Digital Forensics - Lab 9

Class No :	**CH2021221000516**	Slot :	**L49 + L50**
Course Code :	**CSE4004**	Faculty Name :	**Nagaraj SV**

Aadhitya Swarnesh

- 7 October 2021

Question 1 :

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 or some other hexadecimal editor 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.

In this lab experiment, we will explore the file formats in more detail to explore and find patterns in the raw format of many varieties of files and draw conclusions on a key aspect that the file managers and thus the operating systems use.

For this experiment, we use the WInHex Hexadecimal editor in a Windows 7 environment. The choice of a hexadecimal is arbitrary and is irrelevant to this current procedure. We have taken up two files of each format and explored them from the view of an hexadecimal editor. We will now explore many different formats of files and view patterns :

1. **PDF (Portable Document Format)** - This is the format used for sharing and viewing documents, and is a very popular format.

The two different files when viewed under a hexadecimal editor are as follows :

Lab 6.pdf | Win FE.pdf

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	33	0A	25	C4	E5	F2	E5	EB	A7	%PDF-1.3 %Äåòåë§
00000010	F3	A0	D0	C4	C6	0A	33	20	30	20	6F	62	6A	0A	3C	3C	ó ÐÄÆ 3 0 obj <<
00000020	20	2F	46	69	6C	74	65	72	20	2F	46	6C	61	74	65	44	/Filter /FlateD
00000030	65	63	6F	64	65	20	2F	4C	65	6E	67	74	68	20	35	30	ecode /Length 50
00000040	38	38	20	3E	3E	0A	73	74	72	65	61	6D	0A	78	01	D5	88 >> stream x Õ
00000050	5C	DB	92	1B	B7	11	7D	C7	57	20	6F	DC	8A	35	1A	CC	\Û' · }ÇW oÜŠ5 Ì
00000060	7D	5C	2E	57	49	2B	C5	B1	CA	76	E4	68	2B	79	70	F2	}\.WI+Å±Êväh+ypò
00000070	40	CB	94	96	0E	77	2D	AF	56	91	9D	8F	CD	B7	E4	34	@Ë"- w-¯V' Í·ä4

Lab 6.pdf | Win FE.pdf

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	33	0A	25	C4	E5	F2	E5	EB	A7	%PDF-1.3 %Äåòåë§
00000010	F3	A0	D0	C4	C6	0A	33	20	30	20	6F	62	6A	0A	3C	3C	ó ÐÄÆ 3 0 obj <<
00000020	20	2F	46	69	6C	74	65	72	20	2F	46	6C	61	74	65	44	/Filter /FlateD
00000030	65	63	6F	64	65	20	2F	4C	65	6E	67	74	68	20	32	33	ecode /Length 23
00000040	32	36	20	3E	3E	0A	73	74	72	65	61	6D	0A	78	01	A5	26 >> stream x ¥
00000050	59	DB	6E	E3	C8	11	7D	E7	57	54	F2	24	03	1E	5A	A4	YÛnãÈ }çWTò$ Z¤
00000060	A8	1B	B0	58	60	D6	E3	49	26	C8	00	B3	88	80	7D	C8	¨ °X`ÖãI&È ³ˆ€}È
00000070	E6	A1	45	B6	AC	4E	78	D1	88	A4	3D	FE	D0	BC	EE	B7	æ¡E¶¬NxÑˆ¤=þÐ¼î·

We can notice here that the first few bytes are exactly the same. Let us now view the end of these files.

Lab 6.pdf | Win FE.pdf

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00032DC0	74	20	38	31	37	20	30	20	52	20	2F	49	6E	66	6F	20	t 817 0 R /Info
00032DD0	39	32	30	20	30	20	52	20	2F	49	44	20	5B	20	3C	38	920 0 R /ID [<8
00032DE0	35	39	34	30	63	34	66	36	66	36	65	38	32	39	31	35	5940c4f6f6e82915
00032DF0	65	39	35	62	39	63	64	38	33	31	34	31	65	35	35	3E	e95b9cd83141e55>
00032E00	0A	3C	38	35	39	34	30	63	34	66	36	66	36	65	38	32	<85940c4f6f6e82
00032E10	39	31	35	65	39	35	62	39	63	64	38	33	31	34	31	65	915e95b9cd83141e
00032E20	35	35	3E	20	5D	20	3E	3E	0A	73	74	61	72	74	78	72	55>] >> startxr
00032E30	65	66	0A	31	38	39	38	36	34	0A	25	25	45	4F	46	0A	ef 189864 %%EOF

