International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 7, Issue 1 (January 2018), PP. 33-39

Design of a multicriteria support decision-making tool for Computer Forensics Analysis

*Hidalgo Cajo, Iván Mesias[1], Yasaca Pucuna, Saul[2] and Lema Ayala, Luis Angel[3]

*Corresponding author: *Hidalgo Cajo*

[1] *University Professor, Polytechnic School of Chimborazo, ihidalgo@espoch.edu.ec, Ecuador*
[2] *Computer Technician, Polytechnic School of Chimborazo, syasaca@espoch.edu.ec, Ecuador.*
[3] *University Professor, Polytechnic School of Chimborazo, luislg87@yahoo.es, Ecuador*

Abstract:- The objective addressed the problems related to the lack of tools to support decision-making processes in computer forensic. We have performed the preliminary analysis, design and prototyping of a decision-making tool that can be applied to the analysis of personal computing devices and network connected systems. The final result of this work will provide the forensic analyst with a detailed guide to the decision making process from the development of workflows for specific scenarios of analysis. The methodology used follows the "AENOR UNE 71506:2013 Information Technology (IT). Methodology for forensic analysis of electronic evidence", wich is developed in four phases. System commands and software tools needed to investigate specific incidents related to attacks and intrusions on computer systems are recommended for each of the four stages. The proposed tools, together with the selected methodology, will allow the analyst to perform a comprehensive and structured work from a methodological point of view. The prototype (proof-of-concept) developed is limited to the study of two specific scenario analyses: intrusion and extraction of hidden information. The work reveals that the web application was used to make decisions, and that 83.33% facilitates the intrusion and extraction of hidden information with the use of the proposed-model.

Keywords:- Computer forensic, network, decision-making, AENOR UNE.

I. INTRODUCTION

Forensic Science is a scientific method for collecting and examining information about past events. In the context of law enforcement, the forensic examination must be conducted in a robust manner in order to ensure that they collected evidence that stands out in court.

Forensic Computing is the branch of forensic medicine designed to examine digital media validly for legal purposes with the purpose of identifying, preserving, collecting, analyzing data stored on a computer. The ultimate goal of a forensic analysis is to discover and present the facts about the evidence collected.

The key element in Forensic Computing is the reproducibility of results. It is thus fundamental to follow standardized protocols and digital research of methodologies to manipulate and analyze tests. Especially, this is of greater importance in those situations in which the result of the forensic investigation may result in a lawsuit or a criminal prosecution.

There are several methodologies available for Forensic Computing that includes the Digital Integrated Process Research (Carrier and Spafford, 2003, Baryamureeba and Tushabe, 2004), the Smith --- Petreski Methodology (DEFCON18, 2010), and the Advanced Model in the Acquisition of Data (Adams, 2012). Similarly, standards for forensic processes are to include documents and recommendations from organizations such as the International Standards Organization (ISO), the National Institute of Standards and Technology (NIST), the American Society for Testing and Materials (now ASTM International), and the Global Professional Information Community (AIIM).

In Spain, AENOR is the agency that regulates the creation and adoption of standards. Recently, AENOR has published a complete Methodology for the Forensic Analysis of Electronic Evidence (UNE 71506: 2013). The standard defines the process of forensic analysis within the cycle of digital evidence management [1].

1.1 Justification/Problem

The lack of distinction of the common scenarios found in forensic computer research (independent team, network work station) and its relevant associated variables (Operating System, hardware components), a workflow will be developed to describe the decisions made and the actions performed in each scenario in terms

of the variables identified to detail the protocol that describes the actions to be performed in each node of the proposed workflow and in which the protocol will include examples of commands, as well as the appropriate software tools for this way to implement a Web Application for decision making.

1.2. Review of the literatura

Integrated Digital Investigation Process (Carrier and Spafford; Baryamureeba and Tushabe, 2004).

The Digital Forensic Process is a recognized scientific and forensic process used in digital forensic investigations [2]. Forensic investigators define it as a series of steps from the original incident alert through the reporting of results [3] The process is mainly used in computer and mobile forensic investigations and consists of three stages: acquisition, extraction , analysis and reporting.

