Tracing the Development of Computer Forensics Within the Digital Forensic Framework

Carlos Eduardo Ramírez[1], Maria Luisa Gutiérrez[2], João Pedro Silva[3]*
[1]Departamento de Ingeniería Electrónica, Universidad de los Andes, Bogotá, Colombia
[2]Facultad de Ciencias, Universidad Nacional Autónoma de México, Ciudad de México, México
[3]Departamento de Engenharia de Computação, Universidade de São Paulo, São Paulo, Brazil

ABSTRACT

Forensics is a constantly improvising field which can be said as an application of science to the legal process. Digital forensics is a division of forensic science detailing the recovery and investigation of material found in digital devices, frequently in relation to computer based crimes. The term digital forensics was initially used as a synonym for computer forensics and has extended to wrap investigation of all devices capable of storing digital data. Branches of forensic science are embedded in every branch of science and many other aspects of Digital era because of its capability to uncover and present objective evidence from varied areas such as business systems, chemistry, ecosystems and accounting. Forensics is an integral part of the judicial system. This paper reviews the basics of digital forensics with an emphasis on computer forensics.

Keywords: *Forensics; Digital and Computer Forensics; Tools; India; Applications.*

I. INTRODUCTION

Forensic science is the combination of two words – 'forensic' and 'science'. Forensic a Latin word refers to discussions or inspections carried out in public, as trials anciently were normally held in public. The second word science is derived from the Greek refers a systematic way of acquiring knowledge. As a whole, forensic Science can be considered as the process of using the scientific methods and relevant processes in crime solving. Forensic science is the application of science to criminal and civil laws, mainly—on the criminal side—during criminal investigation, as governed by the legal standards of admissible evidence and criminal procedure.

Forensic scientists collect, preserve, and analyze scientific evidence during the course of an investigation. While some forensic scientists pass through to the scene of the crime to accumulate the evidence themselves, others engage a laboratory task, performing analysis on objects brought to them from other resources. Forensic scientists also testify as specialist witnesses in both criminal and civil cases and can work for either the prosecution or the defense. While any field could technically be forensic, certain segments have developed over time to cover the majority of forensically associated cases.

The Prominent Classification of Forensic Science is,

- Forensic Psychology
- Forensic Pathology
- Forensic Odontology
- Forensic Toxicology
- Digital Forensics
- Criminology

Because of this array of subspecialties available within the field, forensic scientists can be drawn in to resolve a crime at any point in the criminal justice process. The use of Computers has increased with the advent of high speed networks and gadgets. The presence of electronic data in digital form such as documents, multimedia has drastically improved over the years. The presence of such data provides digital evidence for trials and cases to be solved. A branch of Forensics which can recover such data even after it is deleted, encrypted and even corrupted from various electronic devices is referred as Digital Forensics. The exponential growth in the volume of data proliferating from various devices and formats has implicitly demanded the rise of digital Forensics.

II. DIGITAL FORENSICS

The science of digital forensics has a seemingly limitless future and as technology advances, the field will continue to expand as new types of digital data are created by new devices logging people's activity. Although digital forensics began outside the mainstream of forensic science, it is now fully absorbed and recognised as a branch of forensic science. Digital forensics is the process of detecting and interpreting electronic data from various sources. The objective of the process is to safeguard every evidence in its most original form. This is concurrently done at tandem while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

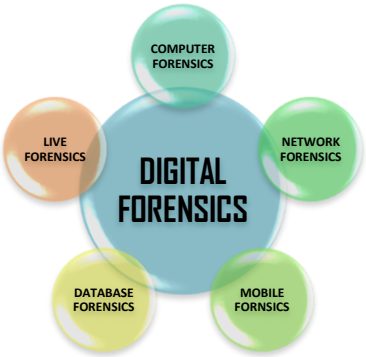

Figure 1: Classification of Digital Forensics

Digital forensics is a constantly evolving scientific field with many sub-disciplines. Some of these sub-disciplines as in Figure1 are:

1. **Computer Forensics** – the identification, preservation, collection, analysis and reporting on evidence found on computers, laptops and storage media in support of investigations and legal proceedings.
2. **Network Forensics** – the monitoring, capture, storing and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, i.e. worms, virus or malware attacks, abnormal network traffic and security breaches.
3. **Mobile Devices Forensics** – the recovery of electronic evidence from mobile phones, smart phones, SIM cards, PDAs, GPS devices, tablets and game consoles.
4. **Digital Image Forensics** – the extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.
5. **Digital Video/Audio Forensics** – the collection, analysis and evaluation of sound and video recordings. The science is the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.
6. **Memory forensics** – the recovery of evidence from the RAM of a running computer, also called **live acquisition**.

