

CSE 4004

Digital Forensics

**Lab
Session 9**

TOPIC: File signature analysis

Name: Makesh Srinivasan

Registration number: 19BCE1717

Slot: L49 + L50

Date: 7-October-2021-Monday

Faculty: Prof. Nagaraj

AIM: Exploring File signature analysis in Microsoft Windows 10 environment

INSTRUCTIONS:

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

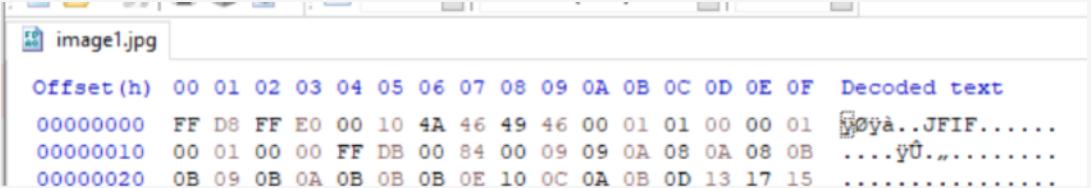
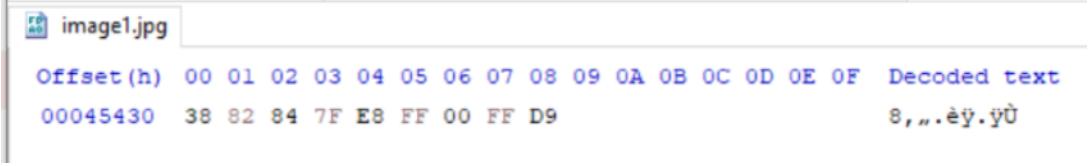
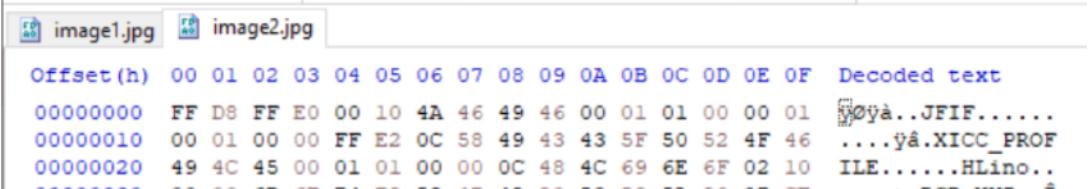
https://www.garykessler.net/library/file_sigs.html

Include screenshots in your submission.

OBSERVATION:**Working directory**

Name	Date	Type	Size	Tags
Wrong files	14-10-2021 12:54	File folder		
Exercise9	14-10-2021 12:12	Rich Text Format	65 KB	
gif1	14-10-2021 12:02	GIF File	1,812 KB	
gif2	14-10-2021 12:02	GIF File	398 KB	
image1	14-10-2021 12:02	BMP File	799 KB	
image1	14-10-2021 12:02	JPG File	278 KB	
image1	14-10-2021 12:02	PNG File	1,278 KB	
image2	14-10-2021 12:02	BMP File	14,401 KB	
image2	14-10-2021 12:02	JPG File	129 KB	
image2	14-10-2021 12:02	PNG File	1,369 KB	
pdf1	14-10-2021 12:12	Microsoft Edge PD...	3 KB	
pdf2	14-10-2021 12:12	Microsoft Edge PD...	608 KB	

