Digital Forensics - Lab 7

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

Aadhitya Swarnesh

- 23 September 2021

Question 1 :

Text editing tools such as Notepad, Wordpad, MS Word provide additional formatting information to text files. 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? How can you tell what type of file you are looking at by what vim or WinHex shows in the Hex window?

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. **Pages** - This is the format used by Apple's Word processing documents.

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

da 1.pages | Lab 6.pages

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	00	00	00	00	37	BC	29	53	88	82	PK 7¼)S^,
00000010	7A	00	AF	24	00	00	AF	24	00	00	16	00	00	00	44	61	z ¯$ ¯$ Da
00000020	74	61	2F	68	65	61	64	65	72	2D	63	72	63	2D	32	34	ta/header-crc-24
00000030	2E	70	6E	67	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	.png‰PNG
00000040	49	48	44	52	00	00	01	B8	00	00	00	96	08	02	00	00	IHDR ¸ –
00000050	01	54	7E	3A	80	00	00	00	19	74	45	58	74	53	6F	66	T~:€ tEXtSof
00000060	74	77	61	72	65	00	41	64	6F	62	65	20	49	6D	61	67	tware Adobe Imag
00000070	65	52	65	61	64	79	71	C9	65	3C	00	00	24	51	49	44	eReadyqÉe< $QID
00000080	41	54	78	DA	EC	56	CB	8D	83	30	10	8D	51	0E	70	40	ATxÚìVË ƒ0 Q p@
00000090	50	C2	76	40	09	50	0A	74	00	15	F0	A9	80	0E	68	05	PÂv@ P t ð©€ h
000000A0	68	00	6E	D9	23	25	20	71	E1	04	79	C2	12	6B	8D	13	h nÙ#% qá yÂ k
000000B0	4C	90	92	DD	68	F3	0E	96	EC	8C	C6	6F	E6	CD	33	61	L ’Ýhó -ìŒÆoæÍ3a
000000C0	F3	3C	9F	FE	3C	B4	D3	3B	E0	BC	3F	94	31	E6	38	8E	ó<Ÿþ<´Ó;à¼?”1æ8Ž
000000D0	E7	79	B6	6D	F3	93	AF	05	6D	DB	86	61	F8	54	96	EC	çy¶mó“¯ mÛ†aøT–ì

da 1.pages | Lab 6.pages

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	00	00	00	00	6C	59	37	53	B6	54	PK lY7S¶T
00000010	16	DD	91	23	00	00	91	23	00	00	12	00	00	00	49	6E	Ý‘# ‘# In
00000020	64	65	78	2F	44	6F	63	75	6D	65	6E	74	2E	69	77	61	dex/Document.iwa
00000030	00	8D	23	00	C9	7F	68	56	08	01	12	52	08	90	4E	12	# É hV R N
00000040	03	01	00	05	18	BF	0C	22	07	0A	03	0A	01	2E	18	01	¿ " .
00000050	22	09	01	09	F0	C2	2F	10	01	18	01	22	0B	0A	05	0A	" ðÂ/ "
00000060	03	0F	01	11	10	03	18	00	2A	24	95	9E	02	96	9E	02	*$•ž –ž
00000070	97	9E	02	81	A0	0D	98	9E	02	A7	95	02	99	9E	02	AD	—ž ž §• ™ž –
00000080	9A	02	A2	9C	02	97	9B	02	8D	9B	02	9A	9E	02	12	04	š ¢œ —› › šž
00000090	08	99	9E	02	1A	04	08	A2	9C	02	22	04	08	8D	9B	02	™ž ¢œ " ›