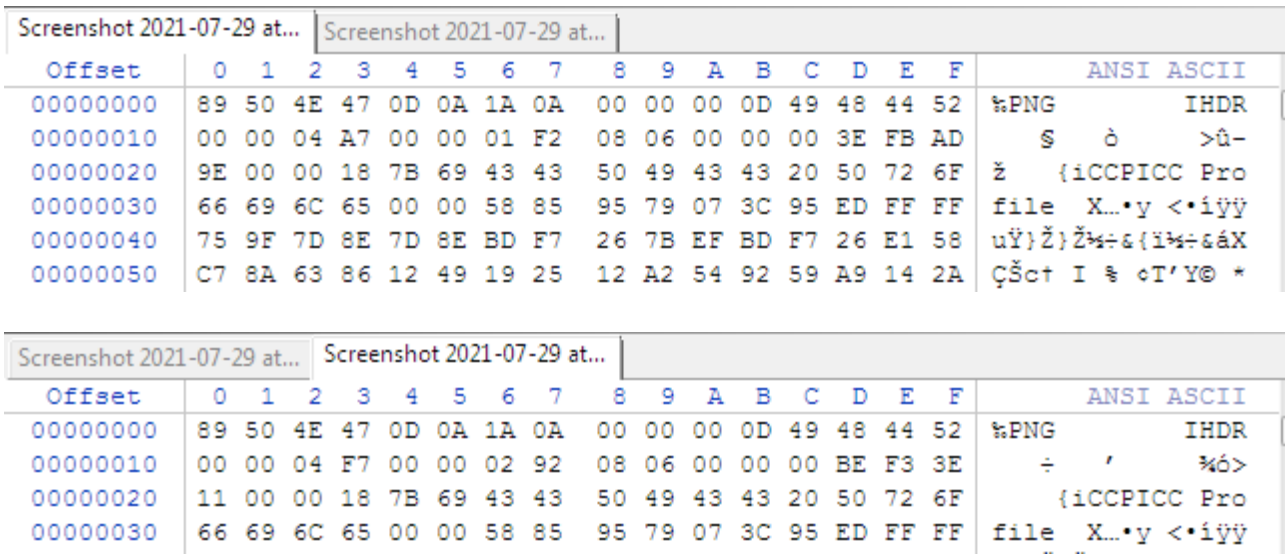
WinFE.pdf : (Last few lines)

0000B070	36	66	38	3E	0A	3C	37	30	62	33	37	62	30	62	34	66	6f8> <70b37b0b4f
0000B080	35	36	31	37	36	31	34	30	34	36	30	66	36	39	33	64	56176140460f693d
0000B090	39	36	36	36	66	38	3E	20	5D	20	3E	3E	0A	73	74	61	9666f8>] >> sta
0000B0A0	72	74	78	72	65	66	0A	34	33	36	39	36	0A	25	25	45	rtxref 43696 %%E
0000B0B0	4F	46	0A														OF

We can notice here that the last few bytes are also the same.

2. **PNG** - This is the format used for storing Image Files.

The two different files when viewed under a hexadecimal editor are as follows :



Screenshot 2021-07-29 at... | Screenshot 2021-07-29 at...

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000010	00	00	04	A7	00	00	01	F2	08	06	00	00	00	3E	FB	AD	§ ò >û-
00000020	9E	00	00	18	7B	69	43	43	50	49	43	43	20	50	72	6F	ž {iCCPICC Pro
00000030	66	69	6C	65	00	00	58	85	95	79	07	3C	95	ED	FF	FF	file X…•y <•íÿÿ
00000040	75	9F	7D	8E	7D	8E	BD	F7	26	7B	EF	BD	F7	26	E1	58	uŸ}Ž}Ž½÷&{ï½÷&áX
00000050	C7	8A	63	86	12	49	19	25	12	A2	54	92	59	A9	14	2A	ÇŠc† I % ¢T'Y© *

Screenshot 2021-07-29 at... | Screenshot 2021-07-29 at...