File signature analysis

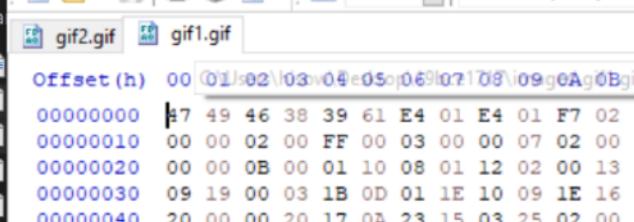
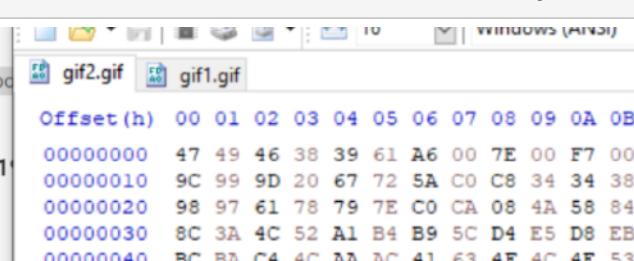
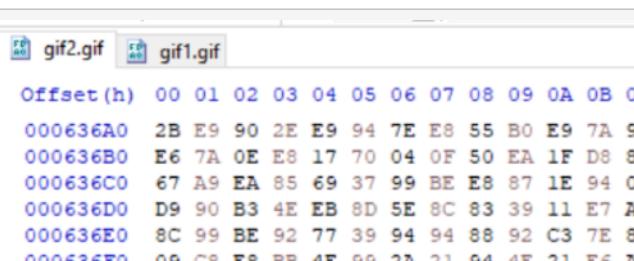
#	JPG
File 1	
Start	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 M...JFIF..... 00000010 00 01 00 00 FF DB 00 84 00 09 09 0A 08 0A 08 0By... 00000020 0B 09 0B 0A 0B 0B 0B 0E 10 0C 0A 0B 0D 13 17 15 </pre>
End	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00045430 38 82 84 7F E8 FF 00 FF D9 </pre> <p style="text-align: right;">8,...éy.y...</p>
File 2	
Start	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 M...JFIF..... 00000010 00 01 00 00 FF E2 0C 58 49 43 43 5F 50 52 4F 46y...XICC_PROF 00000020 49 4C 45 00 01 01 00 00 0C 48 4C 69 6E 6F 02 10 ILE.....HLino.. 00000030 00 00 6D 6E 74 72 52 47 42 20 58 59 5A 20 07 CE ..mntrRGB XYZ .í </pre>
End	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00020090 BC DC 2F 84 7B 39 7B 3F FF D9 </pre> <p style="text-align: right;">4Ü/„{9{?y...</p>

The files image1.jpg and image2.jpg have the same few starting bytes (FF D8 FF E0 10 ...) and this can be viewed in the decoded text section on the right. This is known as the header of the JPG file, this indicates that this is a JPG File. They also have the same bytes at the end, this is known as the footer (FF D9) of the JPG file. The header and footer allow the Operating System to recognise what kind of file this is even if the extension is altered or changed.