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

da 1.pages | Lab 6.pages

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0005AEB0	50	4B	01	02	3E	00	14	00	00	00	00	00	0D	9E	25	53	PK > ž%S
0005AEC0	ED	64	6D	09	24	00	00	00	24	00	00	00	1B	00	00	00	ídm $ $
0005AED0	00	00	00	00	00	00	00	00	00	00	64	7E	01	00	4D	65	d~ Me
0005AEE0	74	61	64	61	74	61	2F	44	6F	63	75	6D	65	6E	74	49	tadata/DocumentI
0005AEF0	64	65	6E	74	69	66	69	65	72	50	4B	01	02	3E	00	14	dentifierPK >
0005AF00	00	00	00	00	00	0D	9E	25	53	94	18	F1	31	0C	01	00	ž%S” ñ1
0005AF10	00	0C	01	00	00	22	00	00	00	00	00	00	00	00	00	00	"
0005AF20	00	00	00	D5	7E	01	00	4D	65	74	61	64	61	74	61	2F	Õ~ Metadata/
0005AF30	42	75	69	6C	64	56	65	72	73	69	6F	6E	48	69	73	74	BuildVersionHist
0005AF40	6F	72	79	2E	70	6C	69	73	74	50	4B	01	02	3E	00	14	ory.plistPK >
0005AF50	00	00	00	00	00	FC	BB	29	53	56	F2	27	A9	81	EA	03	ü»)SVò'© ê
0005AF60	00	81	EA	03	00	0B	00	00	00	00	00	00	00	00	00	00	ê
0005AF70	00	00	00	35	80	01	00	70	72	65	76	69	65	77	2E	6A	5€ preview.j
0005AF80	70	67	50	4B	01	02	3E	00	14	00	00	00	00	00	FC	BB	pgPK > ü»
0005AF90	29	53	48	00	8A	4E	7D	06	00	00	7D	06	00	00	11	00	)SH ŠN} }
0005AFA0	00	00	00	00	00	00	00	00	00	00	00	00	F3	6A	05	00	ój
0005AFB0	70	72	65	76	69	65	77	2D	6D	69	63	72	6F	2E	6A	70	preview-micro.jp
0005AFC0	67	50	4B	01	02	3E	00	14	00	00	00	00	00	FC	BB	29	gPK > ü»)
0005AFD0	53	06	20	A8	FC	E4	39	00	00	E4	39	00	00	0F	00	00	S ¨üä9 ä9
0005AFE0	00	00	00	00	00	00	00	00	00	00	00	B3	71	05	00	70	³q p
0005AFF0	72	65	76	69	65	77	2D	77	65	62	2E	6A	70	67	50	4B	review-web.jpgPK
0005B000	05	06	00	00	00	00	0F	00	0F	00	26	04	00	00	D8	AB	& Ø«
0005B010	05	00	00	00													

da 1.pages | Lab 6.pages

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00043F30	D1	FD	5C	4A	24	00	00	00	24	00	00	00	1B	00	00	00	Ñý\J$ $
00043F40	00	00	00	00	00	00	00	00	00	00	20	AD	01	00	4D	65	- Me
00043F50	74	61	64	61	74	61	2F	44	6F	63	75	6D	65	6E	74	49	tadata/DocumentI
00043F60	64	65	6E	74	69	66	69	65	72	50	4B	01	02	3E	00	14	dentifierPK >
00043F70	00	00	00	00	00	A8	62	15	53	63	D0	BD	B1	17	01	00	¨b ScÐ½±
00043F80	00	17	01	00	00	22	00	00	00	00	00	00	00	00	00	00	"
00043F90	00	00	00	91	AD	01	00	4D	65	74	61	64	61	74	61	2F	‘- Metadata/
00043FA0	42	75	69	6C	64	56	65	72	73	69	6F	6E	48	69	73	74	BuildVersionHist
00043FB0	6F	72	79	2E	70	6C	69	73	74	50	4B	01	02	3E	00	14	ory.plistPK >
00043FC0	00	00	00	00	00	FD	BA	35	53	79	12	DA	23	FE	41	02	ý°5Sy Ú#þA
00043FD0	00	FE	41	02	00	0B	00	00	00	00	00	00	00	00	00	00	þA
00043FE0	00	00	00	FC	AE	01	00	70	72	65	76	69	65	77	2E	6A	ü® preview.j
00043FF0	70	67	50	4B	01	02	3E	00	14	00	00	00	00	00	B0	AA	pgPK > °ª
00044000	35	53	4A	2C	6D	CB	D5	06	00	00	D5	06	00	00	11	00	5SJ,mËÕ Õ
00044010	00	00	00	00	00	00	00	00	00	00	00	00	37	F1	03	00	7ñ
00044020	70	72	65	76	69	65	77	2D	6D	69	63	72	6F	2E	6A	70	preview-micro.jp
00044030	67	50	4B	01	02	3E	00	14	00	00	00	00	00	FD	BA	35	gPK > ý°5
00044040	53	44	E4	59	71	CD	31	00	00	CD	31	00	00	0F	00	00	SDäYqÍ1 Í1
00044050	00	00	00	00	00	00	00	00	00	00	00	4F	F8	03	00	70	Oø p
00044060	72	65	76	69	65	77	2D	77	65	62	2E	6A	70	67	50	4B	review-web.jpgPK
00044070	05	06	00	00	00	00	49	00	49	00	11	16	00	00	5D	2A	I I]*
00044080	04	00	00	00													

