SUMMARY TECHNICAL

The technology has advanced in such a way that already a long time ago had been the time in that all the information was stored in big quantities of paper behind, now the information is stored in digital or magnetic means, such as hard disks, memoirs, Cd, Dvd, etc.

Without a doubt that this represents a great advantage in several aspects but criminal new acts that involve these computer means also arise.

The same as a crime in the physical dimension leaves evidences, a computer crime also leaves evidences, but this evidences are stored in a digital way, in most of the cases happiness information one cannot read or to gather for common means or traditional mechanisms. It is here where the forensic computer science's study is born that provides the knowledge and the instruments to gather evidence and to solve this new type of crimes.

Objectives of the forensic computer science

The forensic computer science in these digital times is very important, but the real importance comes from its objectives that are the gathering, comparison, analysis and evaluation of data coming from any computer mean, in such a way that is like test inside a tribunal of justice.

Process

In the objective I mention you that the important thing is that the gathered evidence you can use inside a penal process, so that this happens it is necessary that the evidence has been extracted with certain standards that vary depending on the country in which is carried out the investigation.

Among the guides of better practices in forensic computation can mention you:

- **RFC3227**, Guides to gather and to store evidence, written in February of 2002, it is a guide of high level to gather and to file data related with

intrusions, he/she also explains some concepts related with the legal part.

- **It guides of IOCE**, The International Organization of Test Computer science presents us "Guide for the best practices in the forensic exam of digital" technology that is a document that provides a series of standards, principles of quality and approaches for the detection and prevention, recovery, examinación and use of the digital evidence for forensic ends. It covers the systems, procedures, personal, team and requirements of comfort that are needed for the whole forensic process of digital evidence, from examining the scene of the crime until the presentation in the court of justice.
- **Investigation in the scene of the crime**, The department of justice of the public United States (Electronic Crime Scene Investigation: To Guide for First Responders), which is focused more than everything in identification and evidence gathering.
- **Forensic exam of digital evidence**, this it is another guide of the Department of Justice of the United States, it is Forensic "Exam of Digital" Evidence (Forensic Examination Digital of Evidence: To Guide for Law Enforcement), this guide motivates the development of political and procedures with the purpose of giving a good treatment to the evidence.
- **Better practices (Hong guides Kong)**, the Society of Computer Security and Forensic surgeon created in Hong Kong, "Computer published Forensics. Part 2: Best Practices." This guide covers the procedures and other necessary requirements involved in the forensic process of digital evidence, from the exam of the scene of the crime until the presentation of the reports in the court of justice.
- **It guides of good practices for evidence based on computers united Kingdom**, ACPO, Association of Chief Police Officers (Association of Bosses of Police), of the United Kingdom, by means of their crime department for computer, "Guide of Good Practices published for Evidence based on Computers (Good Practice Guide For Computer Based Evidence)." The police elaborate this document with the purpose

of being used by their members like a guide of good practices to be in charge of of computers and of other electronic devices that can be evidence.

- **It guides for the evidence handling in IT Australia**, Standards of Australia (Standards Australia) publish in August of 2003 "Guide For The Handling Of Evidence In IT (HB171:2003 Handbook Guidelines for the management of IT evidence)." It is a guide created with the purpose of attending the organizations to combat the electronic crime.

Computer crimes

Almost in a parallel way to the advance of the technology have arisen also a series of denominated illicit computer crimes.

Several they are the definitions of computer crimes but according to my opinion the one that more he/she comes closer it is the one that Mexican Téllez details Valdéz, "a computer crime it implies any illegal activity that already frames in traditional figures well-known as robbery, theft, swindles, fraud, falsification, sabotage, but whenever the computer science involves as mean to carry out the illegality."

Normalization of the computer crimes

To conceptualize the computer crimes he/she takes into account the recognition that you/they make in this respect The United Nations.

Frauds:

Manipulation of the entrance data, is the type of computer well-known fraud as subtraction of data, it is easy to make and difficult to discover.

Manipulation of programs, consists on modifying the existent programs in the systems of the computers, a very well-known method is the famous Horse of Troya.

Manipulation of the exit data, is made fixing an objective to the operation of the computer system, a common example is the duplication of credit cards.

Fraud made by computer manipulation, takes advantage of the automatic repetitions of the computation processes, it is a technique in which you grieve perceptible parts of financial transactions they leave taking repeatedly out of a bill and they are transferred another.