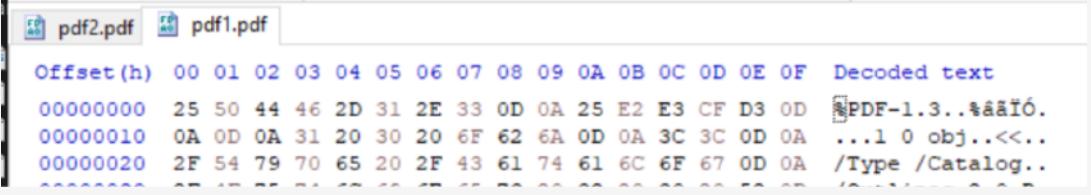
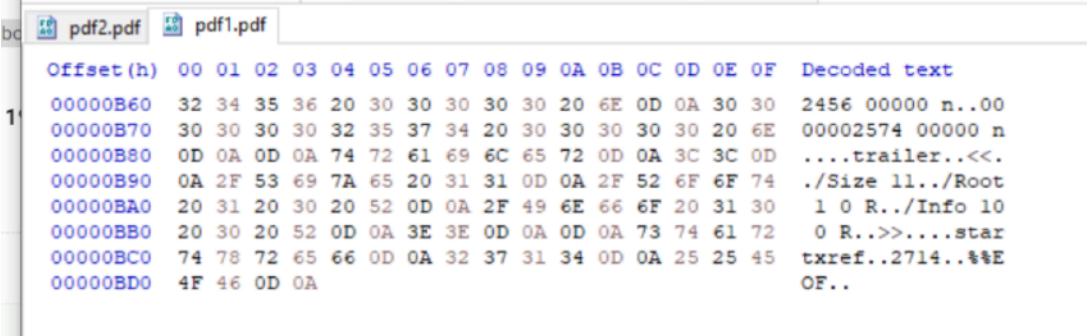
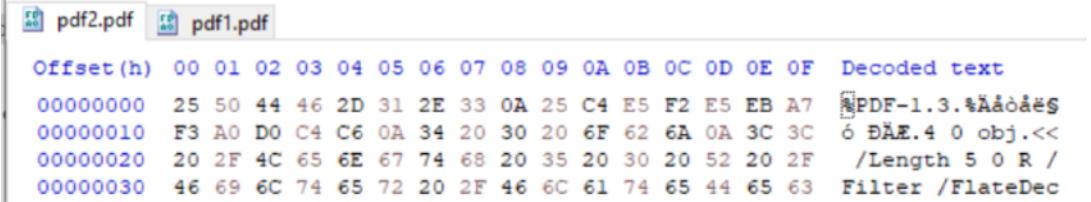
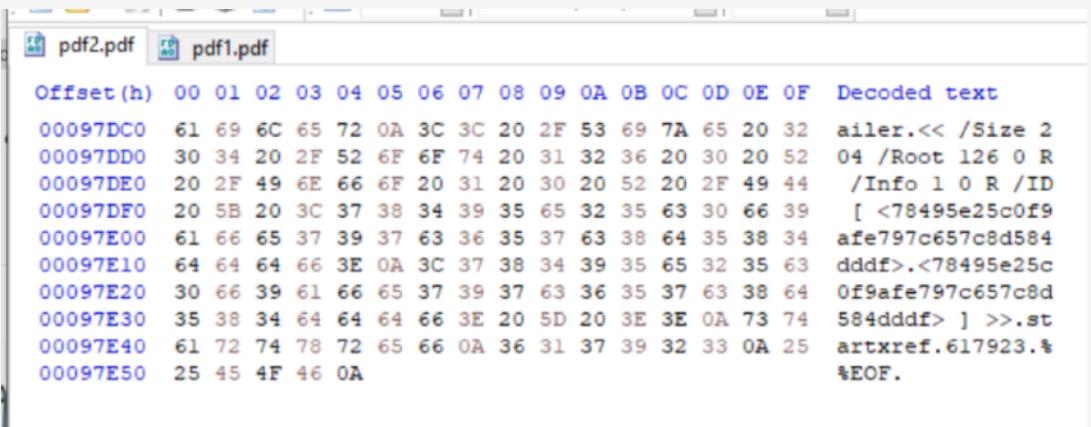
#	PNG																																										
	File 1																																										
Start	<p>image1.png image2.png</p> <table> <thead> <tr> <th>Offset(h)</th> <th>Decoded text</th> </tr> </thead> <tbody> <tr> <td>00000000</td> <td>89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52</td> </tr> <tr> <td>00000010</td> <td>....PNG.....IHDR</td> </tr> <tr> <td>00000020</td> <td>00 00 04 54 00 00 01 FE 08 06 00 00 00 B2 42 5A</td> </tr> <tr> <td></td> <td>....T...p.....BZ</td> </tr> <tr> <td></td> <td>00000020 7F 00 00 0C 49 69 43 43 50 49 43 43 20 50 72 6F</td> </tr> <tr> <td></td> <td>....IiCCP ICC Pro</td> </tr> </tbody> </table>	Offset(h)	Decoded text	00000000	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52	00000010PNG.....IHDR	00000020	00 00 04 54 00 00 01 FE 08 06 00 00 00 B2 42 5A	T...p.....BZ		00000020 7F 00 00 0C 49 69 43 43 50 49 43 43 20 50 72 6F	IiCCP ICC Pro																												
Offset(h)	Decoded text																																										
00000000	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52																																										
00000010PNG.....IHDR																																										
00000020	00 00 04 54 00 00 01 FE 08 06 00 00 00 B2 42 5A																																										
T...p.....BZ																																										
	00000020 7F 00 00 0C 49 69 43 43 50 49 43 43 20 50 72 6F																																										
IiCCP ICC Pro																																										
End	<p>image1.png image2.png</p> <table> <thead> <tr> <th>Offset(h)</th> <th>Decoded text</th> </tr> </thead> <tbody> <tr> <td>0013F400</td> <td>00 00 00 00 49 45 4E 44 AE 42 60 82</td> </tr> <tr> <td></td> <td>....IEND@B`,</td> </tr> </tbody> </table>	Offset(h)	Decoded text	0013F400	00 00 00 00 49 45 4E 44 AE 42 60 82	IEND@B`,																																				
