Computer technique for the suitability of digital evidence in attacking an information system: Forensic analysis for the digital custody chain

Computer technique for the suitability of digital evidence in attacking an information system: Forensic analysis for the digital custody chain

N Jácome-Castilla[1], **and C Villamizar-Nuñez**[2]
[1] Grupo de Investigación Rota, Universidad Francisco de Paula Santander, Seccional Ocaña, Colombia
[2] Universidad de Pamplona, Pamplona, Colombia

E-mail: njjacomec@ufpso.edu.co, cesar.villamizar@unipamplona.edu.co

Abstract. This article presents results of a research project that attempted to create a model of forensics in an information system; since forensic analysis allows to establish the causes of security commitment information system. The aim of the study was to determine the software tools to be used in the management of security incidents in an information system; required for the design of computer art for extracting digital evidence to anchor the chain of custody items. The research methodology was descriptive and applied document type, by analyzing the different tools technique that allows maintenance of digital evidence was designed, preserving the integrity of this as a test mechanism in a judicial process. In this way, the procedures to be performed to store information were established without being altered chain of custody solving the above questions: What is the chronological order in which the events of alteration, transmission or access occurred? What evidence have to believe you are a victim?, what are the damages incurred?, who do responsible for the incident?, what people are suspicious of the event?, who has investigated the incident and which actions has taken to preserve, identify, collect and analyze the data involved?; ensuring this way through technical steps and tools to be used for the preservation of the chain of custody, as an evidence in a court case.

1. Introduction

This article presents computer technology for the appropriateness of digital evidence in the attack on an information system, since forensic analysis allows to obtain adequate and accurate evidence on the different elements that can not be altered in a judicial process for crimes committed information systems, research study focuses on collecting digital evidence and in the process of anchoring the chain of custody.

In this sense the collection by forensic laboratories research raised the effective tools in a computer technique accompanying the preparation, knowledge and techniques creating evidence that serve as evidence in charge judicial proceedings to address this type of cybercrime. According to the above, the present study designed a technique that ensures the appropriateness of digital evidence in the case it has been violated or attacked an information system. For this purpose, it was necessary characterization of Colombian law regarding the standards required to inform the design of computer art for extracting digital evidence and the importance of preserving the chain of custody.

Accordingly, the necessary software tools to be used in security management information system were established, determining the technical requirements that should be used for the design of technology.

2. Methodology

He used a descriptive research, since according (Sampieri, 2014). They allow to analyze a certain phenomenon, identifying important characteristics of people, groups or communities [1]. Similarly so Arias 2012, states that the level of research is the degree of depth of research and way of approach, constituting the object of study at this level research. [2]

Equally it determined a documentary and applied investigation, in which it looked for resolving technical problems with that they allowed to control practical situations, as well as it is expressed by Sabino, 1996 [3].

In this sense and according to the degree of depth of the investigation, the main theoretical referents were the documents of the computer crimes Unity from "Dirección de Investigación Criminal e Interpol (DIJIN)", the notes of computer right of Alexander Diaz [4], author of the law of computer crimes in Colombia Law 1273, Unit of Computer Crimes of the Investigations Technical Body of the "Fiscalía General de la Nación" of Santander, Colombia. To his time took the contributions of Jeimy Cano [5] in his work: discovering the computer traces, computer crimes in the cyberspace by Luis Orlando Paloma Vine and Hackers learns to attack and to defend by Gómez, 2012 [6]

In this context the information was processed for the editorial technician redaction in the processes to be followed for the conservation of the chain of custody and digital evidence.

3. Results

3.1. Technical and legal requirements for the design of the technique for the management of digital evidence in an information system

In the structuring of the technician developed, it was necessary to determine the technical and legal requests that should have been taken into account for the handle of the digital evidence and that this was valid inside a research process. Therefore, if it is observed the forensic analysis or forensic computing base to scientific technicians with technological infrastructure that help to identify, preserve and analyze the digital evidence and preserve the chain of custody in a judicial process.

For this the technician is based in the characterization in which it is designed a forensic reproduction, a copy of digital evidence preserving the original data, so that these are not modified; also it is necessary the analysis of the data by means of skilled software and methods of recollection of the digital evidence where data is analyzed and they are original proofs of a judicial process, the step followed has to realize a report written describing the evidences found and discovered, revealing the conclusions extracted and the restoration of the processes.

