# Digital Forensics

Rupali K.Kulkarni
Student, Dept. of computer science & engineering, India.

Dr.A.D.Gawande
Dr., Dept. of computer science & engineering, India.

**Abstract – Corporates and organizations across the globe are spending huge sums on information security as they are reporting an increase in security related incidents. The proliferation of cloud, social network and multiple mobile device usage is on one side represent an opportunity and benefits to the organization and on other side have posed new challenges for those policing cybercrimes. Cybercriminals have devised more sophisticated and targeted methods/techniques to trap victim and breach security setups. The appearance of exceedingly procedural nature of digital crimes has produced a new division of science known as digital forensics. Digital Forensics is the field of forensics science that deals with digital crimes and crimes involving computers. This paper emphases on updating of digital forensics, classification of digital forensics, overview of digital forensics, the digital forensics process in this fascinated area.**

**Index Terms – Digital forensics, Digital evidence, Digital forensics tools, Network intrusion, Information security.**

## 1. INTRODUCTION

The convergence of the technological advances and the pervasive use of computers and digital devices worldwide have brought about many advantages to mankind, but it also provides avenues for misuse and opportunities for committing crime and wilfully commit social harm. While information security risks have dramatically evolved, security strategies have not kept pace with today's determined adversaries. Consequently, sophisticated intruders can bypass security defences to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many usage well researched phishing activities that target top administrators [1, 2 and 3]. This time's survey displays that identified security incidents have increased, as has the cost of breaks. And hot-button services like cloud computing, mobility, and BYOD (bring your own device) are performed before they are secure [3, 4 and 5].

## 2. RELATED WORK

Due to the increasing in cyber crime demand of the digital forensics researchers have done some study and field work.

- Overview of digital forensics :-
- Classification of digital forensics

### 2.1 Overview of digital forensics :-

A frequently cited definition for Digital Forensic Science is that of the Digital Forensic Research Workshop (DFRWS) of 2001[6]: "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations". The Kruse and Heiser define digital forensics as [7]: "Protection, documentation, abstraction, certification, and explanation of computer media for evidentiary and/or root cause examination".

### 2.2 Classification of digital forensics:-

1) Computer forensics :- The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

2) Network forensics :- Network forensics is a sub-branch of digital forensics connecting to the checking and investigation of computer network movement for the determinations of evidence meeting, authorized evidence, or disturbance detection [1].

3) Database forensics :- Database forensics a branch of digital forensic science relating to the forensic study of databases and their related metadata[1].

4) Email forensics:- The education includes documentation of the actual sender and recipient of the troubled emails, timestamp of the email communication, purpose of mail, record of the whole email operation.

## 3. PORPOSED MODELLING

The digital forensics process :-

The most common goal of performing forensics analysis is to gain a better understanding of an event of interest by finding and analysing the facts and evidences related to that event. Digital forensics may be required in many different conditions, such as evidence group for legal events and internal corrective actions, and behavior of malware incidents and uncommon operational problems. Nevertheless of the need, forensics should be performed using the four-phase process shown in

Figure 1. The particular details of these steps may differ based on the complete need for forensics.

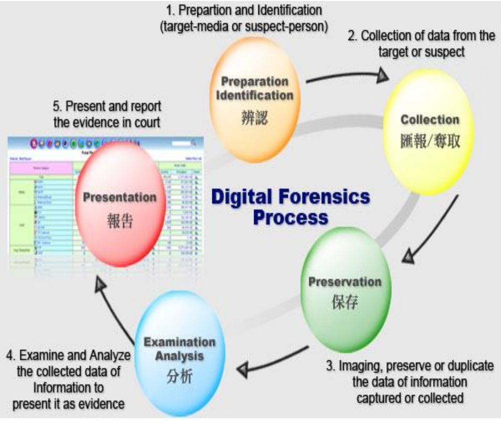
1. Prepartion and Identification
(target-media or suspect-person)
2. Collection of data from the target or suspect
Preparation Identification
辨認
Collection
匯報/奪取
5. Present and report the evidence in court
Presentation
報告
Digital Forensics Process
Preservation
保存
Examination Analysis
分析
4. Examine and Analyze the collected data of Information to present it as evidence
3. Imaging, preserve or duplicate the data of information captured or collected

Fig -1: The digital forensics process

1)COLLECTION:- Identify, isolate, label, record, and collect the data and physical evidence related to the incident being investigated, while establishing and maintaining integrity of the evidence through chain-of-custody.