Offset(h)	Decoded text																																										
0013F400	00 00 00 00 49 45 4E 44 AE 42 60 82																																										
IEND@B`,																																										
	File 2																																										
Start	<p>image1.png image2.png</p> <table> <thead> <tr> <th>Offset(h)</th> <th>Decoded text</th> </tr> </thead> <tbody> <tr> <td>00000000</td> <td>89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52</td> </tr> <tr> <td>00000010</td> <td>....PNG.....IHDR</td> </tr> <tr> <td>00000020</td> <td>00 00 03 FE 00 00 03 8C 08 06 00 00 00 F4 76 68</td> </tr> <tr> <td></td> <td>....p...@.....ôvh</td> </tr> <tr> <td>00000030</td> <td>07 00 00 0C 49 69 43 43 50 49 43 43 20 50 72 6F</td> </tr> <tr> <td></td> <td>....IiCCP ICC Pro</td> </tr> <tr> <td></td> <td>66 69 6C 65 00 00 48 89 95 57 07 58 53 C9 16 9E</td> </tr> <tr> <td></td> <td>file..Hñ.W.XSÉ.ž</td> </tr> </tbody> </table>	Offset(h)	Decoded text	00000000	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52	00000010PNG.....IHDR	00000020	00 00 03 FE 00 00 03 8C 08 06 00 00 00 F4 76 68	p...@.....ôvh	00000030	07 00 00 0C 49 69 43 43 50 49 43 43 20 50 72 6F	IiCCP ICC Pro		66 69 6C 65 00 00 48 89 95 57 07 58 53 C9 16 9E		file..Hñ.W.XSÉ.ž																								
Offset(h)	Decoded text																																										
00000000	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52																																										
00000010PNG.....IHDR																																										
00000020	00 00 03 FE 00 00 03 8C 08 06 00 00 00 F4 76 68																																										
p...@.....ôvh																																										
00000030	07 00 00 0C 49 69 43 43 50 49 43 43 20 50 72 6F																																										
IiCCP ICC Pro																																										
	66 69 6C 65 00 00 48 89 95 57 07 58 53 C9 16 9E																																										