Falsifications:

As object, when they lose temper data of stored documents.

As instruments, the computers can be used to make falsifications of documents.

Damages or modifications:

Computer sabotage, is the act of erasing, to suppress or to modify without authorization functions or computer data with intention of blocking the normal operation of the system.

Virus, is a series of programmatic keys that you/they can adhere to the legitimate programs and to spread to other computer programs.

Worms, it is the same as a virus but east cannot reproduce.

Logical or chronological bomb, they possess a high potential of damage and they cannot be discovered until they are detonated.

At the end they are few the countries that have an appropriate legislation that allows to face the mentioned crimes, among these Germany, Austria, France and United States are.

EVIDENCES DIGITAL

Importance

In today's world the agents of the law are about extracting digital tests of a bigger number of devices, with more storage capacity, the devices that can be

investigated in relation to a crime include computers, laptops, memoirs flash, devices of external storage, digital cameras, the consoles of video games and the cellular telephones. Undoubtedly many more devices of those than you had so alone a couple of years ago.

The contained data in these digital devices can help to make complete the law in a criminal investigation or prosecution of crimes in a variety in ways. For example, the agents of the order can investigate an accusation of sexual infantile abuse analyzing the computer of a suspect, where it could be several images where the suspect abused sexually of smaller.

It evidences him/her it is the most important aspect in any legal or extrajudicial dispute and inside a crime where it is involved direct or indirectly a computer team.

Classification

Harley Kozushko (2003), he/she mentions that the digital evidence you can classify, to compare, and to individualize, that is to say it is the process for which general characteristics of files and data are looked for, characteristic that differentiate similar evidence and that they should be used to the investigator's approach, for example:

Content: An e-mail, for example, it can be classified by their content as SPAM, and it can be individualized starting from the content of their headed, information that in general is not visible for the user. For example, for their origin address.

Function: The investigator can examine how a program works to classify it and sometimes to individualize it. For example, a program that unexpectedly it transfers valuable information from a reliable computer to a remote lease it could be classified as a horse of Troya and it can be individualized by the remote localization to which transfers the information.

Characteristic: the file names, extensions and inclusive those headed internal that identify the different file formats that exist they can being of utility in the classification of the digital evidence.

The fundamental idea is that if one makes an appropriate classification being based on the experience and in the appropriate techniques one will be able to make speak to the "evidences." He/she should remember the doctor's sentence Edmond Locard (1910) and to feel the scientific depth of their message: "The evidences are silent witnesses that don't lie."

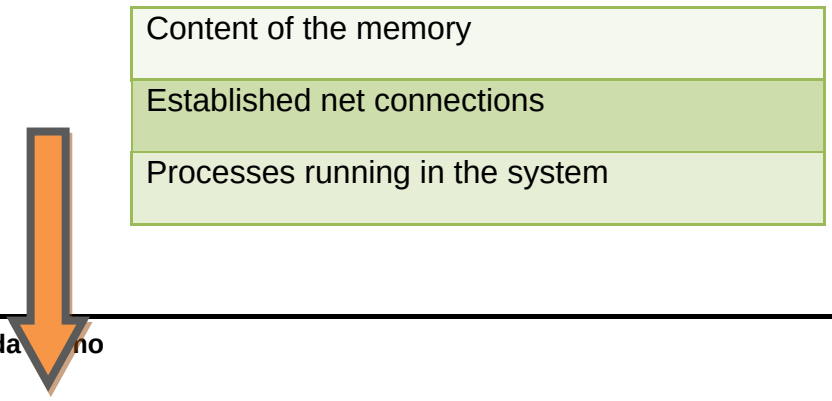
Gathering procedure

The only form of gathering digital evidence is to follow the good practices for this process, since like it has been mentioned before, of this it depends that so successful it is the investigation.

The acquisition of the electronic evidence should always be made so that the examined system it is impacted or modified in its state the minimum thing possible.

For it is important to know the tools to use. It is not only necessary to know the type of information that extracts or how formless it generates, but knowing, with detail which is the interaction of the tool with the system on which runs: how it affects to the memory, what files it modifies, to what resources of the system it consents, etc.

As general rule the evidence in the less destructive possible way should be obtained, and always in order of more volatile to less volatile, specifically in the order that is shown next.



