

## **A Comparative Study of the Performance of Open-Source and Proprietary Disk Forensic Tools in Recovery of Anti-Forensically Doctored Data**

<sup>1</sup>Sonu Mandecha, <sup>2</sup>Kumarshankar Raychaudhuri, <sup>3</sup>M. George Christopher

<sup>1,2</sup>LNJN National Institute of Criminology and Forensic Science, Ministry of Home Affairs  
Govt. of India

<sup>3</sup>State Forensic Science Laboratory, Madiwala, Bengaluru, India

### **ABSTRACT**

Digital Forensics is the technique used for the investigation of crimes related to computers and other digital or electronic devices such as mobile phones, tablets etc. It includes different stages such as collection, extraction, preservation, examination, analysis and documentation of data from different digital storage devices such as hard disks, USB thumb drives, CDs, DVDs etc. In order to evade the digital forensic tools, the criminals or perpetrators use methods and techniques to hide the data or destroy the evidence, which is known as Anti-Forensics. In this research work, our aim is to use open-source and proprietary disk forensic tools to attempt in recovering anti-forensically doctored data. Various anti-forensic tools and techniques are used for hiding data items or manipulating their metadata properties, onto digital exhibits such as USB thumb drive. After performing anti-forensics, the exhibit is examined and analysed using different types of disk forensic tools in an effort to recover the traces of hidden and manipulated data items. Lastly, a comparative analysis is done to determine the relative performances of the disk forensic tools. The results would prove useful for forensic experts to apply appropriate forensic tools for recovering evidences efficiently even when anti-forensics have been done.

### **KEYWORDS**

Disk Forensic Tools, Anti-Forensically, Data Hiding, Autopsy, FTK Analyzer, Bit-shifting, Trail Obfuscation, File Signature Mismatch, Deleted Partition, File Encryption.

### **1 INTRODUCTION**

According to Dr. Debarati Halder and Dr. K. Jaishankar (2011), cybercrime is defined as “An act of offence committed against individuals or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as internet and mobile phones [1]. Cyber-crime can be committed using computer as a tool or target.

For investigation of the cyber-crime incidents, evidential data is identified and collected from computer systems and/or other digital storage media at crime scene or laboratory, scientifically examined and analysed using various software applications and hardware tools, so that it can be made admissible in the court of law. This entire process from the crime scene to the court room is defined as Digital Forensic Investigation [2,3]. The primary goal of digital forensics is to uncover data from various locations of the storage media or computer system, which might relate to the incident. However, in some cases, the precise location of the data might not be apparent and easy to find either for the investigator or the forensic tool being used for extraction [4]. This is because of the use of processes and techniques known as “Anti-Forensics”, which is used by criminals to hinder and the forensic processes and make them ineffective.

Anti-Forensics can be defined as the process of using tools and techniques to destroy, hide or tamper the existing data and metadata in such a manner so that it becomes difficult for computer forensic tools (CFTs) to unearth and extract them easily [14]. The primary aim of criminals using anti-forensic techniques is to tamper the evidences to such an extent so that they are not recoverable in their original state [5,12]. This makes the evidence acquisition phase highly complex and difficult. The common anti-forensic techniques include data erasure, data hiding, and manipulation of the metadata, data encryption, kernel-level rootkit and many more. With the emergence of open-source and free tools available online, the application of anti-forensics has got a boost, making it much easier and effective to execute them.

Over the years, researchers have proved the effectiveness and accuracy of various anti-forensics tools and techniques [6,7,8], making recovery of hidden or tampered data a major challenge for forensic examiners. Earlier, the main motive for using anti-forensic practices was to hide or manipulate evidences from the crime scene. However, in the new generation of anti-forensics, their target has been different digital forensic tools such as EnCase, Forensic Toolkit etc., which has inspired us to carry this research work. In this research, some open-source tools and techniques have been used for hiding, manipulating and tampering data and metadata items (apart from the conventional anti-forensic techniques such as deletion or erasure of data), after which an attempt have been made to recover them in their original state, with the help of both open-source and proprietary digital forensic tools that are popularly and frequently used all over the world. Our motive has been to determine and compare the performance of both types of forensic tools, so as to ascertain their suitability of application for the purpose of examination and analysis of digital artifacts.

## 2 BACKGROUND AND RELATED LITERATURE

The development of computer-aided technologies and software applications also gives rise to anti-forensic activities, distinguishing it to be more of a technology due to its characteristics, procedures, applications and the types of attacks [5]. Liu and Brown identify four primary objectives for anti-forensics, as follows:

- To avoid any kind of detection that some event has occurred.
- To disrupt the collection of information.
- To increase the time duration spent by a forensic examiner on a case.
- To cast doubt on a forensic report or expert testimony [10]

Anti-forensic tools and techniques have evolved over the years. The traditional techniques such as overwriting, cryptography, steganography are the most common forms of anti-forensics available today [9,12]. The availability of tools has enabled even non-technical individuals to operate these tools easily, giving a rise to the application of anti-forensic techniques. The methods involved in this process can be broadly classified into several categories to understand the anti-forensic practices in use.

### 2.1 Commonly used Anti-forensic Techniques

To make investigation of digital artifacts more complicated and hassle-prone, several anti-forensic practices have evolved and the availability of effective open-source tools have made the criminal's task easier and hassle-free. The commonly applied anti-forensic techniques in the cyberspace, include:

- a. **Artifact Wiping:** Artifact Wiping is the technique where the specific file or data item is erased from the disk, removing all its traces. The data is destroyed or sanitized by using repeated overwrites, such that it is not possible to retrieve it

using any tool. Some tools such as BC Wipe, Eraser etc. are available data sanitization tools [11].

