INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 1)
Available online at: www.ijariit.com

Forensic analysis and investigation using digital forensics- An overview

Nikunj Pansari
rangernikunj97@gmail.com
KIET Group of Institutions, Ghaziabad, Uttar Pradesh

Dhruwal Kushwaha
crazydhruwal@gmail.com
KIET Group of Institutions, Ghaziabad, Uttar Pradesh

ABSTRACT

Using Digital forensics and its investigation techniques is a path towards the data retrieval and analysis of different kinds of digital storage devices. Various kinds of digital storage devices like a USB drive (pen drive), hard drive (mainly external), floppy disks, CDs and a few others also. It is a technique or method for extracting the lost or useful data from the storage media, when unavailable. Now, forensic analysis concept comes from Digital Forensics or it can be called as its sub-domain. Certain conditions of the storage devices will be considered like burnt, wet and damaged drives for data retrieval and analysis. Data is a prime concern for every organization or individual or so-called the main component of the architecture and working of the IT industries and thus, so its repercussions can't be ignored. Companies spent almost thousands of dollars on maintaining the security of their enterprise data. Thus, the data protection and its retrieval after data theft (cyber-attacks) or loss is will help in evaluating out large-scale vulnerabilities.

Keywords— *Cyber-attacks, Digital forensics, Data retrieval, Digital storage devices, Large-scale vulnerabilities*

1. INTRODUCTION

Cyber-attacks and data retrieval is an inter-dependent perspective to be defined and executed. It is accordingly also quite useful to be secured from both of these vulnerabilities, as they may affect the functioning as well as the performance and efficiency of the system.

Data loss is very common in today's day and age. Now, with the extensibilities and improvement in the working and efficiency of Computers and new technologies, it is highly flexible to retrieve the data which might otherwise become a nightmare. It becomes a challenge nonetheless. Analysing through the tools and techniques may prove a path for extraction of lost data from internal or external hard disk drives (HDDs), solid-state drives (SDDs), USB flash drives, and other electronic devices. Data loss can occur due to File System Format, Physical drive damage, File Corruption, etc. It should also be noted that sometimes, data recovery can be used in terms of espionage, in which data under context is hidden, rather than damaged, are also recovered. Forensic experts are needed to decrypt the encrypted data.

Now, the term to be defined is how to be secured from cyber-attacks and especially those dealing with data theft and loss. Digital forensics is the solution for that kind of vulnerabilities wherein, it is the sole- responsibility of the forensic expert to deal with all kinds of data theft problems. Also, awareness among the people for these terms and its functioning can also improve this vulnerability to a great extent.

2. DIGITAL FORENSICS

For Data Retrieval through forensic techniques, Digital Forensics is the exact remedy for the problem. Digital forensics (sometimes known as digital forensic science) encompasses the recovery and investigation of material found in digital devices, often in relation to computer crime. Digital forensics investigations have a variety of applications and different domains. Forensics feature from the private sector; such as during internal corporate investigations or intrusion investigation (a specialist probe into the nature and extent of an unauthorized network intrusion) to data loss by the enterprise or individual. [4][7][5]

Now, there are various stages and procedures for the implementation of the effective digital forensics method. It is applicable to all types of digital storage devices. [4][7][5]

It can also prove to be the lifeline to serve as a cure for any kind of incident response, data recovery, and investigation strategies. [4][7][5]

© 2019, www.IJARIIT.com All Rights Reserved

2.1 Branches of Digital Forensics

2.1.1. Computer Forensics: The primary goal of this branch of Digital Forensics is to make sure that the present condition of the digital evidence or artefacts is well explained. These digital artifacts may include, computer systems, electronic documents or any data storage media, basically with rudimentary computing power and onboard memory.

The emphasis lies on dealing with information ranging from logs like internet history and related cache along with the actual files of evidence in the computer system.

2.1.2. Network Forensics: The prime concern of Network Forensics is the controlling and analysis of computer network traffic using both WAN/internet for the purpose of collecting information, detection of intrusion and collection of evidence. The data traffic intercepted is either stored for subsequent analysis or filtered in real time.