Open ports
Connected users to the system
Contents of paging files and swap
Contents of systems of files
Hardware configuration and outlying

Order to obtain the Digital Evidence.

When the evidence is composed of listings of hundred of connections, dozens of processes running, and an image bit-to-bit of a hard disk with many gigabytes, is necessary to establish a plan for the form of approaching the analysis. That is to say, to decide ahead of time what it is important, what it is not it, and in what order to make the things.

No forensic investigation begins without having a suspicion of the behavior or incident at least to investigate, and this allows to adapt the methodology in particular to the case.

All decision that takes from the moment that the investigation begins should be meditated, calculated, and evaluated in relation to its possible benefits and possible damages of the particular case.

The preservation of the evidence what looks for is somehow to reinforce even more the probatory force of the digital information, since the form like the integrity of the same one has been conserved, it generates dependability.

During the gathering process and of analysis of the digital evidence, it is the investigator's duty to use some method to maintain and to verify their integrity, since a key point in the preservation of digital evidence, is that it is gathered without to alter it and to avoid its future manipulation, since in another way they won't be able to be used inside an investigation, neither neither it will be believable.

The good practices for the preservation of the digital evidence are:

To inventory the removable (DVDs, CDs, pendrives, memoirs flash, rigid disks, tapes) devices of storage of digital evidence
To use bags antiestáticas to protect magnetic devices.
To register the elements detailedly to kidnap in the levelling records (example: maker, model and serial number), their location and the possible proprietor or user.

Good preservation practices evidence digital.

Approaches of admissibility

The admissibility is bound with the legal aspect, and in fact being based on modern legislations, they exist four approaches that should be kept in mind to analyze, to the moment to decide about the admissibility of the evidence:

- Authenticity.
- Dependability.
- Completitud or sufficiency.
- Attachment and respect for the laws and rules of the judicial power.

Contrary to the physical evidence or it evidences in non digital means, in the digital ones he/she shows up great volatility and high capacity of manipulation. For this reason it is important to clarify that it is indispensable to verify the authenticity of the tests presented in digital means contrary to those no digital, in those that it applies that the authenticity of the contributed tests won't be refuted.

Evidence types

Once the digital evidence, this one is obtained it can classify in the following types:

- **Best evidence**, evidences primary or original, it is not copy. It is the most convincing form in evidence, also the most difficult of questioning, however, is to be careful in what is considered primary evidence.
- **Secondary**, evidences secondary, it is not as solid as the primary evidence. Frequently they are copies of the primary evidence, and the copies can be altered, what diminishes the force like probatory evidence.
- **Direct evidence**, evidences direct, it proves or it invalidates a fact without the necessity of using presumptions or inferences.
- **Conclusive evidence**, evidences conclusive, it is a very powerful evidence. For itself it establishes a condition or a fact.

TOOLS OF FORENSIC INVESTIGATION

Tools of forensic computer science

In the last years the number of tools has been shot for forensic computation, it is possible to find from the simplest and economic, like programs of very limited benefits and with costs of less deUS$300, until very sophisticated tools that include as much software as hardware. With that wide quantity of alternative, it is necessary to have clear the objective that is pursued, since several basic types of tools exist, not all the products are good for everything, some are designed for very specific tasks and stiller, designed to work on you set very specific, as certain operating system.

Tools for the gathering of digital evidence

The tools for the evidence gathering represent the type of more important tool in the forensic computer science, because their action center is focused in the one that is the central point for many. Their use is necessary for several reasons:

- Great volume of data that you/they store the current computers.

- Variety of formats of files, which can vary vastly, still inside the context of oneself operating system.
- Necessity to gather the information in an exact way that allows to verify that the copy is identical to the original one and also to maintain unaffected the scene of the crime.
- Limitations of time to analyze all the information.
- Volatility of the information stored in the computers, high vulnerability to the one erased, with a single instruction can be eliminated until several gigabytes.
- Employment of encripción mechanisms, or of countersigns.
- Different storage means, hard disks, CDs and tapes.

Some tools of this type are EnCase, The Coroner's Toolkit (TCT), ByteBack - TechAssist, Inc, The Access Forensic Dates Toolkit (FTK), Recovery Kit. LCTechonogy, COFEE, Safe Back - New Technologies Inc, The Forensic Tool Kit, The Sleuth Kit and Autopsy, Helix CD, F.I.R.E (Forensics and Incident Response Bootable CD).

