DIGITAL FORENSICS LAB

Exercise 9	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulagara
Date	12th October, 2021

AIM

Comparing file types and signatures with Hex editors to identify what type of file they are originally.

PROCEDURE AND OBSERVATIONS

Q

Download at least two files with each of the following extensions from the Internet and keep them in a folder: jpg, png, bmp, gif, pdf

Use a hexadecimal editor such as Winhex (see https://www.x-ways.net/winhex/) or some other hexadecimal editor (see https://en.wikipedia.org/wiki/Comparison_of_hex_editors) to look at the hexadecimal contents of the file in order to find headers and footers. Check whether headers and footers are the same for the same file type.

A

We use 4 files: one.jfif, two.png, three.pdf and four.gif. They are shown below:

One.jfif

two.png

Exercise 9

05/10/2021

File signature analysis

File signatures are data used to identify or verify the content of a file. Such signatures are also known as magic numbers. Almost all file types contain a *file signature* at the beginning of a file and some contain particular data patterns at the end of the file. These patterns at the beginning of a file and the end of a file may be called as *headers* and *footers* respectively.

File signature analysis is done primarily to check files are what they claim to be. Changing the extension of a file does not change its contents. For example, suppose we have a genuine jpg file called file.jpg. Renaming it as file.txt will not change its contents. You may check this using a hex editor. So we can easily detect a jpg file impersonating as a txt file by doing file signature analysis.

A signature analysis will compare a file's header or signature to its file extension. A file header identifies the type of file and is located at the beginning of the file's data area. The Windows operating system uses a file's extension to associate the file with the proper application. UNIX and Linux operating systems also use a file's header information to associate file types to specific applications.

Download at least two files with each of the following extensions from the Internet and keep them in a folder: jpg, png, bmp, gif, pdf

Use a hexadecimal editor such as Winhex (see https://www.x-ways.net/winhex/) or some other hexadecimal editor (see https://en.wikipedia.org/wiki/Comparison_of_hex_editors) to look at the hexadecimal contents of the file in order to find headers and footers. Check whether headers and footers are the same for the same file type.

See the following sites for more information about how file signatures look like.

https://en.wikipedia.org/wiki/List_of_file_signatures

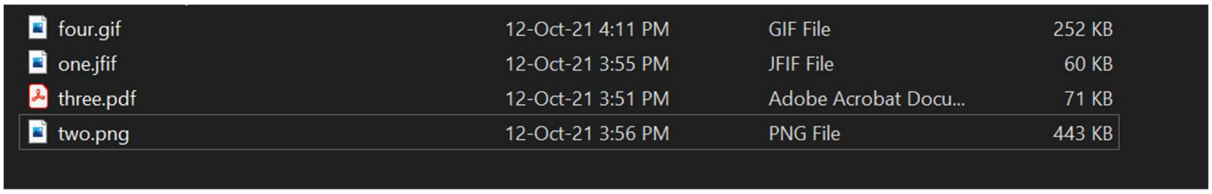
https://www.garykessler.net/library/file_sigs.html

Include screenshots in your submission.

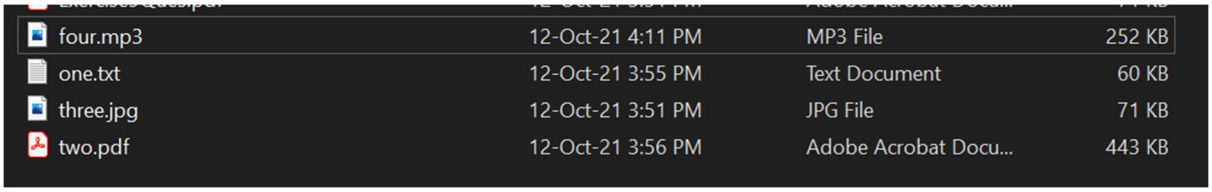
three.pdf

four.gif

We now change their extensions to: one.txt, two.pdf, three.jpg and four.mp3.