2.1.3. Mobile Forensics: Being a sub-branch of Digital Forensics, Mobile Forensics basically deals with mobile device digital evidence and recovery from the same. Mobile forensics is a little different from digital forensics, owing to the fact that it has an inbuilt communication system and personal storage mechanisms. The prime focus in mobile forensics is on simple data like call data and related communications in the form of SMS or Email services. Another important aspect of mobile forensics is the provision of location-based information via GPS. [4][5] [9]

2.1.4. Live Forensics: Live Forensics deals with the evidence related to law present in computer systems. The primary goal of Live Forensics is to mainly focus on collection of data when the computer systems are powered on so that the volatile data which might otherwise be lost due to power failure or the computer system turning off or in the worst case, the data being overwritten by new data, is actually recovered in a safe and sound manner and is collected for evidence for future investigations.

2.1.5. Database Forensics: The onus is laid on the thorough study and analysis of databases and ways into delivering the perfect blend and balance of database data acquisition and ways of figuring out which data is relevant and of use for further study and which has no real in making the forensics progress move forward in the right direction.

Database Forensics finds use in areas where the data present is quite a lot and the forensics team has to filter out only the relevant data from the whole lot.

Fig. 1: Branches of digital forensics

3. PHASES/STEPS OF DIGITAL FORENSICS

3.1 Policy and Procedure Development

Digital evidence collection can be highly sensitive and an equally delicate task, be it related to malicious cyber activity, criminal conspiracy or the intent to commit a crime. Cybersecurity professionals are of full understanding of the value of this information and provide due respect to the fact that it can be very easily breached if not properly handled and conserved. For this reason, it is quintessential to develop and follow strict guidelines and procedures for activities related to computer forensic investigations. Such procedures generally include detailed instructions about when computer forensics investigators are authorizing to recover potential digital evidence, how to properly prepare systems for evidence retrieval, where to store any retrieved evidence, and how to document these activities to help ensure the authenticity of the data. [4][9][10]

3.2 Evidence Assessment

A vital component of the investigative process comprises the evaluation of potential evidence in cybercrime. Central to the frugal assessing of evidence is a clear understanding of the details of the case at hand and thus, the division of cybercrime in question. For instance, if an agency is of the view to prove that an individual has committed crimes related to theft, of identity, computer forensics investigators use sophisticated methods to filter through hard drives, email accounts, social networking sites and other digital archives to access and assess any information that can serve as possible evidence of the crime. [4][9][10]

3.3 Evidence Acquisition

The most vital part of a successful computer forensic investigation is a rigorous, thorough plan for collecting evidence. Extensive and detailed documentation work is needed prior to, during, and after the acquisition process; detailed information must be

© 2019, www.IJARIIT.com All Rights Reserved

recorded and preserved, including all hardware and software specifications, any systems used in the investigation process, and the systems being investigated. [4][9][10]

3.4 Evidence Examination

For proper investigation of potential evidence, procedures must be in place for retrieving, copying, and storing evidence within appropriate databases. Investigators usually examine data from respective archive vaults, using a variety of methods and approaches to analyse information, including harnessing analysis software to search massive archives of data for specific keywords or file types, as well as procedures for retrieving files that have been recently deleted. Data tagged with times and dates is particularly useful to investigators, as are suspicious files or programs that have been encrypted or intentionally hidden. [4][9][10]

3.5 Documenting and Reporting

For computer forensic investigators, all actions related to a particular case should be accounted for in a digital format and saved in properly respective archives. This helps in ensuring the authenticity of any findings by allowing these cybersecurity experts to show exactly when, where, and how evidence was recovered. Thus also allowing experts to confirm the validity of evidence by matching the investigator's digitally recorded documentation to dates and times when this data was accessed by potential suspects via external sources. [4][9][10]

