OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

AN EMPIRICAL STUDY OF DIGITAL FORENSIC TOOLS AND TECHNIQUES FOR DETECTION OF TRACES OF ANTI-FORENSIC ACTIVITIES OF USB DEVICES IN WINDOWS

Dr. Deepak Raj Rao G.[1], Sonu Mandecha[2], Kumarshankar Raychaudhuri[3]

Assistant Professor, *Cyber Forensic Division, LNJN National Institute of Criminology and Forensic Science (MHA), Delhi, India[1]*

M.Sc. Student, *Cyber Forensic Division, LNJN National Institute of Criminology and Forensic Science (MHA), Delhi, India[2]*

Junior Research Fellow, *Cyber Forensic Division, LNJN National Institute of Criminology and Forensic Science (MHA), Delhi, India[3]*

gdeepakrajrao@gmail.com[1], mandechasona@gmail.com[2],ksrc089@gmail.com[3]

Abstract: ***The computer is proving to be a lethal weapon, capable of causing huge loss if used with wrong intentions. In order to investigate cyber-crime, digital forensics techniques are used for collection, extraction, examination and analysis of data from different storage devices such as hard disks, USB thumb drives, CDs, DVDs etc. Anti-forensics, on the other hand is the use of different techniques of hiding data and metadata or destroying the evidence to deceive digital forensic tools and investigators. In this research work, we have performed different anti-forensic activities related to USB devices in Windows. One set of anti-forensic activities have been performed to hide data inside an USB thumb drive, while the other set of anti-forensic techniques have been applied for hiding the traces of usage of USB thumb drive in the computer system. Experiments have been performed using different digital forensic tools and techniques in an attempt to detect whether or not it is possible to track the anti-forensic activities. This type of research work would be beneficial for the forensic fraternity in examination and investigation of cyber-crime cases involving the use of anti-forensics.***

Keywords: *Anti-Forensics, Data Hiding, Autopsy, Trail Obfuscation, File Encryption, Signature Mismatch*

----------∴∴∴----------

I INTRODUCTION

According to DIBS (United States of America), computer forensics involves scientifically examining and analyzing data from computer storage media so that the data can be used as evidence in court [11]. The Scientific Working Group on Digital Evidence defined the term computer forensics as being the "Scientific examination, analysis, and/or evaluation of digital evidence in legal matters" [1]. Similarly, Peisert, Bishop et. Al suggest that digital forensics is more related to the "The inclusion of devices other than general-purpose computer systems, such as network devices, cell phones and other devices with embedded systems" [1]. Nance, Hay et. al further defined the term digital forensics as involving a "Wider variety of digital devices" than more traditional networks and computer systems that form part of an investigative process [1]. National Institute of Science and Technology (NIST) defines digital evidence as "Any piece of data which is recorded, preserved or transferred in/through any medium by a computer system or similar digital devices, that can be read, understood and interpreted by a person, computer or similar digital device.

With the growing number of the digital devices, the criminals are using modern techniques so that they can get away without being convicted, so to avoid the detection of crime the criminals are making use of "anti-forensic" techniques. Anti-Forensics is 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 to unearth and extract them easily [8,12] 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. This makes the evidence acquisition phase highly complex and difficult. The common anti-forensic techniques include data erasure, data hiding, manipulation of the metadata, data encryption, kernel-level rootkit and many more [6,8].

There is a dire need to conduct research on the efficiency of the different forensic tools and techniques to recover the artifacts related to the USB storage devices that has been manipulated using anti-forensic techniques. If the artifacts and logs related to the use of USB storage devices in a computer system (which has been anti-forensically manipulated) have been destroyed or manipulated, recovering those evidences and traces is a challenging task. Therefore, there is arising need to identify the various digital forensic tools and techniques which can be used to recover anti-forensically doctored data from and related to USB storage devices and their logs in Windows OS, that forms the basis and need of our research.