	file..Hñ.W.XSÉ.ž																																										
End	<p>image1.png image2.png</p> <table> <thead> <tr> <th>Offset(h)</th> <th>Decoded text</th> </tr> </thead> <tbody> <tr> <td>00156050</td> <td>C0 EF F3 FD 2F 9F BB 10 F6 CB 00 5C ED E7 05 C6</td> </tr> <tr> <td>00156060</td> <td>Àíóý/Ý».öÈ.\íç.È</td> </tr> <tr> <td>00156070</td> <td>CF 28 BB D0 7F C6 5D 01 CF B9 F5 FF 09 9F 2F 7A</td> </tr> <tr> <td></td> <td>Í(»D.È].Í¹öý.Ý/z</td> </tr> <tr> <td>00156080</td> <td>F2 D4 63 34 8F E7 D1 EE ED 33 9E 04 E8 9A 53 B3</td> </tr> <tr> <td></td> <td>öÖc4.çÑii3ž.èšS°</td> </tr> <tr> <td>00156080</td> <td>AC 67 04 33 2F 4F A2 10 DD 82 02 10 8F 85 C6 3B</td> </tr> <tr> <td></td> <td>-g.3/Oç.Ý,....È;</td> </tr> <tr> <td>00156090</td> <td>63 0F 0F 97 22 C3 19 93 3F 3D 4A EF D7 3F 18 E2</td> </tr> <tr> <td></td> <td>c..—"À."?=Ji×?..â</td> </tr> <tr> <td>001560A0</td> <td>0B E4 F0 A6 05 C2 17 39 10 E5 E2 43 BA 1A 30 F5</td> </tr> <tr> <td></td> <td><äö!.À.9.ååC°.0Ö</td> </tr> <tr> <td>001560B0</td> <td>78 32 35 0C 3C AE 80 DD 85 09 57 27 OC 1A BC E4</td> </tr> <tr> <td></td> <td>x25.<øéÝ...W'..ñä</td> </tr> <tr> <td>001560C0</td> <td>AF 69 58 74 E4 A4 7B 6C 43 26 B6 D4 0A F5 21 OC</td> </tr> <tr> <td></td> <td>"ixtä»(1C&qÖ.ö!.</td> </tr> <tr> <td>001560D0</td> <td>65 F2 FB 28 CD FF 03 1F FD 37 C8 C8 BB E8 B4 00</td> </tr> <tr> <td></td> <td>eðù(fý..ý7ÈÈ»è'.</td> </tr> <tr> <td>001560E0</td> <td>00 00 00 49 45 4E 44 AE 42 60 82</td> </tr> <tr> <td></td> <td>....IEND@B`,</td> </tr> </tbody> </table>	Offset(h)	Decoded text	00156050	C0 EF F3 FD 2F 9F BB 10 F6 CB 00 5C ED E7 05 C6	00156060	Àíóý/Ý».öÈ.\íç.È	00156070	CF 28 BB D0 7F C6 5D 01 CF B9 F5 FF 09 9F 2F 7A		Í(»D.È].Í¹öý.Ý/z	00156080	F2 D4 63 34 8F E7 D1 EE ED 33 9E 04 E8 9A 53 B3		öÖc4.çÑii3ž.èšS°	00156080	AC 67 04 33 2F 4F A2 10 DD 82 02 10 8F 85 C6 3B		-g.3/Oç.Ý,....È;	00156090	63 0F 0F 97 22 C3 19 93 3F 3D 4A EF D7 3F 18 E2		c..—"À."?=Ji×?..â	001560A0	0B E4 F0 A6 05 C2 17 39 10 E5 E2 43 BA 1A 30 F5		<äö!.