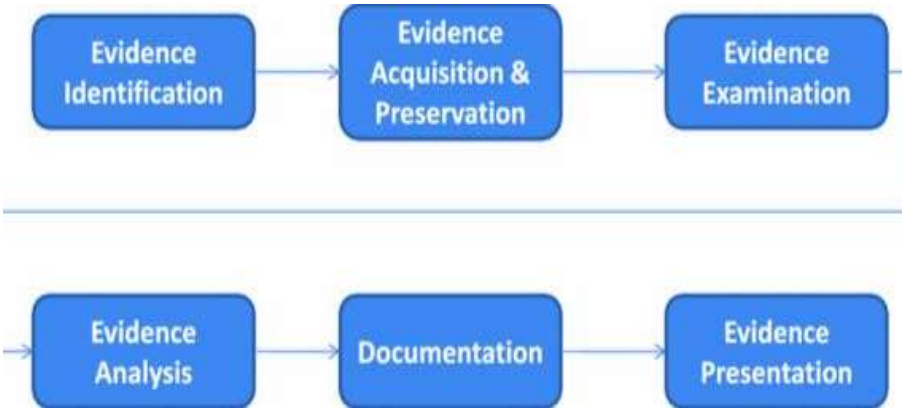

Fig. 2: Steps of digital forensic

4. SERVICES OFFERED BY DIGITAL FORENSICS

4.1 Computer Forensics

A huge amount of data can be captured by digital devices such as computers, external hard drives, and memory cards which are of critical importance to any investigation. Specialist acumen and skills are usually required to fully extract all possible data and present it as an evidential standard. A methodical approach to examining digital media to establish factual information for civil or criminal matters is the Computer Forensic Analysis Process. [10]

4.2 Mobile and Tablet Forensics

Today's Mobile devices hold a huge volume of data. Mobile device Analysis is the digital forensic approach concerned with the systematic examination of mobile phones, tablets, and satellite navigation devices and all attached media. Mobile device apps hold critical evidence of activity and movement, which can when extracted and analysed, support investigations. With the growing functionality of today's Smart mobile devices, more extensive and creative uses for these devices are evident in more and more criminal activity. [10]

4.3 Cell Site Analysis

The technique of placing a mobile device in a specific geographical location, at a certain date and time is known as Cell site analysis, or RFPS (Radio Frequency Propagation Survey) [10]

4.4 Digital Media Investigations

Digital Media Investigations involving social media applications and provide expert advice in this tricky area. Not confined to just social media but conduct online open-source investigations (OSINT) to provide intelligence or evidence also. [10]

4.5 Expert Witness

Forensics can support by fully trained experts experienced in providing testimony, providing technical analysis and opinion acknowledged by the expert. [10]

4.6 Audio and Video Forensics

Audio and Video Forensics can prove crucial in a number of civil and criminal matters, and evidence, on occasion, needs preparation and enhancement in order to aid in both legal and private matters. [10]

4.7 Data Recovery

As Digital Forensic specialists, forensic experts can analyse digital media to produce legal evidence of a crime or unauthorized action. [10]

© 2019, www.IJARIIT.com All Rights Reserved

4.8 Digital Forensic Recovery

Computer incidents take a rise in number, when there is an increase in dependency on information systems' assets, due to increase in presence of businesses online. The topmost goal of system administrators should be to be prepared for any computer network related security incident. **[10]**

5. FORENSIC ANALYSIS OF HARD DRIVES

The architecture of hard drives is very essential components for analysis of data storage, security, and access. The architecture of hard drives can be defined through figure 3. [1][2][4][7]

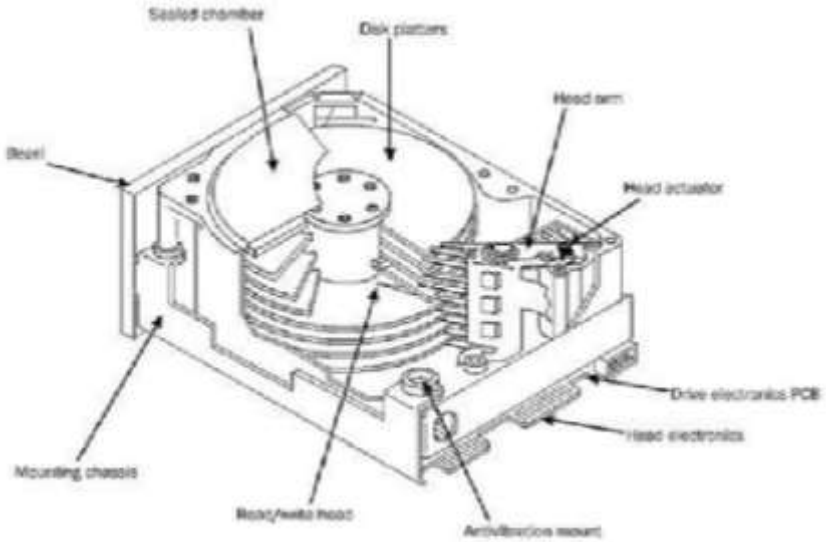

Fig. 3: Architecture of hard drives

Understanding and Analysing all the phases of Digital forensic process helps in effective data retrieval. Whether, the phases like Forensic imaging, evidence acquisition, and analysis, the tool used for automating the process defines the proper functionality and effectiveness of the software (figure 4) [1][2][4][7]