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000010	00	00	04	F7	00	00	02	92	08	06	00	00	00	BE	F3	3E	÷ ' ¾ó>
00000020	11	00	00	18	7B	69	43	43	50	49	43	43	20	50	72	6F	{iCCPICC Pro
00000030	66	69	6C	65	00	00	58	85	95	79	07	3C	95	ED	FF	FF	file X…•y <•íÿÿ

We can notice here that the first few bytes are exactly the same. Let us now view the end of these files.

Last few bytes of file 1 :

000256E0	88	12	22	80	00	02	08	20	80	00	02	08	20	80	00	02	ˆ "€ € €
000256F0	08	20	80	00	02	59	2B	F0	7F	4A	67	0B	DC	2E	45	EC	€ Y+ð Jg Ü.Eì
00025700	62	00	00	00	00	49	45	4E	44	AE	42	60	82				b IEND®B`,

Last few bytes of file 2 :

000286B0	09	30	01	26	C0	04	98	00	13	60	02	4C	80	09	30	01	0 &À ˜ ` L€ 0
000286C0	26	C0	04	98	00	13	60	02	4C	80	09	24	3D	81	FF	03	&À ˜ ` L€ $= ÿ ø
000286D0	6B	B9	26	4D	F1	DA	23	E1	00	00	00	00	49	45	4E	44	k¹&MñÚ#á IEND
000286E0	AE	42	60	82													®B`,

We can notice here that the last few bytes are also the same.

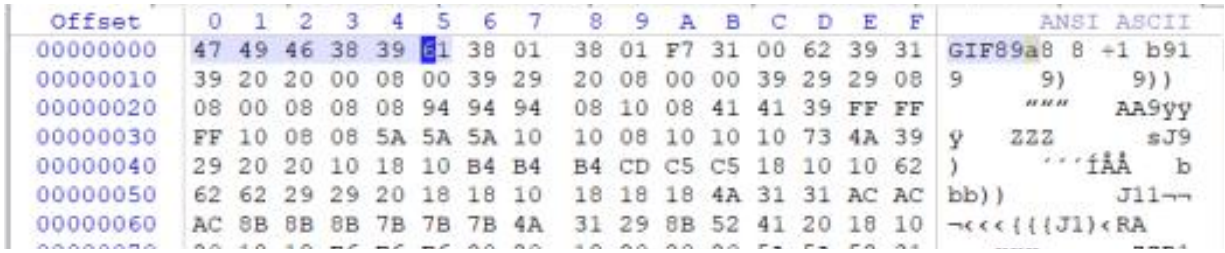
3. **GIF** - This is the format used for sharing and viewing small videos and motion images, and is a very popular format in messaging platforms.

Its General File signature is as follows :

47 49 46 38 37 61 ***or***		GIF87a
47 49 46 38 39 61		GIF89a
	GIF	Graphics interchange format file
		Trailer: 00 3B (. ;)

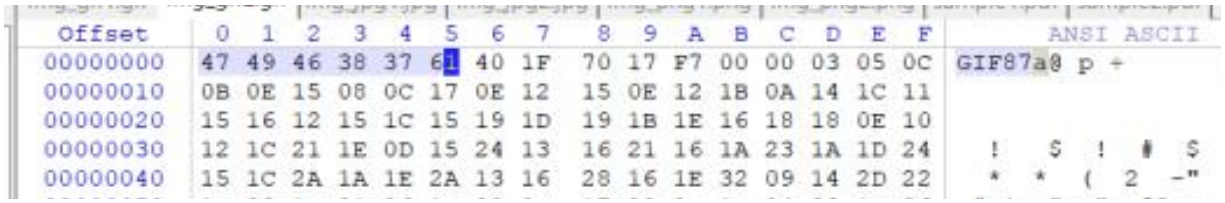
We now take two sample files and proceed with finding patterns in them.