- b. **Steganography:** Steganography is the technique wherein data is hidden or embedded inside another data file, known as the carrier file or cover medium. The objective is to avoid detection. One of the techniques of performing steganography is the use of Least Significant Bit (LSB), which makes detection of hidden data extremely difficult. Some of the tools such as QuickStego, Steghide, StegDetect [24] can be used for steganography.
- c. **File Signature Mismatch:** A file is recognized by the file extension, also known as file signature. File extension is a suffix to the filename, which identifies the file format of its content or usage [2]. Modifying the signature of the file hides its contents and renders it useless as Windows will not be able to open the file.
- d. **Hidden or Deleted Partitions:** Partitions are created either by the operating system or user for storage and management of data. As with files, it is also possible to mark partitions hidden or deleted [18]. The deleted or hidden partitions are not very useful means to hide data because most operating systems and file manager is able to detect them even though they are deleted [13]. The partition can be deleted using the “Disk Management” tool in Windows.
- e. **Trail Obfuscation:** The intent of trail obfuscation is to confuse and disorient the investigation process through techniques like file metadata manipulation. Timestamping, which is an essential part of metadata of any file, consists of Last Modified Time, Last Access Time, Last Created Time and Change Time, also called MACE. This type of anti-forensic activity can make investigation harder and slow it down [15,16]. The timestamps of a NTFS file can be changed using tools such as Attribute Changer, File Touch etc.
- f. **Data Encryption:** Data encryption is yet another effective anti-forensic technique, which renders the data useless unless decrypted. Files can be encrypted by manipulating their header information or by using the “encryption with password” feature of Microsoft Office. The contents of the encrypted file are not recoverable easily.
- g. **Alternate Data Streams (ADS):** Alternate Data Streams is a feature, which is present only in NTFS file system. Every file consists of an attribute “\$DATA”, which describes the content of the file. More than one \$DATA attribute associated with a file is an ADS [25]. The ADS is not visible when browsing files through Windows Explorer and does not affect the size of the carrier file in a significant manner. It goes undetectable without the use of specialized utilities, and enables criminals to hide sensitive information efficiently.
- h. **Bit Shifting:** A well-known technique for data hiding is to alter the byte value of data by shifting the bit patterns. By shifting bits, the data, which is in readable format, changes to data in binary executable format. The scrambling of bits can be done using a tool known as Hex Workshop or WinHex [20].

Digital forensic tools are used for acquisition of information and evidences from digital exhibits. Such evidences might be present in an active state, deleted or in hidden form. Therefore, the strength of these tools lies in their ability to discover data that has been hidden, manipulated

or tampered, which is our effort in this research work.

### 3 EXPERIMENTAL DESIGN

The experimentation process has been performed by preparing sample anti-forensically doctored dataset using a sterile USB thumb drive of capacity 16 GB. This section also describes the different tools used for preparation of sample dataset and the methodology adopted for conducting the experiments.

#### 3.1 Tools Used

The following tools and techniques have been used for preparing the sample anti-forensically doctored dataset and subsequent attempts to recover the same from the USB thumb drive.

**Attribute Changer:** Attribute Changer is an open-source tool, which is used for modifying the date and timestamps information stored in files and folders [17].

**Eraser:** Eraser is an open-source advanced tool for Windows, which can be used to remove sensitive data completely from the hard drive by overwriting it several times using carefully selected patterns [19].

**WinHex:** WinHex is an open-source tool, which is used for editing the raw data contents of a file, unlike other software applications that interpret the data. The raw data content is present in hexadecimal form. This tool can be used for performing operations such as bit-shifting and modification of file header [23].

**Command Prompt:** Command prompt is a powerful in-built feature in Windows, which can be used for executing various anti-forensic operations such as Steganography, Alternate Data Streams etc.

**FTK Imager:** Forensic Toolkit (FTK) Imager is a bit-stream imaging tool, which is used for creating forensic images of a physical drive, logical drive or contents of file and folder in Raw (dd), E01, AFF or SMART format [22].

**FTK Analyzer:** FTK Analyzer is used for forensic analysis of digital exhibits and evidences. It can recover not only active data, but also carve out deleted and hidden data from the digital exhibit or its forensic image [22].

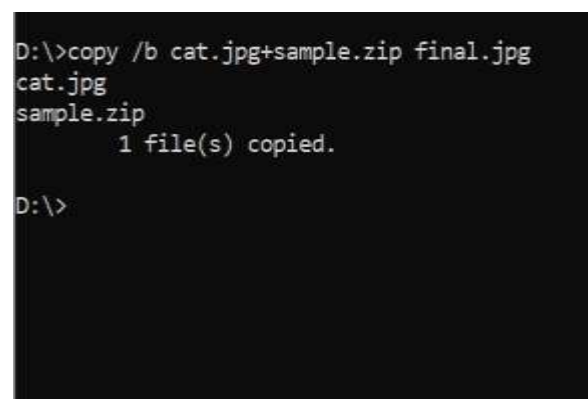
**Autopsy:** Autopsy is a HTML-based digital investigation analysis tool, which can run on both Windows as well as UNIX platform. Both active and deleted files can be analysed and the contents can be viewed in raw or Hex format [21].