There is no single procedure for conducting an investigation. It seems that an intuitive procedure is to apply the same basic phases that are used by the police at the scene of the physical crime, in which instead of having a digital crime scene. Keep in mind that there are several details that will not be mentioned in detail.

The first step is conservation, where you try to preserve the crime scene so that the evidence is not lost. In the physical world, the yellow tape is wrapped around the scene. In a digital world, a copy of the memory is made, turn off the computer, and make a copy of the hard drive. In some cases, the equipment can not be shut down and suspicious change processes are killed and steps are taken to ensure that known evidence is copied and preserved. The second step is to examine the crime scene for obvious evidence. The "obvious" test is the evidence that typically exists with investigations of this type. For example, at the scene of the physical crime where a violent crime has occurred, then the "obvious" evidence may have blood or be damaged. In the digital crime scene, obvious evidence can be found based on file types, keywords and other characteristics.

After locating the obvious evidence, then more thorough searches are carried out to begin filling in the holes. With every piece of evidence that is found, there can be no doubt about how he got there. Questions like 'what application created it' or 'what the user did that was created'? If so, then event reconstruction techniques are needed to determine that an application-level event has occurred, this is similar to the reconstruction, of a particular event [4], in Figure 1 we can look at the use of different areas that the methodology can be applied [5].

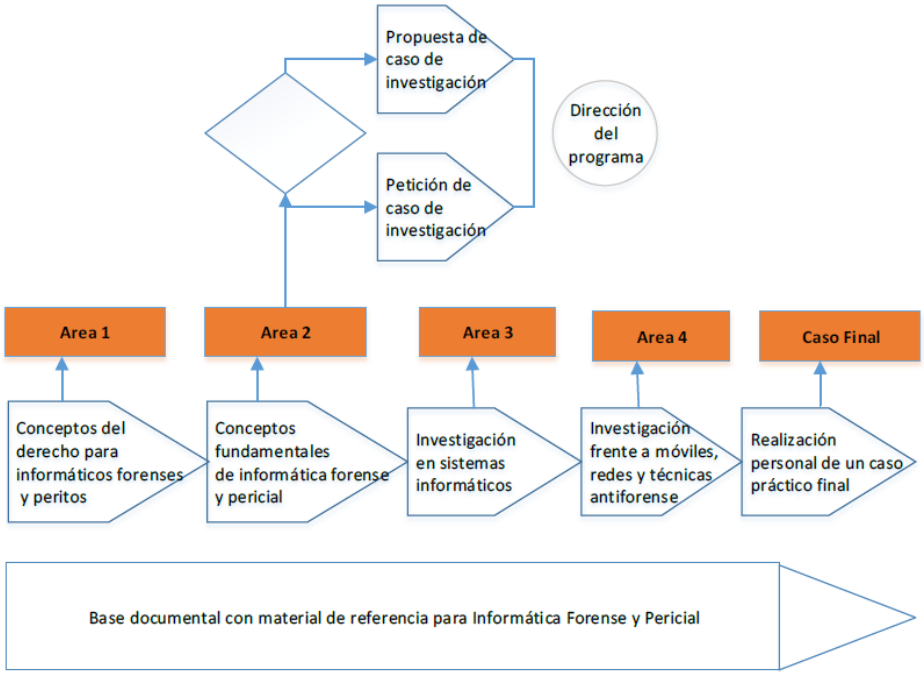

Figure 1. Some areas of application of the methodology

Smith-Petreski (DEFCON18, 2010)

In the methodology, by its abbreviations in English DEFCON is an acronym for 'DEFense CONdition', state of defense. It is used to measure the level of availability and defense of the US Armed Forces. UU These defensive conditions describe progressive states of alert and availability that are activated by the Joint Chiefs of Staff and the commanders of the armed forces. The DEFCON levels are adapted according to the severity of the military situation.

The Methodology consists of the following phases:

Pre-analysis, Analysis and The structured time management [6].

Advanced Data Acquisition Model (Adams, 2012).