This is how within the technique it is important in order to safeguard the data and perform the analysis in an investigation, a specialized software so that the judges can take as digital evidence the ones considered as reliable and that they satisfy the requirements to establish the sanction by the crime committed.

In this sense in United States it is employed the Daubert standard for the admissibility of the tools and forensic processes; the Daubert protocol demands that the technology and the tools of software employed in an investigation are subjected to an empirical proof and checked by specialists, and that the results obtained can be reproduced by other experts.

The technical appearances of the forensic computing are determined also by the type of digital supports that has been researched. Thus, the forensic computing divides in several branches which are in charge of the analysis of machines, networks, databases and mobile devices with forensic ends. This last especially has to face up to the challenges that derive from the nature proprietary of the mobile devices.

In the same way, for the realization of the digital evidence expertise, it is important to describe the way in which the data is obtained, for this purpose it is necessary to refer to the Computer Expertise, which is nothing more than the discipline used to take the test. Expert on the evidences of the case.

For the development of this technician or discipline it is needed a group of professionals like computer engineers and telecommunications engineers, which have the necessary knowledge to offer a clear and concise explanation of the results of the analysis of the evidence. For such case the computer experts have to be up to date, forming with knowledges of computer experts; conceptualizing his expertise in: recovery of erased of archives, access to data in disks damaged and certifications of his professional performance, allowing that the pericial dictamen go besides visa by a professional expert in forensic computing. On the other hand, it would be desirable that were certified like Auditors of Systems of Information or equivalent.

By its part in a judicial case, the computer expert is appointed by the court, in the last years, the computer cases have multiplied and in the judicial courts neither the lawyers nor the judges are able to understand a case of computer crime not being on his speciality, to understand the details of a case, details that may change the stage entirely. In these cases, a professional expert, with the necessary knowledge in computing and the language typical of a trial is able to clear to every part the reality about determinate evidences.

In this sense, for the technique obtaining, it is required tools for the handle of the digital evidence, doing necessary to know the different tools for the resolution of the judicial case that was investigating, the first that has to be contemplated are the tools for the recovery of passwords, becoming these the elements of protect in web pages, programs of mail and office software, among them it is possible to find Browser Password Decryptor: it recovers all the passwords stored in the browsers web; MessenPass: it does many things so much with the users and passwords of Messenger, ICQ,Yahoo, Mail PassView: it rescues the keys of the accounts of local post (in Outlook, Eudora, Thunderbird, etc.) [7]; Bullets PassView, ShoWin and AsteriskKey: reveal the unseen passwords after asterisks; WirelessKeyDump: it obtains the passwords of the networks WiFi- FireMaster: it tries to recover the master password of Firefox [7]; Nirsoft and SecurityXploded: they have a lot of tools devoted exclusively to the recovery of passwords, almost all executable from memories USB. It is worth remembering that they only obtain passwords stored without protection and to break the encryption it is necessary to resort to cryptographic attacks.

3.2. Tools to explore the hard disk

When examining a computer, needs a global vision of folders and archives; SpaceSniffer , Scanner or WinDirStat Portable offer fast summaries of the distribution of space in the hard disks. To create a database of folders, uses getFolder and FileLister [7].

Finally, it may be the case that the machine you have accessed is still on and with open programs. Check out which files are in use with OpenedFilesView and analyze the memory with the help of a hexadecimal editor (for example, WinHex or HxD) [7].

The most advanced are MoonSols Windows Memory Toolkit and Volatility Framework , that analyze dumped by heart and files of hibernation of Windows, pieces of memory “frozen” that they can contain valuable information [7].

3.3. Packaging and securing the digital evidence of the technique to design

Taking into account the computer and legal tools for the correct presentation of the digital evidence and chain of custody in the judicial processes, it is established the following technical, with the end to standardize the procedures for the modalities of research [8].

For making the technique it will be taken into account the process to realize, describing the process for the conservation of the chain of custody and the image that reflects the process to execute. To continue the technique of forensic analysis is established in a system of information.

Step 1. Previous judicial control and back: According to the legal stipulations the opportunity of the judicial control on the performances of the “Fiscalía” and of the judicial police exist differences

between which operates of previous way and the one who occurs subsequently that it has to take into account for the execution of the technique to develop.

In the case of prior control, a judicial action takes place that weighs between the interests of the investigation, the reasons given by the "Fiscalia", the crime investigated and the conditions of the subject over who or whose interests the action would be practiced, in order to avoid an excessive, unnecessary or offensive restriction that, in little or nothing, truly assures the process and, on the contrary, affects the intimacy and privacy of the person involved.