#### 3.2 Methodology

The experiment is conducted by using USB thumb drive to store the anti-forensically prepared dataset i.e. various tools and techniques (as mentioned in sec 3.1) are used for performing anti-forensic activities (data hiding, wiping, manipulation etc.). After preparing the dataset, the thumb drive is imaged using FTK Imager and the bit-stream images are analysed using both proprietary and open-source digital forensic tools to trace evidences of anti-forensic activities and in the attempt, determine the performance of both the open-source and proprietary tools.

The various anti-forensic activities performed, are as follows:

**Steganography:** Steganography is performed using command prompt in which file “sample.zip” of size 64KB is embedded in cover file “cat.jpg” of size 5881KB to prepare the steganographed file “final.jpg” of size 5945 KB, as shown in Fig. 1.



```
D:\>copy /b cat.jpg+sample.zip final.jpg
cat.jpg
sample.zip
        1 file(s) copied.
D:\>
```

**Figure 1:** A snapshot showing Steganography process using command prompt

**Bit-Shifting:** A text file by the name “Sample.txt” is created with content “abcd” and the Right bit-shifting by 1-bit is done using the tool WinHex, as shown in Fig. 2.

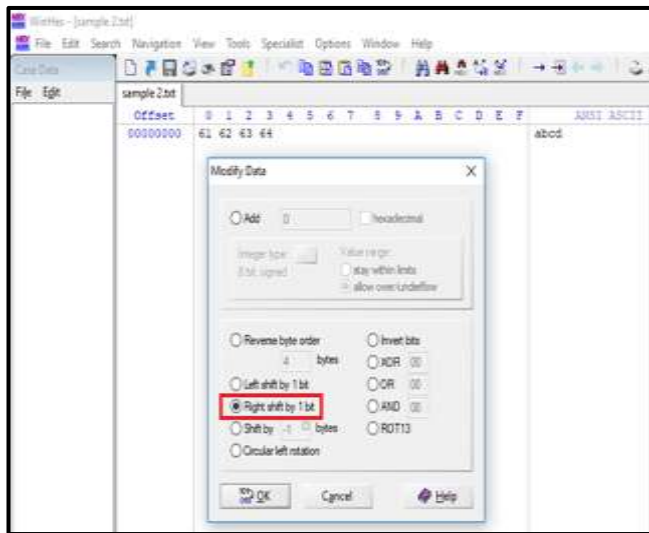


Figure 2: A snapshot showing technique of Bit-shifting using WinHex

**Trail Obfuscation:** A MS-Word file named “Trail\_Obfuscation.docx” is created. The date and timestamp values of the file are changed using the tool Attribute Changer. The creation, modified and accessed date are changed from “13-09-2019” to “13-09-2018” and the timestamps are changed from “17:25:05” to “09:55:23”. The process is shown in Fig. 3.

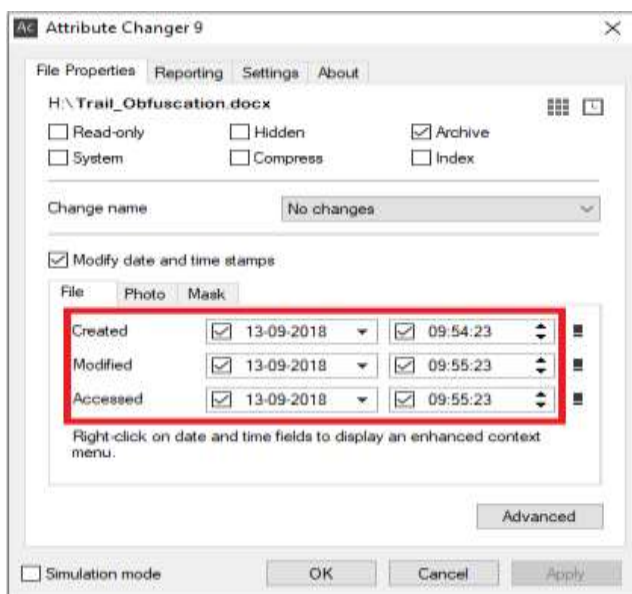


Figure 3: A snapshot showing technique of Trail Obfuscation using Attribute Changer

**Alternate Data Streams:** The command prompt is used for creating an alternate data stream (ADS) named “Hidden.txt” inside another text file named “Alternate.txt”. The ADS created, is not visible to the operating system either through the command prompt or Windows Explorer and no variation in size of the original file is observed. The process is shown in Fig. 4.

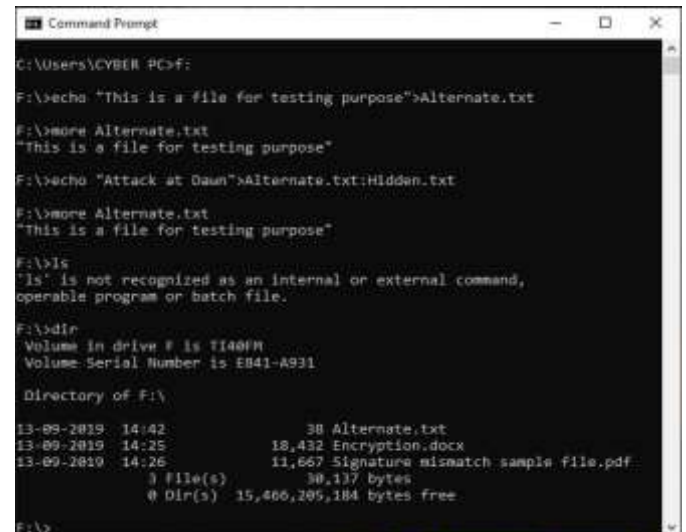


Figure 4: A snapshot showing creation of Alternate Data Streams using command Prompt

**Artifact Wiping:** A word document file by the name “Sample Wiping File.docx” is created and wiped from the storage device using the tool Eraser, as shown in Fig. 5.