II REVIEW OF LITERATURE AND BACKGROUND STUDY

"Anti-forensics" (AF) is a growing collection of tools and techniques that frustrate forensic tools, investigations and investigators. Anti-forensics is a common term for a set of techniques aimed at hindering or preventing a proper forensics investigation process. They may reduce the quantity and quality of digital evidence available.

Anti-forensic techniques are the actions and methods that hinder the forensic investigation process in order to protect the attackers and perpetrators from prosecution in a court of law. These techniques act against the investigation process such as deletion, collection, and analysis of evidence files and sidetrack the forensic investigators. These techniques impact the quality and quantity of the evidence of a crime scene, thereby making the analysis and investigation difficult.

a) Liu and Brown identify four primary goals for anti-forensics:

b) Avoiding detection that some kind of event has taken place.

c) Disrupting the collection of information.

d) Increasing the time that an examiner needs to spend on a case.

e) Casting doubt on a forensic report or testimony [5,9].

Other goals might include:

a) Forcing the forensic tool to reveal its presence.

b) Subverting the forensic tool (e.g., using the forensic tool itself

c) Anti-Forensics is a study of techniques and tools that confuse computer forensic tools (CFTs), investigators and any other forensic processes by hiding or destroying the data and meta data. Dr. Rogers from Purdue University defines anti-forensic as an attempt to cause harm to the evidence that is obtained in the scene and also to make the investigation procedures more complicated to perform [6].

A. Tracking USB storage

Carvey in his article Tracking USB storage: Analysis of windows artifacts generated by USB storage devices analyzed various artifacts generated by Windows when USB is connected in the system and concluded that a single USB can be traced according to the date and time the same has been connected to any system [2].

B. Amcache.hve

Amcache.hve file stores information related to Windows applications experience and compatibility feature in registry hive. Location of Amcache.hve file in Windows 10 is- %System-Drive%/Windows/Appcompat/Programs/Amcache.hve

C. User Assist Key

Mee & Jones, Carvey and Altheide & Mee. Et al. investigated the User Assist Key to identify the external devices connected to run an anti-forensic tool [10]. In [8], the author has investigated behavior of user assist key when applications are executed from different sources, such as external device, Windows store and shared network. Information which can be retrieved from the User Assist Key is that Run count and focus time can provide clue on the frequency and the total time an evil program was executed. Evidence of program execution persisted in User Assist Key even after the target application has been removed from the system [2,3,9].

D. Data Hiding Techniques

According to Garfinkel [5], there are several Data Hiding File System structures, some of these file systems are mentioned below:

TABLE 1: DATA HIDING FILE SYSTEM STRUCTURE (GARHINKEL, 2007)

Slacker	Hides data in slack space
Frag FS	Hides data in Master File Table
Rune FS	Stores data in "bad blocks"
Data Mule FS	Stores data in inode reserved space
KY FS	Stores data in directories
Host Protected Areas	Device Configuration Overlay

III EXPERIMENTAL DESIGN

The experiments will be conducted by using different samples of data files (digital evidences) and tools. This section will provide a brief description of the methodology adopted and the different digital forensic tools used.

A. Tools Used for Experiments

The digital forensic tools used in conducting the experiments, as validated by NIST [4], are as follows:

a) ***SNOW Tool***- SNOW is an open-source tool which is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers.

b) ***Steghide*** - Steghide is a steganography program that is able to hide data in various kinds of image and audio files.

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

d) ***WinHex*** - WinHex is a hexadecimal editor, used in imaging and analysis of disks and files. It can be used for computing and analyzing the hash value of individual files (e.g. text, audio, image, video files etc.) and folders.

e) ***Hex Workshop***- It is an open-source tool, which is used for editing, cutting, copying, pasting, inserting, filling and deleting binary data.

f) ***USB Forensic Tracker***- USB Forensic Tracker is a comprehensive tool that extracts USB connection artefacts from a range of locations within the live system, from mounted forensic images, from volume shadow copies, from extracted windows system files. The extracted information from each location is displayed within its own table view. [12]

g) ***USB Oblivion***- USB Oblivion is a free portable program for the windows operating system that can erase all USB-related connection records from a PC it is started on.

