Computer forensic analysis protocols review focused on digital evidence recovery in hard disks devices

H F Villar-Vega1,2, L F Perez-Lopez1, and J Moreno-Sanchez1
1 Centro de Servicios y Gestión Empresarial, Servicio Nacional de Aprendizaje, Medellín, Colombia
2 Grupo de Investigación en Gerencia y Aplicación de la Ciencia y la Tecnología, Servicio Nacional de Aprendizaje, Medellín, Colombia

E-mail: hvillar@misena.edu.co

Abstract. Fourth Industrial Revolution includes cybersecurity as a key technology, given the increase in the number of devices connected to the Internet, the volume of relevant information available and the incidence of cybercrime on them. Among the lines of study of cybersecurity appears the computer forensic analysis, which seeks to reveal and analyze information in systems based on an analysis of digital evidence. This process involves a series of phases that ensure the integrity of the sources of information from beginning to end. Occupational studies in the area show a deficit of qualified and qualified personnel to cover the demand of processes related to this topic. In order to close this gap, the National Learning Service at Services and Business Management Center implements the Digital Forensic Laboratory. In this paper, workflows of computer forensic analysis procedures described in scientific documents are analyzed and a proposal of a protocol applicable to the laboratory is presented, which allows to rescue digital evidences of hard disks. A six-step procedure is proposed, ranging from the diagnosis of the case, to the presentation of results, through the collection of evidence, the copies of files, the analysis of data and the extraction of information.

1. Introduction
The global increase in the availability of equipment connected to the Internet, with the capacity to generate data has increased the volume of relevant information available to organizations and this in turn has increased the incidence of computer crimes within them [1]. This increase in crimes from digital information media has prompted cybersecurity to take a leading role in business dynamics, regardless of their size. It is important to ensure the information of organizations from the prevention of attacks, the development of secure platforms, and recovery in cases of affectation, among other processes [2].

For the Federal Bureau of Investigation (FBI), forensic computing, computer forensics or computer forensics is the science that is responsible for acquiring, preserving, retrieving and presenting data that has been processed electronically and have been stored in computer media, using techniques and tools developed by the private sector to be used in any physical location and produce non-interpretive data and direct information [3,4].

With the evolution of information technology and communications (ICT), the access and use of information has taken a ubiquitous and immediate character, to the point of being able to safeguard, and manipulate data from multiple sites and devices, at any time [1]. Thus, Industry 4.0, a term associated with the birth of the fourth industrial revolution and used by the German government to refer to
technologies associated with the vision of the factory of the future or intelligent factory, has posed great challenges to current organizations in the field of information management, in which the security related to it has an important role [2-5]. The latter has been called Cybersecurity and is a key element in the development of several technologies participating in Industry 4.0, such as the Internet of Things (IoT), Cloud Computing, Massive Data Analysis (Big Data & Analytics), among others. This evolution in the use of ICT has brought about an increase and specialization in criminal actions related to a large extent related to unauthorized access to private information of individuals and organizations [1,6].

In Colombia, investigations related to this type of crime are under the competence of the Computer Crime Units of the National Police and the National Prosecutor's Office, however, in many cases these units are geared towards advancing investigations at levels basic and prevention activities for such crimes, while complex investigations are carried out by the Directorate General of Criminal Investigation and Interpol (DIGIN), where they have sophisticated equipment and trained personnel for these activities [7]. For John Hambers, CEO of CISCO, the world's leading manufacturer of telecommunications equipment, all companies have at some time presented cybersecurity problems, however, some have not detected them and they have gone unnoticed. These statements presented at the 2015 world economic forum (WEF) annual meeting present a panorama of high demand for solutions and professionals that address this new industry sector [2].

The global cybersecurity index (GCI), a collaborative project between the international telecommunications union (ITU) and ABI Research (private sector) that seeks to include the issue of cybersecurity within the agendas of the governments that are part of them [2]. In the 2017 edition of the GCI Colombia it is located at a medium or maturation level, since complex commitments have been developed in the country and participation in cybersecurity programs and initiatives.