The methodology adopted for this research is the science of design on the basis that it is especially suitable for the task of creating a new process model and an 'ideal approach' in the domain of the problem of digital forensic evidence. The process model used is the Science Research Design Process (DSRP) (Peffers, Tuunanen, Gengler, Rossi, Hui, and Bragge Virtanen, 2006) that has been widely used in information systems research.

A review of the current process models that involve the acquisition of digital data is followed by an evaluation of each of the models from a theoretical point of view, based on the work of Carrier and Spafford (2003) [7], and from a legal point of view based on the Daubert test [8]. The result of the evaluation of the model is that none of them provides a description of a generic process for the acquisition of digital data, although some models contain elements that could be considered for adaptation within the framework of a new model.

Methodology in Spain.

Methodology for the forensic analysis of electronic evidences (UNE 71506: 2013).

"AENOR has made public the UNE 71506: 2013 Information Technology (IT) Standard. Methodology for the forensic analysis of electronic evidence, whose purpose is to establish a methodology for the preservation, acquisition, documentation, analysis and presentation of electronic evidence.

The UNE 71506 Standard, elaborated by the Aenor Technical Standardization Committee AEN / CTN 71 Information Technologies, defines the process of forensic analysis within the cycle of electronic evidence management, complementing all those other processes that make up said management system of electronic evidence, as described in the parts of Standard UNE 71505, whose family of standards has been published. It is intended that this standard provides a response to legal infractions and computer incidents in different companies and entities, since obtaining reliable and robust electronic evidence helps to correctly attribute said facts, being able to discern whether the cause originates from an intentional or negligent.

With this information, the instruments, actions, purposes and other parameters concerning these behaviors can be located correctly.

The UNE 71506: 2013 Standard is applicable to any organization regardless of their will or size, as well as to any competent professional in this field. It is aimed especially at incident and security response teams, as well as technical staff working in laboratories or electronic evidence forensics analysis environments "[9].

1.3. Purpose

- Develop and implement a workflow to describe and characterize the set of decisions (along with their corresponding actions) that must be taken into account during a computer forensic investigation.
- Identify and analyze the different methodologies and relevant standards used by digital forensic science.
- Identify and characterize the common scenarios found in a computer forensic investigation (independent team, network work station) and its relevant associated variables (Operating System, hardware components).
- Develop a workflow to describe the decisions made and the actions carried out in each scenario in terms of the variables identified.
- Detail the protocol that describes the actions that must be performed in each node of the workflow. The protocol will include examples of commands, as well as the appropriate software tools.
- Implement a Web Application for decision making.

1.4. Hypothesis

When implementing a Web Application for decision making, will it facilitate the preliminary analysis and design for the examination of the Computer Forensic Analysis?

II. APPLIED METHODOLOGY

A descriptive study of the usability of the prototyping web application was carried out. For this, a survey was applied considering the criteria and indicators to evaluate the web application. The criteria of the study on the Methodology for the forensic analysis of electronic evidences are considered (UNE 71506: 2013), because in Ecuador there is little information.

2.1. Description of participants

The study population was formed by 30 students chosen at random from 2 universities, with a total of 16 students belonging to the Faculty of Computer Science and Electronics (ESPOCH), where 100% belong to the Systems Engineering degree, while the 14 correspond to the Faculty of Engineering (UNACH), being 100%

of the Systems and Computer Engineering degree, students of these careers were selected because they belong to the same area of knowledge.

2.2. Instruments

- A survey questionnaire.
- Google Drive form.
- Web Application.
- Macromedia Dreamweaver.
- EZAnalyze complement.
- Microsoft Office Excel.

2.3. Process

The first was to structure a survey based on the methodology and the criteria and indicators to evaluate the ease of usability of the web application cited above.
The questions of the survey were raised based on the Likert scale with 5 pesos for its assessment (Table 1).

Table 1. Weights for the evaluation of surveys.

Scale	Interpretation	Weight
Totally agree	Ease of use	5
Agree	Accordance	4
Neither agree nor disagree	Undecided	3
In disagreement	Little difficult	2
Totally disagree	Difficult	1

The steps to perform the Capture / Acquisition in the different scenarios are illustrated in the following Figure 2 and Figure 3.