First few bits of file 1 :



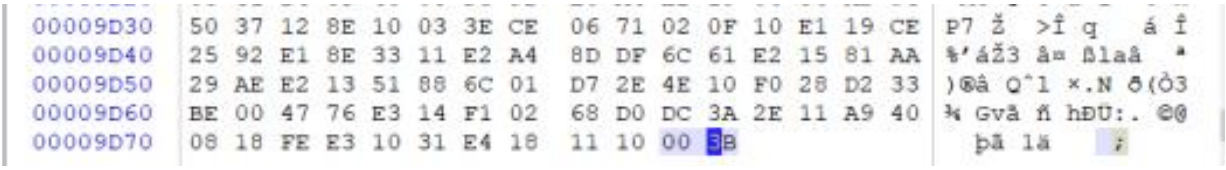
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	47	49	46	38	39	61	38	01	38	01	F7	31	00	62	39	31	GIF89a8 8 ÷1 b91
00000010	39	20	20	00	08	00	39	29	20	08	00	00	39	29	29	08	9 9) 9))
00000020	08	00	08	08	08	94	94	94	08	10	08	41	41	39	FF	FF	””” AA9yy
00000030	FF	10	08	08	5A	5A	5A	10	10	08	10	10	10	73	4A	39	ÿ ZZZ sJ9
00000040	29	20	20	10	18	10	B4	B4	B4	CD	C5	C5	18	10	10	62	) ´´´íÅÅ b
00000050	62	62	29	29	20	18	18	10	18	18	18	4A	31	31	AC	AC	bb)) J11¬¬
00000060	AC	8B	8B	8B	7B	7B	7B	4A	31	29	8B	52	41	20	18	10	¬‹‹‹{{{J1)‹RA

First Few bits of file 2 :



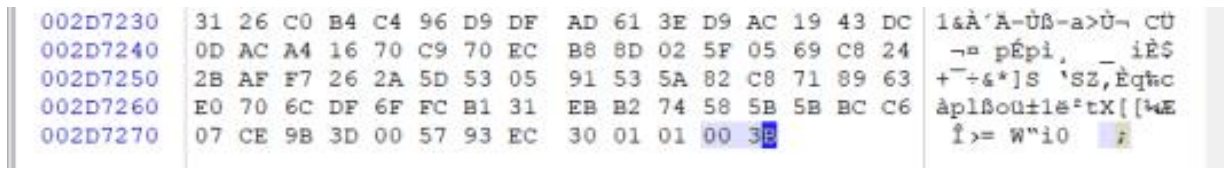
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	47	49	46	38	37	61	40	1F	70	17	F7	00	00	03	05	0C	GIF87a@ p ÷
00000010	0B	0E	15	08	0C	17	0E	12	15	0E	12	1B	0A	14	1C	11	
00000020	15	16	12	15	1C	15	19	1D	19	1B	1E	16	18	18	0E	10	
00000030	12	1C	21	1E	0D	15	24	13	16	21	16	1A	23	1A	1D	24	! $! # $
00000040	15	1C	2A	1A	1E	2A	13	16	28	16	1E	32	09	14	2D	22	* * (2 -"

Last few bits of file 1 :



00009D30	50	37	12	8E	10	03	3E	CE	06	71	02	0F	10	E1	19	CE	P7 Ž >Î q á Î
00009D40	25	92	E1	8E	33	11	E2	A4	8D	DF	6C	61	E2	15	81	AA	%'áŽ3 â¤ ßlaâ ª
00009D50	29	AE	E2	13	51	88	6C	01	D7	2E	4E	10	F0	28	D2	33	)®â Q^l ×.N ð(Ò3
00009D60	BE	00	47	76	E3	14	F1	02	68	D0	DC	3A	2E	11	A9	40	¾ Gvã ñ hÐÜ:. ©@
00009D70	08	18	FE	E3	10	31	E4	18	11	10	00	3B					þã 1ä ;

Last few bits of file 2 :



002D7230	31	26	C0	B4	C4	96	D9	DF	AD	61	3E	D9	AC	19	43	DC	1&À´Ä–Ùß-a>Ù¬ CÜ
002D7240	0D	AC	A4	16	70	C9	70	EC	B8	8D	02	5F	05	69	C8	24	¬¤ pÉpì, _ iÈ$
002D7250	2B	AF	F7	26	2A	5D	53	05	91	53	5A	82	C8	71	89	63	+¯÷&*]S 'SZ,Èq‰c
002D7260	E0	70	6C	DF	6F	FC	B1	31	EB	B2	74	58	5B	5B	BC	C6	àplßoü±1ë²tX[[¼Æ
002D7270	07	CE	9B	3D	00	57	93	EC	30	01	01	00	3B				Î›= W“i0 ;

We can notice here as well that the pattern for GIF format follows.