Among the aspects that should be strengthened in the country are cybersecurity training and the development of education programs in this area [8]. In the same way, the national survey of computer security 2017: Challenges of the fourth industrial revolution, published by the “Asociación Colombiana de Ingenieros de Sistemas (ACIS)” raises the lack of trained personnel among the main problems that arise in cybersecurity [9].

From the judicial field, it is common for the main government agencies to have tools for the analysis of digital evidence, however, the human resource trained to work with this information is limited [1,7]. Studies aimed at determining occupational needs and profiles in the area of cybersecurity have shown that forensic analysis is among the five roles of cybersecurity with the highest demand for personnel [10]. Against the previous scenario, from the “Servicio Nacional de Aprendizaje (SENA)” at “Centro de servicios y gestión empresarial (CESGE)” of the Antioquia Regional was proposed to close the gap from these forms in the areas and the project of implementation of a digital forensic laboratory (DFL) began, aimed at trainees of computer infrastructure programs (technology in data networks, technology in infrastructure maintenance of information technology, technological specialization in implementation and management of digital security, among others).

This space seeks to have tools and equipment that allow the apprentices of the aforementioned programs to strengthen their skills against key aspects of cybersecurity such as forensic information analysis, however, this process involves the definition of workflows. That allow to apply the technological tools of suitable form, according to the main standards of the industry.

This article is divided into sections, the methodology used by the authors for the resolution of the writing will be detailed below, later the reader will discover the results that have been generated after having performed a technical analysis, taking this information we continue with the detailed conclusions of the investigation and finally we give way to the references that were reviewed for the elaboration of the text.

2. Primary studies review process

The system used in the project is of the revision type. The fundamental objective of the review article attempts to identify what is known about the subject, what has been investigated and what aspects remain unknown [11]. A validation of forensic computer analysis workflows is being carried out to generate a
protocol within the Forensic Analysis Laboratory of the SENA CESGE. The base information of the work is being searched in scientific databases, relevant documents and publications have been collected from which the most appropriate ones were selected taking into account the applicability of the processes described in them and a new protocol adapted to the laboratory of the SENA, which will be validated with information retrieval exercises.

Through reliable sources of knowledge such as Institute of Electrical and Electronics Engineers (IEEE), Science Direct, among others; we had access to a large number of workflows that have been put into study, the search criteria were selected through an investigation of the most used terms housed in the summaries, this was done with the help of tools like VOS viewer, which we throw the terms that have more similarity with the theme under study and the keywords. From the analysis performed, some procedures or guidelines were ruled out when demonstrating flaws regarding their applicability and previous studies. The documents analyzed can be detailed in Table 1.

| Computer forensic contribution (title) | Description proposal - explanation |
|--------------------------------------|-----------------------------------|
| Forensic computing in Colombia [1].  | An approach to a forensic computer analysis methodology is provided as well as an approach to different tools that can be used to perform the analysis. |
| National digital forensic investigation framework for Bangladesh [12]. | A framework for the management of the information left by the analysis is proposed, the methodology is aimed at proactive and reactive forensic investigations. |
| Data generation and analysis for digital forensic applications using data mining [13]. | It focuses on the collection and analysis of cyber system data and web browser. |
| Methodological frameworks of digital forensic science [14]. | This document tries to address the diversity of methodologies applied in digital forensic investigations. |
| Digital forensic cybercrime analysis: Best practices and methodologies [15]. | A compact cyber-forensic model is presented for various technological ecosystems, it is proposed that digital investigations should be continually readjusted to address cyber-crimes and prosecute cybercriminals. |
| Search model for searching the evidence in digital forensic analysis [16]. | Their perspective is based on a search model that searches for relevant evidence by analyzing a large amount of data. |
| Hierarchical disc research model [17] | A hierarchical model of hard disk research is presented in its entirety, which can be used to support automated forensic tools. |
| Analysis of the methods of acquiring live digital forensic systems to achieve optimal preservation of the evidence [18]. | The best methods to preserve evidence and minimize data loss at runtime are shown. |
| Forensic experience in USB flash drive storage device: Procedures and techniques for obtaining evidence [3]. | It focuses on shining a methodology to retrieve digital evidence, additional provides information about forensic techniques using tools in storage devices. |
| Forensic disk memory flow analysis of forensic memory frames [19]. | Explain how forensic memory frames analyze the memory of hard drives. |
| Data recovery from solid state drives in an open source environment [20]. | Relevant information such as the TRIM command is addressed, data recovery from a solid state disk (SSD) is experienced and analyzed. |
| Forensic analysis of wear leveling in solid state media [21]. | Different types of flash and solid-state media are analyzed, adding files in them, then experiments are carried out to identify the probability of recovery. |
| A vision of the branches and tools of digital forensic medicine [22]. | Effective forensic methodologies are exposed, the available tools are displayed and detailed. |
| Smart device forensic: Acquisition, analysis and interpretation of digital evidence [23]. | There is talk of a forensic computer guide aimed at smart devices that use Windows, Android and iOS operating systems. |
3. Results and proposal for digital forensics analysis

