click ‘File’->’open’. Then browse for the file and open it. For this question, two forms of text files (one using Notepad and the other using MS Word) were created and a PDF file was also used. When opened in WinHex, the following was displayed on the window.



Made using notepad: test.txt



Made using MS Word: Word.docx



A PDF file: Exercise7Ques.pdf

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

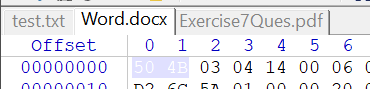
* The windows of each file show us the offset, the content, hexadecimal equivalent of the content and the ANSI ASCII form.
* For text file, the window is simple. We see the contents of test.txt directly on the window and its Hexadecimal equivalent.
* For word files, it is a bit more complicated. We do 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**

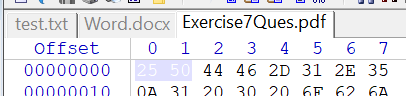
How can you tell what type of file you are looking at by what vim or WinHex shows in the Hex window?

**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**

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

**CONCLUSION**

We have worked with the Windows CLI and with Batch files to retrieve useful information about the device at hand and the network it is connected to.