What does the judge is to protect the rights of the subject investigated, prevent that the prerogatives of the State assigned to the "Fiscalía" and to his technical device, use without concrete purpose, without justification, pointlessly and of disproportionate way, ignoring the fundamental and specially protected nature of the legal rights recognized in the individual rights over which the investigative action operates. Judgment C 334-10 (Corte Constitucional, 2010) [9].

Step 2. Habeas Dates or informative self-determination-scope. The fundamental right to the habeas dates or to the informative self-determination, comports a plexus of faculties such as the one to have of the information on itself same, the one to preserve the own computer identity, that is to say, allow, control or rectify the data concerning to the personality of the title of the same and that, as to, identify it and differentiate in front of the other. The computer self-determination is the faculty of the person to which refer the data, to authorize his conservation, use and circulation, of compliance with the legal regulations. It sentences C 334-10, of agreement to this legal procedure, have 24 hours to find the proofs of digital evidence and its presentation in front of a judge, as it states the article 16. The article 237 of the Law 906 of 2004 [10].

In this last event, they will be applied analogically, according to the nature of the act, the planned rules for the preliminary audience; that is to say once fulfilled the times and processes established by the law of the country, proceeds to the extraction of the digital evidence and conservation of the chain of custody.

Step 3. Process for obtaining forensic images [11]. Once obtained the storage devices in which it is presumed that a crime was committed, we proceed to obtain the forensic image, the computer forensic equipment is prepared, where the analysis software has been installed.

It is proceed to conserve the data of the equipment, a blocker is installed at the software and hardware level to connect the storage equipment to the forensic computer equipment. The forensic image is obtained with a specialized forensic software.

Finally, the process of saving the images obtained is done in a previously sanitized hard disk and a copy of the original is made in this last copy.

Step 4. Obtaining of the HASH. It proceeds to realize the obtaining of the algorithm HASH of all the devices or means of storage, by means of a skilled software that guarantees the integrity of the image obtained and realizes a stamped chronological.

Step 5. Securing the chain of custody. To obtain the securing chain of custody it is important to have to take into account some processes that guarantee the date, hour in that it took, that has not been changed, the one who realize it, that has not been altered and that conserves integrate so that it serves as a half evidential in a judicial case.

Step 6. Tools to use in the obtaining of the digital evidence. It is important to have the necessary tools to handle the digital evidence and the means of computation that have the digital evidence.

Hand-held tools: screwdrivers, tweezers, analog camera that makes the HASH of the photographs.

Tools of personal protection: Gloves of latex or rubber, glasses of protection, antistatic bracelets to avoid that the electrical downloads alter the evidence or the teams of computation and slap.

Step 7. Findings. It is necessary to document and take out photographies of the place where the evidences were found. It has to find the computer and server, the means and devices of storage, with mark and model. Next, it realizes the process of the obtaining of the digital evidence, using the tools of protection and hand-held.

They take photographies of the inner part of the team of computation and to its time photographs of the location of the means of storage and digital evidence

Step 8. Obtaining of the evidence**.** Once it identifies and they situate the devices extracts using the hand-held tool. It identifies in detail the mark of the devices.

Step 9. Obtaining HASH MD5**.** The type of file or group of files will be extracted, the fingerprint will be extracted through the HASH D5 process; This procedure must be carried out on all the files contained in a technological storage medium, which is ultimately digital evidence, that is, the Probatory Material Element. The fingerprint extraction program is executed in the medium that is located.

Once the program has been executed on the storage medium where this software is located, it activates a window very similar to a Windows explorer, where the files or digital data are located to which the fingerprint will be extracted; Once the detailed location is given in the Create Sums option. Depending on the specific location listed above, it will show the folders and / or files to which it is expected to generate the process, they are selected through any of the action buttons on the bottom, then choose the option OK and the system automatically starts generating fingerprints through the HASH MD5 process to each of the files contained in the folders selected by the server specialized in computing. When the execution of this action ends, a pop-up window is activated that gives the option to store the MD5 HASH in any technological storage medium [12].

Step 10. Packaging. The next step is the process of packaging digital evidence, for the preservation of due process in obtaining it and that constitutes a means of proof. The evidence must be packed so that it can be transported, moved and handled without causing changes or physical damage, protecting it from human and electrical or magnetic damage.