Tools for the monitoreo and/or control of computers

If what is required is to know the use of the computers, it is necessary to have tools that the monitoreen to gather information. Tools that allow to gather from the keyboard pulsations until images of the screens that are visualized by the users, exist and other where the machines are controlled far.

Tools of marked of documents

Basically the objective of this type of tools is the one of inserting a mark to the sensitive information to be able to detect the robbery or traffic with the same one, although LoJack is not equal to the system of I rake and localization of stolen vehicles, if it could be compared with the marks that it is made to the vehicles. Through these tools it is possible to not mark single documents, but also software.

Hardware Tools

The process of evidence gathering should be the possible less invasivo in order to not modifying the information. This has given origin to the development of tools that you/they include devices like connectors, recording units, etc. it is the case of tools like "Portable DIBS Evidence Recovery Unit" and a series of tools of Intelligent Computer Solutions; Link MASSter Forensic Soft Marries, Link MASSter Forensic Hard Marries, Image Alone MASSter 2 Forensic Kit With Hard Marries.

Td1 - Forensic Duplicador

FORENSIC COMPUTER SCIENCE, ARTIFICIAL INSERT

Forensic computer science and their procedural reality in Ecuador

The computer crime put on in fashion in Ecuador since in 1999 he/she put on in the mat the discussion of the bill of Electronic commerce, Messages of Data and Electronic Signatures.

According to this law and their penal corresponding code you can conclude that the owner of the penal action and of the investigation so much procedural as preprocesal he/she is the District attorney who will have the help of the Judicial Police so that the investigation of the crimes is made.

At the present time in Ecuador a Specialized Unit doesn't exist, like it exists in other countries, such it is the case of United States where the FBI has COMPUTER CRIME UNIT, or in Spain the Civil Watch has a department specialized in this class of crimes, that alone to mention some.

In the case of Ecuador in a beginning you creó the one unit of Computer Crimes of Ministry, this it was denominated UDIMP and it was structured in the following way:

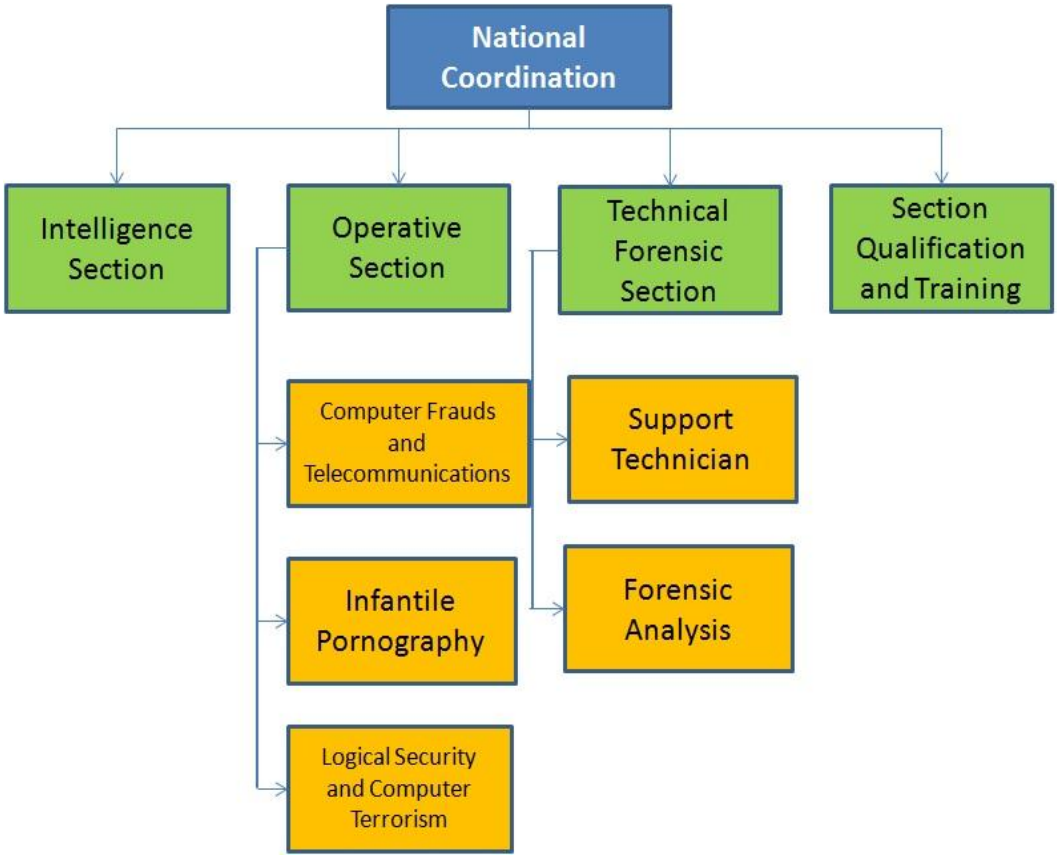
National coordination, is the one in charge of giving the politicians and general guidelines of the investigation from the Computer Crimes to national level.