h) ***Regedit***- Regedit is a GUI tool used to list, write, change, delete, import and export registry keys in Windows Operating System.

i) ***Registry Explorer***- Registry Explorer is an Erric Zimmermann's tool. This tool is used to retrieve the deleted USBSTOR key by USB Oblivion tool.

j) ***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.

k) ***Autopsy***- Autopsy is a HTML-based digital investigation analysis tool, which can run on both Windows as well as UNIX platform.

l) ***EnCase***- EnCase Forensic, the industry-standard computer investigation solution which performs sound data collection and analysis

m) ***Aletheia*** - Aletheia is an open source image steganalysis tool for the detection of hidden messages in images. To achieve its objectives, Aletheia uses state-of-the art machine learning techniques.

n) ***John the Ripper***- John the Ripper is a free and Open Source Software, distributed primarily in source code form. Its primary purpose is to detect weak Unix Passwords.

B. Methodology

The methodology used for conducting the experiments are as follows:

a) 4GB USB thumb drives have been considered for preparing of samples.

b) Different samples of anti-forensically doctored data set are prepared in the USB thumb drives.

c) After preparing the dataset, a bit-stream image of each thumb drive is captured using FTK Imager.

d) The bit-stream images are analysed using various digital forensic tools to trace evidences of anti-forensic activities.

e) Also, the USB thumb drives are analysed directly using digital forensic tools for tracking the anti-forensic activities

IV RESULTS AND ANALYSIS

All the samples prepared in the USB thumb drives were tested using various digital forensic tools and techniques and the results were found, which have been discussed in this section.

A. Results of detection of Data Wiping

Two USB thumb drives of 4GB each (with two MS-word documents in both of the thumb drives) were wiped using CCleaner tool and then both of these thumb drives were imaged using FTK Imager as well as EnCase Imager and were analysed by using EnCase, FTK Analyser and Autopsy. However, no data could be recovered using either of the forensic tools.

B. Results for detection of Trail Obfuscation

A text file named "example.txt" is created. The date and timestamp values i.e. the MAC values of the file were

changed using the tool Attribute Changer. The Created date of the file were changed from 11 March, 2020 to 11 October, 2019 and the Modified and Accessed date of the file were changed from 11 March, 2020 to 13 October 2019 while timestamps value remains the same. After imaging of the USB thumb drive, it was analysed by various Disk Forensic Tool. Modified date and time were recovered by the Disk Forensic Tool Autopsy, as indicated in the snapshot in Fig. 1

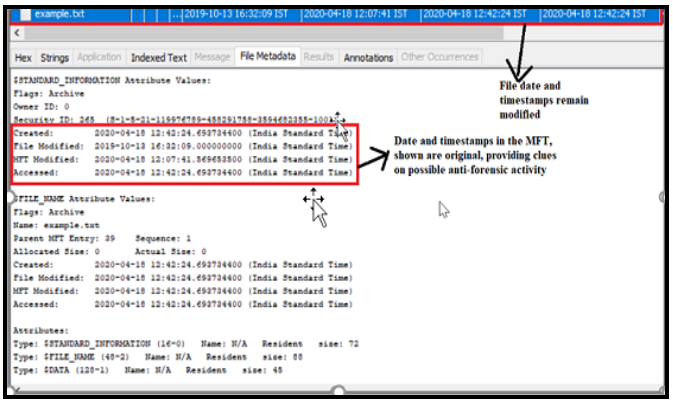

Figure 1: Snapshot of Detection of original values of date and timestamps by Autopsy

C. Results for detection of 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 through the command prompt or Windows Explorer and no variation in size of the original file is observed. After imaging of the USB thumb drive, it was analysed by various Disk Forensic Tools. ADS named "Example.txt", which was hidden inside the text file "Alternate.txt" could be recovered by Autopsy, along with its content, as shown in Fig. 2