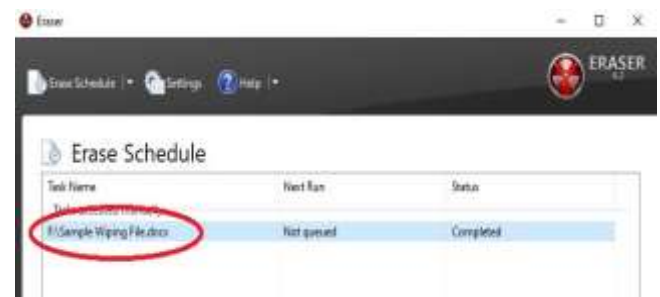


Figure 5: A snapshot of data wiping technique done using Eraser

**File Signature Mismatch:** The file signature of a word file is changed from “.docx” to “.pdf” using the feature of Windows Explorer in Windows, as shown in Fig. 6.



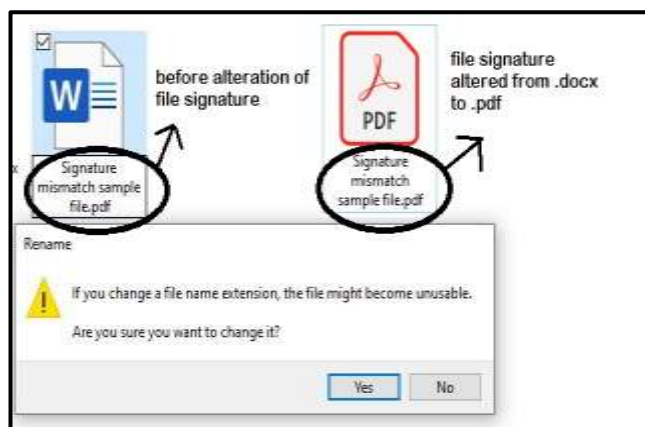


Figure 6: File Extension/Signature changed from .docx to .pdf

**File Encryption:** Two different files (1 MS-Word file and 1 Image file) are created and used for encryption. The word document is encrypted using the “Encryption by Password” feature available in Microsoft Word, while the image file is encrypted by replacing some of the bit values in its header portion, rendering it unreadable (shown in Fig. 7).



Figure 7: A snapshot of file encryption by replacing bit values in its header, using WinHex

**Deleted Partition:** A separate partition of 4GB is created in the USB thumb drive and different types of data files (text, image, audio and video

files) are stored in the partition. After storing the data files, the partition is deleted using disk management features available in Windows Operating System, thus rendering it invisible.

## 4 RESULTS AND ANALYSIS

The anti-forensic activities (as mentioned in Sec 3.2) are performed using different tools and techniques and sample is prepared. A bit-stream imaging of the USB thumb drive is done using FTK Imager and the acquired image is analysed using both FTK Analyzer 7.0 (proprietary tool) and Autopsy 4.12.0 (open-source tool) in an attempt to recover the data items in their original state. The results obtained for each of the anti-forensically doctored data item is illustrated in this section, as follows:

### 4.1 Examination and Analysis of Image Steganography

On examination by both types of disk forensic tools, it is seen that none of the tool could detect that the file “final.jpg” has another image file embedded in it. No trace of steganography could be found even on analysing the file metadata, as shown in Fig. 8, respectively.

### 4.2 Examination and Analysis of Bit-Shifting

The file “sample modified.txt”, which has been subjected to bit-shifting is also undetectable by either by the proprietary or open-source tool. The content as seen during analysis and examination is different from the original content of the file. Hence, it is not possible to trace evidences of bit-shifting using disk forensic tools, as shown in Fig. 9, respectively.



Figure 8: Snapshot of FTK Analyzer 7.0 used for the analysis and examination of Steganographed image

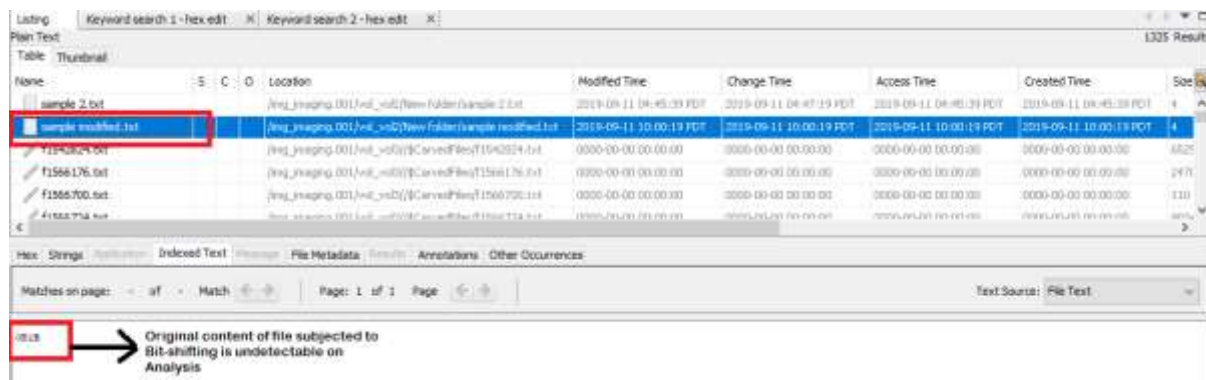


Figure 9: Snapshot of Autopsy used for analysis and examination of data file subjected to bit-shifting

