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.

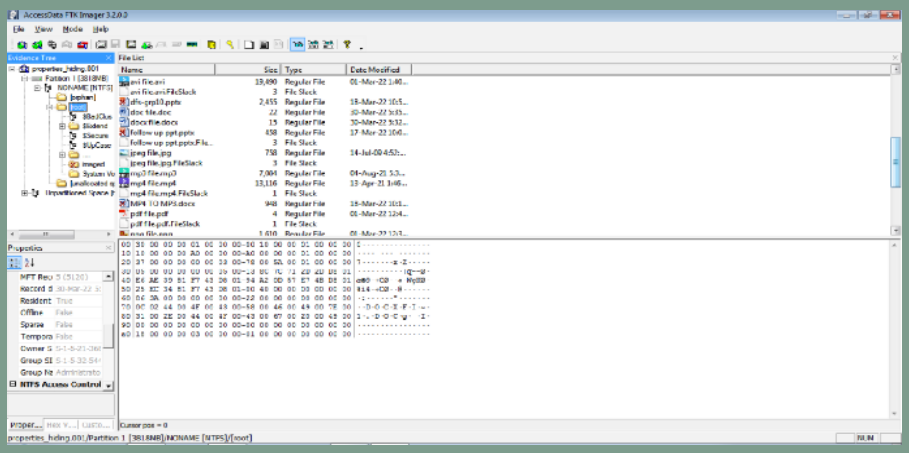

Fig 1. AccessData FTK Imager screenshot

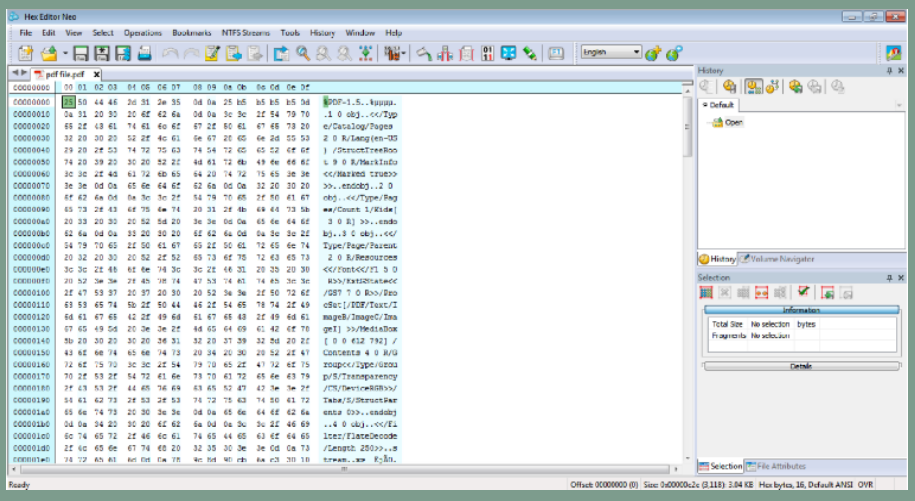

Fig2. Hex Editor Neo screenshot

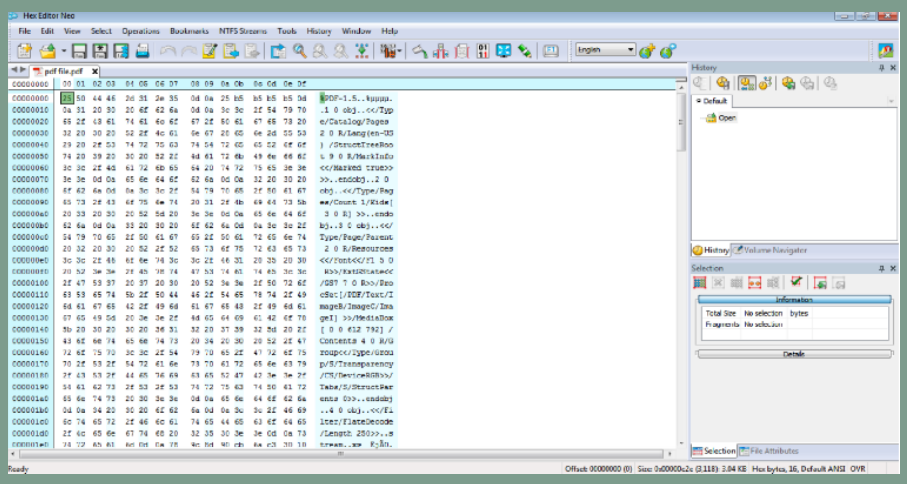

Fig 3. AccessData FTK Imager identifying the hidden PDF file.

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? | UpGuard. [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.easytechjunkie.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