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

Let us see another file format :

2. **RTF (Rich Text Format)** - This is the format used as a more advanced version of the traditional txt files.

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

Exercise6.rtf | Exercise7.rtf

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	7B	5C	72	74	66	31	5C	61	64	65	66	6C	61	6E	67	31	{\rtf1\adeflang1
00000010	30	32	35	5C	61	6E	73	69	5C	61	6E	73	69	63	70	67	025\ansi\ansicpg
00000020	31	32	35	32	5C	75	63	31	5C	61	64	65	66	66	30	5C	1252\uc1\adeff0\
00000030	64	65	66	66	30	5C	73	74	73	68	66	64	62	63	68	33	deff0\stshfdbch3
00000040	31	35	30	35	5C	73	74	73	68	66	6C	6F	63	68	33	31	1505\stshfloch31
00000050	35	30	36	5C	73	74	73	68	66	68	69	63	68	33	31	35	506\stshfhich315
00000060	30	36	5C	73	74	73	68	66	62	69	30	5C	64	65	66	6C	06\stshfbi0\defl
00000070	61	6E	67	31	36	33	39	33	5C	64	65	66	6C	61	6E	67	ang16393\deflang
00000080	66	65	31	36	33	39	33	5C	74	68	65	6D	65	6C	61	6E	fe16393\themelan

Exercise6.rtf | Exercise7.rtf

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	7B	5C	72	74	66	31	5C	61	64	65	66	6C	61	6E	67	31	{\rtf1\adeflang1
00000010	30	32	35	5C	61	6E	73	69	5C	61	6E	73	69	63	70	67	025\ansi\ansicpg
00000020	31	32	35	32	5C	75	63	31	5C	61	64	65	66	66	30	5C	1252\uc1\adeff0\
00000030	64	65	66	66	30	5C	73	74	73	68	66	64	62	63	68	33	deff0\stshfdbch3
00000040	31	35	30	35	5C	73	74	73	68	66	6C	6F	63	68	33	31	1505\stshfloch31
00000050	35	30	36	5C	73	74	73	68	66	68	69	63	68	33	31	35	506\stshfhich315
00000060	30	36	5C	73	74	73	68	66	62	69	30	5C	64	65	66	6C	06\stshfbi0\defl
00000070	61	6E	67	31	36	33	39	33	5C	64	65	66	6C	61	6E	67	ang16393\deflang
00000080	66	65	31	36	33	39	33	5C	74	68	65	6D	65	6C	61	6E	fe16393\themelan

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

0000F910	0D	0A	30	30	30	30	30	30	30	30	30	30	30	30	30	30	00000000000000
0000F920	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
0000F930	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
0000F940	30	30	30	31	30	35	30	30	30	30	30	30	30	30	30	30	0001050000000000
0000F950	30	30	7D	7D													00}}

00010C00	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
00010C10	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
00010C20	30	30	30	30	30	30	30	30	30	30	30	30	30	30	31	30	0000000000000010
00010C30	35	30	30	30	30	30	30	30	30	30	30	30	30	7D	7D		5000000000000}}

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

Let us see for yet another file format :

3. **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.

4. **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.

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.