Digital forensics investigations support or negate a hypothesis before criminal or civil courts have a variety of applications. It also features in the private sector; during internal corporate investigations where information technology is used to commit or conceal an offense. The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved; computer forensics, network forensics, forensic data analysis and mobile device forensics. The typical forensic process encompasses the seizure, forensic imaging (acquisition) and analysis of digital media and the production of a report into collected evidence.

III. KEY PROCESSES IN DIGITAL FORENSICS

Digital Forensics includes a sequence of process in extracting data from evidences in resources. The following are basic steps in digital forensics. The sequence of process is,

- Identification
- Collection
- Preservation
- Examination
- Analysis
- Interpretation

- Documentation and
- Presentation of computer evidence stored on a computer.

Identification refers to what type of data can be retrieved using various computer tools and software suites. The next step is to collect all the available data sources that are imperative to the retrieval process. The data extracted through tools is preserved for further process. The Examination process analyses the data retrieved with detail introspections. The Studied data is exactly interpreted with relevant supporting documents. Finally the presentation is done through retrieved data. The presentation normally helps in trials and to solve cases pertaining to the crime. Figure 2 describes the basic process in digital forensics.

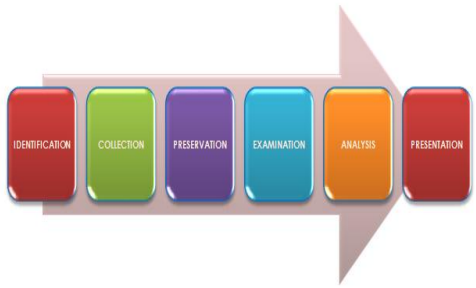

Figure 2: Process in Digital Forensics

This process can be represented in terms of stages by which data is retrieved in forensics. In the First Stage, the investigation preparation is done. The objective of the investigation and the resources pertaining to that are identified. In the Second Stage, Evidence is acquired. The digital sources are identified and evidence is preserved. In the third stage, the evidence is analysed through tools and procedures. The result is then interpreted. In the Final Stage, the result is disseminated for report findings. Then the reports are presented for further actions.

IV. COMPUTER FORENSICS

Computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law. Computer forensics is emerging as an important tool in the fight against crime. Computer forensics may be defined as the investigation of situations where there is computer-based (digital) or electronic evidence of a crime or suspicious behaviour, but the crime or behaviour may be of any type not otherwise involving computers. Therefore, computers facilitate both the commission and investigation into the act in question. Specialists in the area follow structured methodologies to ensure the integrity of the evidence that they collect and process.

It is not just law enforcement that is budding the computer forensics field. Increasingly, commercial and non-commercial organisations are requiring expertise the field to investigate incidents. Thus, there are many applications of computer forensics tools and techniques other than for criminal prosecution, such as:

- Determine Primary cause of an event to ensure its non recurrence.
- Identify accountability for an action
- Inner investigation within the location
- Intelligence operations
- Inspection and Review
- Recovering lost records

Computer forensics investigations require much duration to conduct due to the increasing size of storage media that is being encountered. Prior to an investigation, the analyst must understand the purpose of the investigation to determine the tools and techniques used for the resulting investigation. In the next step, evidence must be collected.

This must be conducted vigorously and sustain the reliability of the evidence. Once the evidence is collected, a copy of the material is made and all analysis is performed on the copy.