Tools of packaging like: plastic stock exchanges of paper, of bubble, antistatic stock exchanges. Boxes or cases Foams, corks and insulating strip. Process of packaging: With the insulating strip proceeds to seal the ports of connection of the means of storage. Store the evidence in an antistatic bag, metalized bags or with conductive strips, which will prevent electrostatic discharges to digital evidence. Wrap the digital evidence of plastic in bubbles, foam or use the original packaging if you still have it. The next step is in a box filled with soft material halfway, insert the device and protect it, taking into account that it is forbidden to use paper not to store moisture. Once the above procedure is performed, the chain of custody format with the continuity record is labeled and processed, with information on how the digital evidence was found, obtained and entered.

Step 11. Crimes with emails. In accordance with the request of the crime committed, requires determine the origin of the email, with the purpose to verify which damages can cause in the computers or networks of data. It proceeds to save the email from the account and the computer where it is received. This process is realized by taking into account the norms of finding, recollection and packaging.

With the forensic computer team required it is realized the verification of the email to determine the location of origin and the possible damages that would cause in the computer where the query is realized. The email will be displayed this way:

a) Text of the email.
b) Headed of the email.
c) Attachments of the email.

The attachments to the email are listed and a screenshot is taken; the location of the server from which the mail was sent is established, verifying the reputation of the site from which it was sent. With the specialized software for Forensic Computing, a bit-by-bit image and an MD5 hash are acquired to the e-mail. A chronological stamp of the file is made with the Kronos Certicamara software to guarantee its existence at the time of the expert.

The IP address: 114.80.68.240, belongs to the server or computer programmed for sending the emails, with the end of obtaining massive form data of accounts of email, passwords of the same and personal data of the user, this IP address can be verified in the headed.

4. Conclusions

The tools for obtaining evidence are the most important elements of forensic computing, since for their operations it is necessary to have technology to analyze the large volume of data stored by computers, the variety of files, the accuracy required of the information copied and the time limitations to analyze the information. It was determined that in Colombia the laboratories of the DIJIN or specialized unit in cybercrime rely on ENCASE tools and private companies such as Adalid corp. and Mattica.

The technical and legal requirements for the technique design for the management of digital evidence in information systems is based on scientific management and technological infrastructure to ensure the digital evidence and validation required within the investigative process. For the proper preservation of the digital evidence and the chain of custody, the characterization and protection of the data, the respective analysis of the information and the written report describing the evidences found and the restoration of the events must be carried out as a minimum.

Techniques were proposed for the packaging and assurance of digital evidence, based on computer and legal tools for the correct presentation and chain of custody for judicial processes. The technique of forensic analysis in an information system considers 11 detailed steps such as: Step 1. Prior and subsequent judicial control, Step 2. Habeas data or informative self-determination, Step 3. Process for obtaining forensic images, Step 4. Obtaining the HASH, Step 5. Securing the chain of custody. Step 6. Tools to be used in obtaining digital evidence, Step 7. Findings, Step 8. Obtaining the evidence, Step 9. Obtaining HASH MD5, Step 10. Packing and Step 11. Related to crimes with emails.

References

[1] Sampieri R 2014 *Metodología de la investigación* (México: McGraw-Hill)
[2] Arias, F 2012 *El Proyecto de Investigación* (Caracas: Episteme)
[3] Sabino 1996 *Método de investigación* (Caracas: Panapo)
[4] Díaz A 2014 *Apuntes de Derecho informático* (Bogotá: Habeas Data Consultores)
[5] Cano J 2013 *Computación forense, descubriendo los rastos informáticos* (Bogotá: Alfaomega)
[6] Gómez J 2012 *Hackers aprende a atacar y a defenderse* (Bogotá: Alfaomega)
[7] Arnedo & García 2014 *Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos* (Colombia: Universidad Internacional de la Rioja)
[8] Paloma L 2012 *Computer crimes in the cyberspace* (Bogota: Juridical Editions)
[9] Corte Constitucional Republica de Colombia 2010 *Sentencia C-334/1* (Colombia: Corte Constitucional República de Colombia)
[10] Senado de Colombia 2004 *Ley 906 de 2004* (Secretaria del Senado de Colombia).
[11] Fiscalía General de la Nación 2004 *Manual de procedimientos del sistema de cadena de custodia* (Colombia: Fiscalía General de la Nación)
[12] Valdes, & Tejedor 2015 *Hashing. Un concepto, una realidad* (Panamá: Universidad Tecnológica de Panamá)