2) INVESTIGATION:- Recognize and abstract the applicable information from the composed data, using suitable forensic tools and techniques, while ongoing to maintain reliability of the evidence.

3) ANALYSIS: - Analyse the results of the examination to generate useful answers to the questions presented in the previous phases.

4) BROADCASTING:- Reporting the results of the analysis, including:

- Findings relevant to the case

- Actions that were performed

- Actions left to be performed

-Recommended improvements to procedures and tools

## 4. RESULTS AND DISCUSSIONS

The digital forensics tools:-

A wide variety of digital forensics tools, both commercial and open source, are currently available to digital forensics investigators. These tools, to changing degrees, provide levels of generalization that permit investigators to safely make copies of digital evidence and perform predictable investigations, without becoming overcome by low level details, such as physical disk organization or the specific structure of complicated file types, like the Windows / OS registry. Many existing tools provide an intuitive user interface that turns an investigation into something resembling a structured process, rather than an arcane craft. The main impartial of digital forensics tools is to abstract digital evidence which can be acceptable in court of law. Various digital forensics tools and their description are provided in [8, 9].

1) Coroner's Toolkit

2) Sleuth Kit/Autopsy Browser

3) Encase Forensics

4) I2Analyst's Notebook

5) Forensic Toolkit

6) LogLogic LX2000

7) Mandiant First Response etc.

## 5. APPLICATION

1) ACKNOWLEDGMENT:- Meta data and other logs can be used to attribute actions to an individual.

2) EXCUSES AND STATEMENTS:- Information delivered by those involved can be cross checked with digital evidence.

3) COMMITTED:- As well as finding objective evidence of a crime being committed, investigations can also be used to prove the intent.

4) VALUATION OF SOURCE:- File artifacts and meta-data can be used to identify the origin of a particular piece of data.

5)DOCUMENT AUTHENTICATION:- Related to "Evaluation of source," meta data associated with digital documents can be easily modified.

## 6. CONCLUSION

The threat of cybercrime is increasingly apparent to individuals and organizations across the globe. From phishing to equitation, cheating to training, and botnets to cyber-terrorism, the variety and originality of activities perform to expand constantly. Also the improvement in the digital forensic investigation tools, the organizations or procedures established to obtain the information also become more advanced. Individual of the key factors of the condition is contributed by the way computing technology grows. The fast development of computing devices needs new procedures or tools to be used by the digital forensic investigators to achieve the evidences as a legally developed evidence to be presented in the court. As the computing technology evolves the way computer user use or transfer the data in their environment also different from traditional computing system. As an initial step to decrease the confidentiality issue, it is essential to battle the complications at the root level.

## REFERENCES

[1] Anna Burgard and Christopher Schlembach , "Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet ", International Journal of Cyber Criminology, vol 7 (2): 112–124, July – December 2013.

[2] Deloitte," Cyber Crime: A Clear and Present Danger; Fighting the Fastest Increasing Cyber Security Threat", Center for Security & Privacy Solutions. p. 1-16, 2010.

[3] The Global State of Information Security Survey 2014 released by PwC US in conjunction with CIO and CSO magazines, Available at: www.pwc.com/gsiss2014.

[4] Information Security Breaches Survey 2013, technical report conducted by PwC in association with infosecurity, Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200455/bis-13-p1842013-information-security-breaches-survey-technical-report.pdf.

[5] Information security predictions for 2014 from Symantec, Available at: http://www.symantec.com/connect/blogs/2014-predictions-symantec-0.

[6] Palmer, G." A Road Map for Digital Forensic Investigation". DFRW Technical Report 2001.

[7] Kruse W. G. & Heiser J. G. Computer Forensics. Incident Response Essentials. Addison-Wesley 2001.

[8] List of digital forensics tools - Wikipedia, the free encyclopedia. Available at: http://en.wikipedia.org/wiki/List_of_digital_forensics_tools

[9] Andrew Zammit Tabona," Top 20 Free Digital Forensic Investigation Tools for SysAdmins", 2013. available at : http://www.gfi.com/blog/top-20-free-digital-forensic-investigation-tools-for-sysadmins/