Subsequently, an examination of the previously selected articles is carried out so that, based on them, the creation of an applicable proposal can be carried out in the DFL in SENA CESGE. Thus, 24 guides were chosen characterized by being primary studies on the subject, these provide us with the raw material with which we can build a protocol with a solid foundation that fully encompasses the aspects mentioned therein. For several years, from the IT support areas, it has been working with a general model for the recovery of digital evidence on hard drives, this covers in general what forensic computing is. It will be reflected in Figure 1.

3.1. Proposed methodology for digital forensics process

The proposed methodology has been agglomerated in phases, since in this way, it is possible to go much further and detail the recommended procedures that must be executed in each of the stages so that a much more assertive result can be obtained. Each of these six phases fully encompasses recommendations and good practices to be more likely to succeed in managing data recovery. To reach these conclusions, each of these models was tested in a controlled environment and the most relevant
parts that we have added to the proposed model were extracted. The steps of the methodology is described in Figure 2.

![Proposed process diagram](image-url)

**Figure 2.** Proposed process.

3.1.1. Analysis, preparation and identification. Once the crime has been committed, an identification consisting of knowledge and verification of the criminal act must be initiated; It is usually done with an evaluation of the resources, scope and objectives to carry out the investigation [34]. In addition, it must identify the technological elements that may constitute digital evidence such as storage media, computers, servers, laptops, among others [35]. The analyst must have knowledge of the affected system to review the income logs that allow him to determine if changes were made, there are tools that facilitate the search for this information [36].

3.1.2. Cloned discs, acquisition of digital evidence. A forensic investigation is not carried out directly on the crime scene, for this it is necessary to make an exact copy of the digital information (images of discs, USB, CD) or of the device to be investigated (Hard Disk) in computer media previously sterilized [1]. As a general rule it is recommended that forensic images of hard drives are always made for later analysis, preventing work directly on the original physical medium, the images can be made with tools such as Forensics Toolkit (FTK) Imager, OSForensics [35].

3.1.3. Recovery of deleted evidence. This is where the data extraction task is carried out, it is advisable to have at hand a set of tools that can help to perform a correct forensic computer analysis of the affected equipment.

3.1.4. Study of recovered evidence, details. Once the digital evidence is collected and stored properly, the forensic analysis is carried out, whose objective is to reconstruct the chain of events that took place from the moment with all the available data immediately preceding the criminal conduct, until the moment of its discovery [35]. Once this analysis is completed, the computer experts can obtain a pattern of behavior of the investigated user, in relation to: creation, modification, deletion of messages, activity in an email, and frequent contact with certain people or visits to specific places [1].