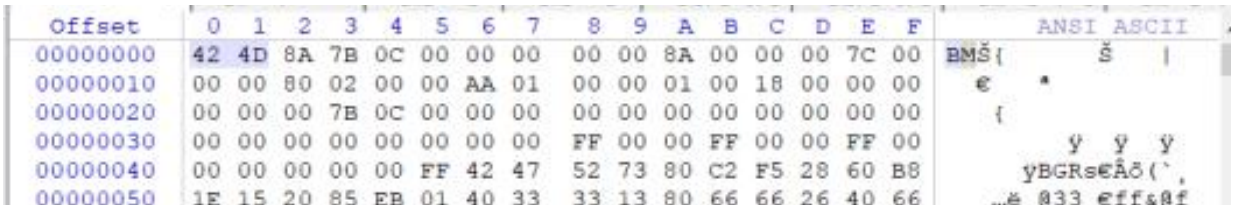
4. **BMP** - This is the format used for images.

Its General File signature is as follows :

42 4D		BM
	BMP, DIB	Windows (or device-independent) bitmap image
		NOTE: Bytes 2-5 contain the file length in little-endian order.

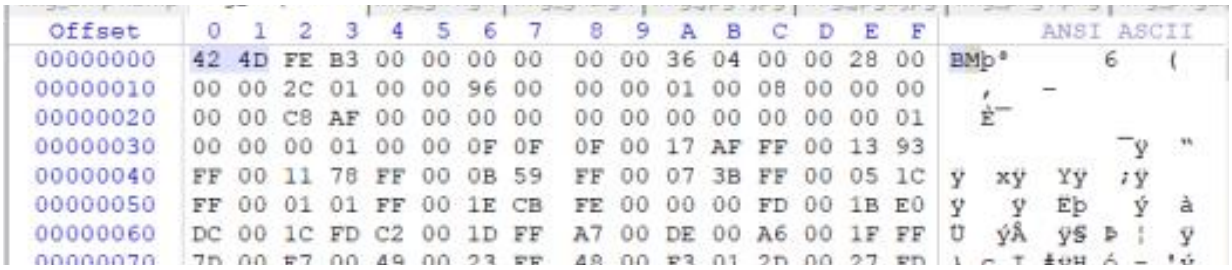
We now take two sample files and proceed with finding patterns in them.

First few bits of file 1 :



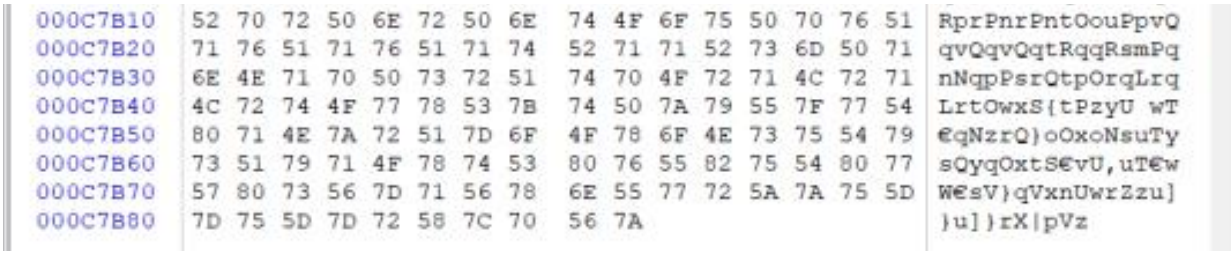
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	42	4D	8A	7B	0C	00	00	00	00	00	8A	00	00	00	7C	00	BMŠ{ Š |
00000010	00	00	80	02	00	00	AA	01	00	00	01	00	18	00	00	00	€ ª
00000020	00	00	00	7B	0C	00	00	00	00	00	00	00	00	00	00	00	{
00000030	00	00	00	00	00	00	00	00	FF	00	00	FF	00	00	FF	00	ÿ ÿ ÿ
00000040	00	00	00	00	00	FF	42	47	52	73	80	C2	F5	28	60	B8	ÿBGRs€Âõ(`,
00000050	1E	15	20	85	EB	01	40	33	33	13	80	66	66	26	40	66	…ë @33 €ff&@f