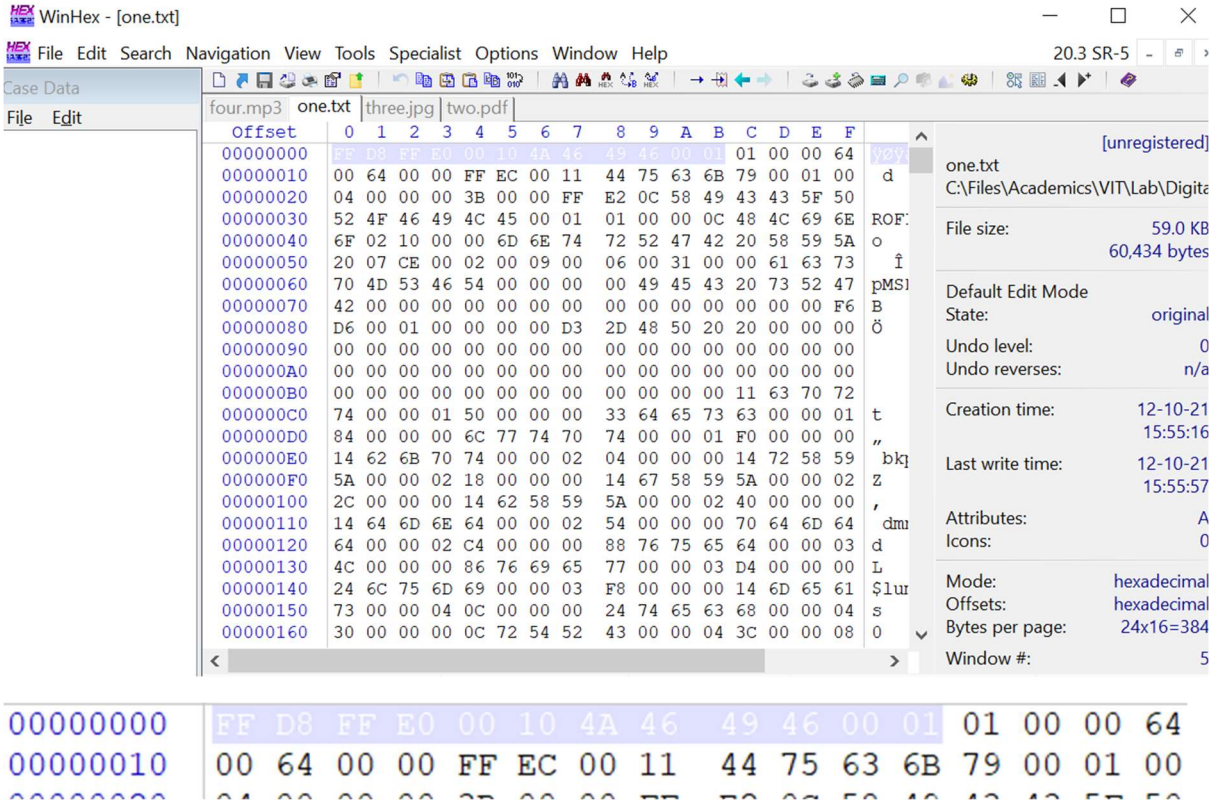
Before



After

We now open these files in WinHex and see their contents.

One.jfif/.txt

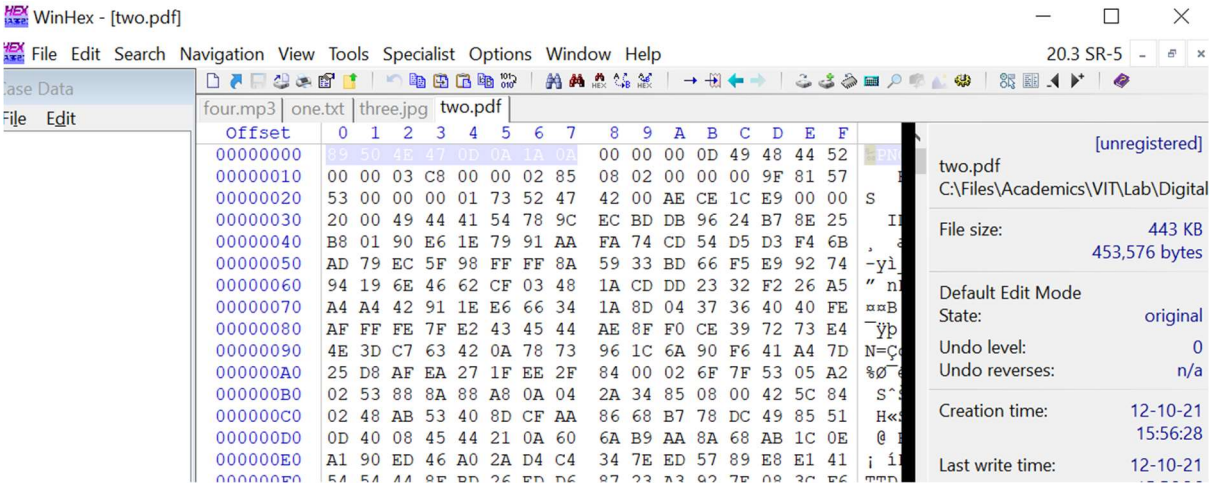


Header of another JFIF file

The file opened in the editor is named ‘one.txt’ and the File Explorer recognises it as a text file. But, when we open it with a hex editor, we see the header to have this Hex signature, (highlighted in the image above) which reads: `FF D8 FF E0 00 10 4A 46 49 46 00 01.`

This is the signature of a JFIF file. Hence, we now know that the file is actually a JFIF file. When checked with another JFIF file’s header they are the same, but the footers are different. This may be due to the fact that they have different content.