### 4.3 Examination and Analysis of Trail Obfuscation

The file “Encryption.docx”, which was modified using Attribute Changer is examined using both Autopsy and FTK Analyzer. It is observed that the date and timestamp of the file are shown to be modified even by the tools. However, the value of date and timestamps as present in the Master File Table (MFT) entry (File Metadata) are the original values when the file is actually created, accessed or modified, as shown in Fig. 10, respectively.

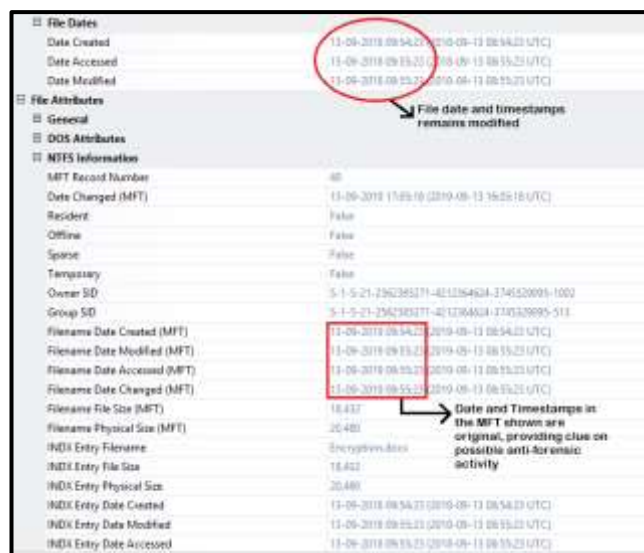


Figure 10: Snapshot of Detection of original values of date and timestamps by FTK Analyzer

Hence, it can be inferred that in detection of trail obfuscation as an anti-forensic activity, both proprietary and open-source tools show similar performances.

### 4.4 Examination and Analysis of Wiped Artifact

The file “Sample Wiping file.docx”, which is wiped using specialized artifact wiping software, could not be recovered by either of proprietary or open-source tools. No traces of the file could be detected either in the slack space or unallocated space of the disk.

### 4.5 Examination and Analysis of File Signature Mismatch

The altered file extension could be detected by both FTK Analyzer (as shown in Fig. 11 respectively) and Autopsy. Both the tools show similar performances.

### 4.6 Examination and Analysis of Alternate Data Streams (ADS)

On analysing and examining the bit-stream image of the USB thumb drive, it is found that the ADS named “Hidden.txt”, which was hidden inside the text file “Alternate.txt” could be recovered by both the tools, along with its content. On careful examination of the file metadata, especially the entries in the MFT, the date and time of creation could also be found (as shown in Fig. 12). Hence, it can be inferred that the tools show similar performances in recovery of Alternate Data Streams, which are not visible through normal browsing activities in Windows.