3.1.5. Protection of evidence, chain of custody protection. Although the first reason that will have led to the collection of evidence about the incident is the resolution of the incident, you may need them later to initiate a judicial process and in that case you must document in a clear way how the evidence has been preserved after collection using appropriate methods for storing and labeling the evidence. As a first step you must make two copies of the evidence obtained, generate a checksum of the integrity of each copy using hash functions such as MD5 or SHA1. Include these signatures on the label of each copy of the evidence on the CD or DVD itself, also include on the label the date and time the copy was created, name each copy [35].

3.1.6. Presentation of evidence obtained and analyzed in a report. Each step that is taken in the forensic analysis must be documented, so it is essential for the investigation and in the case that the analyst documents any change, file opening, or modification made to the file to be treated or the image obtained from the copy it is recommended that information be manipulated in controlled environments with audio and video recording devices [36].
4. Conclusions
Applying search and selection methods mentioned above, a protocol based on primary studies on the subject could be developed, on forensic computer analysis oriented to availability in terms of infrastructure and equipment that has SENA CESGE, this guide is constituted by six phases: (i) analysis, preparation and identification, (ii) disk cloning, acquisition of digital evidence, (iii) recovery of deleted evidence, (iv) study of recovered evidence, details, (v) protection of the evidence, chain of custody protection, (vi) presentation of evidence obtained and analyzed in a report. This methodology will be used in the DFL of SENA, a constant feedback to the current model is expected since the CESGE will test its effectiveness in controlled environments through fully trained students, who will use high-tech equipment out the development of the tests.

5. Acknowledgments
The authors acknowledge the financial support of the project to the Research, Technological Development and Innovation System of SENA (Sennova) through CESGE.

References
[1] Castillo Saavedra L, Bohada J A 2015 Informática Forense en Colombia Rev. Ciencia, Innovación y Tecnol. 2(1) 83
[2] Joyanes Aguilar L 2017 Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0) Cuad. Estrateg. 185(1) 19
[3] Campos L M O, Gomes E, Martins H P 2016 Forensic expertise in storage device usb flash drive: procedures and techniques for evidence IEEE Lat. Am. Trans. 14(7) 3427
[4] Noblett M G, Pollitt M M and Presley L A 2000 Recovering and examining computer forensic evidence (USA: Forensic Science Comunications)
[5] Heng S 2014 Industry 4.0 Upgrading of Germany’s industrial capabilities on the horizon Deutsche Bank Research 1(1) 1
[6] Couceiro Mato A, Hernández Serrano J 2017 Estado del arte de las técnicas digitales forenses para dispositivos Android (España: Universitat Politècnica de Catalunya)
[7] Avella Pinzón R, Gil Gamboa M S, Bohada J A 2013 Realidades de un delito informático en Boyacá Rev. Ciencia, Innovación y Tecnol. 1(1) 83
[8] International Telecommunication Union (ITU) 2017 Global cybersecurity index 2017 (Geneva: International Telecommunication Union)
[9] Almanza A 2017 XVIII Encuesta nacional de seguridad informática. Evolución del perfil del profesional de seguridad digital desafíos de la cuarta revolución industrial Revista Sistemas 147(1) 16
[10] Pastor Acosta Ó, Martínez Herráiz J J 2017 Capacitación profesional y formación especializada en ciberseguridad Cuad. Estrateg. 185(1) 291
[11] Kitchenham B 2004 Procedures for performing systematic literature reviews Join Technical Report I 33
[12] Haque M M, Hosssain S A 2018 National digital forensics framework for Bangladesh (Bangladesh: 3rd Int. Conf. Electr. Inf. Commun. Technol.)
[13] Khobragade P K, Malik L G 2014 Data generation and analysis for digital forensic application using data mining (India: 4th Int. Conf. Commun. Syst. Netw. Technol.)
[14] Čisar P and Čisar S M 2011 Methodological frameworks of digital forensics (Serbia: International Symposium on Intelligent Systems and Informatics)
[15] Sabillon R, Serra-Ruiz J, Cavaller V, Cano J J 2017 Digital forensic analysis of cybercrimes: Best practices and methodologies Int. Journal of Informat. Security and Privacy 11(2) 25
[16] Mascarnes S, Lopes P, Sakhare P 2016 Search model for searching the evidence in digital forensic analysis (India: Int. Conf. Green Comput. Internet Things, ICGCIoT)
[17] Karabiyik U, Aggarwal S 2016 Model of hierarchical disk investigation (USA: 4th Int. Symp. Digit. Forensics Secur. ISDFS)
[18] Jones J, Etzkorn L 2016 Analysis of digital forensics live system acquisition methods to achieve optimal evidence preservation SoutheastCon (Norfolk: IEEE)
[19] Prem T, Selwin V P, Mohan A K 2018 Disk memory forensics: Analysis of memory forensics frameworks flow (India: Innov. Power Adv. Comput. Technol.)
[20] Aldaee A, Ahamad M G, Uddin M Y 2017 Solid state drive data recovery in open source environment (Abha: 2nd Int. Conf. Anti-Cyber Crimes, ICACC)
[21] Neyaz A, Shashidhar N and Karabiyik U 2018 Forensic analysis of wear leveling on solid-state media 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (New York: IEEE)

