**DIGITAL FORENSICS REPORT**

***Report submitted to***

***Career Dreams Education ,Technophilia 1.0***

***For the fulfillment of intern project***

### Degree of

# **Bachelor of Technology**

In

**Computer Science and Engineering**

**SUBMITTED BY**

**A.Manisha Sushma**

*Under the supervision of*

**PN SUMANTH Sir**

****

**CAREER DREAMS EDUCATION ,TECHNOPHILIA 1.0**

**JAIPUR, RAJASTHAN 302015**

©️Manisha, JULY 2021. All rights reserved.

**ABSTRACT :**

The field of digital forensics has evolved to allow security professionals to examine evidence from the increasing plethora of digital devices to help determine what individuals might have done in the past. The evidence collected is used in a wide variety of settings: from corporate server farms to police raids on criminals' houses to the modern battlefield, and now to international cloud environments. This year, we accepted three papers for presentation in the Digital Forensics -- Education and Research Minitrack which should promote some interesting discussions in some emerging areas of digital forensics. The papers in this session represent much of the ongoing work in the forensics community and are an exciting representation of a larger body of work dedicated to ensuring that digital evidence remains available and useful for the good of the public.

**Keywords:** digital forensics, digital forensic science, computer forensics, network forensics.

**INTRODUCTION :**

Digital forensics1, the art of recovering and analysing the contents found on digital devices such as desktops, notebooks/netbooks, tablets, smartphones, etc.was little-known a few years ago. However, with the growing incidence of cyber crime, and the increased adoption of digital devices, this branch of forensics has gained significant importance in the recent past, augmenting what was conventionally limited to the recovery and analysis of biological and chemical evidence during criminal investigations.

The field of digital forensics has evolved to allow security professionals to examine evidence from the increasing plethora of digital devices to help determine what individuals might have done in the past. The evidence collected is used in a wide variety of settings: from corporate server farms to police raids on criminals’ houses to the modern battlefield, and now to international cloud environments. This year, we accepted three papers for presentation in the Digital Forensics – Education and Research Minitrack which should promote some interesting discussions in some emerging areas of digital forensics.

The papers in this session represent much of the ongoing work in the forensics community and are an exciting representation of a larger body of work dedicated to ensuring that digital evidence remains available and useful for the good of the public.

The papers this year are diverse in topic including Android, educating the judiciary, and file matching based on content similarity rather than hashing. The diversity in topics provides a well-rounded view of the current state of digital forensics and some focus areas that need additional attention.

**LITERATURE SURVEY :**

Nowadays, with the demand of web applications there is also an increase in the number of problems and crimes that demand an investigation that requires digital forensics techniques in order to manage web evidence. Although there are several studies that address cyber forensics, they are mainly oriented to manage evidence at server side, as far as we know, no systematic literature reviews have been reported on how cyber forensics is addressed at clients' side; considering the international standards. Thus, this paper presents a literature review about how cyber forensics is addressed at clients' side related to techniques of identification, collection, analysis, preservation and report of digital evidence. Also, a review of how standards are being used in cyber forensics focused on the client side. The aim of this study is to provide a background of relevant activities that are considered by investigators to handle potentially digital evidence from web environments, considering what international standards are solving for this purpose. Thus, a total of 37 studies have been selected and analyzed in this study. Moreover, this study provides important insights about the need to create methodologies aligned with formal standards that support the management of the evidence in an appropriate way.

A systematic literature review is a means of categorizing and summarizing all available research that is relevant to a particular research question, topic area, or phenomenon of interest [7]. Also, it is used to identify, evaluate and interpret all available studies related to a particular research topic. In this section, a set of primary studies has been analyzed, which contributes in answering the gaps addressed during the web forensics research when it has been considered the evidence found at clients’ side. In order to perform this literature review, the Kitchenham methodology [19] has been applied. This methodology has three main activities: i) planning the review, ii) conducting the review, and iii) reporting the review. A. Planning the Review The first step towards accomplish this step is to define the research question, the search strategy, the selection of the primary studies, and finally, define the extraction criteria. The research question to be answered is: Which forensics procedures are considered by forensic researchers for the management of digital evidence hosted on the clients’ side of a web environment? The research sub-questions are: (a) RQ1: What kind of digital evidence from web environments can be found on clients’ computers? (b) RQ2: Where could be found the web evidence at client’s side? (c) RQ3: How is it possible to preserve digital evidence in order to guarantee its integrity? (d) RQ4: In which way could the standards be used in the management of digital evidence? The period covered starts in 2004, this milestone was chosen because it is the start point of web 2.0. To perform this study, different sources have been chosen (i.e., representative books, important journals, conferences and workshops). For the automatic search, the selected digital libraries are: IEEEXplore, ACM Digital Library, SpringerLink, and SinceDirect.