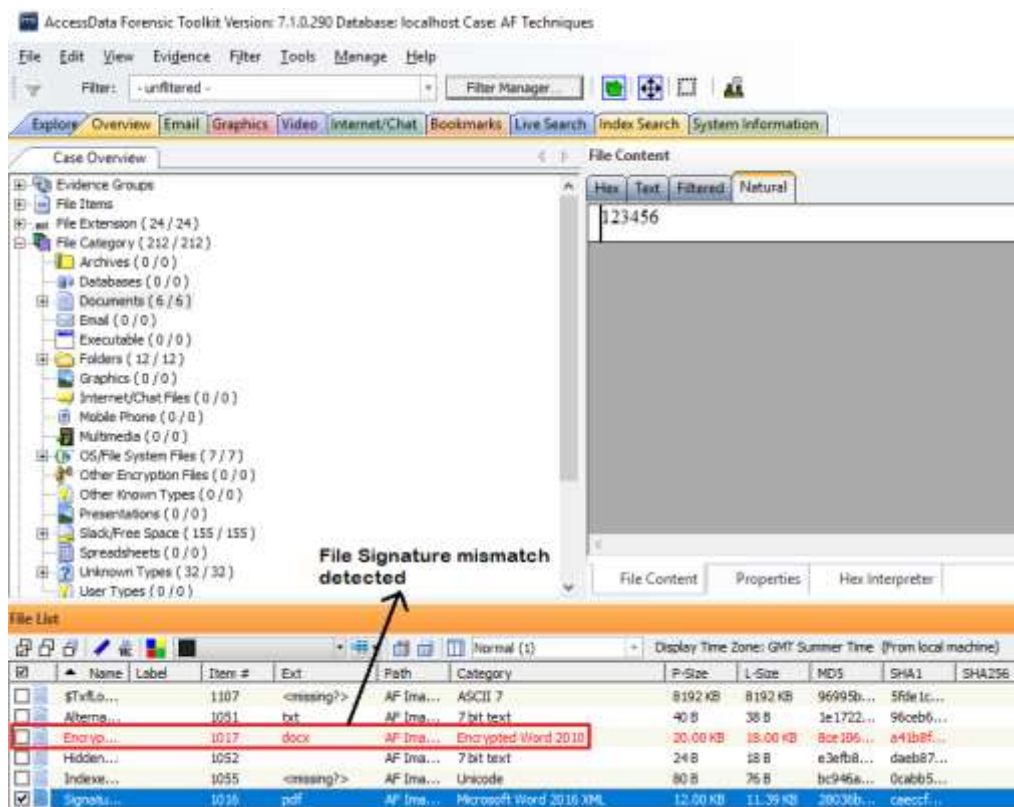


Figure 11: File Signature Mismatch detected during analysis by FTK Analyzer

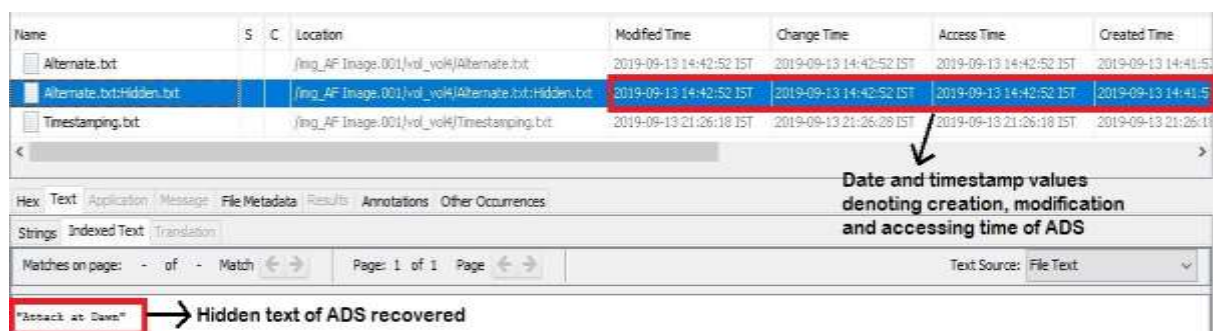


Figure 12: Detection of Alternate Data Streams (ADS) by Autopsy

#### 4.7 Examination and Analysis of Deleted Partitions

The data stored in the deleted partition could be recovered along with its complete metadata information, using the disk forensic tools. The recovered data consists of text document, image file, audio file and a video file (as mentioned in Sec 3.2), as shown in Fig. 13, respectively. The reason for data recovery is because that the partition was simply deleted and not formatted or wiped, as a result of which the data still resided in the device. Thus, in this scenario, both tools are able to show same performances.

#### 4.8 Examination and Analysis of Encrypted Files

Two different files have been encrypted using different techniques. The MS-Word file “Encryption.docx” is encrypted using the “Encryption by Password” feature of Microsoft Word, as a result of which both the tools are able to detect it. However, none of the tools could either recover the file content or the password for decryption, as shown in Fig. 14, respectively. The other file, which is encrypted by modifying the raw bits in the file header, is also found along with contents, which is not in readable format.



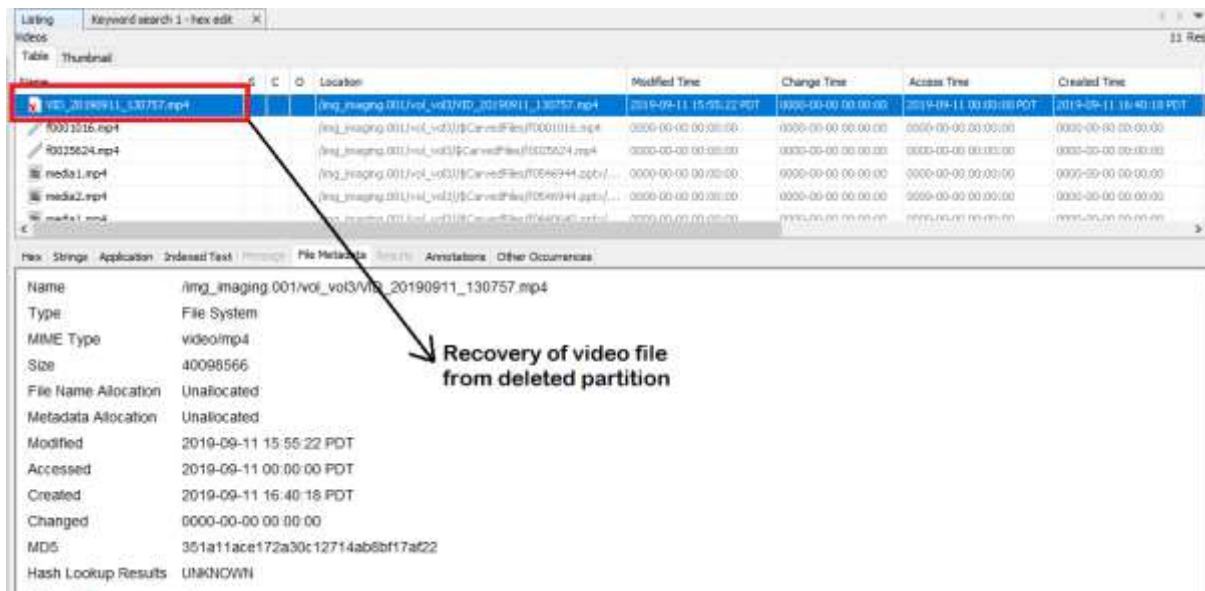


Figure 13: Recovery of Video file from deleted partition of the USB thumb drive, using Autopsy