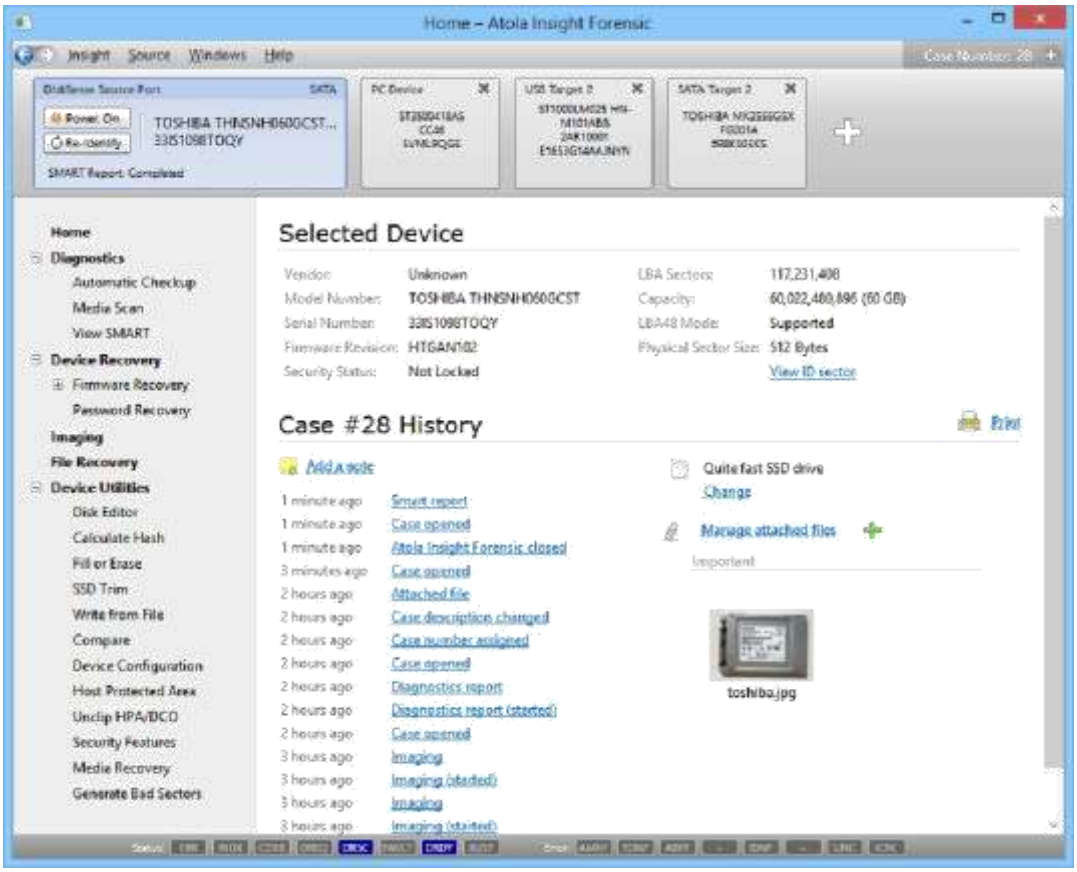

Fig. 4: Tool used for automating the process

6. FORENSIC ANALYSIS OF USB DRIVES

USB drives are a small, easy and integral solution for defining the data storage and retrieval purpose. Now, from the point of view of forensic investigation and analysis of these drives, effective and proper storage in USB drives are important. The defined architecture of USB drives depicted in figure 5. [2][6][7]