Question 2 :

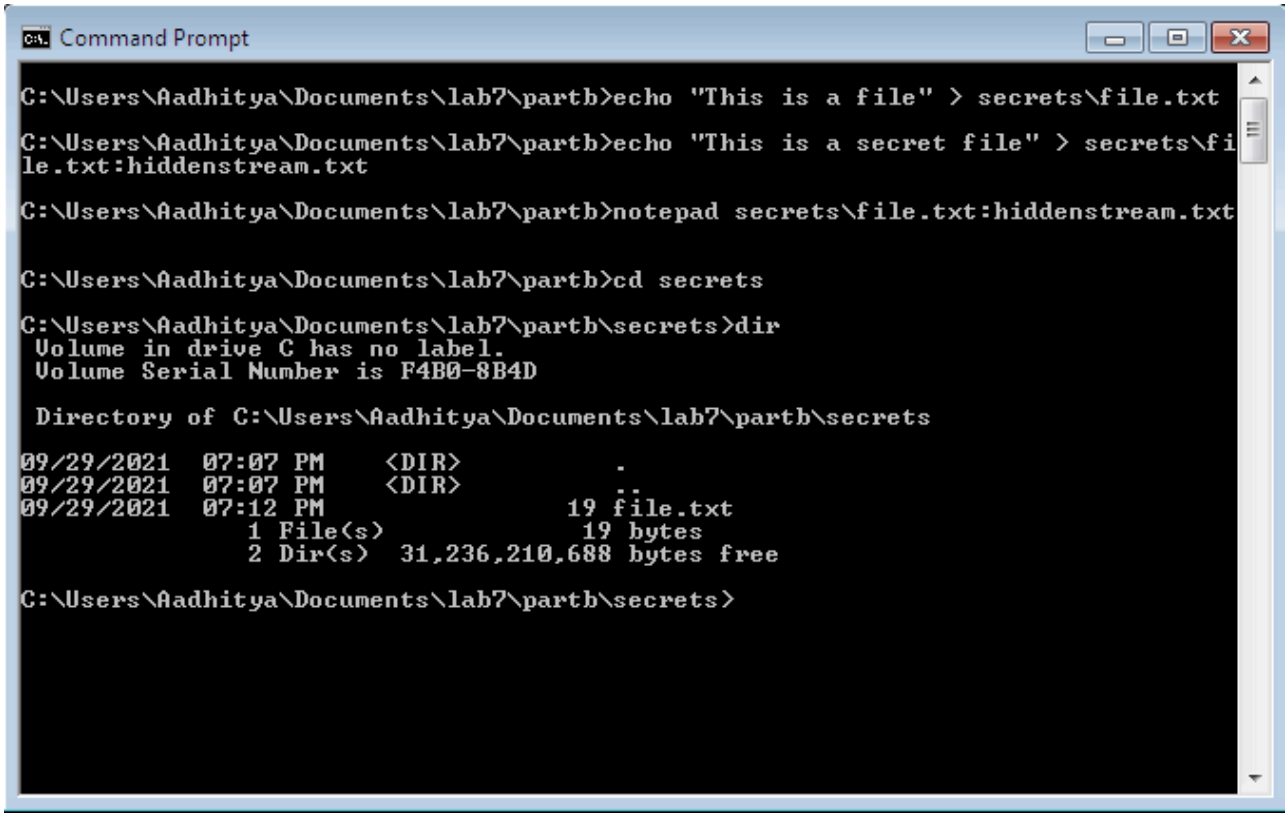
NTFS hidden streams - Explore the hidden streams in a NTFS file system and demonstrate the creation, and viewing such hidden files.

Use the Microsoft streams to view such hidden streams associated with the files which are otherwise hidden and is invisible to the folders and the command line scripts.

Hidden streams are a feature in NTFS file systems which allows for the storage of secret streams of data files which are essentially invisible unsells looked for specifically. They are called ADS or Alternate Data Streams.