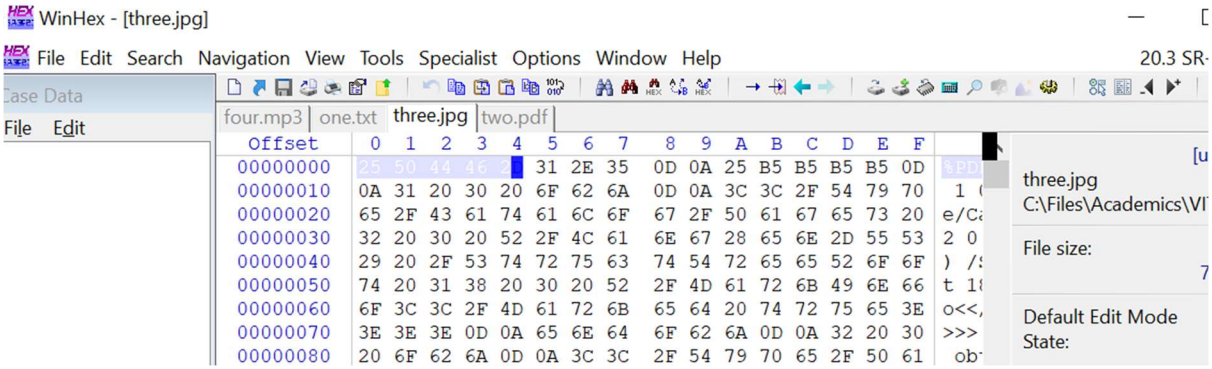
two.png/.pdf



The file opened in the editor is named ‘two.pdf’ and the File Explorer recognises it as a PDF file. But, when we open it with a Hex editor, we see the header to have this Hex signature, (highlighted in the image above) which reads: `89 50 4E 47 0D 0A 1A 0A.`

This is the signature of a PNG file and PDF has a different hex signature as we will see in a following output. Hence, we now know that the file is actually a PNG image file. When compared to the header of another PNG’s header, we see that they are matching.

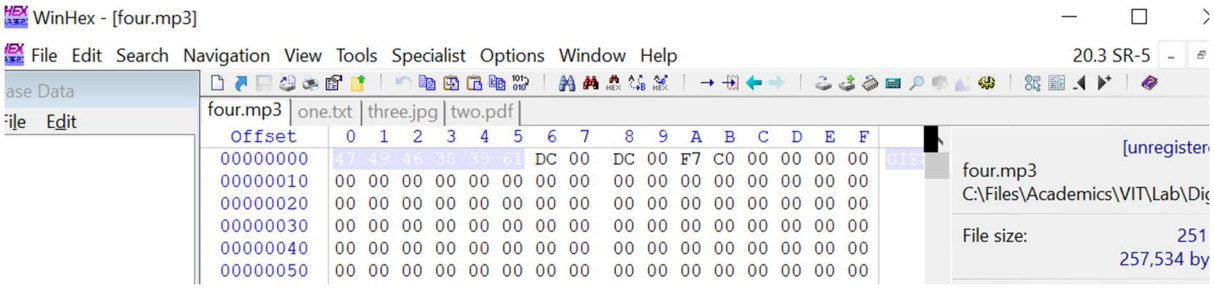
three.pdf/.jpg



The file opened in the editor is named ‘three.jpg’ and the File Explorer recognises it as a JPG file. But, when we open it with a hex editor, we see the header to have this Hex signature, (highlighted in the image above) which reads: `25 50 44 46 2D.`

This is the signature of a PDF file. Hence, we now know that the file is actually a PDF file.

four.gif/.mp3



The file opened in the editor is named ‘four.mp3’ and the File Explorer recognises it as an MP3 file. But, when opened with an MP3 player, it doesn’t play the file and closes due to corrupt data. When we open it with a hex editor, we see the header to have this Hex signature, (highlighted in the image above) which reads: `47 49 46 38 37 61.`

This is the signature of a GIF and MP3 has a different hex signature. Hence, we now know that the file is actually a GIF image.

OBSERVATIONS

Files of the same type always have the same file signatures in their header. This doesn’t change if the file’s extension is changed as their contents remain intact. The rest of the content excluding the header may vary for different files of the same type.

CONCLUSION

We now know how to identify file types with their header content which consists of their file signature. This is done with the help of a Hex editor such as win hex.