Section of Intelligence, is the one in charge of picking up the information, data and other indications that have relationship with the cometimiento of one or computer more crimes.

Operative section, in charge of carrying out the investigations of all the related with the call computer crime rate.

Technical and Forensic section, in charge of to offer the technical support and to carry out the forensic analysis of the evidences found in the scene of the crime.

Section of Qualification and Training, take charge of the continuous formation of the personnel of the unit mediating qualification shops, seminars, chats and practical.



It Structures of the Unit Computer Crimes Ministry.

Source: Operative plan of creation of the Unit of Computer Crimes of the one Ministry. Dr. Santiago Acurio of the Pine

At the present time UDIMP now is, the Department of Investigation and Forensic Analysis of the General Prosecutor's office Of the State.

Forensic computer science, international laws

Among the countries that more they stand out at the moment so much for their laws as their infrastructure to treat this type of crimes Spain, United States, Bolivia, Argentina, Chile, Brazil, Colombia, France, Holland, Great Britain, Venezuela are.

Legislation of Latin American Countries	Intellectual Property Law	Law of Habeas Dates	Electronic commerce law, Messages of Data	Law of Computer Crimes	Transparency Law and Access to the Computer Science	Law of Infantile Pornography	Law of electronic mail Use
Argentina	●	●	●	●			
Bolivia					Project		
Brasil		●	●				
Chile	●		●	●		●	
Colombia		●	●	●	●		
Costa Rica				●			
Ecuador	●	●	●		●		
Guatemala			●				
México				Proy.	●		
Panamá			●				
Paraguay					●		
Perú			●	●	●		●
República Dominicana			●				
Uruguay							Proy.
Venezuela			●	●			

Laws in Latin American countries.

Source: Statistical of the Organization of American (OAS) States

Ecuadorian and international laws

Although it is certain, the Ecuadorian law of Electronic commerce he/she was carried out already based on laws existent in other countries, this was coupled therefore to the reality of our country it is highly a law territorial.

In this sense the penal Ecuadorian code sustains that the penal law is applicable when the infraction has been made inside the territory, at this time

this should change, keeping in mind the new scenario where you/they show up this type of crimes that you/they are of transnational character, that is to say crimes that are made in the Cyberspace, a place where they don't exist opposite.

But in the case of the computer crimes as it was mentioned it should be applied the universality principle and world justice, this principle basically what says it is that the applicable law is the law of the country that first capture the criminal.

Other considerations

Ecuador has taken the first steps however in the development of initiatives that you/they allow the investigation and sanction of the computer crimes, it is necessary to develop, to improve and to implement mechanisms that allow that this investigations are developed inside regulated marks, controlled and by means of the use of appropriate technology on the part of the entities and professionals dedicated to its investigation.