First Few bits of file 2 :



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	42	4D	FE	B3	00	00	00	00	00	00	36	04	00	00	28	00	BM³ 6 (
00000010	00	00	2C	01	00	00	96	00	00	00	01	00	08	00	00	00	, –
00000020	00	00	C8	AF	00	00	00	00	00	00	00	00	00	00	00	01	È¯
00000030	00	00	00	01	00	00	0F	0F	0F	00	17	AF	FF	00	13	93	¯ÿ "
00000040	FF	00	11	78	FF	00	0B	59	FF	00	07	3B	FF	00	05	1C	ÿ xÿ Yÿ ;ÿ
00000050	FF	00	01	01	FF	00	1E	CB	FE	00	00	00	FD	00	1B	E0	ÿ ÿ Ëþ ý à
00000060	DC	00	1C	FD	C2	00	1D	FF	A7	00	DE	00	A6	00	1F	FF	Ü ýÂ ÿ§ Þ ¦ ÿ
00000070	7D	00	E7	00	49	00	23	FF	48	00	E3	01	2D	00	27	FD	} ç I #ÿH ã - 'ý

Last few bits of file 1 :



000C7B10	52	70	72	50	6E	72	50	6E	74	4F	6F	75	50	70	76	51	RprPnrPntOouPpvQ
000C7B20	71	76	51	71	76	51	71	74	52	71	71	52	73	6D	50	71	qvQqvQqtRqqRsmPq
000C7B30	6E	4E	71	70	50	73	72	51	74	70	4F	72	71	4C	72	71	nNqpPsrQtpOrqLrq
000C7B40	4C	72	74	4F	77	78	53	7B	74	50	7A	79	55	7F	77	54	LrtOwxS{tPzyU wT
000C7B50	80	71	4E	7A	72	51	7D	6F	4F	78	6F	4E	73	75	54	79	€qNzrQ}oOxoNsuTy
000C7B60	73	51	79	71	4F	78	74	53	80	76	55	82	75	54	80	77	sQyqOxtS€vU,uT€w
000C7B70	57	80	73	56	7D	71	56	78	6E	55	77	72	5A	7A	75	5D	W€sV}qVxnUwrZzu]
000C7B80	7D	75	5D	7D	72	58	7C	70	56	7A							}u]}rX|pVz

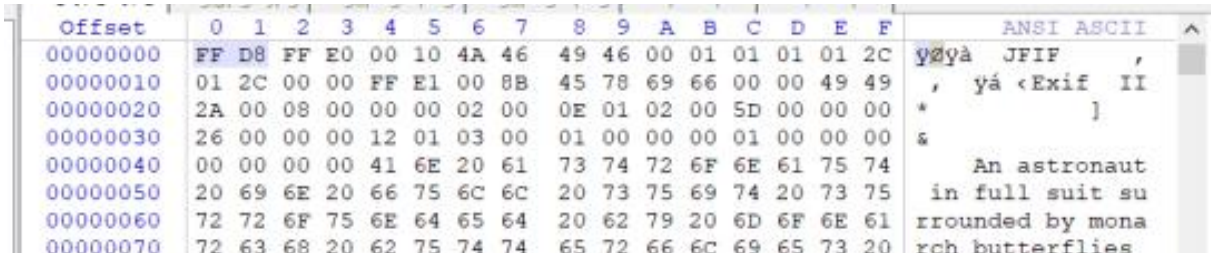
We can notice here as well that the pattern for BMP format follows.

5. **PNG** - This is the format used for storing Image Files.