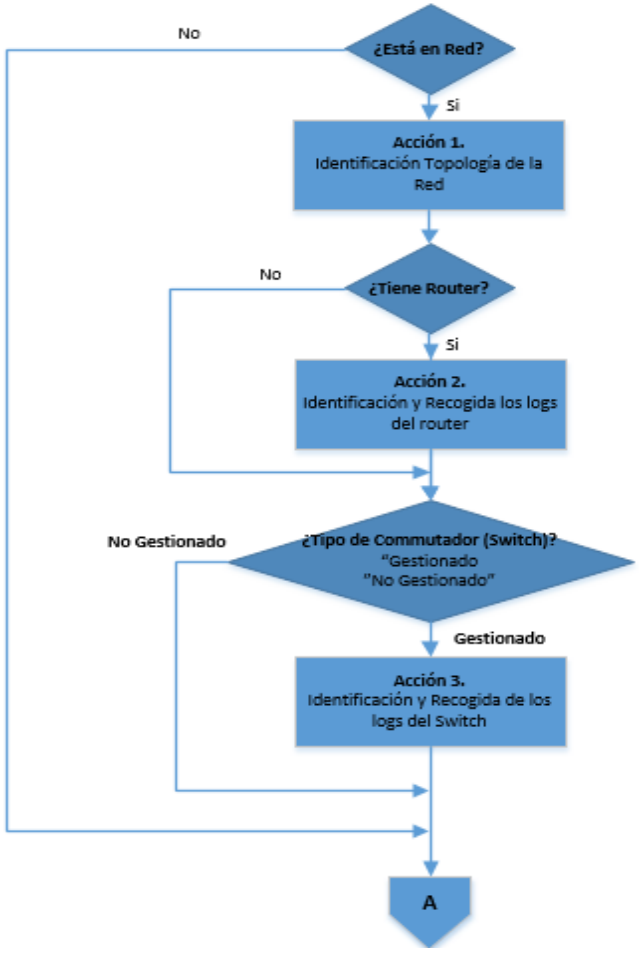

Figure 2. Scenarios involved in Pc Capture / Acquisition

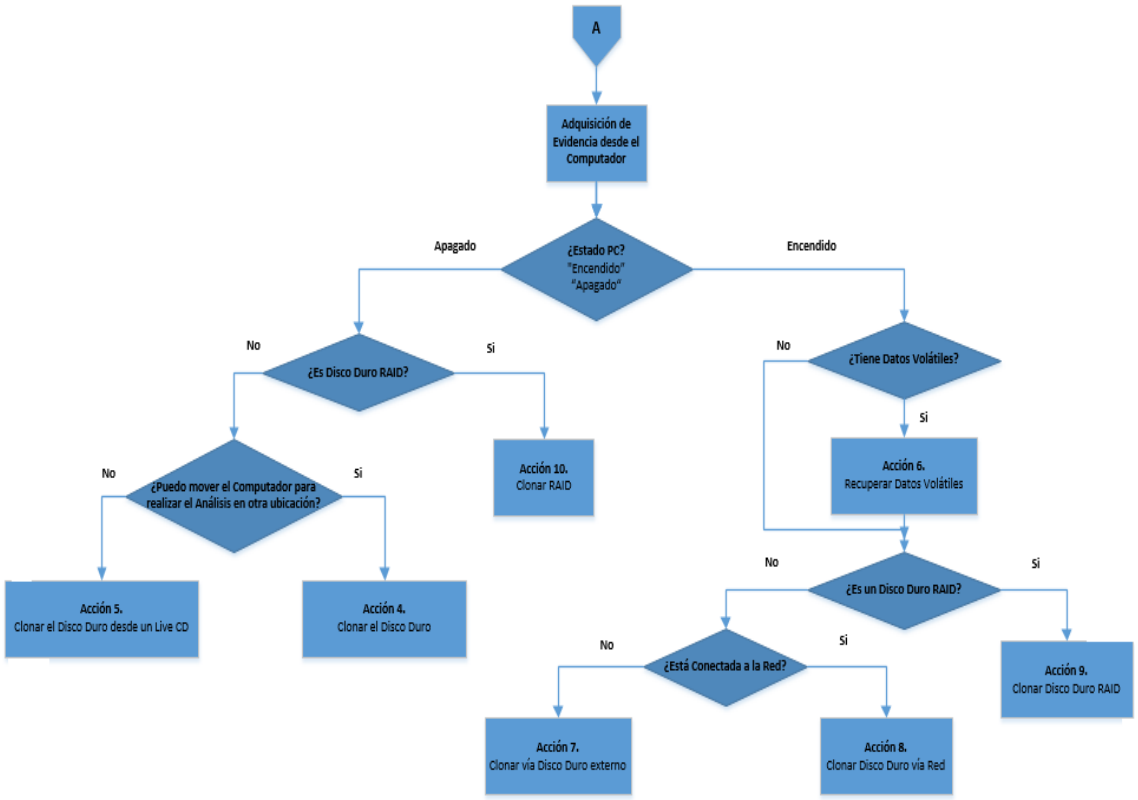

Figure 3. Scenarios involved in Pc Capture / Acquisition in network

The different actions will be composed by its Title, Action Protocol, System Commands (Windows, Linux, MAC), Recommended Forensic Tools, Other Forensic Tools and a Real Example; as shown in Figure 3.

ACCIÓN 2	TITULO: Identificación y Recogida los logs del router

PROTOCOLO DE ACTUACION:

1. Identificar el modelo y fabricante del router
2. Identificar la dirección IP
3. Identificar la máscara de red
4. Acceder a recoger los registros o logs que tiene el router.
   - Abrir sesión de un navegador de internet.
   - Ingresar a la dirección IP del router a analizar
   - Ingresar el nombre de usuario y contraseña
   - Abrir la interfaz del router en la ventana del navegador de internet.
   - Ingresar al menú del Router a la opción de "Registros" "Datos" u otro término similar en la interfaz basada en el navegador.

Figure 3. Identification and Collection of switch logs

Once the web application was used, the survey was applied, where the results were designed and published on the Google Drive platform for data collection.

