Bibliography details

Name of the Serial/Publication: Veritas

Volume No.: 2

Issue No.: 1

Month & Year of publication: August 2022

Page numbers: Research Articles (39-42)

Title of Article: Detection of hidden files and find out its hidden mechanism

CONTRIBUTOR (s)

- 1. Ms. Jocelyn Kunju John
- 2. Ms. Catherine Maria Johny
- 3. Mr. Thomas Prince Kuruppen Parambil
- 4. Mr. Justin Babu

DETECTION OF HIDDEN FILES AND FINDING OUT ITS HIDDEN MECHANISM

Ms. Jocelyn Kunju John Ms. Catherine Maria Johny Mr. Thomas Prince Kuruppen Parambil Mr. Justin Babu

INTRODUCTION

Digital forensics, on a broad spectrum, can be defined as a complete understanding and analysis of digital data present on the computer or laptop. Digital forensics can also be explained as the investigation of digital artefacts from the scene of the crime for certain facts and information. It deals with the recovery of legal evidence within the digital devices and the digital storage media. The procedure is carried out by the usage of digital tools, which enables us to retrieve the desired information. Imaging is a technique where the bit-by-bit storage space along with the data present in the device is replicated onto another device. The suspect device is not used for further analysis, but its image file is used.

AIM AND OBJECTIVES OF THE STUDY

•To determine the hidden data in a device.

•To understand the mechanism behind the hidden data and thus deduce a technique to recognize the same.

•To identify and study if the already existing tools could detect the hidden data within the computer system.

METHODOLOGY

An external storage device (SanDisk Cruzer Blade Pen drive) was formatted using the New Technology File System (NTFS). Ten files with different file extensions were selected and copied onto the USB device.

The 10 files of different file formats were as follows:

- 1. .AVI
- 2. .DOC
- 3. .DOCX
- 4. .MP3
- 5. .MP4
- 6. .PDF
- 7. .PNG
- 8. JPEG
- 9. .WAV
- 10..TXT

Using different hiding methods, such as lockdir, lockbox, etc., the data were hidden, which was followed by subjecting the pen drive to the imaging process in order to find the hidden data.

FINDINGS

From the study, it could be concluded that using imaging tools, it is possible to find the hidden data.

With the properties hiding method and hiding using different software, the files were detected without modifications to the metadata and hash values.

With the file signature and file extension change, there was a change in the metadata as well as the hash value.

The file signature detected in the image file was not of the original file format but the one that was changed to. When the details of the files are checked, the details correspond to

the details of the original file format. This proves that the file has been altered.

Hence, no matter what the data is or how it is hidden by cybercriminals, it can be recovered and used as court evidence.