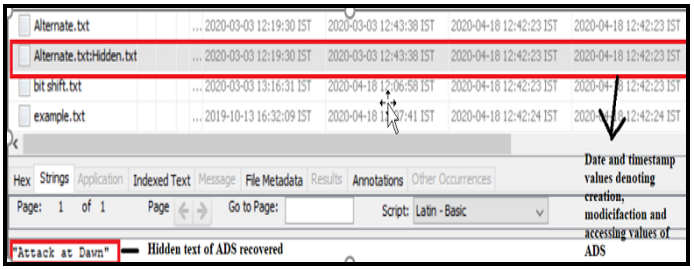

Figure 2: Detection of Alternate Data Stream (ADS) by Autopsy

D. Results for detection of Steganographed Data

Steganography is performed by using two command line tool i.e., SNOW and Steghide tool. SNOW tool was used to embed text message 'hi' in cover file "sample.txt" of size 20 bytes by setting up a password to prepare a Steganographed file "output.txt of size 39 bytes. Steghide tool was used to embed a text file "secret.txt" of size 1KB is embedded in cover file "sample.jpg" and of size 99.3KB and the resultant file is "sampl.jpg" of size 100KB which is password protected also. After imaging of the USB thumb drive, it was analysed by various Disk Forensic Tools. Notepad++ tool was also used for analysis. Steganographed data could be identified by Cyber Check Suite tool and Aletheia tool. Notepad++ tool is able to identify white space steganography, as shown in Fig. 3

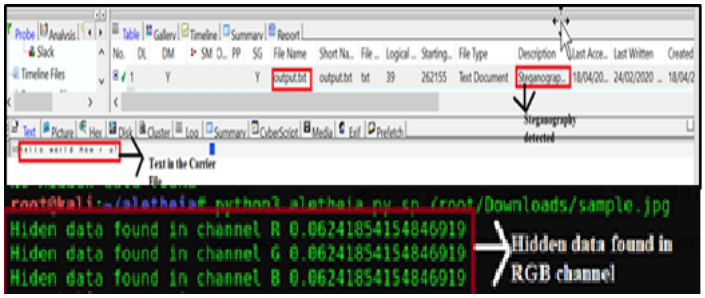

Figure 3: Detection of Steganographed text file and hidden data using Cyber Check Suite and Alethia

E. Results for detection of File Encryption

The MS-Word file "Encryption.docx" is encrypted using the "Encryption by Password" feature of Microsoft Word. After imaging of the USB thumb drive, it was analysed using autopsy tool and John the Ripper tool is also used to recover the password of the file. Autopsy tool is able to identify the password protected file. After the identification of password protected file, John the Ripper tool is used to recover the password and the password is recovered which is "password123", as displayed in Fig. 4

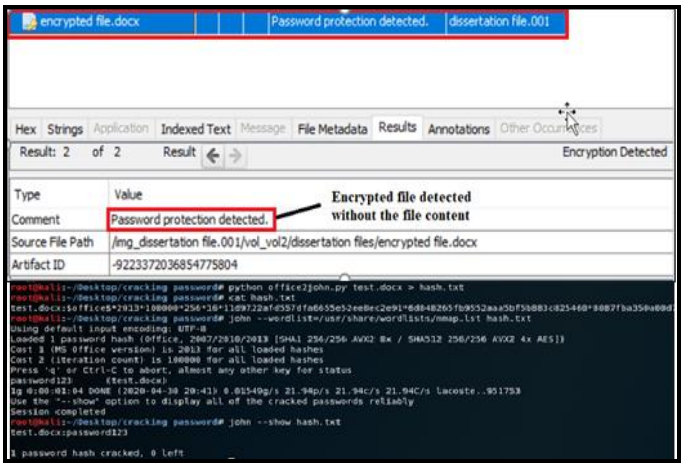

Figure 4: Detection of Encrypted file and the password using Autopsy and John the Ripper