À.9.ååC°.0Ö	001560B0	78 32 35 0C 3C AE 80 DD 85 09 57 27 OC 1A BC E4		x25.<øéÝ...W'..ñä	001560C0	AF 69 58 74 E4 A4 7B 6C 43 26 B6 D4 0A F5 21 OC		"ixtä»(1C&qÖ.ö!.	001560D0	65 F2 FB 28 CD FF 03 1F FD 37 C8 C8 BB E8 B4 00		eðù(fý..ý7ÈÈ»è'.	001560E0	00 00 00 49 45 4E 44 AE 42 60 82	IEND@B`,
Offset(h)	Decoded text																																										
00156050	C0 EF F3 FD 2F 9F BB 10 F6 CB 00 5C ED E7 05 C6																																										
00156060	Àíóý/Ý».öÈ.\íç.È																																										
00156070	CF 28 BB D0 7F C6 5D 01 CF B9 F5 FF 09 9F 2F 7A																																										
	Í(»D.È].Í¹öý.Ý/z																																										
00156080	F2 D4 63 34 8F E7 D1 EE ED 33 9E 04 E8 9A 53 B3																																										
	öÖc4.çÑii3ž.èšS°																																										
00156080	AC 67 04 33 2F 4F A2 10 DD 82 02 10 8F 85 C6 3B																																										
	-g.3/Oç.Ý,....È;																																										
00156090	63 0F 0F 97 22 C3 19 93 3F 3D 4A EF D7 3F 18 E2																																										
	c..—"À."?=Ji×?..â																																										
001560A0	0B E4 F0 A6 05 C2 17 39 10 E5 E2 43 BA 1A 30 F5																																										
	<äö!.À.9.ååC°.0Ö																																										
001560B0	78 32 35 0C 3C AE 80 DD 85 09 57 27 OC 1A BC E4																																										
	x25.<øéÝ...W'..ñä																																										
001560C0	AF 69 58 74 E4 A4 7B 6C 43 26 B6 D4 0A F5 21 OC																																										
	"ixtä»(1C&qÖ.ö!.																																										
001560D0	65 F2 FB 28 CD FF 03 1F FD 37 C8 C8 BB E8 B4 00																																										
	eðù(fý..ý7ÈÈ»è'.																																										
001560E0	00 00 00 49 45 4E 44 AE 42 60 82																																										
IEND@B`,																																										