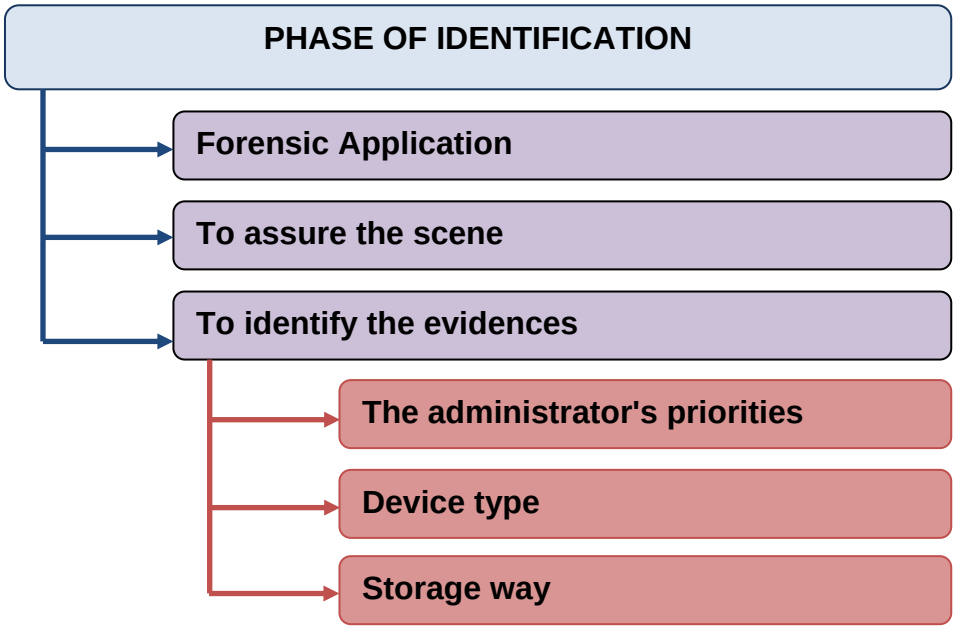
It is certain the technological advance and the necessity mechanisms that allow the persecution of illicit made acts using technological means to settle down.

For what should get ready to a new generation of professionals that you/they give answer to the growing necessity of the society of having advisers experts, and able to offer sustenance and legal back to each one of the activities that are developed with support of the technologies of the information.

METHODOLOGY OF WORK FOR INVESTIGATION

At the present time many methodologies exist to carry out a computer forensic analysis, but a methodology should be distinguished for its practice and the efficiency that he/she offers.

Identification Phase



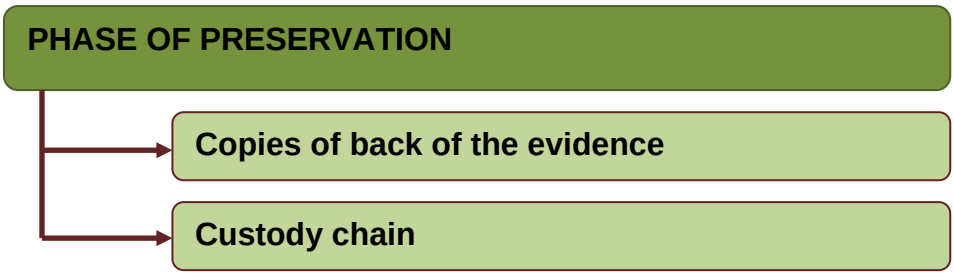
Component Identification Phase

The identification phase refers to the summary of necessary information to work on the source of data presented by the administrator of the servants (forensic application). Here he/she wonders:

- What information is it needed?
- How to take advantage of the presented information?
- In what order do I locate the information?
- Do work necessary to continue for the forensic analysis?

The final product of this phase, he/she should give a detailed document with the information that allows to define a beginning point for the acquisition of data and for the elaboration of the final document.

Preservation Phase

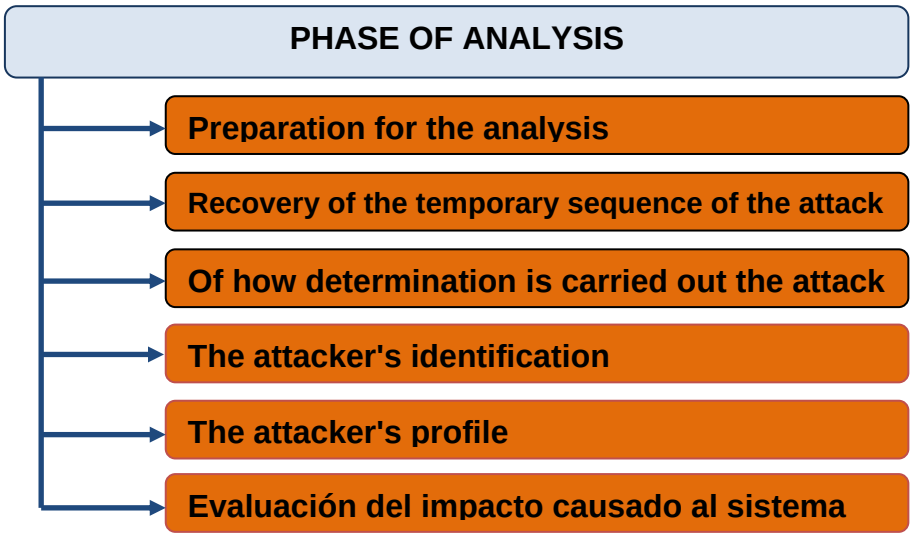


Component Preservation Phase

Although the first reason of the summary of evidences is the resolution of the incident, it can be that later on he/she needs to begin a legal process against the attackers and in such a case it will be documented in a clear way how the evidence has been preserved after the summary.