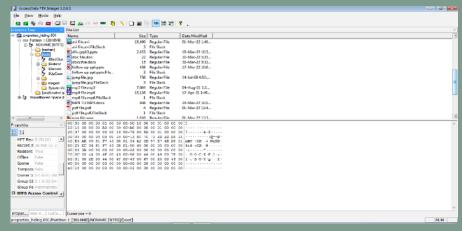


Fig 1. AccessData FTK Imager screenshot

🕹 HexEdit															
File Edi	File Edit View Select Operations Boolumerks NTF5 Streams Tools History Window Help														
1	- 🗔	1	a 🔒	P	~ 🛛	8	3 🖻	0	Q Q 🗶 🐘	541	a 🖁 🕻	s 💊 📖	English	• 🕜 🕜	2
4 b 📆 pc	ffilendf	×											11		History # X
00000000			01.05	06 07	08 09	0a Ob	06 0d 1	le Df							' ୧୦ 🚳 🖳 🐉 🗞 ୧୫ ୧୬
00000000	25 50	44 45	2d 31	2e 35	Od Oa	25 b5	b5 b5 1	5.04	PDF-1.5. tunua.					^	
00000010		20 30			0d 0a	30 30		79 70	.1 0 objcc/Typ						
00000020		43 61	74 61		67 25			78 20	e/Catalog/Pages						
00000000	32 20	30 20	52 21	4c 61	Ge 67	20 65	6e 2d 3	55 53	2 0 R/Lang(en-US						
0000040	29 20	22 53	74 72	75 63	74 54	72 65	65 52 1	er or) /StructIreeRoo						
00000050	74 20	39 20	30 20	52 20	4d 61	72 eb	49 de 1	t6 6C	t 9 0 R/MarkInfo						
00000060	3c 3c	22 44	61 72	6D 65	64 20	74 72	75 65 3	Be Be	<c harked="" th="" truepo<=""><th></th><th></th><th></th><th></th><th></th><th></th></c>						
00000070	3e 3e	0d 0a	65 6e	64 65	62 6a	0d 0a	32 20	30 20	>>endobj2 0						
00000000	6f 62	6a 0d	0a 3c	3c 2f	54 79	70 65	2f 50 (E1 67	obj< <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>						
00000000		2# 43	6f 75	6e 74	20 31	2f 4b	69 64 1	73 Sb	es/Count 1/Kids[
0000000		20 30	20 52	5d 20	3e 3e	Od Oa	65 6e I	54 <u>65</u>	3 0 R] >>endo						
соссовьс		0d Oa		30 20	6f 62	6a 0d	Ga Se :	ic 2f	bj3 0 obj< </th <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>						
00000000		70 65		61 67	65 2£			6e 74	Type/Page/Parent						
000000d0		20 30	20 52	2f 52	65 73	6f 75		65 73	2 0 R/Resources						History Olume Navigator
000000e0		2£ 46	61 6e	74 3c	36 22			50 20	< <th></th> <th></th> <th></th> <th></th> <th></th> <th>Selection # x</th>						Selection # x
0000010		38 38	28 45		47 53	74 61	74 65 3		RSS/Estimitedd						
00000100		53 37			20 52		2f 50		/987 7 0 Roo/Reo						🏢 🗵 🏢 🖬 📓 📓 📓
00000110		65 74		50 44		54 65	78 74 3		cSet[/DDF/Text/I						Information
00000120		67 65	42 21		61 67	65 43		6d 61	mageB/ImageC/Ima						Total Size No selection bytes
		49 50	20 Je	Je 2f	4d 65	64 69			geI] >>/MediaBox						Fragments Ne selection
C0000140 C0000150		50 Z0 60 74	30 Z0 65 66	36 31 74 73	3Z 20 20 34	37 39 20 30		25 022	[0 0 612 792] / Contents 4 0 B/G						
00000150		75 70			79 70	65 21	47 72		roupce/Type/Grou						f Details
00000170		53 20			73 70	61 72		63 79	p/S/Transparency						· Detais ·
00000180		53 25	44 65	76 69	53 65	52 47		1e 2f	/CS/DeviceRGB>>/						
00000190		62 73	24 53	27 53	74 72	75 63		1 72	Tabs/S/StructPar						
C00001e0		74 73	20 30	30 30	Od Da	65 60		12 64	ents (>>endobj						
000001b0		34 20			6a 0d	04 30	30 22		4 0 ski /Ei</th <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>						
000001c0		65 72			74 65	44 65	63 6g (lter/FlateDecode						
000001d0		65 Ge		€0 20		30 3e	Je Od I		/Length 250>>s						
000001e0	74 72	65 61		Ca 75		90 cb	6a c3		treammp RyAD.					-	here a letter with a
٠	_							_							Selection 🚰 File Attributes
Ready												4	Offset: 0000000	(0) Size: 0+00000c	2c (3,118): 3.04 KE Hex bytes, 16, Default ANSI OVR

Fig2. Hex Editor Neo screenshot

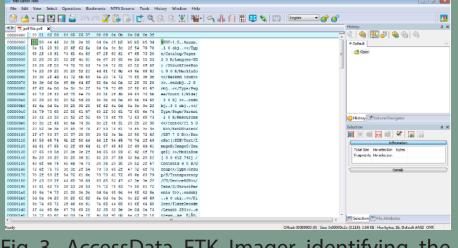


Fig 3. AccessData FTK Imager identifying the hidden PDF file.

REFERENCES:

- Guo, R., Wu, F., Li, Y., Zhu, R., & Sheng, K. (2015). The information hiding mechanism based on compressed document format. International Journal Of Computing Science And Mathematics, 6(1), 97. Retrieved from https:// doi.org/10.1504/ijcsm.2015.067547
- Cao, F., Qian, X., & An, B. (2020). Low-complexity reversible data hiding in encrypted image via MSB hierarchical coding and LSB compression. Multimedia Systems, 27(3), 317-330. Retrieved from https://doi.org/10.1007/s00530-020-00700-6
- Hassan, N. A., & Hijazi, R. (2017). Data hiding techniques in Windows OS. Syngress, 2, 23-43.
- Upguard.com. 2022. What is Digital Forensics? | Up-Guard. [online] Retrieved from https://www.upguard. com/blog/digital-forensics. [Accessed 13 April 2022]
- EasyTechJunkie. 2022. What Is a File Signature? (with picture). [online] Retrieved from https://www.easytech-junkie.com/what-is-a-file-signature.htm. [Accessed 13 April 2022].

DID YOU KNOW?

Which crime lab unit is responsible for examining body fluids and organs for the presence of drugs and poisons?

Answer: Toxicology Unit