© 2019, www.IJARIIT.com All Rights Reserved

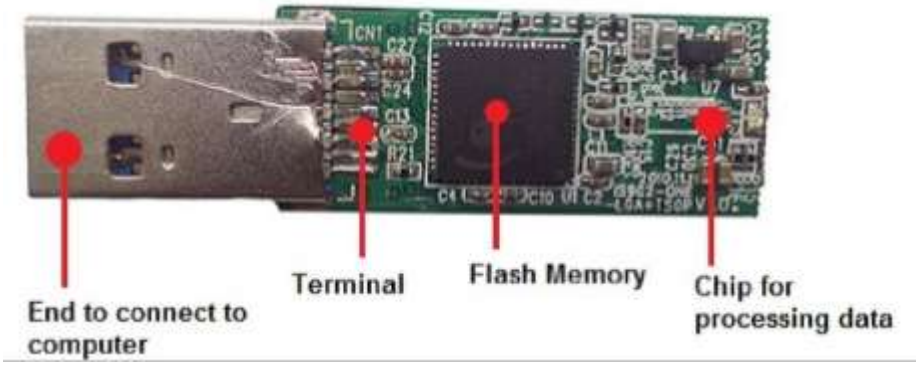

Fig. 5: Architecture of USB drives

For actual understanding and implementation of data retrieval in USB drives through forensic techniques, a slightly different process is defined mainly based on the architecture of the USB drives. Its sole purpose is the data accessing and extraction process. (Figure 6) [2][6][7]