The search string is “(FORENSIC) AND (WEB OR BROWSER OR CLOUD) AND (DIGITAL) AND (EVIDENCE)”. In order to include the primary studies to be analyzed, the following inclusion criteria have been selected: a) Studies presenting methods to collect and process digital evidence from the use of web applications. b) Studies presenting methods to safeguard digital evidence. c) Studies presenting tools, which allow to automate computer forensic processes. The exclusion criteria are: d) Introductory papers of special issues, books and workshops. e) Duplicate reports of the same study in different sources. f) Short papers with less than five pages. g) Papers not written in English. Moreover, the strategy to obtain the data was defined by breaking down each research question into more specific extraction criteria

**DIGITAL FORENSICS ANALYSIS PROPOSED METHODOLOGY :**

The complete definition of digital forensics is as follows: 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.3,4 The key elements of digital forensics are:

The use of scientific methods

• Collection and preservation

• Validation

• Identification

• Analysis and interpretation

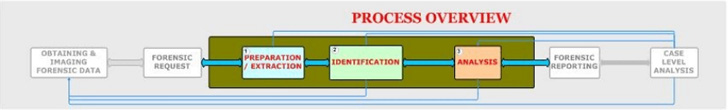
• Documentation and presentation

In general, the goal of digital forensic analysis is to identify digital evidence for an investigation. An investigation typically uses both physical and digital evidence with the scientific method to draw conclusions. Examples of investigations that use digital forensics include computer intrusion, unauthorized use of corporate computers, child pornography, and any physical crime whose suspect had a computer. At the most basic level, digital forensics has three major phases:

1. Acquisition Phase: It saves the state of a digital system so that it can be later analyzed. This is analogous to taking photographs, fingerprints, blood samples, or tire patterns from a crime scene. As in the physical world, it is unknown which data will be used as digital evidence so the goal of this phase is to save all digital values. At a minimum, the allocated and unallocated areas of a hard disk are copied, which is commonly called an image. Tools are used in the acquisition phase to copy data from the suspect storage device to a trusted device. These tools must modify the suspect device as little as possible and copy all data.5,6

2. Analysis Phase: It takes the acquired data and examines it to identify pieces of evidence. There are three major categories of evidence we are looking for: – Inculpatory evidence, which supports a given theory

3. Presentation Phase: Although It Is Based Entirely On Policy and law, which are different for each setting, this phase presents the conclusions and corresponding evidence from the investigation. In a corporate investigation, the audience typically includes the general counsel, human resources, and executives. Privacy laws and corporate policies dictate what is presented. In a legal setting, the audience is typically a judge and jury, but lawyers must first evaluate the evidence before it is entered. In order to be admissible in a US legal proceeding, scientific evidence must pass the so-called Daubert tes



The three steps in the forensics process discussed in this article come after examiners obtain forensic data and a request, but before reporting and case-level analysis is undertaken. Examiners try to be explicit about every process that occurs in the methodology. In certain situations, however, examiners may combine steps or condense parts of the process. When examiners speak of lists such as "Relevant Data List," they do not mean to imply that the lists are physical documents. The lists may be written or items committed to memory. Finally, keep in mind that examiners often repeat this entire process, since a finding or conclusion may indicate a new lead to be studied.

**CONCLUSION:**

As examiners and requesters go through this process, they need to think about return on investment. During an examination, the steps of the process may be repeated several times. Everyone involved in the case must determine when to stop. Once the evidence obtained is sufficient for prosecution, the value of additional identification and analysis diminishes.

It was found that there are few studies that mention or use standards, also the majority of research and second studies focused on server side and the possible attacks. Moreover, the ISO/IEC 27000 family that affects digital evidence analysis was presented. Each document has an impact in the area of investigation, and helps to the standardization for the method development. The guidelines provide a way to ensure the results of the investigation, the investigators should adapt them to the changes and new standards in order to guarantee the development of the analysis method. Researchers must adapt to changes and new rules to ensure the proper development of the method of analysis. It is important to emphasize that the standards provide guidelines for the correct handling of digital evidence; however, there are only few studies that use them for solving the forensics cases. The processes associated with the standards (identification, collection, acquisition and preservation) are used for the research process. They maintain the integrity of the evidence, provide an acceptable methodology, manage systematically and preserve their integrity. As further work, it is planned to study the field of mobile devices (e.g., cellphones, tablets, smartwatches) and its specific needs; identifying current methods, tools, guidelines to manage digital evidence. It will help investigators to understand new challenges, restrictions, and solutions for the next few years.