F. Results for detection of File Signature Mismatch

The file signature of a MS-Word document file is changed from ".jpg" to ".png" using the feature of Windows Explorer in Windows. After imaging of the USB thumb drive, it was analysed by using various Disk Forensic Tool. File signature mismatch is identified by the Autopsy Tool and

the actual contents of the file could also be detected and viewed using the tool Autopsy, as shown in Fig.5

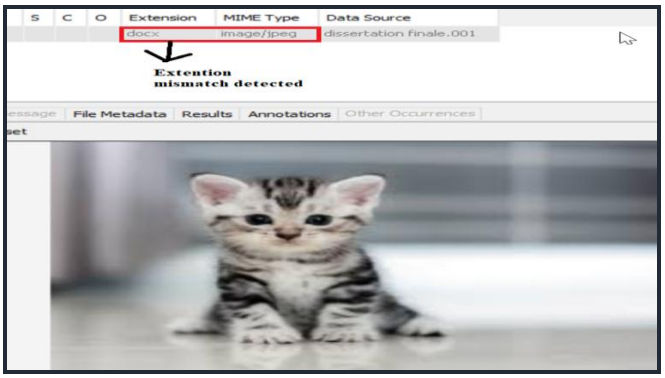

Figure 5: Detection of File signature mismatch by using Autopsy

G. Results for detection of Traces of Uninstalled Application

The USB thumb drive "SCSI DISK USB Device" with serial number "1A754B0CBE0097871175" is uninstalled by using the USB Deview tool. Regeditor tool is used to check the traces of uninstalled applications. Traces of the uninstalled application are present in registry of Microsoft Windows OS.

H. Results for detection of traces of USBSTOR Key

The USB Oblivion tools is used to remove the USBSTOR key of the registry by enabling "Do real clean" option in the tool. After the USB Oblivion tool, the USBSTOR key of the registry has been deleted. The system hive is then analyzed by Registry explorer in order to recover the deleted keys. USBSTOR key is recovered by using Registry Explorer tool, as shown in Fig. 6.

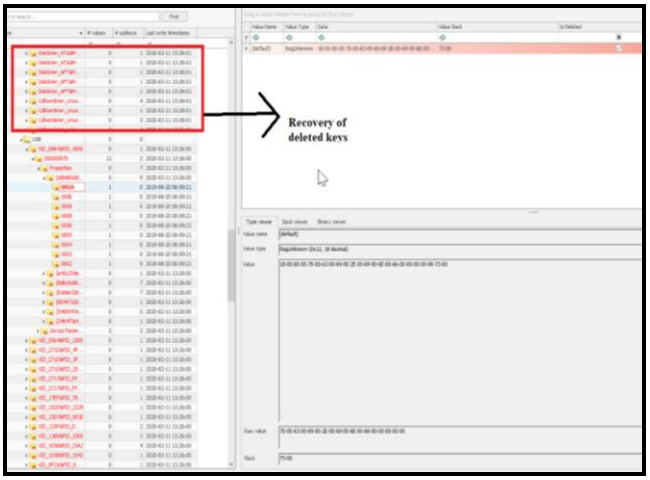

Figure 6: Snapshot showing recovery of deleted USBSTOR key by Registry Explorer

I. Results for detection of traces of UserAssist Keys

Regedit built in tool is used to delete the user assist key present in registry corresponding to a particular application. User Assist keys are recovered by using Registry Explorer Tool, as shown in Fig. 7.

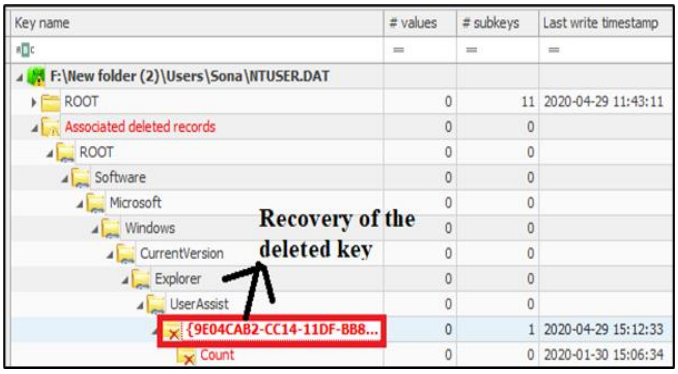

Figure 7: Snapshot showing recovery of deleted User Assist Key using Registry Explorer

J. Results for detection of Traces of Amcache.hve file

The Amcache.hve file present in the system is analyzed by using the tool AmcacheParser which is a command line tool. Amcache.hve file is able to recover the entire information about the portable executable applications in the system, as displayed in Fig. 8.