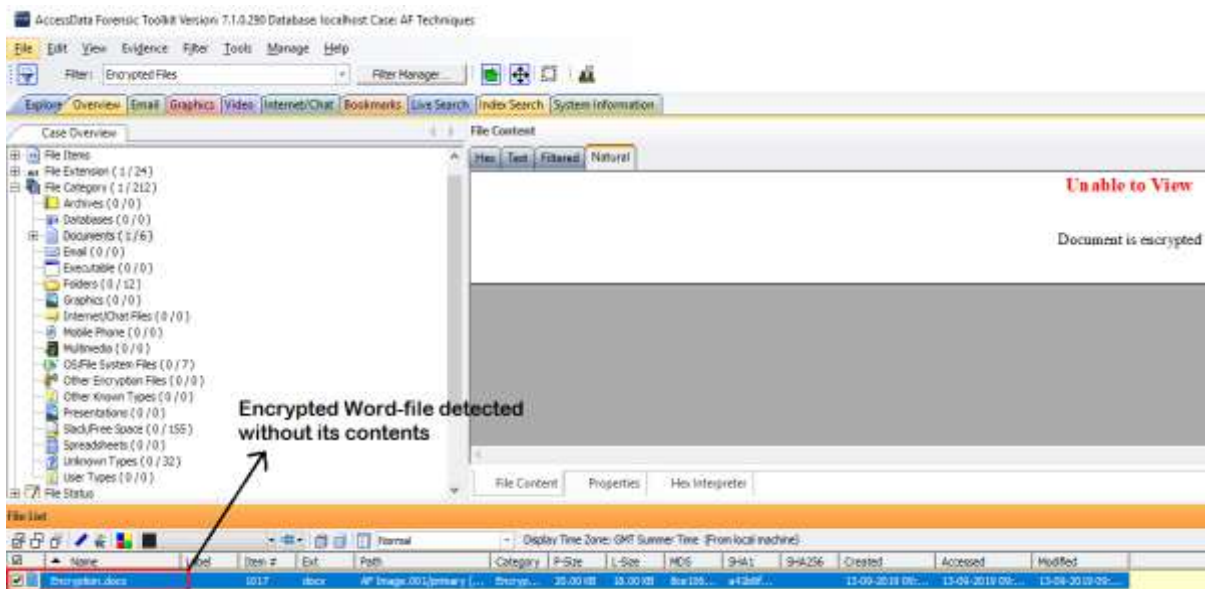


Figure 14: Detection of Encrypted Word file without its content, using FTK Analyzer

Therefore, based on the observations made during analysis and examination of the anti-forensically doctored data samples, using both open-source

and proprietary disk forensic tools, their results and comparison of performances can be summarized, as given in Table 1.

Table 1: Comparative Analysis of the performance of FTK Analyzer and Autopsy based on examination and analysis of anti-forensic activities

S.No	Anti-Forensic Activity Performed	Tools used	Detection by Autopsy	Detection by FTK Analyzer	Remarks, if any
1	Steganography	Command Prompt	×	×	Cover Image found but steganography not detected
2	Bit-Shifting	WinHex	×	×	Original content not detected
3	Trail Obfuscation	Attribute Changer	✓	✓	Changed date and timestamps detected

4	Artifact Wiping	Eraser	×	×	Wiped artifact destroyed beyond recovery
5	File Signature Mismatch	Change of file extension	✓	✓	Altered file extension detected
6	Alternate Data Streams (ADS)	Command prompt	✓	✓	ADS detected successfully
7	Deleted Partitions	Disk Management (Windows)	✓	✓	All data recovered successfully
8	Encrypted Files	Encryption by password	✓	✓	Encrypted file detected but contents not recovered
		Encryption by changing file header	×	×	Contents unreadable

Based on examination of the forensic image, a comparative analysis of the performance of both types of disk forensic tools has been done, as shown in Table 1. From Table 1, it is observed that majority of the anti-forensic activities such as trail obfuscation, file signature mismatch, ADS, deleted partitions and file encryption (using password) could be detected by both Autopsy as well as FTK Analyzer. However, some of the other activities like steganography, artifact wiping, bit-shifting and file encryption by header modification went undetected by the tools. In the case of encryption using password, although the encrypted file could be detected, however, the contents of the file could not be recovered by either of the tools. Also, while analysing steganographed image, the cover image could be recovered without being able to detect the presence of hidden information or file in it. Both the ADS and its hidden content were recovered and extracted successfully.

## 5. CONCLUSION AND SUGGESTIONS

This research work has been conducted with the objective of comparing the relative performance of well-known and frequently used open-source and proprietary Disk Forensic tools in recovering of anti-forensically doctored (i.e. hidden, wiped, encrypted etc.) digital artifacts. The experiments

have been conducted on samples of anti-forensically doctored datasets, prepared using different tools and techniques in sterile USB thumb drive. The analysis and examination of the thumb drives have been done using both open-source (Autopsy) and proprietary (FTK Analyzer) digital forensic tools on an acquired bit-stream image of the exhibit

Based on the experiments undertaken in this research work, it has been concluded that both open-source (Autopsy) and proprietary (FTK Analyzer) portray relatively similar performance, while recovering or finding traces of anti-forensically doctored artifacts. Both types of tools have certain drawbacks, which hinder their ability in unearthing traces of certain anti-forensic activities like steganography, bit-shifting and encryption due to file header alteration. Since both open-source and proprietary tools portray similar performance, therefore, expert opinion and forensic report given based on the results of open-source tool like Autopsy should also be considered admissible in the court of law.