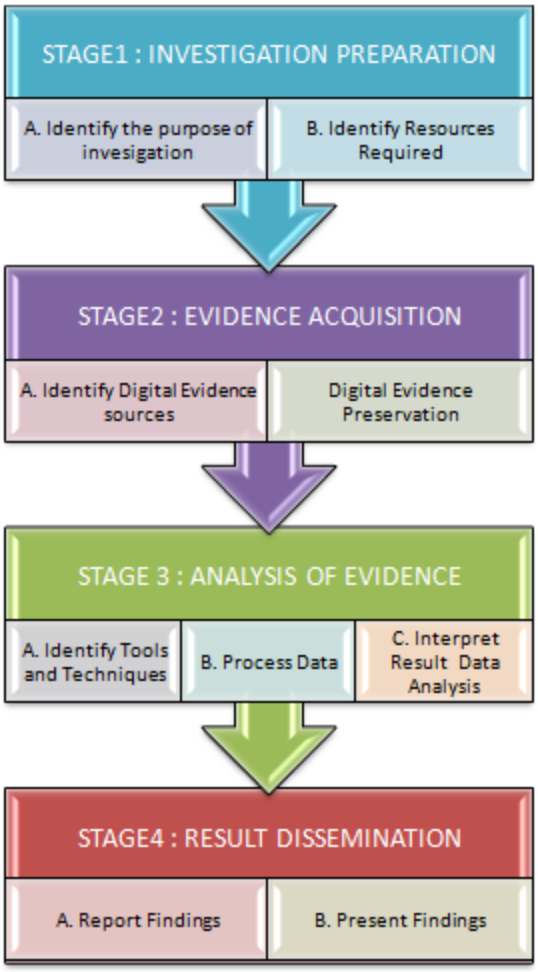

Figure 3: Stages in Digital Forensics

This makes sure that the original evidence is not polluted in any way. The analysis of the evidence is conducted with forensics tools. Once this is done, the analyst may have to try and view both extant and deleted files to build a picture of the suspect's activities.

The analyst will then report any suspicious or malicious files and supply supporting evidences with data such as, the time and date the file was created, accessed or modified and which user was liable.

Finally, the analyst must present evidence in the law enforcement. The commonly used forensic tools for such purposes are listed in the table 1.

Table 1: List of forensic tools

Name	Description
Autopsy	A digital forensics platform and GUI to The Sleuth Kit
COFEE	A suite of tools for Windows developed by Microsoft
Digital Forensics Framework	Framework and user interfaces dedicated to Digital Forensics
EPRB	Set of tools for encrypted systems & data decryption and password recovery
EnCase	Digital forensics suite created by Guidance Software
FTK	Multi-purpose tool, FTK is a court-cited digital investigations platform
ILOOK	Comprehensive forensics tool without needing expensive hardware
ISEEK[2]	Hybrid-forensics tool running only in memory - designed for large networked environments
IsoBuster	Essential light weight tool to inspect any type data carrier
Netherlands Forensic Institute / Xiraf[3]	Computer-forensic online service.
Open Computer Forensics Architecture	Computer forensics framework for CF-Lab environment
OSForensics[4][5]	Multi-purpose forensic tool
PTK Forensics	GUI for The Sleuth Kit
Registry Recon	Forensics tool that rebuilds Windows registries from anywhere on a hard drives and parses them for deep analysis.
SafeBack[6]	Digital media (evidence) acquisition and backup
SANS Investigative Forensics Toolkit - SIFT	Multi-purpose forensic operating system
The Coroner's Toolkit	A suite of programs for Unix analysis
The Sleuth Kit	A library of tools for both Unix and Windows
Windows To Go	Bootable operating system
Wireshark	Open-source packet capture/analyzer, backend library used is [win]pcap.

V. APPLICATIONS OF COMPUTER FORENSICS

Law enforcement agencies have been among the earliest and heaviest users of computer forensics and consequently have often been at the forefront of developments in the field. It is not just the content of emails, documents and other files which may be of interest to investigators but also the 'metadata' associated with those files. A computer forensic examination may reveal when a document first appeared on a computer, when it was last edited, when it was last saved or printed and which user carried out these actions.

More recently, businesses have used computer forensics to their benefit in a variety of cases such as,

- Intellectual Property theft
- Industrial espionage
- Employment disputes

- Fraud investigations
- Forgeries
- FCPA investigations
- Inappropriate email and internet use in the work place
- Regulatory compliance

VI. DIGITAL FORENSICS IN INDIA

Cyber forensics is a looming field in India and Indian legal and judicial system has to adapt itself according to the same. As of now in India cyber forensics is not widely and appropriately used by the law enforcement agencies, lawyers, judges, etc. As a result most of the cyber criminals are either not prosecuted at all or they are acquitted in the absence of adequate evidence.