**FUTURE SCOPE & STUDY :**

Cybercrime Forensic investigation is a complicated science with its own history, implications and future. It is not sufficient merely to consider it a branch of criminology, or the study of cyber criminal behavior, or research into the relationship between the causes of tech related crime and social policies. For cyber criminals, their knowledge and their crimes are bound together. The possible suspects are rich in knowledge and technical skills. They have mastered the technology better than the technology’s creators, and they know how to use technology against technology.

A multidisciplinary approach is required to fully foresee the future of cybercrime forensics. It requires a team of specialists from different disciplines within the IT industry and related industrial and social segments such as telecom and law. However, in this article the author looks at the future of cybercrime forensics based on his knowledge and experience in this field.

**Cybercrime Forensics for Governments**

Cybercrime forensics at the governmental level will be more complicated in the future. Governments will need to turn more to their national security organisations to hunt down cyber criminals. In addition, they will need to invent anti-forensic tools and methods to keep their activities and information assets secret.Cyberspace security and computer related technologies will be a real challenge for governments. The platforms and protocols for computer related technologies may have both domestic and international uses. Therefore, it will be difficult for governments to reach an agreement for international cyber security policies.

At the same time, some countries are the technology owners and this intellectual property ownership will give them an advantage compared to other countries without such a privilege. The technology ownership issue will force the other countries to utilise the open source platforms to develop their own customised operating systems and software.

**Cybercrime Forensics in Universities:** It is sad to note that more and more often information technology advances are coming from industry rather than universities. Within IT, a few companies dominate the industry and therefore the innovations. It will be the same for cybercrime forensics; the companies with market share have the money for research and development. The main issue with academic institutions is their approach, which is slow and traditional compared to the faster speed of development and implementation found in industry.

**Cybercrime Forensics in Professional Institutions:** Cybercrime forensics is a new battleground for professional institutions. Currently, there is no real internationally recognised authority to govern cybercrime forensics practices, regulations and certification. Therefore, professional institutions are offering cybercrime forensic investigation training programs, certifications and conferences. Currently, some of these institutions are forming alliances (as trade and training partners) to achieve their sales targets. In the future, it is likely that these institutions will start to attack each other to gain market share

**Cybercrime Forensics for Corporates:**Currently a few companies have dominated the cybercrime forensic markets. These are the pioneers in cybercrime forensics and analysis. They have the tools and the solutions for cyber forensic investigation. They train law enforcement agencies to use their tools and solutions and some of them even have special tools just for governmental use. There are also many small companies with one or two consultant partners who are either retired law enforcement officers or former IT professionals from Fortune 500 companies. These people use their contacts and credentials to achieve some market share. However, in the future, cybercrime forensics at the corporate level will be diversified to education and certain specialties and products. It will be difficult for small companies to build a team with the right core competencies. In addition, due to security clearance requirements and national security interests, most of these companies will only practice in their country of origin.

**REFERENCES**

[1] K. Nance and M. Bishop, "Introduction to Digital Forensics -- Education, Research and Practice Minitrack," 2016 49th Hawaii International

Conference on System Sciences (HICSS), 2016, pp. 5596-5596, doi: 10.1109/HICSS.2016.692.

[2] Anghel, Catalin. (2019). Digital Forensics – A Literature Review. 42. 23-27. 10.35219/eeaci.2019.1.05.

[3] B. Coronel, P. Cedillo, K. Campos, J. Camacho and A. Bermeo, "A Systematic Literature Review in Cyber Forensics: Current Trends from the Client Perspective," 2018 IEEE Third Ecuador Technical Chapters Meeting (ETCM), 2018, pp. 1-6, doi: 10.1109/ETCM.2018.8580266.

.

[4] C. L. Grande and R. S. Guadrón, "Computer forensics," 2016 IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI), 2016, pp. 1-6, doi: 10.1109/CONCAPAN.2016.7942361.

[5] N. Kumari and A. K. Mohapatra, "An insight into digital forensics branches and tools," 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016, pp. 243-250, doi: 10.1109/ICCTICT.2016.7514586.

[6] K. S. Singh, A. Irfan and N. Dayal, "Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks," 2019 4th International Conference on Information Systems and Computer Networks (ISCON), 2019, pp. 584-590, doi: 10.1109/ISCON47742.2019.9036214.