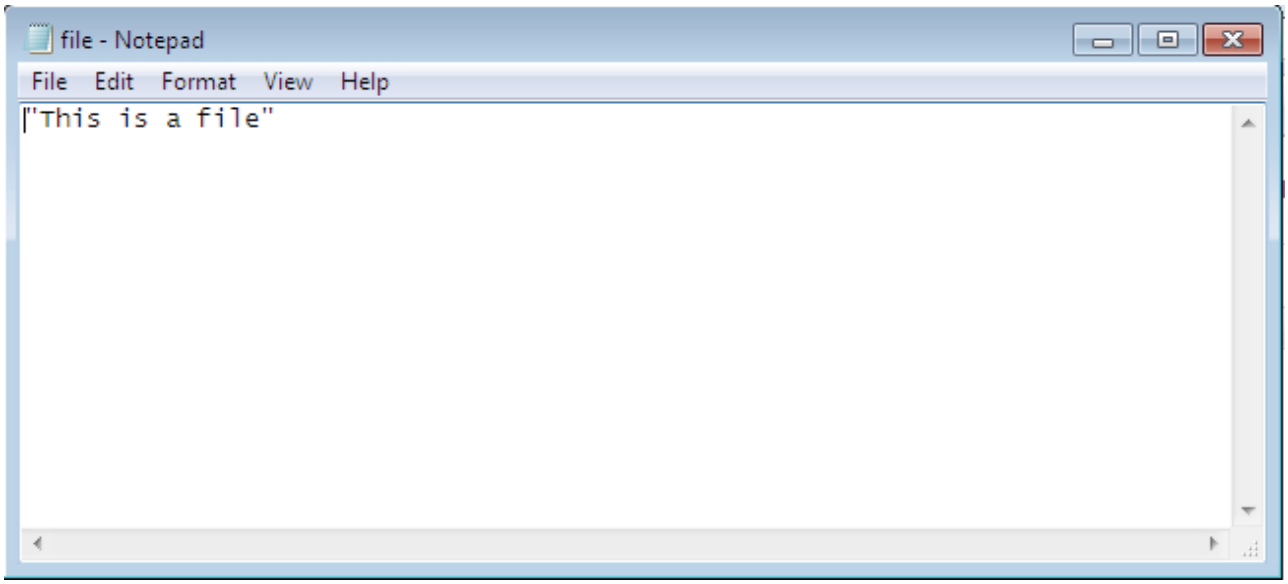
In this lab experiment, we will essentially demonstrate the creation of such streams and also demonstrate what it takes to identify such files.

In the following diagram, we create a file called "**file.txt**" with some text, and then we create an alternate stream of the file **"hidden stream.txt"** with different text.

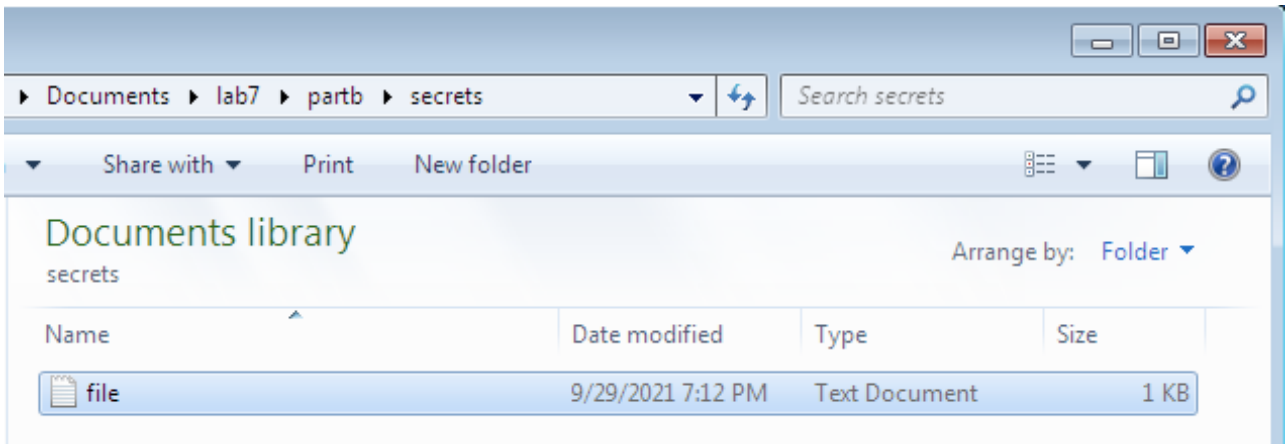


We can notice here that the "**dir**" command has failed to retrieve or display or even acknowledge the presence of the alternate stream.