Use of cyber forensics and e-discovery methodologies is going to increase in India in the near future. Indian government has also realized this aspect and has already started modernization of police force of India. This includes inculcating cyber law awareness, cyber crimes investigation trainings, trainings regarding use of cyber forensics, etc to the law enforcement agencies of India. Nevertheless the need to develop cyber forensics best practices in India and strengthening of cyber forensics and cyber crimes investigation capabilities in India has not yet been addressed by Indian government. Even the announced regulations and guidelines for effective investigation of cyber crimes in India are missing till date.

Clearly handling of digital evidence is a big challenge for the law enforcement agencies of India. This is a set back and it is evident troubling our law enforcement agencies in Kalmadi Case, Aadharsh Case, Aarushi Talwar's murder case, IPL Match Fixing case, Bitcoins websites investigation, Nokia's tax violation case, Spectrum Cases, Rajnath Singh Son's case, Amrita Rai's G-Mail account hacking case, etc. Indian government must seriously consider empowering law enforcement agencies of India with suitable trainings and technologies.

To help cracking cases and faster trials, RCCF was set. Resource Centre for Cyber Forensics (RCCF) is a pioneering institute, pursuing research activities in the area of Cyber Forensics. The centre was dedicated to the nation by the then Honorable union minister in August 2008.

RCCF was set up with the following objectives:

1. Developing indigenous Cyber Forensics tools.
2. Providing training on Cyber Forensics to Law Enforcement Agencies (LEAs)
3. Providing technical support to LEAs for cybercrime investigation and analysis.

Also, Centre for Development of Advanced Computing (C-DAC) is the premier R&D organization of the Department of Electronics & Information Technology (DeitY), Ministry of Communications & Information Technology (MCIT) for carrying out R&D in IT, Electronics and associated areas. Different areas of C-DAC, had originated at different times, many of which came out as a result of identification of opportunities.

The setting up of C-DAC in 1988 itself was to build Supercomputers in context of denial of import of Supercomputers by USA. Since then C-DAC has been undertaking building of multiple generations of Supercomputer starting from PARAM with 1 GF in 1988.

Electronic Research and Development Centre of India (ER&DCI) with various constituents starting as adjunct entities of various State Electronic Corporations had been brought under the hold of Department of Electronics and Telecommunications (now DeitY) in around 1988. They were focusing on various aspects of applied electronics, technology and applications.

C-DAC has today emerged as a premier R&D organization in IT&E (Information Technologies and Electronics) in the country working on strengthening national technological capabilities in the context of global developments in the field and responding to change in the market need in selected foundation areas.

VII. CONCLUSION

Digital forensics is imperative in solving crimes with digital devices and against people where the evidence may exist in a device. It is evident that any breakthrough in a trial is possible only through forensic tools and procedures. The process of forensic science has grown leaps and bounds. Despite boundless tools, procedures and methods evolving in this information technology era, digital forensics still provides a lot of potential for heavier research across various forensic domains. Next generation may witness purely computer based investigations with substantial digital evidences aiding faster trials and judgments.

REFERENCE

1. *Casey, Eoghan (2004)Digital Evidence and Computer Crime, Second Edition. Elsevier.ISBN 0-12163104-4.*
2. *Leigland, R (September 2004). "A Formalization of Digital Forensics"*
3. *JISTEM -Journal of Information Systems and Technology Management Vol. 12, No. 2 May-Aug 2015 pp.233-244 ISSN online: 1807-1775*
4. *Ankit Agarwal, Megha Gupta, Saurabh Gupta & S.C. Gupta. (2011). Systematic Digital Forensic Investigation Model, International Journal of Computer Science and Security (IJCSS).Volume(5).Issue (1)*
5. *https://www.fbi.gov/investigate/cyber*
6. *http://www.cyberforensics.in/Aboutcdac.aspx*
7. *http://www.cert.org/digital-intelligence/September 2017*
8. *https://www.us-cert.gov/sites/default/files/publications/forensics.pdf*
9. *https://www.ncjrs.gov/pdffiles1/nij/199408.pdf*