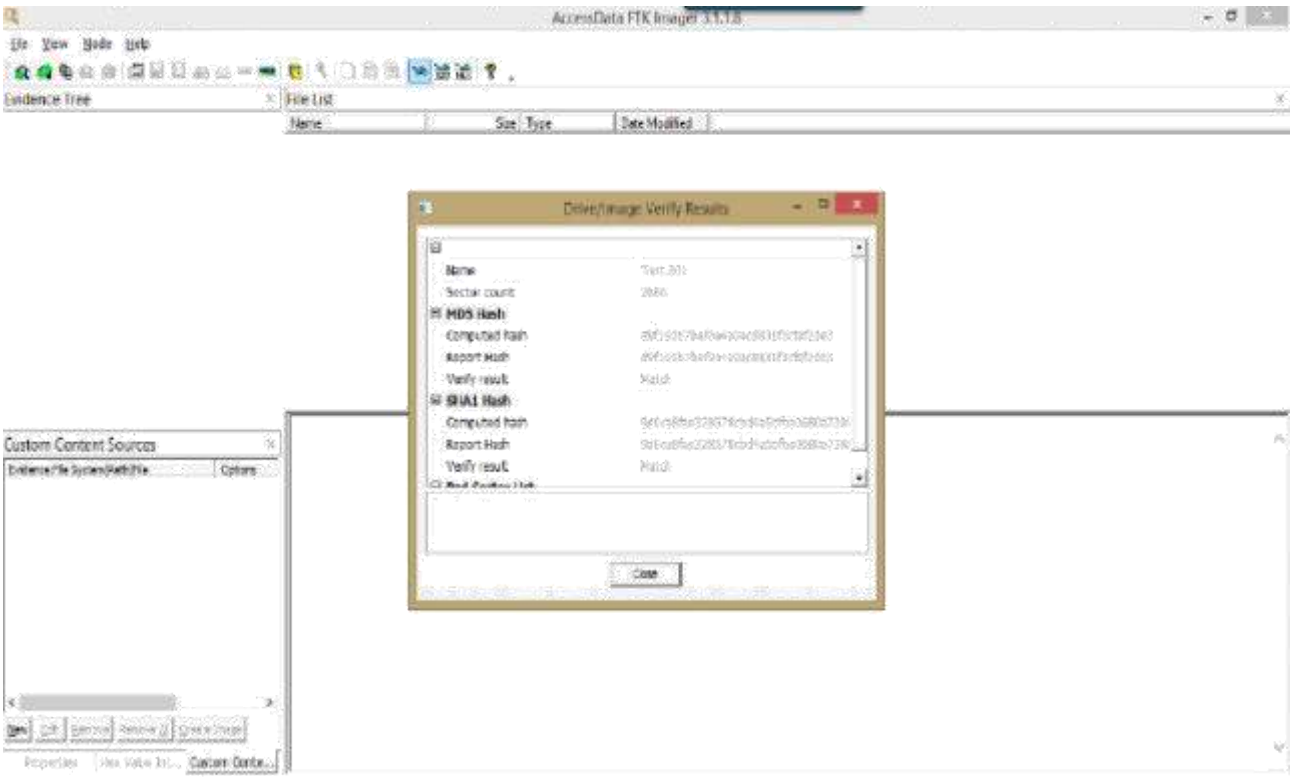

Fig 6: Data accessing and extraction process

7. CONCLUSION

The forensic analysis provides a domain for defining the repercussions of data loss or data theft. Now, it can be a vital breakthrough if people are made aware of all the pros and cons of digital forensics and especially when it comes to the data security perspective domain. Secondly, hard drives, USB drives, and other digital storage devices provide a path for data accessing and retrieval but can also prove to be a disaster when it comes to the loss of most important part of any system or workspace. Defining tools for implementing digital forensic at an organization, criminal investigation or individual level are developed, where some are the proprietor and some GPL. Various branches of digital forensics also define us as a solution for maintaining integrity at different levels of software development. Different stages of digital forensic also define a relationship and inter-dependence of data retrieval or extraction scenario through its effective and secure implementation. All the services provided by Digital forensic are evaluated and helpful enough to access the various domains of data or individual property loss related to data and cyber-crimes, which somehow includes forensic analysis.

8. ACKNOWLEDGEMENT

It gives us a huge deal of satisfaction, to finally get to mention the names of the people, who have worked tirelessly with us, in one way or the other, so that this work of us becomes a small success. First and foremost, we would like to thank our parents and siblings who have continuously stood by us, throughout the development phases of this venture, providing us with valuable insights, as and when necessary. A special thanks to our mentor Dr Ajay Agarwal Professor in Department of Information Technology, KIET Group of Institutions, Ghaziabad, Uttar Pradesh, India

We thank all our mentors for their assistance with the Cyber and Digital Forensics concept and for comments that greatly improved the manuscript of the Paper. All in all, the project is an outcome of a complete team effort, we as individuals have

© 2019, www.IJARIIT.com All Rights Reserved

worked as a team and stuck to our guns, working upon this project, putting our heart and soul into this piece of work. In the end, we would like to thank the Almighty God, for giving us the strength to push us through the hard times.

9. REFERENCES

[1] Identification and Analysis of the hard disk drive in digital forensic by Kailash Kumar, Dr Sanjeev Sofat and Dr Naveen Agarwal (IJCTA)| Sept-Oct 2011 [ISSN:2229-6093]
[2] Forensic Analysis of Virtual Hard Drives by Patrick Tobin, Nhien-An Le-Khac and Tahar Kechadi, The Association of Digital Forensics, Security and Law (ADFSL).
[3] Forensic Analysis of USB Flash memory drives by Krishnun Sansurooah, Security Research Centre School of Computer and Security Science, Edith Cowan University at 7th Australian Digital Forensics Conference.
[4] An Introduction to Digital Forensics by Irma Recendez, Pablo Martinez, and the John Abraham University of Texas-Pan American.
[5] An Examination of Digital Forensic Models by Mark Reith, Clint Carr, Gregg Gunsch, International Journal of Digital Evidence Fall 2002, Volume 1, Issue 3.
[6] FORENSIC ANALYSIS OF USB MEDIA EVIDENCE by Jesús Alexander García Luis Alejandro Franco Juan David Urrea Carlos Alfonso Torres Manuel Fernando Gutiérrez, UPB 2012.
[7] Digital Forensics Explained International Standard Book Number: 978-1-4398-7495-0 (Hardback) © 2013 by Taylor & Francis Group, LLC.
[8] https://www.digital4n6journal.com/

[9] https://www.guidancesoftware.com/blog/digital-forensics/
[10] https://www.intaforensics.com/digital-forensics/
[11] https://en.wikipedia.org/wiki/List_of_digital_forensics_tools

BIOGRAPHY

Nikunj Pansari
Bachelor of Technology in Information Technology
KIET Group of Institutions, Ghaziabad, Uttar Pradesh, India

Dhruwal Kushwaha
Bachelor of Technology in Information Technology
KIET Group of Institutions, Ghaziabad, Uttar Pradesh, India

© 2019, www.IJARIIT.com All Rights Reserved