RESUMEN EJECUTIVO

En este trabajo de tesis se empieza hablando sobre la influencia de la informática en la vida del ser humano y como los llamados ciberdelincuentes se aprovechan de esta influencia para cometer delitos, aquí es donde surge la informática forense, la cual busca recabar evidencia que permita atrapar a los delincuentes, por tanto la informática forense intenta descubrir e interpretar la información que se encuentra dentro de los medios informáticos.

Así mismo se hace un análisis de los diferentes tipos de delitos informáticos y como se tipifican estos delitos en varios países ya que cada país tiene sus propias leyes relacionadas con este tipo de delitos.

Un requisito básico para que la informática forense tenga efecto es la evidencia digital, la cual es decisiva al momento de declarar a un sospechoso culpable o inocente, en esta misma línea se habla de cómo se debe recolectar la evidencia digital y como debe clasificarse para que la evidencia sea admitida como valor probatorio dentro de un caso, ya que ciertos países ante este nuevo tipo de evidencia han tenido que reglamentar su admisión en una corte de justicia.

Se revisará las herramientas más populares tanto de hardware como de software disponibles en el mercado y que son indispensables para recolectar evidencia digital, siempre tomando en cuenta que la recolección de evidencia en el sitio del crimen es una da las tareas más críticas y fundamentales en el proceso de investigación ya que dicha evidencia debe ser idéntica a la original y debe permanecer inalterada la escena del crimen, por eso es necesario que el investigador forense conozca las herramienta disponibles y cual debe aplicar en cada caso.

Se hará un estudio de la realidad procesal en el Ecuador, se encontrará que ya nuestra Policía Nacional cuenta con una unidad que se encarga de

atender los delitos informáticos, pero se encuentra un poco relegada gracias a las leyes existentes, también se detalla ciertas características de leyes vigentes en países del área.

Por último en la parte teórica se hace un estudio de la metodología más adecuada de informática forense en el estudio de un crimen, básicamente esta metodología se divide en cuatro fases que son: Fase de identificación, preservación, análisis y presentación de las pruebas.

En lo que respecta a la parte práctica se presenta la resolución de dos casos, uno con la imagen de un disco duro perteneciente a un sospechoso de pedofilia cuyo sistema operativo es Windows, y el otro con una imagen de una memoria USB perteneciente a un sospechoso de narcotráfico y que fue creada con sistema operativo Linux. La búsqueda de evidencia se hace con herramientas de software compatibles en Windows y otras compatibles con Linux.

De esta forma con la resolución de los dos casos mencionados se prueba la aplicación de la metodología de informática forense.

EXECUTIVE SUMMARY

This thesis begins by speaking about the influence of computer science on the life of the human being, and how the so called cyber/delinquents profit of this influence to commit crimes. This is where the forensic computer science, which seeks to gather evidence that will allow catching the delinquents, and therefore the forensic computer science seeks to discover and interpret the information found within the computer media.

Besides, an analysis is also made of the different types of computer crimes and how these crimes are typified in different countries, given that each country has its own laws related to this kind of crime.

A basic requirement for the forensic computer science to have any effect is digital evidence that is decisive at the moment of declaring a suspect guilty or innocent.

In this same context, there is talk of how digital evidence must be gathered and classified in order for the evidence to be admitted as a evidentiary value within a case, as, in the face of this new type of evidence, certain countries have had to regulate its admission in a court of law.

The most popular tools will be reviewed, hardware as well as software available on the market, that are indispensable for gathering digital evidence, always taking into account that the gathering of evidence at a crime scene is one of the most critical and fundamental tasks in the investigation process, because said evidence must be identical to the original and the crime scene must remain unaltered. It is therefore necessary that the forensic investigator must know the available tools and which ones to utilize in each case.

A study shall be made of the procedural reality in Ecuador. It will be found that our National Police already has a unit in charge of dealing with these computer crimes, but it is a little relegated, thanks to the existing laws. Certain characteristics of valid laws in countries in that area will also be detailed.

Lastly, in the theoretical part a study is carried out of the most adequate methodology of forensic computer science in the investigation of a crime. Basically this methodology is divided into four stages, which are: stage of identification, preservation, analysis and presentation of the proof.

As for the practical part, a resolution is presented of two cases, one with the image of a hard drive belonging to a suspect of pedophilia, whose operative system is Windows, and the other with an image of a USB memory belonging to a suspect of drug trafficking and that was created with a Linux operative system. The search for evidence is carried out with software tools that are compatible with Windows and others with Linux.

This way, by solving the two mentioned cases, the application of the methodology of forensic computer science is proven.