In this phase, it is indispensable to define the appropriate methods for the storage and labelled of the evidences. Once it is had all the evidences of the incident it is necessary to conserve them intact since they are the "prints of the crime", they should make sure these evidences to all coast. For it is followed it the following process.

Analysis Phase

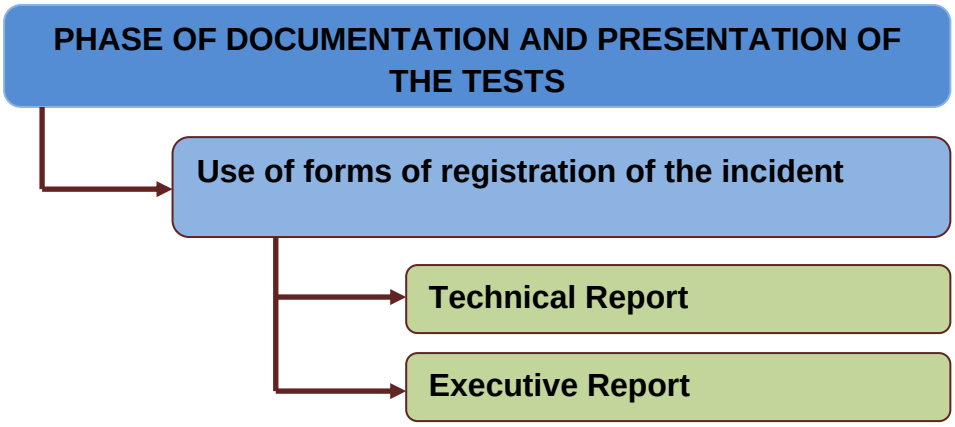


Before beginning this phase they should get ready them tools, technical, monitoreo authorizations and administrative support to begin the forensic

analysis on the obtained evidences or presented by the administrator of the servants. Once he/she has the digital gathered evidences and stored in an appropriate way, the most laborious phase, the Forensic properly this Analysis, begins whose objective is to reconstruct with all the available data the temporary line of the attack, determining the chain of events that you/they took place from the beginning of the attack, until the moment of its discovery.

This analysis will be given had concluded when he/she is discovered how the attack took place, who or who took it to end, under what circumstances he/she took place, which the objective of the attack was, what damages they caused, etc. In the analysis process the tools characteristic of the operating system are used and (host) those that got ready in the extraction phase and preparation.

Documentation phase and presentation of the tests



It is very important to begin to take notes on all the activities that are carried out. Each given step should be documented and dated since he/she is discovered the incident until the process of forensic analysis concludes, this will allow to be more efficient and more effective at the time than he/she will decrease the error possibilities when negotiating the incident.

CONCLUSIONS

The Forensic Computer science at the present time has taken great importance because he/she allows to find the necessary and enough evidences of a catastrophe, it evidences that they can be of great value in the moment to solve a case, in many of these cases it can be the available only evidence.
This work in some way seeks to give to know the Forensic Computer science's importance. Because this science integrates other concepts like: audit, inverse engineering, esteganografía, as well as legal aspects that are framed in the professional integral profile.

At the end of the investigation you could determine that the non alone methodology you can apply to operating systems Windows and Linux like it outlined it to him the work but rather you can apply to any other operating system.

Recommendations

The best form of avoiding situations or acts criminal computer specialist is establishing controls, but the best form of defending it is to promote a culture of security in the homes and organizations.

To include in the academic offer of the universities of the country at least a matter that is related with the Forensic Computer science's topic, as well as to impart seminars and to offer forensic challenges that even motivate more to the students and professional futures.

The technological changes and processes global demand bigger speed, effectiveness, effectiveness and a bigger control, reason why the professors and students linked to the investigation, as well as the directive of the educational institutions should deepen in these topics of present time.