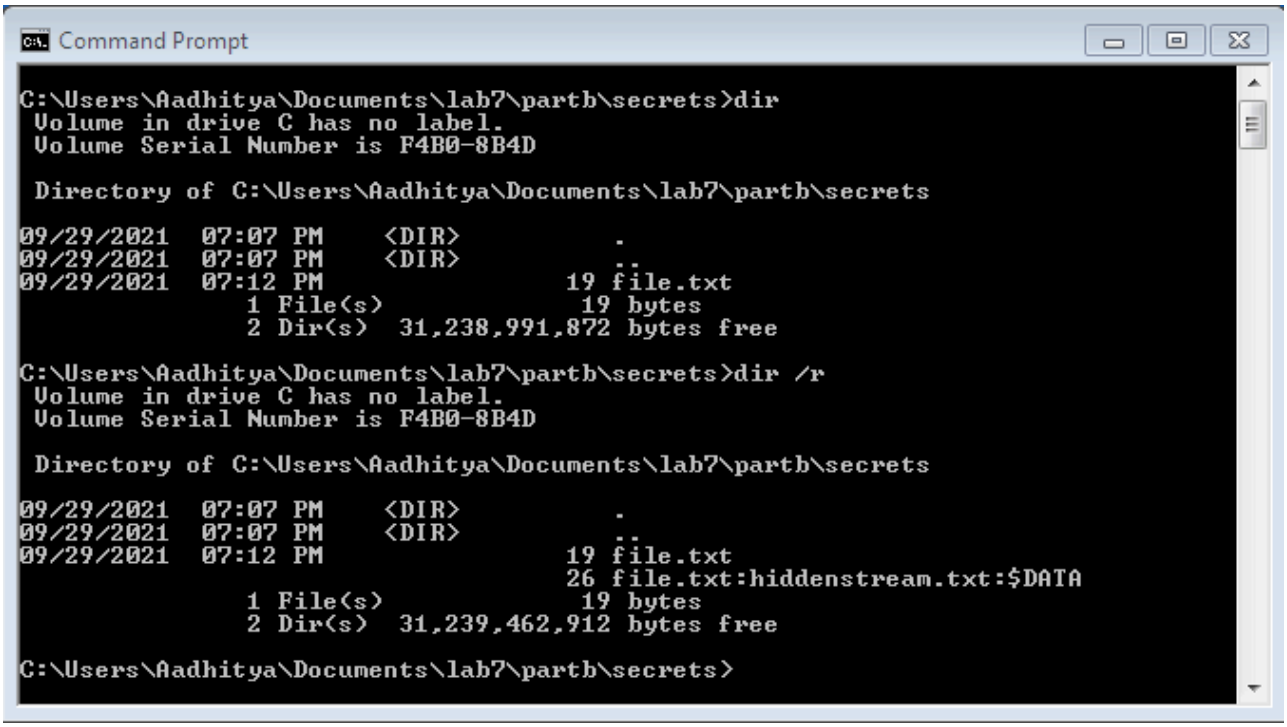
This is the file which is visible from the normal explorer :



We cannot access the hidden files using the explorer window as it is not visible there or in any other command line tools like "**dir**". For example take a look at the image of the folder, we can notice that the alternate streams are invisible here.