Its General File signature is as follows :

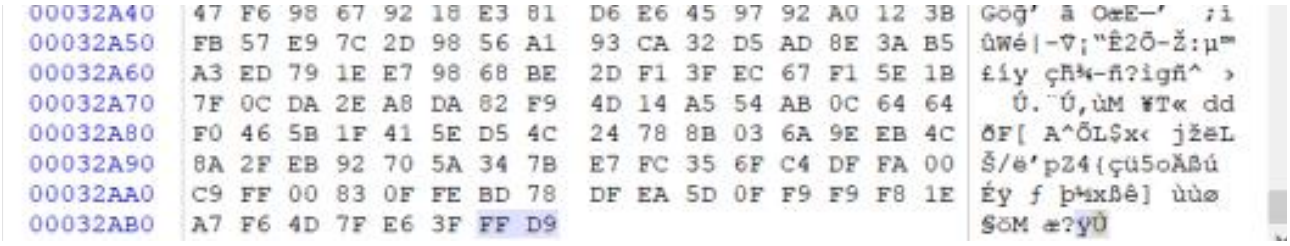
FF D8		ÿØ
	JPE, JPEG, JPG	Generic JPEGimage file
		Trailer: FF D9 (ÿÙ)

The two different files when viewed under a hexadecimal editor are as follows :
First few bits of file 1 :



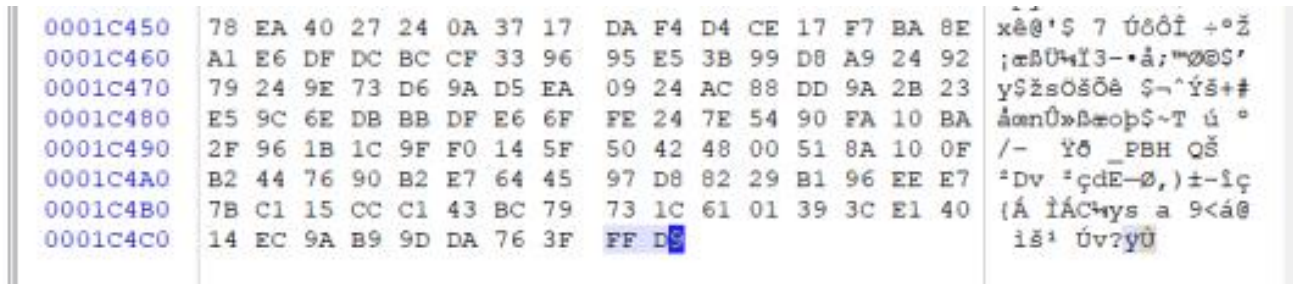
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	01	2C	ÿØÿà JFIF ,
00000010	01	2C	00	00	FF	E1	00	8B	45	78	69	66	00	00	49	49	, ÿá ‹Exif II
00000020	2A	00	08	00	00	00	02	00	0E	01	02	00	5D	00	00	00	*]
00000030	26	00	00	00	12	01	03	00	01	00	00	00	01	00	00	00	&
00000040	00	00	00	00	41	6E	20	61	73	74	72	6F	6E	61	75	74	An astronaut
00000050	20	69	6E	20	66	75	6C	6C	20	73	75	69	74	20	73	75	in full suit su
00000060	72	72	6F	75	6E	64	65	64	20	62	79	20	6D	6F	6E	61	rrounded by mona
00000070	72	63	68	20	62	75	74	74	65	72	66	6C	69	65	73	20	rch butterflies

First Few bits of file 2 :