The results achieved from this research would be useful in overcoming the hurdles that computer forensic tools might present in front of Anti-Forensic Techniques, assisting forensic examiners during digital investigations. Also, this would make it easier for them to perform

examination using open-source tools producing reliable and efficient results. Although, earlier researches with similar objectives have been conducted, but none of them have portrayed an analysis in the performance of open-source and proprietary tools. Since, both Autopsy and FTK Analyzer are very frequently used digital forensic tools in majority of cyber-crime investigation cases, therefore, the results of our research work would prove to be significant in modifying the approach and perspective of digital forensic practitioners towards carrying out investigation of digital exhibits, especially focussing on hidden and manipulated data items.

In the future, the same experiment can be conducted to determine the performance of other disk forensic tools and in-turn develop stronger tools that can be used for unearthing maximum hidden data and counter anti-forensic practices.

## 6 REFERENCES

1. Halder, D., & Jaishankar, K.: Cyber-crime and the Victimization of Women: Laws, Rights, and Regulation, Hershey, PA, USA: IGI Global (2011).
2. Nelson B., Phillips A., Steuart S.: Guide to Computer Forensics and Investigations, 4th Edition, Cengage Learning (2013).
3. Karie M., Kebande V.: Building Ontologies for Digital Forensic Terminologies. In: International Journal of Cyber-Security and Digital Forensics, vol. 5, issue 2, pp 75-82, SDIWC (2016).
4. Azad M.M., Sharmin S.S.: Cyber Crime Problem Areas, Legal Areas and the Cyber Crime Law, International Journal of New Technology and Research (IJNTR), Vol.3, Issue 5, pp. 1-6, (2016).
5. Hiley S.: Anti-forensics with a small army of exploits, International Journal of Digital Investigations, Elsevier, pp. 13-15, (2007).
6. Provos N., Honeyman P.: Hide and Seek: An Introduction to Steganography, IEEE Security and Privacy, Vol.1, No.3, pp. 32-44, (2003).
7. Chhabra G.S., Jain A.: Anti-Forensic Techniques: An Analytical Review, IEEE, (2014).
8. Leng J., LI T.: Research on Computer System Information Hiding Anti-Forensic Technology, 8<sup>th</sup> International Conference on Social Network, Communication and Education, Advances in Computer Science Research, Vol. 83, Atlantis Press, (2018)
9. Garfinkel S.: Anti-Forensics: Techniques, Detection and Countermeasures, 2nd International Conference on Information Warfare and Security (ICIW), Monterey, CA, (2007).
10. Liu and Brown.: Bleeding-Edge Anti-forensics, InfoSec World Conference & Expo, MIS Training Institute, (2006).
11. University of California – Riverside.: Security using Data Sanitization, Available: <http://cnc.ucr.edu/security/datsan.html>, (2011).
12. Beer R., Stander A., Belle JP.: Anti-Forensics: A Practitioner Perspective. In: International Journal of Cyber-Security and Digital Forensics, vol. 4, issue 2, pp 390-403, SDIWC (2015).
13. Davis J., McClean J., Dampier D.: Methods of Information Hiding and Detection in File Systems, ResearchGate, (2010) DOI: 10.1109/SADFE.2010.17
14. Erasani S.: Implementation of Anti-Forensic Mechanisms and Testing with Forensic Methods, Graduate Project Report, Department of Computing Sciences, Texas A&M University-Corpus Christi Corpus Christi, Texas, (2010).
15. Salam H.F.A, Shaat E.A.: Estimation of Post-Mortem interval using thanatochemistry and post-mortem changes, Alexandria Journal of Medicine, Vol. 48, pp. 335-344, (2012).
16. Ding X., Zou H.: Time Based Data Forensic and Cross-Reference Analysis, 26<sup>th</sup> Symposium on Applied Computing, Proc. Of ACM Symposium on Applied Computing, pp. 185-190, (2011).
17. Attribute Changer.: Attribute Changer 9, [www.petges.lu](http://www.petges.lu).
18. Namgung J., Hong Young Il., Park J., Lee C., Lee S.: A Research for Partition Restoration Technique, Lecture Notes in Electrical Engineering 276, Springer-Verlag Berlin Heidelberg, (2014) DOI: 10.1007/978-3-642-40861-8\_45.
19. Eraser.: Secure Erase files from Hard Drive- An Advanced Security tool for Windows, <https://eraser.heidi.ie/>

20. Bit-Shifting, [http://www.rcbc.edu/files/PDFFiles/service-learning/bdd/Session%201\\_Bitshift\\_handout\\_wp1c.pdf](http://www.rcbc.edu/files/PDFFiles/service-learning/bdd/Session%201_Bitshift_handout_wp1c.pdf)
21. Autopsy “Autopsy-The Sleuth Kit”, <https://www.sleuthkit.org/autopsy>
22. FTK Imager v 3.2.0 and FTK Analyzer v7.0, <https://accessdata.com/>
23. Win-Hex: Hex Editor and Disk Editor, Computer Forensics and Data Recovery Software, [www.x-ways.net/winhex](http://www.x-ways.net/winhex).
24. Provos N.: Steganography Detection with StegDetect, <http://www.outguess.org>
25. Carrier B.: File-system Forensic Analysis, Addison-Wesley, Upper Saddle River, NJ, (2005).