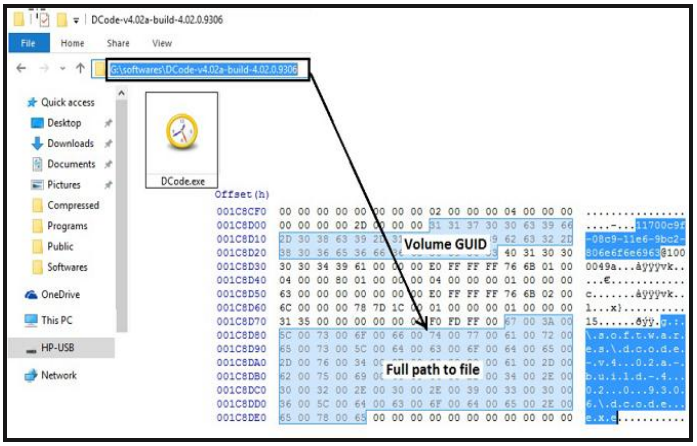

Figure 8: Snapshot of Recorded information related to portable executable in Amcache.hve

V CONCLUSION AND SUGGESTIONS

This research work has been carried on with the objective of conducting An empirical study of Digital Forensic tools and techniques for detection of traces of Anti-Forensic activities of USB Devices in Windows OS that is testing the effectiveness of Open-source as well as Proprietary Disk Forensic Tools in recovering the anti-forensically doctored (i.e., hidden, encrypted, wiped etc.) digital artefacts. The experiments have been conducted on samples of anti-forensically doctored datasets, prepared using different tools and techniques in sterile USB thumb drive. In addition to the anti-forensically prepared dataset in the sterile USB thumb drive, anti-forensic activities are also conducted in the Windows OS in order to erase the evidence of usage of

USB thumb drive in the system. The analysis and examination of the thumb drives have been done using both open-source and proprietary (FTK Analyzer) digital forensic tools on an acquired bit-stream image of the exhibit. For the examination of the Windows OS in order to find out the traces of anti-forensic activities, registry of the system is acquired with the help of FTK Imager and then the registry hives are analysed by using various tools and techniques.

Based on the experiments conducted in this research work, it can be concluded that there are still some drawbacks in the current disk forensic tools and techniques as they are not capable of unearthing traces of certain anti-forensic activities like wiping, Full Disk encryption, Bit-shifting, File Signature Manipulation. While recovering the anti-forensically doctored artefacts of usage of USB thumb drive from the computer system, registry analysis by registry explorer tool is effective in recovering the artefacts. Various log files such as Amcache.hve and Iconcache.db are also essential in analysing the traces of deleted application that have been executed or deleted on the user's computer as well as in analysing the applications installed or executed by external portable device such as USB thumb drive.

It can be concluded that if the artefacts of the USB thumb drive are deleted from the system and the applications executed using USB thumb drive are deleted from the system still the artefacts are recoverable as well as the traces of applications executed by external portable device such as USB thumb drive can also be recovered by analysing various log files such as Amcache.hve file, Iconcache.db file etc. The uninstalled applications from the system are also recoverable by analysing Registry of the system. The deleted User Assist Keys can also be recovered.