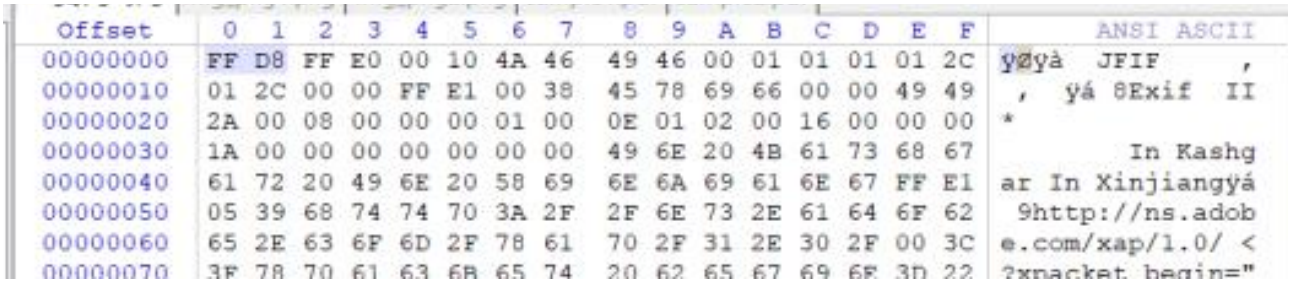
00032A40	47	F6	98	67	92	18	E3	81	D6	E6	45	97	92	A0	12	3B	Gög' ã OæE–' ;
00032A50	FB	57	E9	7C	2D	98	56	A1	93	CA	32	D5	AD	8E	3A	B5	ûWé|-˜V¡"Ê2Õ-Ž:µ
00032A60	A3	ED	79	1E	E7	98	68	BE	2D	F1	3F	EC	67	F1	5E	1B	£íy çh¾-ñ?ìgñ^ ›
00032A70	7F	0C	DA	2E	A8	DA	82	F9	4D	14	A5	54	AB	0C	64	64	Ú. ¨Ú‚ùM ¥T« dd
00032A80	F0	46	5B	1F	41	5E	D5	4C	24	78	8B	03	6A	9E	EB	4C	ðF[A^ÕL$x‹ jžëL
00032A90	8A	2F	EB	92	70	5A	34	7B	E7	FC	35	6F	C4	DF	FA	00	Š/ë'pZ4{çü5oÄßú
00032AA0	C9	FF	00	83	0F	FE	BD	78	DF	EA	5D	0F	F9	F9	F8	1E	Éÿ ƒ þ½xßê] ùùø
00032AB0	A7	F6	4D	7F	E6	3F	FF	D9									§öM æ?ÿÙ

Last few bits of file 1 :



0001C450	78	EA	40	27	24	0A	37	17	DA	F4	D4	CE	17	F7	BA	8E	xê@'$ 7 ÚôÔÎ ÷ºŽ
0001C460	A1	E6	DF	DC	BC	CF	33	96	95	E5	3B	99	D8	A9	24	92	¡æßÜ¼Ï3–•å;™Ø©$'
0001C470	79	24	9E	73	D6	9A	D5	EA	09	24	AC	88	DD	9A	2B	23	y$žsÖšÕê $¬ˆÝš+#
0001C480	E5	9C	6E	DB	BB	DF	E6	6F	FE	24	7E	54	90	FA	10	BA	åœnÛ»ßæoþ$~T ú º
0001C490	2F	96	1B	1C	9F	F0	14	5F	50	42	48	00	51	8A	10	0F	/– Ÿð _PBH QŠ
0001C4A0	B2	44	76	90	B2	E7	64	45	97	D8	82	29	B1	96	EE	E7	²Dv ²çdE–Ø‚)±–îç
0001C4B0	7B	C1	15	CC	C1	43	BC	79	73	1C	61	01	39	3C	E1	40	{Á ÌÁC¼ys a 9<á@
0001C4C0	14	EC	9A	B9	9D	DA	76	3F	FF	D9							ìš¹ Úv?ÿÙ

Last few bits of file 2



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	01	2C	ÿØÿà JFIF ,
00000010	01	2C	00	00	FF	E1	00	38	45	78	69	66	00	00	49	49	, ÿá 8Exif II
00000020	2A	00	08	00	00	00	01	00	0E	01	02	00	16	00	00	00	*
00000030	1A	00	00	00	00	00	00	00	49	6E	20	4B	61	73	68	67	In Kashg
00000040	61	72	20	49	6E	20	58	69	6E	6A	69	61	6E	67	FF	E1	ar In Xinjiangÿá
00000050	05	39	68	74	74	70	3A	2F	2F	6E	73	2E	61	64	6F	62	9http://ns.adob
00000060	65	2E	63	6F	6D	2F	78	61	70	2F	31	2E	30	2F	00	3C	e.com/xap/1.0/ <
00000070	3F	78	70	61	63	6B	65	74	20	62	65	67	69	6E	3D	22	?xpacket begin="

We have until now observer many file formats and have noticed a pattern which seem to exist in the documents of the same format towards the beginning and the end, but this pattern is different across different patterns.

This serves an important role in the file management and thus in digital forensics. This is how the operating systems and hence forensic experts identify the format of the files and label them as pdf, doc, pages, png, etc.

CONCLUSION

In this lab experiments, we have dealt with file formats namely how they are identified by the file management system and also thus by the operating systems which provide useful functionalities for ease of forensic analysis.