The files image1.png and image2.png have the same few starting bytes (89 50 4E 47 0D ...) and this can be viewed in the decoded text section on the right. This is known as the header of the PNG file, this indicates that this is a PNG File. They also have the same bytes at the end, this is known as the footer (42 60 82) of the PNG file. The header and footer allow the Operating System to recognise what kind of file this is even if the extension is altered or changed.

The files image1.bmp and image2.bmp have the same few starting bytes (42 4D 8A) and this can be viewed in the decoded text section on the right. This is known as the header of the BMP file, this indicates that this is a BMP File. They DO NOT have the same bytes at the end (footer of the file). The header allows the Operating System to recognise what kind of file this is even if the extension is altered or changed.

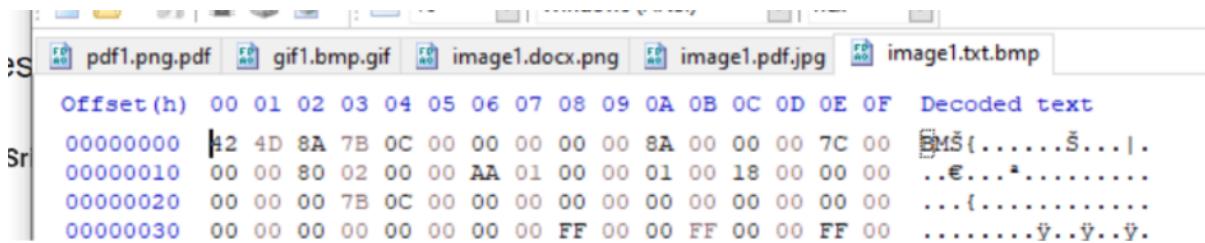
#		GIF
		File 1
Start	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00000000 47 49 46 38 39 61 E4 01 E4 01 F7 02 31 00 00 00 GIF89aa.ä.+.1... 00000010 00 00 02 00 FF 00 03 00 00 07 02 00 08 00 00 0Bÿ..... 00000020 00 00 0B 00 01 10 08 01 12 02 00 13 0C 02 14 0D⠄..... 00000030 09 19 00 03 1B 0D 01 1E 10 09 1E 16 10 1F 00 00⠄..... 00000040 20 00 00 20 17 0A 23 15 03 25 02 00 26 00 00 28#..%..z...!</pre>	
End	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 001C4C30 08 5D D4 00 CE 67 C9 86 86 6A 9F AA DE A3 1E D6 .jÓ.ÍgÉttjÝ*Þ£.Ö 001C4C40 63 23 36 C1 1B F4 A3 DB EC 00 F8 CD E3 A1 D4 63 c#6Á.ð£Ùí.øíå;Óc 001C4C50 42 E6 61 6B 48 D6 D3 3D DD 60 B1 C0 43 7A 00 6B ßæakHÓÓ=Ý+íACz.k 001C4C60 E5 13 6A 1E D1 B1 F2 53 69 31 11 8F EE E8 8E 2E Å.j.ÑtðSil..ieŽ. 001C4C70 0E F6 05 69 F1 0C C1 10 D8 26 20 7A 0D 09 18 54 .ö.ifn.Á.Ø&z...T 001C4C80 92 7E 91 73 D6 16 93 AE 07 B9 96 2B 71 04 04 00 '~-sÖ."®.¹-+q... 001C4C90 3B ;</pre>	
		File 2
Start	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00000000 47 49 46 38 39 61 A6 00 7E 00 F7 00 00 38 96 A0 GIF89a;~.+.8- 00000010 9C 99 9D 20 67 72 5A C0 C8 34 34 38 D4 D2 D5 73 oem. grZÀÈ4480ÖÖs 00000020 98 97 61 78 79 7E C0 CA 08 4A 58 84 78 84 24 7E ~-axy~ÀÈ.JX,,x.,\$~ 00000030 8C 3A 4C 52 A1 B4 B9 5C D4 E5 D8 EB EB A9 E5 E1 G:LR;`~\ÓâØëëÓâá 00000040 BC BA C4 4C AA AC 41 63 4F 4C 4E 53 6F C0 CE 24 ¼ºÄL~AcOLNSoáfs</pre>	
End	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 000636A0 2B E9 90 2E E9 94 7E E8 55 B0 E9 7A 9E 95 03 41 +é.~é~Ùºézž*.A 000636B0 E6 7A 0E E8 17 70 04 0F 50 EA 1F D8 8E 08 11 79 æz.~é.p..Pè.ØŽ..y 000636C0 67 A9 EA 85 69 37 99 BE E8 87 1E 94 09 39 75 79 g@È..i7ºé‡.~.9uy 000636D0 D9 90 B3 4E EB 8D 5E 8C 83 39 11 E7 A1 95 9F 79 Ü.~Né.~Gf9.ç;.Ýy 000636E0 8C 99 BE 92 77 39 94 94 88 92 C3 7E 86 BE BE 18 Gºé%w9""~'Å~+íé. 000636F0 09 C8 E8 BB 4E 99 2A 21 94 4E 21 E6 A8 10 10 00 .Èè»Nºé!N!æ"... 00063700 3B ;</pre>	