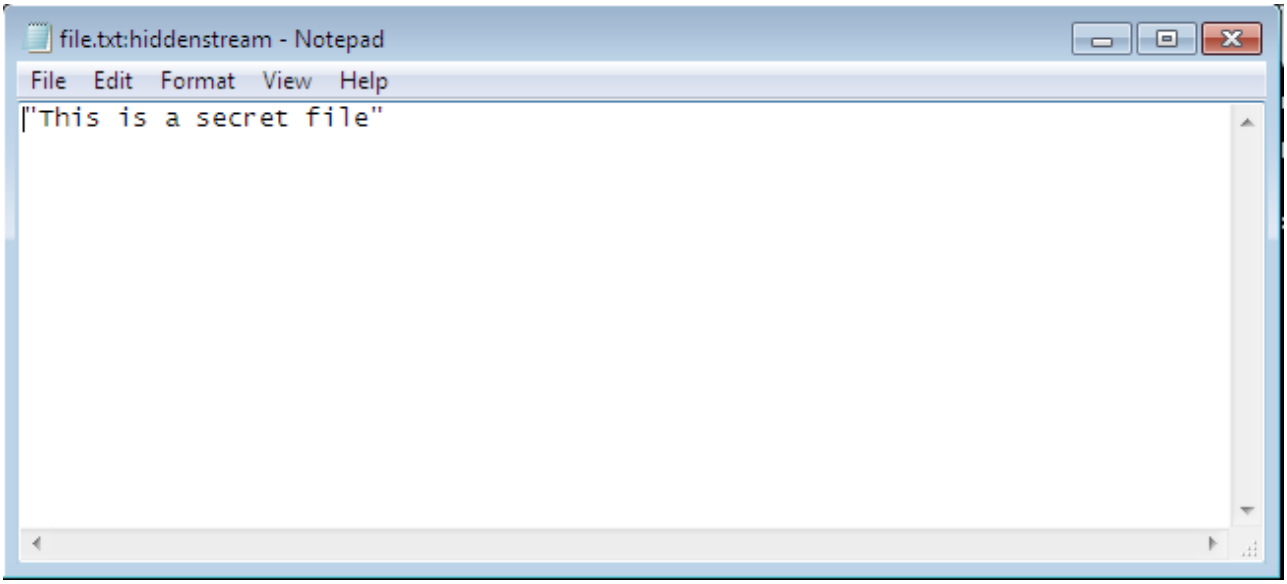
But we can access these file by using the "**dir /r**" command which displays the hidden files. This is different from the "**dir**" command executed and shown earlier as it did not acknowledge the alternate streams but when used with the "/**r**" flag, it does so.



We can also use the command in the earlier diagram to view the secret file :

>> notepad secrets\file.txt:hiddenstream.txt

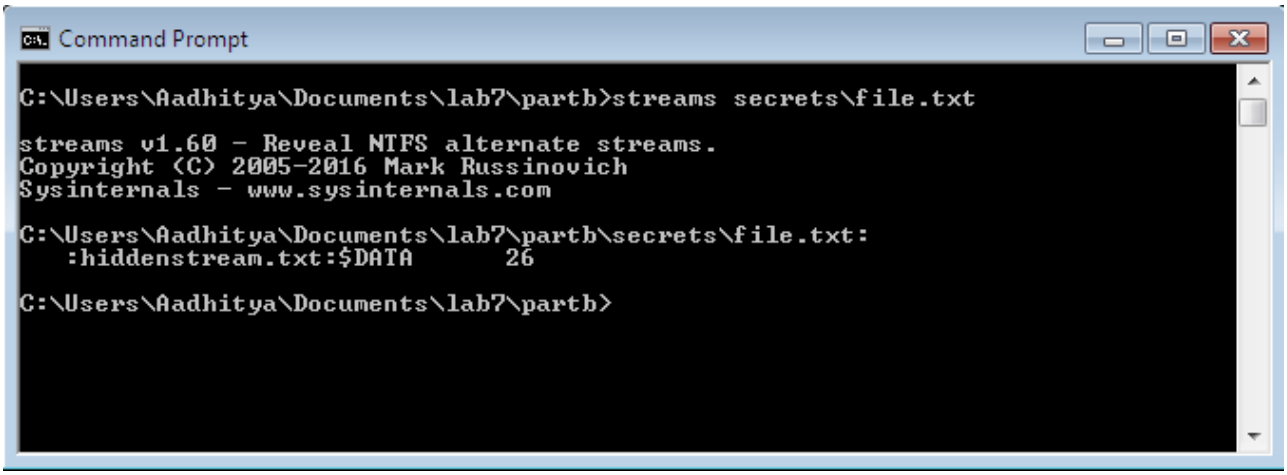
This command is used to display or open the hidden stream associated with the file. It opens it in the notepad application, and it looks as follows :



The presence of secret files can also be found and identified by using the “secrets” command line tool which is available through the Microsoft website —

https://docs.microsoft.com/en-us/sysinternals/downloads/streams

This tool when used in our case produces output as follows :



This command was successful in identifying the hidden streams associated with a particular file. It can also be extended to use with folders, 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.

We have also dealt with hidden data streams in the NTFS file systems, and have discussed ways in which to track them and also to open them. These are of almost importance when we consider the field of forensic analysis as these are needed to figure out evidence from a perpetrators computer system which could act as evidence in solving crimes.