The results obtained from this dissertation report would be useful in overcoming the hurdles that computer forensic tools might present in front of anti-forensic techniques assisting forensic examiners during digital investigation specifically in a scenario where a USB and a Windows computer system is found at the scene of crime and there is the need to link USB to the computer system. Also, this dissertation report will make it easier for the investigators to perform examination using open-source tools producing reliable and efficient results. And it is also important to note that no single tool is capable of performing the entire examination, combinations of different tools and techniques should be used in order to unearth the hidden artefacts or evidences for example, first autopsy is used for the detection of password protected file and after its detection other tools specific for password detection like John the Ripper is used in order to recover the password. Similarly, neither Cyber Check Suite nor Autopsy is able to detect Steganography in image file, so another tool known as Aletheia is used which is not only able to detect steganography but is also able to detect in the channel RGB the data is embedded.

REFERENCES

[1] B. Nelson, A. Phillips and C. Stewart, "Guide to Computer Forensics and Investigations", Cengage Learning, vol.4, 2013.

[2] M, Simms, "Portable Storage Forensics Enhancing the Value of USB Device Analytics and Reporting", School of Computing and Mathematical Sciences, 2012.

[3] S, Erasani, "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.

[4] S. Mandecha, K. Raychaudhuri, "A Comparative Study of the performance of Open-Source and Disk Forensic Tools in Recovery of Anti-Forensically Doctored Data, International Journal of Cyber Security and Digital Forensics, 2019.

[5] S. Hiley, "Anti-Forensics with a small army of exploits", International Journal of Digital Investigations, 2007.

[6] S. Garfinkel, "Anti-Forensics Techniques, Detection and Countermeasures", 2nd International Conference on Information Warfare and Security, 2007.

[7] H. Carvey and C. Altheide, "Tracking USB storage: Analysis of Windows artefacts generated by USB storage devices", Digital Investigation, 2005.

[8] P. Singh, "Leveraging the Windows Amcache.hve file in Forensic Investigation", The Journal of Digital Forensics, Security and Law, 2016.

[9] S. Upasana and S. Bhupendra, "Program Execution Analysis Using User Assist Key in Modern Windows".

[10] Mee V., Tryfonas T., Sutherland I., "The Windows Registry as a Forensic Artefact: Illustrating evidence collection for internal usage", Digital Investigation, 2006.

[11] S. Garfinkel, "Forensic feature extraction and cross drive analysis", DFRWS, 2007.

[12] Orion, "USB Forensic Tracker- Orion Forensics Thailand", 2017.

BIOGRAPHY

Dr. Deepak Raj Rao G.: Dr. Deepak Raj Rao G. is a PhD holder in the field Cyber Crime Investigation and Digital Forensics from Madras University. He has been working as an Assistant Professor in the Cyber Forensics Division at LNJN National Institute of Criminology and Forensic Science, Ministry of Home Affairs, Govt. of India since 2015. Prior to this, he has served as the Head of Forensic Service at Keonics Cyber Lab, Bengaluru and Senior Mentor – Information Security and Cyber Forensics at iNurture Education. He has been successfully conducting various training courses in the field of digital forensics and cyber-crime investigation for high-level officials of Law Enforcement Agencies, Defence and Intelligence Agencies, Judiciary, Central and State Forensic Labs of India and SAARC Nations since the last 5 years. He has published several research articles in International Journals of repute and his research areas include Digital Forensics, Cyber-crime investigation and Information Security.

Sonu Mandecha.: Sonu Mandecha is currently pursuing M.Sc. Forensic Science with specialization in Cyber Forensics from LNJN National Institute of Criminology and Forensic Science, Ministry of Home Affairs, Govt. of India. She has done her graduation in Forensic Science from Amity University. She has published research article in International Journal and her research interests include Digital Forensics, Cyber-crime investigation etc.

Kumarshankar Raychaudhuri: Kumarshankar has done his post-graduation in Information Security from GGSIP University, Delhi. He is currently working as JRF in the field of Digital Forensics and Cyber-crime investigation at LNJN National Institute of Criminology and Forensic Science, Ministry of Home Affairs, Govt. of India. He has presented and published various research articles in International Conferences and Journals and his research interests include Digital Forensics, Cyber-crime investigation and Social Media Investigation