We proceeded to apply the survey to the students of the two universities at the same time they finished using the web application. For the tabulation and analysis of the individual results, the EZAnalyze complement was used as a data processing tool, while the T-Student statistical for a sample was used for the global assessment. Finally, to analyze the hypothesis the database product of the survey in Microsoft Office Excel is imported.

III. RESULTS

Of the 30 users it was observed that 25 participants chose the correct option being an equivalent of 83.33% of the scale "Totally agree" with an interpretation of Ease of use with a Weight of 5, of the 5 participants who chose the option "Agree" being an equivalent of 16.67% of the scale According to an interpretation of Conformity with a Weight of 4, as shown in Figure 4.

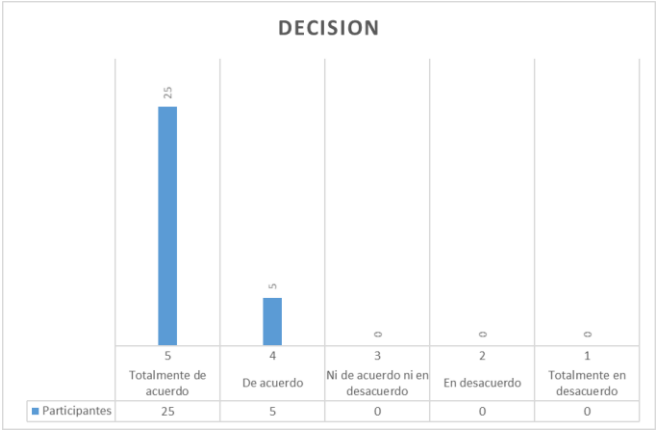

Figure 4. Ease of use of the web application.

For the verification of the hypothesis, the data of the different indicators that are the result of applying the survey were used. In the first instance, it was intended to perform the Student T statistic for a sample, for which homoscedasticity had to be verified, and in this case if it meets the variable analyzed, as shown in Figure 4, therefore when implementing an Application Web for decision making if it facilitates in the preliminary analysis and design for the examination of Computer Forensics Analysis.