The files gif1.gif and gif2.gif have the same few starting bytes and this can be viewed in the decoded text section on the right. This is known as the header of the GIF file, this indicates that this is a GIF File. They also have the same bytes at the end, this is known as the footer of the GIF file. The header and footer allow the Operating System to recognise what kind of file this is even if the extension is altered or changed.

#	PDF
	File 1
Start	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00000000 25 50 44 46 2D 31 2E 33 0A 25 E2 E3 CF D3 0D %PDF-1.3..%äöö. 00000010 0A 0D 0A 31 20 30 20 6F 62 6A 0D 0A 3C 3C 0D 0A ...1 0 obj..<<. 00000020 2F 54 79 70 65 20 2F 43 61 74 61 6C 6F 67 0D 0A /Type /Catalog.. 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 />> ..<<. </pre>
End	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00000B60 32 34 35 36 20 30 30 30 30 30 20 6E 0D 0A 30 30 2456 00000 n..00 00000B70 30 30 30 30 32 35 37 34 20 30 30 30 30 30 20 6E 00002574 00000 n 00000B80 0D 0A 0D 0A 74 72 61 69 6C 65 72 0D 0A 3C 3C 0Dtrailer..<<. 00000B90 0A 2F 53 69 7A 65 20 31 31 0D 0A 2F 52 6F 6F 74 ./Size 11../Root 00000BA0 20 31 20 30 20 52 0D 0A 2F 49 6E 66 6F 20 31 30 1 0 R../Info 10 00000BB0 20 30 20 52 0D 0A 3E 3E 0D 0A 0D 0A 73 74 61 72 0 R..>>....star 00000BC0 74 78 72 65 66 0D 0A 32 37 31 34 0D 0A 25 25 45 txref..2714..%%E 00000BD0 4F 46 0D 0A OF.. </pre>
	File 2
Start	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00000000 25 50 44 46 2D 31 2E 33 0A 25 C4 E5 F2 E5 EB A7 %PDF-1.3.%ÄööäëëS 00000010 F3 A0 D0 C4 C6 0A 34 20 30 20 6F 62 6A 0A 3C 3C ö ðæ.4 0 obj..<< 00000020 20 2F 4C 65 6E 67 74 68 20 35 20 30 20 52 20 2F /Length 5 0 R / 00000030 46 69 6C 74 65 72 20 2F 46 6C 61 74 65 44 65 63 Filter /FlateDec </pre>
End	 <pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00097DC0 61 69 6C 65 72 0A 3C 3C 20 2F 53 69 7A 65 20 32 ailer..<< /Size 2 00097DD0 30 34 20 2F 52 6F 6F 74 20 31 32 36 20 30 20 52 04 /Root 126 0 R 00097DE0 20 2F 49 6E 66 6F 20 31 20 30 20 52 20 2F 49 44 /Info 1 0 R /ID 00097DF0 20 5B 20 3C 37 38 34 39 35 65 32 35 63 30 66 39 [<78495e25c0f9 00097E00 61 66 65 37 39 37 63 36 35 37 63 38 64 35 38 34 afe797c657c8d584 00097E10 64 64 64 66 3E 0A 3C 37 38 34 39 35 65 32 35 63 ddddf>.<78495e25c 00097E20 30 66 39 61 66 65 37 39 37 63 36 35 37 63 38 64 0f9afe797c657c8d 00097E30 35 38 34 64 64 64 66 3E 20 5D 20 3E 3E 0A 73 74 584dddf>] >>.st 00097E40 61 72 74 78 72 65 66 0A 36 31 37 39 32 33 0A 25 artxref.617923.%EOF. 00097E50 25 45 4F 46 0A </pre>

The files pdf1.pdf and pdf2.pdf have the same few starting bytes and this can be viewed in the decoded text section on the right. This is known as the header of the pdf file, this indicates that this is a PDF File. They also have the same bytes at the end, this is known as the footer of the pdf file. It is sometimes common to find “..” after EOF but the hexadecimal values 45 4F 46 are representing the EOF which is unique to PDF files

Example of when the file extortion is forcefully modified:



Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00000000	42 4D 8A 7B 0C 00 00 00 00 00 8A 00 00 00 7C 00	MS(.....S....)
00000010	00 00 80 02 00 00 AA 01 00 00 01 00 18 00 00 00	..€....*
00000020	00 00 00 7B 0C 00 00 00 00 00 00 00 00 00 00 00	...{.....
00000030	00 00 00 00 00 00 FF 00 00 FF 00 00 FF 00 00 FFÿ.ÿ.ÿ.

The file is a bmp type, but the extension txt when added does not change the signature of the bmp file. The first few bytes are those of the BMP file types as seen in the previous sections.

Conclusion

The file signatures (header and sometimes, footer) can help identify the type of file even if the extension is modified. The changes to the extension do not modify the contents of the file and this was explored using the HxD editor. The header and footer allow the Operating System to recognise what kind of file this is even if the extension is altered or changed.