[22] Kumari N, Mohapatra A K 2016 An insight into quento digital forensics branches and tools (India: Int. Conf. Comput. Tech. Inf. Commun. Technol. ICCTICT)

[23] Kalaimanman E 2016 Smart device forensics - Acquisition, analysis and interpretation of digital evidences (USA: Int. Conf. Comput. Sci. Comput. Intell. CSCI)

[24] Dogan S and Akbal E 2017 Analysis of mobile phones in digital forensics (Croatia: 40th International Convention on Information and Communication Technology, Electronics and Microelectronics)

[25] Barakat A, Hadi A 2016 Windows forensic investigations using powerforensics tool (Jordan: Cybersecurity Cyberforensics Conf. CCC)

[26] Hajdarevic K, Dzaltur V 2015 An approach to digital evidence collection for successful forensic application: An investigation of blackmail case (Croatia: 38th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO)

[27] Amato F, Cozzolino G, Mazzeo A, Mazzocca N 2017 Correlation of digital evidences in forensic investigation through semantic technologies 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA) (Taiwan: IEEE)

[28] Salunkhe P, Bharne S, Padiya P 2017 Data analysis of file forensic investigation (India: Int. Conf. Signal Process. Commun. Power Embed. Syst.)

[29] Varol A, Ülgen Sönmez Y 2017 The Importance of Web Activities for Computer Forensics (Turkey: International Conference on Computer Science and Engineering)

[30] Aziz N A, Yusof M S M, Malik M H B A, Rasyad A, Abd L H 2019 Acquiring and analysing digital evidence - a teaching and learning experience in class (Malaysia: Cyber Resil. Conf. CRC)

[31] Kao D Y, Chao Y T, Tsai F, Huang C Y 2019 Digital evidence analytics applied in cybercrime investigations IEEE Conference on Application, Information and Network Security (AINS) (Langkawi: IEEE)

[32] Al Mutawa N, Bryce J, Franqueira V N L, Marrington A, Read J C 2019 Behavioural digital forensics model: embedding behavioural evidence analysis into the investigation of digital crimes Digit. Investig. 28(1) 70

[33] Di Iorio A H, Curti H, Greco F, Podestá A, Castellote M, Iturriaga J I, Trigo S, Constanzo B, Ruiz De Angeli G, Lamperti S 2015 Construyendo una guía integral de informática forense (Argentina: Info Lab Universidad FASTA)

[34] López Grande C E, Guadron Gutiérrez R S 2017 Informática forense: cuando el delito hace uso de la tecnología Revista Tecnológica 10 20

[35] Rodríguez G and Ricardo J 2013 Modelo para el Análisis Forense de una Plataforma Windows (Colombia: Universidad Piloto de Colombia)

[36] Florez Fuentes A S, Santos Jaime L M 2012 Metodología para el análisis forense en linux Rev. Colomb. Tecnol. Av. 2(1) 90