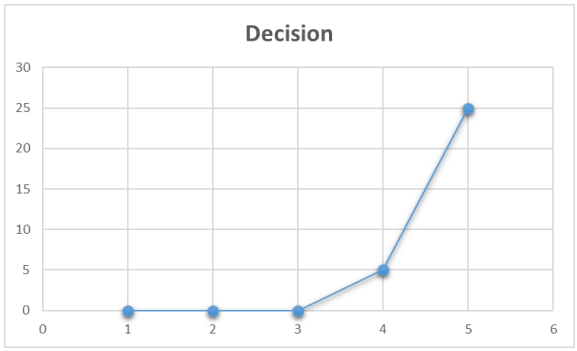

Figure 5. Correlation Test

IV. DISCUSSION AND CONCLUSIONS

A simple and HTML-based proof of concept of the process of guidance and decision for Computer Forensics has been developed. To increase the effectiveness and reliability of a tool of these characteristics, we could complement it with a multicriteria decision analysis system to facilitate the optimization of the sequence of analysis processes based on the potential value of the information obtained and the cost associated with obtaining it.

- The use of a standardized methodology (eg the AENOR - Standard UNE 71506: 2013 Information Technology (IT) Methodology for the forensic analysis of electronic evidence) provides a systematic framework that facilitates the analysis tasks, study, and acquisition of the elements subject to a computer expert. These methodologies add to the process a high degree of efficiency, reliability and safety that contributes to give a greater veracity to the results obtained.
- The development of a tool to support the decision-making process during the forensic analysis is an essential component to ensure the correct application of the analysis methodologies and therefore contributes to give greater strength to the conclusions that may be derived from the analysis. This aspect is especially relevant in those cases in which an expertise is required that must be defended in front of a judge.
- The continuous technological changes mean that the forensic analyst and the methodologies used are subject to a process of constant updating. In this sense, the use of standardized methods and flexible tools to support the decision-making process is revealed as a fundamental element to facilitate that this process of constant updating is carried out in an appropriate manner.

REFERENCES

[1]. I.M. Hidalgo, *Análisis preliminar y diseño de una herramienta de toma de decisiones como soporte para las tareas de análisis forense informático*, maestría, Universitat Rovira i Virgili, España, ES, 2014. (9)

[2]. Eoghan Casey, Electronic Crime Scene Investigation Guide, Academic Press (Ed.), *Handbook of Digital Forensics and Investigation,* 4 (United States: San Diego, 2010) p. 567.

[3]. Casey, Eoghan, *Digital Evidence and Computer Crime* (Second Edition, 2010).

[4]. Brian D. Carrier, <<Basic Digital Forensic Investigation Concepts>>, Brian D. Carrier, 2006, [En línea]. Disponible en: http://www.digital-evidence.org/di_basics.html. [Accedido: 16-sep-2014].

[5]. Antonio Salmerón, <<Informática Forense y Pericial>>, Antonio Salmerón, 2017, [En línea]. Disponible en: http://www.forense.info/articulos/moduloinformaticaforenseenredeseinternet.html. [Accedido: 12-oct-2017].

[6]. David C. Smith, Samuel Petreski, *A New Approach to Digital Forensic Methodology* (Georgetown, Washington DC: 2008).

[7]. K Mushtaque, K AhsanY and A. Umer, Digital forensic investigation models: an evolution study, *Journal of Information Systems and Technology Management, 12(2),* 2015, 233-244.

[8]. The Law Commission, *The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales* (United States, US: Edmond, 2010).

[9]. CCN-CERT, Defensa frente a las ciberamenazas, Publicado el 11 Septiembre 2013, *CCN-CERT, 106(1),* 2013, 14.

*****Hidalgo Cajo, Iván Mesias. “Preliminary Analysis And Design of A Tool for Decision-Making To Support Computer Forensic Examination .” International Refereed Journal of Engineering and Science (IRJES), vol. 07, no. 01, 2018, pp. 33–39.